EN-Version: 2.2 October 27, 2025

Transparency statement in accordance with the EU Data Act
(Regulation (EU) 2023/2854)

Manufacturer:
BLANCO GmbH + Co KG
Flehinger Straße 59, 75038 Oberderdingen, Germany

Product name:
Digital BLANCO products – in particular BLANCO CHOICE, All, EVOL-S Pro SODA, and BLANCO AQUA UVC-AC – in conjunction with the BLANCO UNIT app

Status: October 27, 2025
Responsible: Global Products

1. Subject of the declaration

In accordance with Articles 3–6 of the EU Data Act, this declaration describes which data-generating functions are available in BLANCO digital products, what types of data are generated, how they are processed, and who has access to this data.

2. Devices and digital services

Device/service	Description
EVOL-S Pro SODA	Water treatment system for filtering, cooling, and carbonating. From product revision F onwards, also compatible with the BLANCO UNIT app and the BLANCO Cloud.
BLANCO CHOICE.All	Water treatment system for filtering, cooling, heating, and carbonating. Compatible with the BLANCO UNIT app and the BLANCO Cloud.
BLANCO AQUA UVC-AC	Filtration unit consisting of UV filtration (UVC) and activated carbon filtration (AC). Compatible with the BLANCO UNIT app and the BLANCO Cloud.
BLANCO UNIT app	Mobile companion app for control and device monitoring via Bluetooth and the cloud.
BLANCO Cloud Watch	Enables BLANCO Service to perform a remote analysis of the digital BLANCO product. The analysis is based on the device data in the BLANCO Cloud. Access to the cloud data is enabled via the serial number and service code of the digital BLANCO product. The customer must actively provide BLANCO with both pieces of information in order to receive a remote analysis.
BLANCO Cloud (AWS)	Central data platform for processing and storing device data. Optional service for BLANCO customers. Digital BLANCO products do not need to be permanently connected. The BLANCO Cloud enhances

	the user experience with device status, statistics, notifications, and remote service.
BLANCO Smart Home API	Enables access to the cloud data of digital BLANCO products for smart home applications.

3. Types of data collected (data generated by the devices – telemetry data)

Category	Description	Personal reference
Device status and system data	Serial number, firmware version, operating hours, status/error codes, sensor values (temperature, level of CO_2, filter status, etc.).	Pseudonymised
Usage and consumption data	Number and type of water dispensing events, temperature/hardness settings, CO_2 and filter consumption, cleaning cycles.	Pseudonymised
Event/process data	Dispensing events, system events, status events, error events (including timestamps). These events allow the use of digital products to be assigned to a specific time.	Pseudonymised
App/device identifiers	App ID and device ID (SHA-256 hash), linked without personal information.	Anonymised/ Pseudonymised
Support data (optional)	Only if the customer actively transmits the service code and serial number to BLANCO (e.g., for remote support).	Only in these circumstances referable to a specific device
Cloud metadata	Log/error logs for system security, access tokens, app usage statistics.	Pseudonymised

The devices are capable of generating data continuously and in real time.

4. Format and data volume

- Data exchange in **standardised JSON formats** via encrypted MQTT messages
- Typical data volume: a few kilobytes per event
- Aggregated historical data is used for app visualisation or maintenance functions

5. Storage period

- Operational, pseudonymised device data: until the user requests deletion
- Aggregated system data: anonymised/pseudonymised, unlimited for statistical purposes
- Support data: deleted after completion of the service case (service code)

- Diagnostic data: maximum **12 months**

6. Purpose of data collection and processing

- Provision of connectivity, control, and monitoring functions
- Displaying device status, statistics, and consumption data in the app
- Performing firmware updates
- Provision of new device functions (OTA update)
- Facilitation of technical support (remote service)
- Improving quality and products through aggregated data analysis

7. Storage and processing locations

- Regional separation of AWS data centres (BLANCO Cloud)
    - EU/EMEA: Ireland
    - USA: North Virginia
    - APAC: Sydney
    - China: Ningxia
- All market-related data remains in the respective region. This includes the storage, processing, and provision of data
- Data is not transferred between regions

