Technical and Organizational Measures to Secure the Personal Data

Confidentiality (Art 32 (I) 1 lit b GDPR)

Entry control:

The Data Processor monitors its servers and the rooms in which the servers are deployed with perimeter cameras. It requires its co-location facility partners to restrict physical access to its servers to persons that have been authorized in advance to access the servers, inter alia by picture identification. Such persons are checked in and escorted to the servers by the personnel of the Data Processor's co-location facility partner. The Data Processor also requires its co-location facility partners to enforce verification of the requester prior to answer any service request. The co-location facility partner may not attempt to gain any sort of access to the Data Processor's data systems without written instructions from the Data Processor. Physical access to the servers by field technicians for purposes of first instalment or maintenance is limited to the technical functions of the servers. Field technicians do not have control over the ability of such servers to process the customer's ("Data Controller's") content.

Access control:

The Data Processor limits the access to its data systems according to its business requirements and the least privilege principle. For example, field technicians are not granted administrative access to servers processing Data Controller's content. Field technicians performing system diagnostics and analysis are provided with read-only logins. Administrative access is restricted to trained and authorized employees of the Data Processor. Field technicians are not granted administrative access to the servers processing the Data Controller's content. Remote administrative access is only available via cryptographically secure connections, systems authenticate administrative connections using asymmetric key cryptography. User administrative access is provided through an access control gateway, which enforces a need-have access grant authorization model. All connections through the authorization gateway are logged. User SSH system are routinely rotated and access is immediately removed in case of reports of theft of devices or the termination of a person's employment.

A system of grants is used to track and permit access to all data processing systems of the Data Processor.

Access to the Data Processor's systems used to process the Data Controller's content is gained via the Data Processor's authorization gateway. Access to the authorization gateway itself requires possession of a grant authorized by one or more second parties, as well as a deployed SSH key. Issuance of a deployed SSH key requires access to the corporate network environment using a device with a corporate PKI issued Network Access Control (NAC) certificate, valid corporate authentication credentials for the Data Processor's corporate web services, and either confirmation of possession of a usable, unexpired prior key or the confirmation by the Data Processor's Network Operations Command Center (NOCC) of the user's identity.
Access to the Data Processor's corporate network requires using a device with a corporate PKI issued NAC certificate. Access to data processing systems within the corporate network requires the NAC certificate as well as user authentication via either the Duo Security, Inc. Trusted Access System or the corporate active directory username and password management system.
In case of password authentication, the complexity of the password is ensured by the Data Processor's password policy (e.g. multiple character types, length of min. 8 characters, change requirement after 120 days, inability to reuse a password within the following 12

month).

The Data Processor does not provide user accounts to servers transmitting content. Administrative access to such servers is limited to a number of authorized employees of the Data Processor. Access to these servers by authorized employees on a user level is logged by an authentication gateway. Remote access via the authentication gateway utilizes SSH keys and asymmetric cryptography. Introduction of a new SSH key requires either direct confirmation of identity with the Data Processor's NOCC or possession of the prior SSH key, the prior SSH key password, a machine's NAC for the Data Processor's corporate network and a corporate Active Directory username and password.

Segregation control

The Data Processor separates the environment for development, software, engineering, from the environment for testing and the environment for operations and has put in place several controls to ensure the code development, testing and production data handling environments are separated. E.g. employees within the development team do not have access to the same systems as the employees within the test or operation team. Separate cryptographic credentials are used to access development, test, operations and production environments, critical network operations systems are further isolated from the corporate, development and test network environments. The separation is supervised by granular logging of access to the production and operations servers, change control processes and by the responsible management.

Pseudonymization (Art 32 (1) lit a GDPR, Art 25 (1) GDPR

In most cases Data Processor does not pseudonymize or anonymize the personal data it processes. For the personal data in the Data Controller's web properties this would require modifications of the web properties which would mean a violation of the integrity of the Data Controller's web properties.

For personal data in log files this data is required in raw and clean for the purpose of the processing activities. E.g. Data Processor could not perform security analytics using pseudonymized or anonymized IP addresses.

For personal data in Data Controller employees' contact details this data is required in raw and clean for the purpose of the processing activities. E.g. Data Processor could not contact the Data Controller's employees using pseudonymized or anonymized IP contact details.

Integrity (Art 32 (1) lit b GDPR

Transmission control

The Data Processor has put in place a robust alert management system that provides for extensive monitoring of all servers. Fine grained monitoring of running processes allows the definition of predefined alerts to catch unexpected and suspicious behavior, including the execution of rogue processes.

In addition, the Data Controller can control access to the personal data in its content while having the Data Processor transmitting traffic to its server over encrypted and authenticated connections by its configuration of the services in the Data Processor's Customer Center. The Data Controller can control storage of personal data in its content by configuring property specific content caching rules. By its configuration the Data Controller can also limit the storage of personal data in its content to servers with enhanced physical security controls only. The integrity of the Log Data is ensured by various storage controls (e.g., log retention control) that are subject to several regular third-party assessment, e.g., the Data Processor's annual ISO 27002 assessment.

Input control

Access to the Data Processor's server is logged and monitored via audit systems and processes. Log data gathered by web-servers is digitally signed by "Edge Servers" and is

audited by the distributed data processing facilities, to ensure that it is not modified or corrupted. Respective access logs consisting of aggregated and anonymized log data are provided to the Data Controller as part of the Data Processor's "Log Delivery Service" offering.

Availability and resilience (Art 32 (1) lit b GDPR

The Data Processor's web server networks have been created matching the principles of availability. The server network is self-curing and ensures that the content of the Data Controller is transmitted via the server network, even in case of an outage of single servers. This prevents an outage of the services which would require a fast recovery of the services (Art 32 (1) lit c GDPR.

Evaluation of effectiveness (Art 32 (1) lit d GDPR and Art 25 (1) GDPR:

The Data Processor has data protection management in place, which is evaluated in the course of the annual third-party audits under the Data Processor's ISO 27002, SOC 2 Type 2, PCI DSS 3.2 and other assessments and certifications. In addition, the Data Processor maintains an Incident Response Management that is evaluated in the course of the annual third-party audits under the Data Processor's ISO 27002, SOC 2 Type 2, PCI DSS 3.2 and other assessments and certifications. Further the Data Processor ensures by its privacy by design (Art 25 (2) GDPR) set up that personal data that it is processing is protected. E.g. the Data Controller ensured that for new service developments GDPR's data protection principles are complied with. In addition, the Data Processor is offering, where doable considering the purpose of the services, the anonymization of personal data and thereby complying with the data minimization principle.

Role Control:

The Parties ensure that personal data is processed by the Data Processor only in accordance with the instructions of the Data Controller by agreeing on this DPA. In addition, the Data Processor's robust alert system ensures that it transmits the Data Controller's web content only in accordance with the instructions of the Data Controller (which he has provided by way of its configuration how to process the content within the Data Processor's Customer Center).