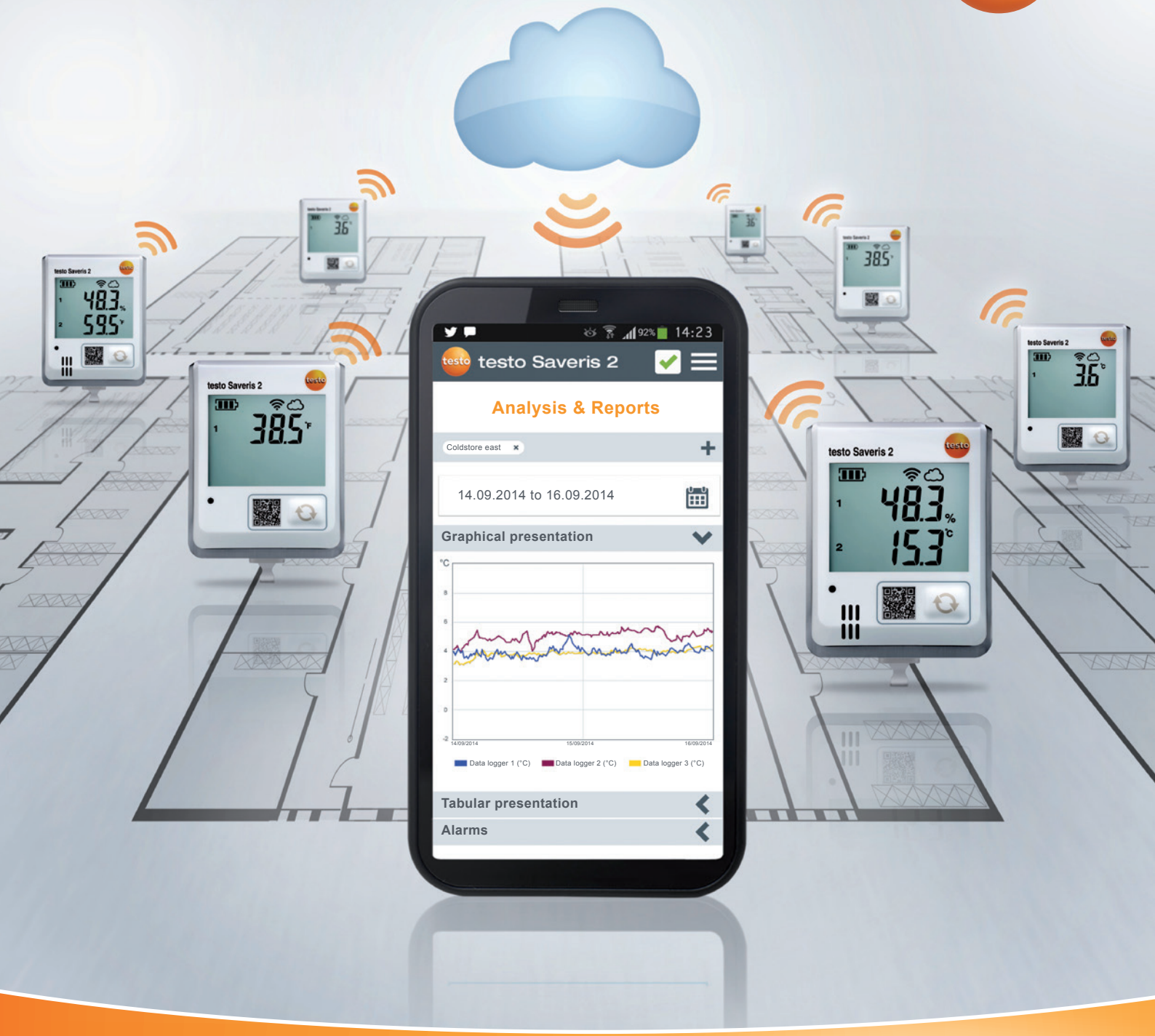
We measure it. testo



testo Saveris 2
Security Dossier.

Your security is important to us.

Protection of data and privacy with testo Saveris 2.

In order to guarantee the integrity and intactness of your personal data and your measurement values when using testo Saveris 2, Testo AG and our IT partners meet the highest security standards, guidelines and regulations.

In this document, we have assembled all relevant information which you need to know for the protection of your data and your privacy. If you have any further questions, we are available to help at all times.

1. Which data are stored?
Apart from the name given, and the e-mail addresses or mobile telephone numbers provided for the purposes of alarms when limit values are violated, no personal data at all are stored. The latter are used exclusively to be able inform you when limit values are exceeded.

When the measurement values are saved, an older measurement value is not overwritten by the respective new one. Instead, all data are documented as a time progression. For one thing, this allows the data to be retrieved at any time. For another, it is possible to reconstruct which value occurred at which time. This guarantees unrestricted traceability in case of emergency.

2. Where are my data?
All data are stored in the internationally recognized provider Host Europe's ISO/IEC 27001:2005-certified data center in Germany, and are subject to the stringent German data protection regulations.

Host Europe is certified by TÜV Süd according to ISO/IEC 27001:2005 for the "Provision of high-availability data center capacity, including network integration and its operation." Thanks to the TÜV-tested information security management system (ISMS), Host Europe guarantees excellent data security and unrestricted adherence to data protection. This means: Optimum protection with regard to the availability, confidentiality, integrity and authenticity of your data and systems.

