DATA PROCESSING ADDENDUM

1. **Definitions.** Unless the context requires otherwise, the following terms shall have the meaning set out in this section 1:

"Affiliates" means a company, person or entity that is owned or controlled by, that owns or controls or is under common ownership or control with a Party. Ownership shall mean direct or indirect ownership of more than 50% of the shares in a company or entity, and control shall mean any power to appoint persons to the board of directors of a company or entity;

"**Applicable Data Protection Law**" shall mean Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on June 28, 2018 (California Consumer Privacy Act, "**CCPA**"), 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**")), together with any replacement legislation or any equivalent legislation of any other applicable jurisdiction and all other applicable laws and regulations in any relevant jurisdiction relating to the processing of personal data and privacy (such as, without limitation, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as may be amended from time to time and any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the European Union);

"**Controller**" means (i) the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of personal data; or (ii) a "**Covered Business**" as the term is defined in the CCPA.

"**Data Subject**" means (i) an identified or identifiable natural person who is in the EEA or whose rights are protected by the GDPR; or (ii) a "**Consumer**" as the term is defined in the CCPA;

"**Data Subject Rights**" means those rights identified in the GDPR and the CCPA granted to Data Subjects;

"**Personal data**" means information that directly or indirectly identifies or relates to a Data Subject;

"**Processor**" means (i) a natural or legal person which processes personal data on behalf of the controller; or (ii) a "**Service Provider**" as the term is defined in the CCPA.

"**Selling**" shall have the meaning defined in the CCPA.

"Schedule" shall mean a schedule to this Agreement, which shall form an integral part of this DPA;

"Security Measures" means description of the technical and organisational security measures implemented by TeleSign in its provision of the Services to Client as set out in Appendix 2 to this DPA.

"**Sub-processor**" means (i) any processor engaged by the Processor or by any other Sub processor of the Processor who agrees to receive the personal data exclusively intended for processing activities to be carried out on behalf of the Controller after the transfer in accordance with Controller's instructions and in connection with the Agreement for the provision of services to the Controller; or (ii) a "**Service Provider**" as defined in the CCPA;

"**Supervisory Authority**" means either (as applicable): (i) an independent public authority which is established by an EU Member State pursuant to Article 51 of the GDPR; or (ii) the California Attorney General; and

"**Third Party**" means a natural or legal person other than the Data Subject, Controller, Processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

The terms used in this DPA not defined herein shall have their meanings given in the Applicable Data Protection Law.

1A. Formation of this DPA

1A.1 This DPA comes into effect on the Effective Date, which shall be the earlier of:

(a) the date on which this DPA is signed by the Client;

(b) the date which is thirty (30) calendar days after the date on which this DPA is sent by TeleSign to the Client,

except where the Client objects to the terms of this DPA in accordance with section 1A.2 below.

1A.2 If, following receipt of this DPA, the Client objects to its terms it shall notify TeleSign in writing of its objection within thirty (30) calendar days after the date on which the DPA is sent by TeleSign to the Client. The Parties shall then work together promptly and in good faith to resolve the Client's objections and to agree upon a mutually satisfactory form of this DPA, whereupon the Effective Date shall be the date on which the agreed form of the DPA is signed by the Parties.

2. Processing of personal data

2.1 The provisions of this DPA shall apply to the extent TeleSign would process, on behalf of the Client, any personal data provided by that Client or its Affiliates, directly or indirectly, in connection with the Agreement as described in the Data Processing Schedule attached to this DPA (the "Data"). With regard to the processing of such Data, TeleSign processing the Data on behalf of the Client will act as Processor and Client on which behalf the Data is processed will act as Controller. Data may include personal data relating to (a) end-users of Client's or its Affiliates' customers and/or (b) individuals who are employed by or have a working relationship with Client or its Affiliate. Processing may include processing by TeleSign or any of its Affiliates.

