Privacy & Security Addendum

ARCHIVED – MAY 2018

1. Definitions

"**Agreement**" means the TeleSign Master Services Agreement between TeleSign and Client.

"**Client Data**" means any information transmitted by or on behalf of Client or a Client Affiliate during the execution of an electronic request to the Services.

"**Data Privacy and Security Law**" means EU Data Protection Law and any other national laws or regulations relating to the protection of personal data or personal information as applicable to the Client and Client Affiliates (if applicable) and to TeleSign.

"**EU Data Protection Law**" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, the national legislation adopted pursuant thereto, or any superseding legislation as applicable to the Client and Client Affiliates (if applicable) as the data controller of Client Data and to TeleSign as the data processor of Client Data.

"**Information Security Program**" means TeleSign's internal policies and procedures intended to protect Client Data, including the Security Measures described in section 4.1 of this PSA.

"**Instructions**" means instructions provided by Client via web-based administrative tools provided by TeleSign, instructions initiated by the Client and Users in their use of the Services, the written instructions of the Client specified in this Agreement (as amended or replaced) and any subsequent written instructions agreed to between the Client and TeleSign.

"**Privacy & Security Addendum" or "PSA**" means this addendum and any annexes hereto.

"**Security Incident**" means accidental or unlawful distribution or accidental loss, alteration, or unauthorised disclosure or access to Client Data by TeleSign, its Subprocessors or any third party, provided that such incident is not directly or indirectly caused by Client's, or Client's Affiliates' or User's act or omission.

"**Standard Contractual Clauses**" means the agreement that may be executed by and between Client and TeleSign in the form set out at https://www.telesign.com/telesign-Standard-Contractual-Clauses pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under EU Data Protection Law.

"**Subprocessors**" means those members of the TeleSign Group and Third Party Suppliers that have logical access to, and process, Client Data.

"**TeleSign Group**" means TeleSign and those TeleSign Affiliates that may be used to provide the Services to Client.

"**Third Party Suppliers**" means the third party suppliers engaged by the TeleSign Group for the purposes of processing Client Data in the context of the provision of the Services.

The terms "personal data", "processing", "controller" and "processor" will have the meanings ascribed to them in the EU Data Protection Law.

Unless the context requires otherwise, definitions used in the Agreement have the same meaning as when used in this PSA.

2. Term.

This PSA will automatically terminate upon the expiration or termination of the Agreement.

3. Processing of Client Data

3.1. **Processor**. With respect to Client Data under this Agreement, the parties acknowledge and agree that, for purposes of EU Data Protection Law, Client is the controller and TeleSign is a processor. Client will comply with its obligations as a controller and TeleSign will comply with its obligations as a processor under this Agreement. Where a Client Affiliate is the controller (either alone or jointly with the Client) with respect to certain Client Data, Client represents and warrants to TeleSign that it is authorized to instruct TeleSign and otherwise act on behalf of such Client Affiliate in relation to the Client Data in accordance with this Agreement.

3.2. **Scope of Processing.** TeleSign will process Client Data in accordance with Client's Instructions. Client instructs TeleSign to process Client Data to: (i) provide the Services (which may include the detection, prevention and resolution of security and technical issues, as well as the improvement of the Services themselves) and (ii) respond to customer support requests. TeleSign will only process Client Data in accordance with this Agreement and will not process Client Data for any other purpose.

4. Data Security

4.1. **Security Measures.** TeleSign will take and implement appropriate technical and organizational measures designed to protect Client Data against a Security Incident ("**Security Measures**"). As of the Effective Date of this Agreement TeleSign has implemented the Security Measures described in Appendix 1 of this PSA. 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.

4.2. **TeleSign Staff.** TeleSign will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance.

4.3. **Security Incident.** If TeleSign becomes aware of a Security Incident, TeleSign will notify Client of such Security Incident as soon as reasonably practicable, having regard to the nature of such Security Incident. TeleSign will use commercially reasonable efforts to work with Client in good faith to address any known breach of TeleSign's security obligations under the Agreement. As between TeleSign and Client, Client is exclusively responsible for fulfilling any third party notification obligations, except to the extent that TeleSign is required under Data Privacy and Security Law to make any such notifications on its own behalf.

