



CAVOTEC DATA GOVERNANCE STATEMENT

Last updated: Nov 1st, 2022

This Cavotec Data Governance Statement describes the practices of Cavotec S.A. (together with our Affiliates, "Cavotec," "we," "us" or "our") for collecting and using information, from customers directly or via our Affiliates (as defined below) relating to machines, products or other assets and their associated worksites (collectively "Assets"), for the purposes of delivering functioning products and quality services. We collect this information through online and offline means via our Digital Offerings including: (1) applications and platforms for use on or through computers, APIs, and mobile devices; (2) telematics or other devices on Assets, whether manufactured by Cavotec or by other companies ("Devices" and, together with the Applications, "Digital Offerings"). As used in this Data Governance Statement, "you" means you individually and, as applicable, the company or entity you represent and each of its employees, agents and representatives.

You should regularly review this Statement carefully to understand what information our digital offerings receive, generate and transmit - and what we do with that information. By providing System Data, Operations Data, or other data to us, you agree to the terms and conditions of this Data Governance Statement, including our collection, use and sharing of that information.

WHAT INFORMATION WE MAY COLLECT

"System Data" is information that is ingested or used by or generated through Digital Offerings, which may include:

- Device, Asset and Component Information, including model number, serial number, order number, software and hardware version numbers, performance, and configuration, including work tools or other peripheral devices attached to Assets.
- Electronic Data, including sensor logs, trends, histograms, event data, other alerts, digital state data, fault codes, idle time, daily and cumulative fuel consumption, emissions data, service meter hours, electronic data files downloaded manually or automatically from an Asset, troubleshooting data, and other data, depending on the customer and Asset and communication channel used by a Device.
- Inspection Data, including results of inspections using a Cavotec or third-party inspection system.
- Device Location Information, including the physical location of an Asset (e.g., determined using satellite, GPS, cell phone tower, Bluetooth, Wi-Fi signals or any other similar means of determining location).
- Fluid Data, including analysis results of fluid samples (such as oil, hydraulic and coolant fluids) obtained using Cavotec or third-party tools.
- Event Recorder Data, including location, speed, direction and associated video recordings, use of controls and positive train control information.
- Service and Maintenance History, including but not limited to work orders (records of all maintenance, repair, parts purchases, replacement and modification to an Asset), component life (history of usage and wear life of a component), maintenance schedule, planned maintenance, warranty coverage data, maintenance and repair contracts, service intervals

(scheduled interval for planned maintenance of component replacement activities for an Asset), component lists (lists of parts that make up an Asset) and service letters (describing special service actions recommended by Cavotec to correct a known problem with an Asset).

- Site and Environmental Conditions, including but not limited to the type of work being done, condition of roads or tracks, altitude, climate and material tracking.

“Operations Data” is additional information we may collect from Assets while providing the Digital Offering such as patterns of usage, user input or status of user, operation parameters and maintenance cycles.

“Personal Data” in the form of Personal Identifiable Information (PII), or similar, is not collected, nor in any way either “Systems Data” or “Operations Data”, or other data in the control of Cavotec- is combined to result to such PII.

Information collected by Cavotec may simultaneously constitute System Data and Operations Data, or any combination thereof. If you submit any System Data or Operations Data, including System Data that may relate to Devices or Assets that are not manufactured by Cavotec, you represent that you have the authority to do so and to permit Cavotec to use the information in accordance with this Data Governance Statement.

Data related to other aspects of your interaction with Cavotec, not related with Assets, Devices or Digital Offerings, do not fall under this Data Governance Statement, and are covered by the general privacy notice / terms and conditions.