2.2 Each Party shall fully comply with the obligations that apply to it under the Applicable Data Protection Law. It is expressly agreed upon between the Parties that the Data shall remain at all times the Controller's property.

2.3 In its capacity as Processor, TeleSign shall:

(a) Treat the Data as Confidential Information and process the Data solely and exclusively for the purpose of providing Services to the Controller and on Controller's behalf. The processing by the Processor shall consist of all permitted processing operations as stipulated in the Data Processing Schedule or in the Agreement. The categories of personal data to be processed by the Processor will be limited to the Data that are necessary to deliver the Services to the Controller. The duration of the processing by the Processor is limited to the duration described in the Agreement or the Data Processing Schedule.

(b) The Processor shall provide at all times during the performance of this DPA sufficient guarantees for its compliance with the requirements of the Applicable Data Protection Law. The Processor shall not process any Data for purposes other than that which is strictly necessary for the performance of its obligations under the Agreement, and shall only process the Data strictly in accordance with the Controller's documented instructions (the "Permitted Purpose") given in this DPA, the Agreement or by any other means during the performance of this DPA. If the Processor would be required by any applicable legislation to process any Data otherwise than as permitted herein, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the Applicable Data Protection Law and shall provide details of the breach or potential breach.

(c) Implement appropriate and sufficient, technical and organisational security measures prior to and during processing of any Data to protect the security, confidentiality and integrity of the Data and to protect the Data against any form of accidental, unlawful or unauthorized processing. In particular, without limitation, the Processor shall protect the Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, use or access to Data transmitted, stored or otherwise processed and against any form of unlawful processing. The Processor shall ensure a level of security appropriate to the risks presented by the processing of Data and the nature of such Data. Such measures shall include, as appropriate:

i. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
ii. The ability to restore the availability and access to the Data in timely manner in the event of a physical or technical incident;
iii. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

At a minimum, such measures shall include the organizational and technical measures, which meet or exceed relevant industry practice. These measures shall remain in place throughout the duration that Processor provides Services to the Controller or until Processor ceases to process Data (whichever is later). As of the Effective Date of this Agreement, TeleSign has implemented the Security Measures. TeleSign may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the security of the Services;

(d) Treat Data with strict confidence and take all appropriate steps to ensure that disclosure of or access to Data is restricted to its employees, consultants or agents that strictly require such Data to perform the tasks allotted to them by the Processor in the performance of the Processor's obligations under the Agreement (the "Authorized Persons") and excluding all access to Data which are not strictly necessary for the Authorized Persons to perform its part of the Services. The Processor shall ensure that the Authorized Persons who will process Data:

i. Are aware of and shall comply with the provisions of this DPA;
ii. Are under a duty of confidentiality with respect to the Data no less restrictive than the duties set forth herein prior to any access to the Data. Processor shall ensure that such confidentiality obligations survive the termination of the employment or contracting agreement;
iii. Have received appropriate training in relation to the Applicable Data Protection Law;

iv. Are subject to user authentication and log-on processes when accessing the Data; and
v. Shall only process the Data as necessary for the Permitted Purpose and in accordance with the Controller's instructions.

(e) Save and except for the Sub-processors set out in Appendix 1 herein, not engage any subcontractor for the processing of Data without the Controller's prior written specific or general written authorisation approval (the "Approved Sub-processor"), to be provided in Controller's sole discretion but not to be unreasonably withheld. In the frame of the Parties' relationship as of the date of this Agreement, Client allows TeleSign to be assisted by subcontractors strictly with a view to deliver and improve the agreed Services, provided TeleSign has contracted with said subcontractors with terms substantially similar to the ones included herein. When the use of subcontractors does not fall within the scope of the present general authorization, the Processor shall inform the Controller at least one month in advance and by means of a written communication about its intention to engage a subcontractor, including details on the identity of the subcontractor, the location where the Data will be processed by such subcontractor and the concerned data processing activities. The Processor will enter into written contracts with such Approved Sub-processor guaranteeing at least a level of data protection and information security as provided for herein and in any event Processor will remain fully liable to the Controller for any breach of the Approved Sub-processor that is caused by an act, error or omission of the Approved Sub-processor. The Processor shall maintain and provide upon reasonable request a copy of the list of concerned subcontractors. If the Controller would refuse to consent to the appointment of a subcontractor on grounds relating to the protection of the Data, then the Processor will not appoint such subcontractor.