4.4. **Security Audit.** During the Term, TeleSign shall have an annual security assessment conducted by an independent third party auditor with the requisite qualifications to sufficiently assess TeleSign's security controls and its compliance therewith. The security assessment shall examine TeleSign's logical security controls, physical security controls and system availability, and shall culminate in a report documenting the auditor's findings ("Audit Report"). A summary of the most recent Audit Report findings ("Audit Report Summary") shall be made available to Client upon request and Client shall treat the Audit Report Summary as TeleSign's Confidential Information.

4.5. **Audit Rights.** TeleSign has included the security and audit obligations in Sections 4.1 and 4.4 of this PSA at the request of the Client, and where Client or a Client Affiliate has entered into the Standard Contractual Clauses with a TeleSign Group entity as described under Section 7.2, Client agrees that the security and audit obligations of this PSA will fully satisfy the audit rights granted under clauses 5(f) and 12(2) of such Standard Contract Clauses with respect to Client and any applicable authorized Client Affiliate.

5. Data Access, Correction, Blocking and Deletion

5.1. **User Requests.** TeleSign will not materially respond to requests from Client's Users without Client's prior written consent, except to redirect such Users to Client or as otherwise required by applicable law. For the Term of the Agreement TeleSign will provide Client with reasonable assistance in responding to any such User requests related to access, blocking, correction or deletion of personal data.

5.2. **Data deletion.** Upon expiry or termination of the Agreement, TeleSign will delete all Client Data as soon as reasonably practicable and within a maximum period of 180 days. Client agrees to this data deletion schedule with regard to TeleSign's obligations under clause 12(1) of the Standard Contractual Clauses.

6. Data Privacy Officer. TeleSign's privacy representative can be contacted at:

TeleSign UK Limited
Attn: Privacy Officer
4th Floor, 210 High Holborn
London, WC1V 7DL
UK

or

privacy@telesign.com

7. Data Transfers

7.1. As part of providing the Services, TeleSign may transfer, store and process Client Data in the United States or any other country in which TeleSign and its Subprocessors maintain facilities.

7.2. **Standard Contractual Clauses.** During the Term, Client (or an authorized Client Affiliate) may enter into the Standard Contractual Clauses with TeleSign if Client or such Client Affiliate is established in the European Economic Area.

8. Subprocessors

8.1. TeleSign may engage Subprocessors to provide parts of the Services. Client consents to such subcontracting in accordance with this Agreement and if Client (or an authorized Client Affiliate established in the European Economic Area) enters into the Standard Contractual Clauses with TeleSign, Client consents to TeleSign subcontracting the processing of Client Data in accordance with the terms of the Standard Contractual Clauses. For the avoidance of doubt, Subprocessors do not include network transit providers or transport service providers responsible for the transmission of telecommunications services such as voice and SMS communications sent on behalf of Client.

8.2. **Subprocessing Restrictions.** TeleSign will ensure that Subprocessors only access and use Client Data in accordance with the terms of the Agreement and that they are bound by written obligations no less protective of Client Data than in this PSA.

8.3. **Additional information.** At the written request of the Client, TeleSign will provide additional information regarding Subprocessors and their locations. Client must direct such requests to TeleSign's Data Privacy Officer via the contact details provided in this PSA.

9. Third Party Requests. TeleSign shall, to the extent legally permitted under Applicable Law, promptly notify Client of any requests by third parties, including law enforcement or other governmental representatives, for access to or disclosure of Client Data. TeleSign will not disclose or otherwise provide access to Client Data to any unauthorized third party unless obligated to do so under Applicable Law.

10. Third Party Beneficiary. Notwithstanding anything to the contrary in the Agreement, where TeleSign Corporation is not a party to the Agreement, TeleSign Corporation will be a third party beneficiary of Sections 4.5, 5.2 and 8 of this PSA.

Appendix 1 to the Privacy and Security Addendum

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.