HOW WE MAY COLLECT INFORMATION

We may collect information in a variety of ways, including:

- Through Devices: We may receive information via cellular or satellite link, or radio or ethernet connections from Assets equipped with a Device, which may include System Data (such as information relating to the Device or Asset) or Operations Data (such as from usage related data, or information generated by fatigue monitoring devices, on-board camera and proximity detection systems). Some information may be collected automatically, such as fault codes, hours of operation and oil levels.
- Through Applications and Online: We may collect information through Applications (e.g., when you enter maintenance information) or when you use our online services or platforms.
- Offline: We may collect information from the Assets, offline.
- From Component Manufacturers and OEMs (Original Equipment Manufacturer): We may obtain System Data from manufacturers of the components in your Assets or of Assets manufactured by others you use. This information may be provided to us automatically.
- Through Wearable Technology: We may collect information through wearable technology, such as fatigue monitoring devices or RFID (Radio Frequency Identification) tags embedded in hardhats or safety vests.
- From Asset Owners: We may receive additional information from Asset owners, Distribution Networks, operators and any other entities who might have management responsibility for an Asset.
- From Other Sources: We may collect or generate information from troubleshooting data, from your service providers (such as fluid analysts and site inspectors) or from maintenance, inspection and/or warranty records.

HOW WE MAY USE INFORMATION

We may use collected information for the following purposes:

To Provide Services to you:

- To provide you monitoring of the status of Assets, to provide you use of Applications, and other related services.
- To fulfil technical support agreements, perform maintenance and repairs, root cause analysis of incidents and deliver Assets or parts.
- To make recommendations regarding safety, Asset health, (condition) maintenance, worksite efficiency and productivity training for operators.
- To enhance the safety of machine operations, including by tracking proximity to Assets, other objects or humans.
- To enable remote technician services, such as remote troubleshooting, and remote tuning.
- To enable communications to manage the connection to the Asset (Equipment) or Device and allow other user applications to communicate with each other.

For General Business Purposes:

- To perform data analytics, audits, improving products, developing new products, enhancing, improving or modifying our Digital Offerings, identifying usage trends and operating and expanding our business activities and for statistical analysis based on aggregated and de-identified data, such as benchmarking reports.
- To provide services to Cavotec and its customers, manage workflow, monitor repairs, project future maintenance and service, and troubleshoot issues.
- To validate effectiveness of recommendations, resolve complaints, and fulfil orders.
- To manage inventory so we can provide you parts and services.
- To maximize the efficiency of operations.
- To develop digital applications.

With respect to audio-visual data that, such as information generated by fatigue monitoring devices, on-board camera and proximity detection systems, we will use that data only to provide products and services to our customers, including to make recommendations regarding safety, Asset health(condition), maintenance, worksite efficiency and productivity training for operators, and to improve our products and services. Cavotec equipment stores this audio video data locally only.

Data Retention: Cavotec stores data as needed to accomplish the purposes identified above and to meet legal requirements that might be relevant record retention. This storage period may extend beyond the term of your relationship with Cavotec.

HOW WE MAY DISCLOSE INFORMATION

We may disclose information:

- To the entities directly or indirectly controlling, controlled by or under common control with Cavotec S.A. ("Affiliates") for the purposes described in this Data Governance Statement. Cavotec S.A. is the entity responsible for information jointly used with its Affiliates.
- To Asset owners, to permit them to manage their use of their Asset.

- To our service providers who provide services such as data analytics, information technology and related infrastructure provision, application development, platform hosting, customer service, product development, auditing, advisory and other services.
- To component manufacturers, to permit them to study the use of their products, to improve their products and to develop new products.
- To a third party provided Cavotec gives you 15 days prior notice in the event of reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our or any of our Affiliate's business, Assets or stock (including in connection with any bankruptcy or similar proceedings).
- To additional recipients as agreed by you and us.

We may use or disclose information, as we believe to be necessary or appropriate, on a need basis only: (a) under applicable law, including laws outside your country of residence; (b) to comply with legal process; (c) to respond to lawful requests from public and government authorities, including public and government authorities outside your country of residence; (d) to carry out our terms and conditions; (e) to safeguard our operations or those of any of our Affiliates; (f) to protect our rights, privacy, safety or property, and/or that of our Affiliates, you or others, including for purposes of information security; and (g) to allow us to pursue available remedies or limit the damages that we may sustain.