3. International transfers of personal data

The Processor or any Approved Sub-processor shall not process or transfer any Data (nor permit the Data to be transferred) outside of the European Economic Area unless an adequate level of protection in accordance with the Applicable Data Protection Law is ensured (the "Safeguards"). Such Safeguards may include without limitation: (1) a transfer to countries which ensure an adequate level of data protection according to an adequacy decision of the European Commission, or (2) such transfer is needed for the performance of the Agreement, or (3) it is governed by the EU Standard Contractual Clauses (Processors) in the Annex to the European Commission Decision of February 5, 2010, which are deemed incorporated herein by reference. The transfer of Data outside of the European Economic Area shall immediately cease to take place from the moment the adequacy decision from the European Commission or such Safeguards are no longer valid or its conditions to apply are no longer fulfilled.

4. Duty to Notify and Cooperate

Processor shall promptly give written notice to and/or shall fully cooperate with the Controller:

(a) if for any reason (i) Processor cannot comply, or has not complied, with any portion of this DPA, (ii) it would be in breach of or has breached any Applicable Data Protection Law governing its processing of Data, or (iii) Applicable Data Protection Law no longer allows the lawful transfer of Data from the Controller to Processor. In such cases, Processor shall take all reasonable, necessary and appropriate steps to remedy any non-compliance, or cease further processing of Data, and the Controller may immediately terminate the Agreement and this DPA or access to Data, or take any other necessary action, as determined in its sole discretion;

(b) to enable the Controller to comply with its obligations with regard to the security of the processing of Data, taking into account the nature of the processing and the information available to the Processor;

(c) upon becoming aware of any Data breach. In such case, the Processor shall promptly inform the Controller of the Data breach without undue delay and shall provide all such timely information and cooperation as the Controller may reasonably require including in order for the Controller to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Processor shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Data breach and shall keep the Controller up-to-date about all developments in connection with the Data breach;

(d) in the preparation of any data protection impact assessments performed by the Controller, whether on a mandatory or voluntary basis. The Processor shall provide the Controller with all such reasonable and timely assistance as the Controller may require in order to conduct a data protection impact assessment in relation to the Data and, if necessary, to consult with its relevant data protection authority. Processor agrees and acknowledges that if the Controller receives a request from a data protection authority, the Controller may share the terms of this DPA, the Agreement and any other information Processor provides to demonstrate compliance with this DPA or Applicable Data Protection Law.

In addition to the foregoing, if the Processor believes or becomes aware that its processing of the Data is likely to result in a high risk (as defined in the Applicable Data Protection Law, relevant regulatory guidance and case law) with regard to the data protection rights and freedoms of data subjects, it shall promptly inform the Controller.

(e) cooperate, at its own expense, as requested by the Controller to enable it to respond and comply with (i) the exercise of rights of data subjects pursuant to Applicable Data Protection Law (such as their right of access, right to rectification, right to object to the processing of their personal data, right to erasure and as from 25 May 2018, their right to restriction of processing of their personal data and their right to data

portability) and (ii) any other correspondence, enquiry or complaint received from a data subject, regulatory authority or any other third party in respect of Data processed by the Processor under this DPA.