8. Access to data

Actor	Access level	Purpose
End user (UNIT app)	Live status, consumption statistics for own device, settings, and error detection	Operation, maintenance
BLANCO 1st Level Support	After consent and transmission (by telephone or e-mail) of serial number and service code by the customer	Error diagnosis, support
BLANCO backend systems	Aggregated, non-personal statistical data	Quality assurance, analysis
AWS (cloud provider)	Technical operation, security, and update functions	Infrastructure operation

9. Security measures

- End-to-end encryption (TLS/SSL and AES-256)
- Access control via multi-level "Request Cloud Access" (RCA) procedure
- No user accounts required (app ID and device ID link replace traditional user account)
- Data access only after validation by multi-level authentication mechanisms
- AWS Secret Manager for certificate management

10. Data user rights (in accordance with the EU Data Act)

- Right to access data generated by the device
- Right to portability (export of structured usage data upon request)
- Right to deletion or deactivation of the cloud connection
- Right to information about third-party access and security incidents

Furthermore, the customer has the right to lodge a complaint with the competent authority pursuant to Art. 37 EU Data Act for a violation of Chapter II of the EU Data Act. In Germany, this is the Federal Network Agency.

11. Intended use/collection and processing purposes

Potential data owners expect to use readily available data themselves.

It is not intended to allow a third party to use the readily available data for purposes agreed with the user.

12. Contact

BLANCO GmbH + Co KG

Department: Global Digital Product Development
Flehinger Straße 59, 75038 Oberderdingen, Germany
Email: info@blanco.com

13. Glossary of technical terms

Term	Meaning / Explanation
EU Data Act (Regulation (EU) 2023/2854)	EU law governing access to and sharing of device-generated data. It requires manufacturers to be transparent and grants users rights to data use and portability.
Transparency statement	Document that informs users about the type, purpose and processing of, and access to device-generated data (mandatory under Art. 3 – 6 EU Data Act).
Device-generated data / telemetry data	Operating, usage, or error data automatically generated by the device (e.g., temperature, level of CO_2, status codes).
Pseudonymisation	Data processing in which personal information is replaced so that it can only be assigned to a person via additional information.
Anonymisation	Complete removal of personal references; no traceability to individual persons or devices possible.
BLANCO UNIT app	Mobile app for controlling and monitoring devices via Bluetooth or the cloud.
BLANCO Cloud (AWS)	Cloud platform (Amazon Web Services) for storing and processing device data. Location-dependent (e.g., Ireland, Ningxia).
AWS (Amazon Web Services)	External cloud provider whose infrastructure is used to operate the BLANCO Cloud.
MQTT (Message Queuing Telemetry Transport)	Standardised protocol for data exchange between devices and servers, especially in the context of IoT.
JSON (JavaScript Object Notation)	Standard data format for structured, easily readable data transfer between systems.

Term	Meaning / Explanation
OTA update (over-the-air update)	Remote firmware update via the internet or cloud, without a physical connection.
Firmware version	Version of the device control software; determines the range of functions and compatibility.
App ID / Device ID (SHA-256 hash)	Unique but anonymised identifiers for app instance or device.
RCA procedure (Request Cloud Access)	Multi-level authentication procedure for secure access to cloud data.
TLS/SSL / AES-256	Cryptographic procedures for end-to-end encryption of data transfers.
AWS Secret Manager	AWS service for secure management of keys, certificates, and passwords.
1st Level Support	First level of technical support (customer contact, error analysis with service code provided by the customer).
Service code / serial number	Combination of unique identifiers that the customer releases for remote analysis.
Aggregated data	Summarised data sets from multiple devices, without individual reference, for analysis and quality improvement.
Cloud metadata	Operating data from cloud systems (e.g., log files, access tokens, usage statistics).
Usage data / consumption data	Data on water volumes, CO_2 consumption, filter cycles, etc. – basis for visualisation in the app.
Diagnostic data	Data stored for a short period of time for technical error analysis, max. 12 months.
Regional data separation	Principle according to which data remains within a region (EU, USA, China, etc.) and is not transferred.
Data portability	Right of the user to receive or transfer structured data (e.g., JSON export).
Remote analysis / remote service	Option for the manufacturer to diagnose devices remotely if the customer actively consents.
Federal Network Agency	German supervisory authority for the EU Data Act (Art. 37) – contact for complaints.