Technical and Organizational Measures to Secure the Personal Data

Confidentiality:

Entry control:

The Data Processor monitors its server system 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 server system 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:

Access to the personal data in the Data Controller's web properties that is transmitted via the Data Processor's server system is controlled by encrypted and authenticated connections and by other controls put in place during the configuration of the services in the Data Processor's Customer. E.g. the Data Controller can choose between a transmission via the Enhanced TLS Platform and the Standard TLS Platform. In addition, the Data Controller chooses the level of encryption of the web properties, e.g., the level of bit keys. The Data Controller can control no-storage of personal data in its web properties by configuring web property specific content caching rules.

The Data Processor limits the access to its server system 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 web properties. Field technicians performing system diagnostics and analysis are provided with read-only logins to single servers. Administrative access is restricted to trained and authorized employees of the Data Processor. Remote administrative access by the Data Processor's employees 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 server system used to process the Data Controller's web properties 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:

The end user IP address in log files the Data Processor processes when providing its services are pseudonymized. The Data Processor does not identify the individual using the device the IP address relates to. It does not even have the data required to identify the end user.

Anonymization:

Where possible considering the processing purpose, the Data Processor anonymizes personal data at the earliest stage when processing such data.
E.g. for the service mPulse the end user IP address in a log fle is anonymized once processed for routing and general platform security purposes on the edge servers. So the onward processing of the log file is not classified as processing of personal data anymore.

Integrity:

Transmission control

The Data Processor has put in place a robust alert management system that provides for extensive monitoring of all servers to ensure the integrity of the Data Controller's web properties that are transmitting the Data Processor's servers. Fine grained monitoring of running processes allows the definition of predefined alerts to catch unexpected and suspicious behavior on a server, including the execution of rogue processes.
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 ISO 27002 assessment or its SOC 2 Type 2 report.

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:

The Data Processor's server system has been created matching the principles of availability. The server system is self-curing and ensures that the of the Data Controller's web properties are transmitted via the server system, even in case of an outage of single servers. As the server system consists of more than 300,000 servers, a single server outage or even a regional outage generally does not impact the availability and resilience of the platform as a whole.

Evaluation of effectiveness:

The Data Processor has data protection measures are 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 principles that its services and systems are developed and designed in compliance with privacy principles and that personal data processed is appropriately protected. E.g., to the extend consistent with the processing purpose the Data Processor is anonymizing personal data at the 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 contractual and technical measures. Contractually the parties agree on a data processing agreement. Technically, the Data Processor processes the data as configured in its control center. That is where the Data Controller's instructions are documented and logged.