The Processor shall promptly inform the Controller of any requests relating to the exercise of such rights or complaints, enquiry or correspondence if they are received directly by Processor and shall provide all details thereof. Furthermore, Processor shall provide all Data requested by the Controller, within a reasonable timescale specified by the Controller and shall provide such assistance to the Controller to comply with the relevant request within the applicable timeframes. Processor understands that any response to such direct requests requires prior written authorization from the Controller. If necessary, the Processor shall co-operate with the competent supervisory authority;

(f) upon the Controller's request, to make all such records, appropriate personnel, data processing facilities and any relevant materials available relating to the processing of the Data available to the Controller in order to allow the Controller to demonstrate compliance with its obligations laid down in the Applicable Data Protection Law. In particular, the Controller or a third party appointed by the Controller (the "Auditor") may enter the Processor's premises and more specifically the rooms or locations where the Data is processed by the Processor to verify Processor's compliance hereunder, provided that such inspection shall be carried out with reasonable notice (except where such notice would defeat the purpose of the Audit) during regular business hours and under a duty of confidentiality. The Controller or the Auditor may inspect, audit and copy any relevant records, processes and systems to verify compliance with the Applicable Data Protection Law and this DPA. The Controller shall take all reasonable measures to prevent unnecessary disruption to the Processor's operations. The Controller will not exercise its inspection rights as set forth in this clause more than once in any twelve (12) calendar month period and with ninety days' prior written notice, except (i) if and when required by instruction of a competent data protection authority or (ii) the Controller believes a further audit is necessary due to a Data breach suffered by the Processor.

5. Effect of Termination

As soon as it is no longer required for the performance of the Services and at the latest upon the expiration or termination of the Agreement, Processor shall promptly notify the Controller of all Data in its possession and promptly return or delete all such Data (at the Controller's sole election) and any existing copies thereof, at Processor's sole expense, unless any applicable law requires the further storage of the Data. The Processor shall certify to the Controller that all Data has been returned or destroyed in accordance with the foregoing and Controller's instructions. If the Processor cannot destroy or delete the Data due to technical reasons, the Processor will immediately inform the Controller and will take all appropriate steps to:

i. Come to the closest possible to a complete and permanent deletion of the Data and to fully and effectively anonymize the remaining Data; and
ii. Make the remaining Data which is not deleted or effectively anonymized unavailable for any further processing except to the extent required by any applicable law.

6. Indemnification

The Processor acknowledges that the obligations set forth in this DPA are essential and that any violation thereof may seriously harm the Controller. The Processor shall have full and sole liability for all damages resulting from a failure on its part to comply with the provisions of this DPA. Should any data subject to whom the Data relates, a data protection authority or any other regulatory body lodge a claim for compensation against the Controller that results from the Processor's breach of its obligations under the Applicable Data Protection Law (a "Claim"), the Processor shall assist and intervene in the Controller's defence against such Claim upon the Controller's request and shall indemnify and hold harmless the Controller against all costs and damages resulting from such Claim. The Controller shall give the Processor prompt written notice of any such Claim and shall provide all reasonable cooperation in the defence and settlement of such Claim, at the Processor's expense. The Controller shall not make any admission as to the Processor's liability in respect of such a Claim and shall not agree to any settlement in respect of such a Claim without the Processor's written consent.

7. California Consumer Privacy Act

To the extent that CCPA is applicable, except as permitted under the Agreement, this Section 7 shall take precedence to the extent of any contradictory term otherwise contained herein solely with respect to Processing of Personal Data in the Agreement:

a) TeleSign is a "Service Provider" as defined in CCPA Section 1798.140(v).
b) TeleSign shall not be considered a Third Party.
c) Client discloses Personal Data to TeleSign solely for: (i) a valid business purpose; and (ii) TeleSign to perform the Services.
d) TeleSign is prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing the Personal Data outside of the Agreement between TeleSign and Client.
e) Both Parties understand the prohibitions outlined in Section 7.

8. Order of Precedence

In the event of a conflict between the provisions of this DPA and those of the Agreement in respect of the processing and protection of Data, the provisions of this DPA will prevail. Except as expressly modified herein, all terms and conditions of the Agreement shall remain in full force and effect.