REMOTE SERVICES AND UPDATES

Depending on your Device and Asset configuration, we may use System Data to remotely:

- Examine and update Devices that we manufacture or otherwise provide (e.g., to update system settings or to manage the communications carriers used to connect to Cavotec).
- Update software that controls machine operations for your Cavotec Asset, and we may push the software update files to the Asset in preparation for an update.

Remote Software Updates provides value to Cavotec's customers by:

- Keeping the Assets secure, improving reliability, offering faster issue remediation and uptime,
- Decreasing the need for travel to physically access the equipment,
- Lowering the cost of support services needed by customers,
- Providing better and more reliable data for more efficient asset performance,
- Providing additional services, as they become available.

As a basic principle, Cavotec uses its best commercial efforts to provide customers with timely notices of update. Notice of update will be provided through a variety of means as deemed appropriate by Cavotec including but not limited to emails or application notifications. The customer will be deemed accepting the update unless otherwise stated in writing within 48 hours of receiving the Notice of update. Naturally our ability to provide notice to customer is dependent on receiving the most current contact information and Cavotec will not be responsible or obliged to notice the customer in anyway whatsoever shall it did not receive said most current contact information.

SECURITY

We use commercially reasonable organizational, technical and administrative measures, including information technology security and physical security measures, designed to protect information within our organization. No data transmission, storage or use on any system, application or network can be guaranteed to be 100% secure; by using best practices and a risk-based approach, we apply best effort to lower risk, mitigating where possible relevant high-risk areas. As control of the relevant Assets, and/or

worksite environment, might fall under your direct or indirect oversight, your best efforts when it comes to good digital and physical security also aid to the overall data protection and security of Assets and relevant information. If you have reason to believe that there's any type of breakdown in security (potential data breach, a compromised system or any other indication of compromise), please immediately notify us in accordance with the "Contacting Us" section below.

OTHER IMPORTANT INFORMATION

Third Party Content: This Data Governance Statement does not address, and we are not responsible for (i) the privacy, information or other practices of any third party operating any website or online service to which a Digital Offerings links (e.g., our Applications may include, for your convenience, a hyperlink to local weather information provided by a third party with whom we have no business relationship) and (ii) Personal Information controlled by a third party, such as a supplier, service provider, or customer, even if such Personal Information is collected or otherwise processed by Cavotec. Further, the inclusion of a link in a Digital Offering does not imply endorsement of the linked site or service by us or by our Affiliates.

Cross Border Transfers: Your information may be stored and processed in any country where we operate or where our service providers operate, and by using a Digital Offering or otherwise providing data to us consistent with this Data Governance Statement you consent to the transfer of information to countries outside of your country of residence, including the United States, which may have data protection rules that are different from those of your country.

Sensitive Information: Our Digital Offerings are not designed for you to send us sensitive Personal Information such as social security numbers, information related to racial or ethnic origin, political opinions, religion or other beliefs, or genetic characteristics, criminal background or trade union membership. We request that you do not send such information or similar information on or through Digital Offerings or otherwise to us.

REVIEW AND UPDATES TO THIS DATA GOVERNANCE STATEMENT

We may change this Data Governance Statement. The "LAST UPDATED" legend at the top of this page indicates when this Data Governance Statement was last revised. Any changes will become effective when we post the revised Data Governance Statement. Your use of Digital Offerings following these changes means that you accept the revised Data Governance Statement.

A periodic assessment of the data types collected, used, stored and shared is executed for determining any change in data, and linked data governance related changes that might be required to be actioned.

CONTACTING US

If you have any questions about this Data Governance Statement, or for any other Data Governance, Privacy or any other reasons as stated above, please contact us at

Cavotec S.A. Data Protection Officer, e-mail: dpo@cavotec.com or by mail to the address listed below.

Attn: Data Privacy Team
Cavotec S.A.
Via G.B. Pioda 14,
6900 Lugano, Switzerland