Growatt's Developments in Data- and Product Security

As part of our ongoing efforts to improve product safety, we have taken active measures in the following matters.

In regards to device security:

1. Our new generation of dataloggers have additional encryption built in, making use of both TLS and AES.
2. To prevent unauthorized access, the datalogger will not passively broadcast any signal.
3. Our dataloggers are in compliance with the IoT security certification **ETSI EN303-645.** The ShineLink-X has already been fully certified, while the ShineWiFi-X and ShineLAN-X are currently undergoing certification testing.

Network Security:

1. Communications will now make use of HTTPS connection by default to improve security.
2. The API makes use of three factor authentication to ensure secure access. These factors are: 1.) User authentication 2.) Unique token assignment 3.) IP whitelisting
3. Improved firewalls and attack mitigation on our networks to quickly identify and stop potential threats.

Account Security:

1. An installer account is required prior accessing the Installer cloud platform 'OSS' (Online Service System). The Installer account needs to be approved server side before becoming active. End user registration is required to link installations with the installer. This gives the installer access to device information on our cloud platform, allowing further operations and maintenance.

GDPR Compliance:

1. In 2018, Growatt's monitoring platform received GDPR compliance guidance from SGS, including a differential analysis and rectification action plan. Based on this information, Growatt taken active efforts to improve on our systems.
2. Currently, Growatt is collaborating with SGS to certify our cloud platforms according to the GDPR standards.