9. Governing law

Notwithstanding anything in the Agreement to the contrary, this DPA will be governed exclusively by and interpreted in accordance with the laws of Belgium, excluding its conflicts of law principles. All disputes arising out or in connection with this DPA will be submitted exclusively to the competent courts of Brussels.

Schedule 1: Data Processing Schedule

1. Categories of Data

The Data processed are the personal data provided by the Controller to the Processor in connection with the Services provided by the Processor, including but not limited to first name, last name, address, e-mail address, telephone number, location data, contact information and device information.

2. Categories of data subjects

Data subjects are the persons whose Data are processed by the Data Processor may include end users or employees and members of the staff of the Controller

3. Permitted processing operations for the Processor

The processing consists of all data processing activities that are performed following the instructions of the Controller and that are necessary to deliver the Services to the Controller and for the Permitted Purposes.

4. Permitted Purposes

The Processor may process Data in accordance with the purposes set out in the Agreement and, generally: to provide its Services to the Controller; for fraud detection, prevention and mitigation purposes; for offering, maintaining and enhancing the Services it or its Affiliates offer, as well as to enhance or further develop its services' offer or the one of its Affiliates as contracted by other customers, as the case may be by processing Data in aggregated form only.

5. Duration

The duration of the processing is limited to the duration needed to perform its obligations under the Agreement, unless a legal obligation applies. The obligations of the Processor with regard to the Data processing shall in any case continue until the Data have been properly deleted or have been returned at the request of the Controller.

APPENDIX 1

Name of Processor/Sub-processor	Role (Data Processor or Sub-processor)	Location
TeleSign Corporation, which has data centers in the US, UK, and the Nederlands.	Processor	US, and the Nederlands
TeleSign UK Limited	Sub-processor	UK
TeleSign d.o.o. Beograd-Novi Beograd	Sub-processor	Serbia
Adroiti Technologies	Sub-processor	Lithuania
Amazon Web Services	Sub-processor	Global
Group of carriers, network transit providers or transport service providers, providers responsible for the transmission of telecommunications services such as voice and SMS communications and data services	Sub-processor	Global

Appendix 2
Security Measures

Description of the technical and organisational security measures implemented by TeleSign in its provision of the Services to Client:

1. Security.

1.1. Security Management System.

(a) **Organization.** TeleSign designates qualified security personnel whose responsibilities include development, implementation, and ongoing maintenance of the Information Security Program.

(b) **Policies.** The data importer's executive management reviews and supports all security related policies to ensure the security, availability, integrity and confidentiality of Client Data. These policies are updated at least once annually.

(c) **Assessments.** TeleSign engages a reputable independent third-party to perform risk assessments of all systems containing Client Data at least once annually.

(d) **Risk Treatment.** TeleSign maintains a formal and effective risk treatment program that includes penetration testing, vulnerability management and patch management to identify and protect against potential threats to the security, integrity or confidentiality of Client Data.

(e) **Subprocessor Management.** TeleSign maintains a formal and effective subprocessor management program.

(f) **Incident Management.** TeleSign reviews security incidents regularly, including effective determination of root cause and corrective action.

(g) **Standards.** TeleSign maintains a formal controls framework that aligns with the ISO 27002:2013 standard.

2. Personnel Security.

2.1. TeleSign personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. TeleSign conducts reasonably appropriate background checks on any employees who will have access to Client Data under this Agreement, including in relation to employment history and criminal records, to the extent legally permissible and in accordance with applicable local labor law, customary practice and statutory regulations.

2.2. Personnel are required to execute a confidentiality agreement in writing at the time of hire and to protect Client Data at all times. Personnel must acknowledge receipt of, and compliance with, TeleSign's confidentiality, privacy and security policies. Personnel are provided with privacy and security training on how to implement and comply with the Information Security Program. Personnel handling Client data are required to complete additional requirements appropriate to their role (e.g., certifications). TeleSign's personnel will not process Client data without authorization.