Included in the certification were not only the existing processes at Host Europe, but also the sustainable measures for future adherence to security standards. The measures for the protection of data security include the following aspects, depending on the product:

Availability
Host Europe guarantees the the availability and usability of your data by:
- Daily back-up
- Offsite back-up
- Routine virus scans
- Regular security and function updates

Confidentiality
Measures with which Host Europe ensures that your data and information are available only to authorized persons:
- Protection from access to buildings and data
- Various security zones
- Secure disposal of data and data storage devices
- Internal security training

Integrity:
Host Europe protects data and information completely from unauthorized alteration by:
- Access security
- Prevention of unauthorized storage, processing, use or forwarding of data.
- Encrypted data transfer
- Protection from hacking

Authenticity:
Host Europe guarantees the reliability of transactions and information exchange with external partners with the help of:

- Multi-level authentification processes
- Secure user identification
- Pro-active sealing of security gaps

Physical protection
Over and above this, Host Europe follows a comprehensive program for the protection of the data centers, e.g. by:

- Regular stress tests of the infrastructure, as well as the creation of data redundancies.
- Fire protection
- Protection from water
- Contingency plans for natural disasters
- Emergency management
- Protection from environmental risks

Trusted Cloud
In order to eliminate the organizational, legal and technical risks involved with the implementation of Cloud Computing, Host Europe decided to have the security of their Cloud-based services tested by TÜV TRUST IT. Based on a comprehensive requirement catalog from TÜV TRUST IT for Cloud Services, the Cloud-based services from Host Europe were examined at infrastructure level (IaaS) regarding data security, data protection and compliance, and in November 2011, were the first hosting provider awarded the Trusted Cloud Service certificate. For you, secure Cloud Computing thanks to the Trusted Cloud certification means: optimum availability, confidentiality and integrity for your data and systems.

3. Are my data safe?

Protection of your privacy
All data are transferred to your internet browser exclusively by SSL encryption. In addition to this, the servers on which your measurement data are stored are situated in Germany, and are therefore subject to German data protection law – among the strictest in the world.

The entire web traffic is logged by the web server temporarily for a maximum of one month. However, this is done only for servicing purposes or in order to ensure the operation of the system. These data are then subsequently deleted or made anonymous.

In case of net attacks on the infrastructure, the data flows can be temporarily redirected via an external security service provider who analyzes them in order to filter out hostile requests.

Protection from data loss
The data center where the data are stored has two mutually isolated fire zones. The term “fire zone” is to be taken literally: If an emergency occurs and a database fails completely – due to a fire, for example – its job is taken over by the other fire zone. We of course notify you of such cases comprehensively and transparently.

The database with your measurement values is a multi-level High Availability Cluster. This is divided into a database master and a database slave, which are situated in different fire zones. Daily back-ups ensure that both databases are always up to date, and that their data can be recovered completely at any time should a database fail. In addition to this, all data are also archived on a spatially separated server.

In addition to the databases, there is also an application cluster in each fire zone, containing a so-called “broker”, the communication interface between WiFi data loggers and the databases. Each application cluster is only ever used to a capacity of maximum 50 %. This ensures that the measurement values are still securely transferred from the WiFi data logger to the database, even if a broker fails due to a system malfunction.

4. Who has access to my data?

- You and all those persons whom you have allowed access to your account.
- Staff at Testo AG in Germany, in order to service testo Saveris 2, and to guarantee the smooth running of the system. The measurement data are neither altered nor deleted.

5. Which data protection legislation are my data subject to?

The servers on which your data are stored are situated in Germany, and are therefore subject to German data protection law.

6. Which certificates are there?

Host Europe has the ISO/IEC 27001:2005 certificate.

ISO/IEC 27001:2005 is the leading international standard for Information Security Management Systems (ISMS). It applies to private commercial and public enterprises as well as to organizations, and defines the requirements for the introduction, implementation, monitoring and improvement of an Information Security Management System.

The standard specifies non-industry-specific requirements for the implementation of suitable security mechanisms, which should be adapted to the individual requirements of the respective organizations. ISO/IEC 27001:2005 was developed in order to ensure the selection of suitable security mechanisms for the protection of all information values of a company.

7. What do my IT supervisors need to know?

- The testo Saveris 2 WiFi data loggers communicate with the broker via the Port 1883 and the MQTT standard protocol.
- The time synchronization of the data loggers with the SNTP takes place via Port 123.
- The DNS name resolution takes place via Port 53
- All three ports (1883, 123, 53) must only be opened to the outside. No bi-directional port approvals are necessary.
- The default gateway, which must be communicated to the probe via DHCP or manually, must answer the PING request of the WiFi data logger. Note: During the first configuration, it is possible to select whether DHCP or Static IP is used. Please select the expert mode for the relevant information.
- Each testo Saveris 2 WiFi data logger has a unique MAC address.
- The IP address of each testo Saveris 2 WiFi data logger is dynamic, but can be individually altered to static.
- testo Saveris 2 supports 2.4 GHz WLAN (IEEE 802.11 b/g/n).
- The encryption method used for the communication between the WiFi data logger and the router is WPA2.
- The testo Saveris 2 web application is accessible with an internet browser. The standard TCP ports http (80) and https (443) are used.