1 Product data sheet Digital Services

1.1 Connectivity

The product is equipped with functionality that, when enabled, will connect to the Swegon INSIDE Cloud when given access to the internet. Such connection is made either through the building's local internet access point or by using a supplied modem. When connecting through the building's internet access point, the local firewall must be configured to allow traffic according to the firewall settings. The functionality is by default disabled and can be enabled in the product. By enabling this functionality the customer agrees to the general terms and conditions for Digital Service, DS-23. The customer can disable the connection to the Swegon INSIDE Cloud in the product user interface at any time.

1.2 Which data is sent

Through the connection to Swegon INSIDE Cloud, the product will exchange data to Swegon INSIDE Cloud about certain actions and parameter settings of the product. Each data point has different thresholds for when to send data to Swegon, therefore the data sent depends on the data point type and configuration. The data is sent in intervals, at which point the data is aggregated together with other data from that interval.

1.3 Who has access to the data

The data sent to Swegon INSIDE Cloud is used by Swegon for purposes of performance, functionality and development of the product. Consequently, Swegon has the right to use the data sent from all products connected to Swegon INSIDE Cloud. The data is used in accordance with Swegon's DS-23 general terms and conditions, and our sales agreement with the customer.

1.4 Requirements

To connect a product to Swegon INSIDE Cloud, a secure internet connection via the property's internal network or via Swegon's external modem is required. In addition to a secure internet connection, a valid certificate for each individual product is also required to approve them to share data with INSIDE Cloud. Some products will come with a valid certificate out of the factory, while other products need to be equipped with a certificate to authorize the product to share data.

To find out if the product is INSIDE Ready (i.e. ready to share data) or not visit INSIDE Ready | www.swegon.com.

1.5 Security

The Swegon INSIDE product is connected to azure IoT Hub. The connection uses MQTT and is secured using TLS and client certificates (MTLS). DigiCert is used as registration authority and key management. The Swegon cloud platform uses Azure SaaS offerings for hosting of applications and APIs. Digital services communicate with Swegon Cloud using standard technologies such as Rest APIs and message Queues. Users and authorization is handled by an internal identity provider.

1.6 Firewall settings for Swegon Cloud

Swegon cloud solution is using Microsoft Azure services and certificates from DigiCert to secure the connection. If the firewall in front of the products is allowing outbound traffic to internet it will work. If the firewall is set up to control outbound traffic the following ports and destinations must be allowed. If only filtering on ports, 443 and 8883 are used.

Domain (including sub domain)	Port	Protocol	Note
***.azure-devices-provisioning.net** (dps-SwegonCloud-common-we.azure-devices-provisioning.net global.azure-devices-provisioning.net)	443 8883	https mqtt	Azure Device Provisioning Service
***.azure-devices.net** (iot-SwegonCloud-prod-we.azure-devices.net)	443 8883	https mqtt	Azure IoT Hub
***.blob.core.windows.net** (stswciotfilestorageprod.blob.core.windows.net)	443	https	Azure storage
clientauth.one.digicert.com	443	https	DigiCert Enrolment over Secure Transport (EST) for certificate enrolment and reenrolment