3. Access and Site Controls.

3.1. Site Controls.

(a) **On-site Data Center Security Operation.** TeleSign's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

(b) **Data Center Access Procedures.** TeleSign maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities.

Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

(c) **On-site Data Center Security Devices.** TeleSign's data centers employ an electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

3.2. Access Control.

(a) **Access Management.** TeleSign maintains a formal access management process for the request, review, approval and provisioning of all personnel with access to Client Data to limit access to Client Data and systems storing, accessing or transmitting Client Data to properly authorized persons having a need for such access. Access reviews are conducted periodically (no less than annually) to ensure that only those personnel with access to Client Data still require it.

(b) **Infrastructure Security Personnel.** TeleSign has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. TeleSign's infrastructure security personnel are responsible for the ongoing monitoring of TeleSign's security infrastructure, the review of the Services, and for responding to security incidents.

(c) **Access Control and Privilege Management.** TeleSign's and Client's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized user or administrator.

(d) **Internal Data Access Processes and Policies – Access Policy.** TeleSign's internal data access processes and policies are designed to protect against unauthorized access, use, disclosure, alteration or destruction of Client Data. TeleSign designs its systems to only allow authorized persons to access data they are authorized to access based on principles of "least privileged" and "need to know", and to prevent others who should not have access from obtaining access. TeleSign employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. TeleSign requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with TeleSign's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies follow industry standard practices. These standards include password complexity, password expiry, password lockout, restrictions on password reuse and re-prompt for password after a period of inactivity.

4. Data Center & Network Security.

4.1. Data Centers.

(a) **Infrastructure.** TeleSign maintains geographically distributed data centers. TeleSign stores all production data in physically secure data centers.

(b) **Redundancy.** Infrastructure systems have been designed to minimize single points of failure and the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow TeleSign to perform certain types of preventative and corrective maintenance without

interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

(c) **Power.** The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions.

(d) **Server Operating Systems.** TeleSign's servers are customized for the application environment and the servers have been hardened for the security of the Services. TeleSign employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

(e) **Disaster Recovery.** TeleSign replicates data over multiple systems to help to protect against accidental destruction or loss. TeleSign has designed and regularly plans and tests its disaster recovery programs.

(f) **Security Logs.** TeleSign's systems have logging enabled to their respective system log facility in order to support the security audits, and monitor and detect actual and attempted attacks on, or intrusions into, TeleSign's systems.

(g) **Vulnerability Management.** TeleSign performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis, with Critical, High and Medium security patches for all components installed as soon as commercially possible.

4.2. Networks & Transmission.

(a) **Data Transmission.** Transmissions between data centers are designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. TeleSign transfers data via Internet standard protocols.

(b) **External Attack Surface.** TeleSign employs multiple layers of network devices and intrusion detection to protect its external attack surface. TeleSign considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

(c) **Intrusion Detection.** Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. TeleSign intrusion detection involves:

(i) Tightly controlling the size and make-up of TeleSign's attack surface through preventative measures;

(ii) Employing intelligent detection controls at data entry points; and

(iii) Employing technologies that automatically remedy certain dangerous situations.

(d) **Incident Response.** TeleSign maintains incident management policies and procedures, including detailed security incident escalation procedures. TeleSign monitors a variety of communication channels for security incidents, and TeleSign's security personnel will react promptly to suspected or known incidents, mitigate harmful effects of such security incidents, and document such security incidents and their outcomes.

(e) **Encryption Technologies.** TeleSign makes HTTPS encryption (also referred to as SSL or TLS) available.

5. Data Storage, Isolation, Authentication and Destruction. TeleSign stores data in a multi-tenant environment on TeleSign-controlled servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. TeleSign logically isolates the data exporter's data from that of other customers of data importer. A central authentication system is used across all Services to increase uniform security of data. The data exporter may choose to make use of certain logging capabilities that TeleSign may make available via the Services, products and APIs. TeleSign ensures secure disposal of Client Data through the use of a series of data destruction processes.