Status as of: 17/09/2025

Information sheet

under Article 3 EU Data Act

Related service: e-FOLLOW.cloud & e-FOLLOW Essential/Professional

Manufacturer Control Systems GmbH & Co. KG

Provider: Toshiba TEC Germany Imaging Systems GmbH

1. Classification

e-FOLLOW Essential/Professional is software installed and operated by the customer. Control Systems is not involved in the customer's operations; therefore, the customer provides the associated service under Regulation (EU) 2023/2854.
Control Systems will only access customer data when explicitly provided for support purposes and act as a data processor.

e-FOLLOW.cloud is operated by Control Systems in its Azure environment. As the operator, Control Systems provides the associated service under Regulation (EU) 2023/2854 and will publish the data policy required under Article 3.

2. Processing purposes

Authenticating multifunctional printer (MFP) users and authorising access to the print, scan and copy functions.
Saving, managing and releasing queued print jobs.
Capturing order and transaction details for accounting, billing, quota and balance management (user balances are only for locally installed versions).
Providing reporting and monitoring for administrators, including usage per user, MFPs, departments and projects; the cloud version includes dashboard metrics such as most printed and uploaded pages per user and most printed pages by device.
Supporting with operational requirements and troubleshooting (logging, diagnostics and temporary access, if explicitly granted by the customer).
Storage of records required for audit, legal or contractual compliance.
Using aggregated and anonymised statistics to monitor system status and improve product functionality. No personal data is sold or used for third-party marketing.
Processing configurations (which define attributes to be read, storage settings, deletion rules, and dashboard visibility) are controlled by the customer administrator.

3. Processing types

User account attributes that are retrieved from the customer directory (Entra ID, Active Directory or any LDAP-compatible directory). The exact set of read attributes (e.g. full name and email address) can be configured and defined by the customer administrator.
The authentication attributes used for login and authorisation include a fixed user name and configurable attributes such as email address, PIN and card ID.
Order and transaction records with order details and processing results, accounting and balance adjustments, and other transaction metadata used for reporting and billing. User balances (current credit/money) are recorded for local software version.
Content of queued print jobs temporarily stored for release: e-FOLLOW.cloud content is stored encrypted in the provider environment while e-FOLLOW Essential/Professional content remains on the customer server.
Login and activity traces used for monitoring and displayed in administrative dashboards (e.g. login events and metrics with the highest usage).
Operational and support logs, including default system logs may be stored and managed according to configured storage and sizing rules. They may only be shared with the provider by the customer for support purposes.

4. Data access and release

Customer administrators have primary access and control over their data and can configure which directory attributes are read and who can see dashboards and reports. With e-FOLLOW Essential/Professional, data remains on the customer's server and is only accessible to the customer's administrators and those expressly authorised. The customer's authorised administrators can access their data via the service portal for e-FOLLOW.cloud; Control Systems operates the service and stores customer data in its environment to provide the service.
Control Systems does not access customer data during normal operation. Access by Control Systems personnel will only occur in explicit, customer-initiated support scenarios (e.g. when logs are provided or remote access is granted) and will be limited and subject to the applicable Data Processing Agreement.

Customers control further transfer of their data (e.g. export of reports or integration with other systems). Any disclosure required by law will be handled under legal requirements and, where possible, the customer will be notified.

5. Data retention

Authentication data: The user name is defined for each user. Other authentication attributes such as e-mail, PIN or card ID are saved as configured by the customer and can be deleted by the customer administrator. If a user is removed from the directory, the customer administrator can decide whether the user account will also be removed from e-FOLLOW during the next synchronisation.

Usage and billing/reporting data: Transaction and usage data (order history, order details, balance changes, accounting records, login activity) is retained for operational and reporting purposes. Storage depends on the provision and configuration: e-FOLLOW.cloud stores the data in the provider environment. When using e-FOLLOW Essential/Professional, the data remains on the customer server. The customer administrator can configure the automatic deletion of old data (e.g. deletion of data records older than a year) and permanently delete report data at any time.

Print jobs: For e-FOLLOW.cloud, queued print jobs are stored encrypted in the provider environment until they are released or deleted under the configured retention policy.
e-FOLLOW Essential/Professional print jobs remain queued on site on the customer server and follow the retention settings set by the customer. Paused print jobs can be automatically deleted after a time set by the customer.

Support and system logs: Log files are generated by default and stored in the system. Logs are only deleted automatically if the log directory exceeds a configured size limit. Log files or temporary data provided by the customer to Control Systems for support purposes will be deleted after the support case has been resolved.

Notes and restrictions: Retention settings and deletion actions are controlled by the customer administrator. Control Systems cannot guarantee the deletion of locally stored data unless the customer's administrator carries out the deletion or instructs us to do so as part of an agreed process. e-FOLLOW.cloud data is deleted under the configured retention policy and contractual settings.

6. User Rights

Users have the right to access, rectify or erase their personal data. The customer administrator controls how these rights are implemented. Control Systems can only provide assistance in support cases if expressly authorised by the customer.

7. Support data

As part of support cases, customers can provide log files or grant temporary remote access. Log files are generated on the customer system by default and remain there unless the log directory exceeds the configured maximum size. The data transmitted to Control Systems for support purposes will only be used to process the support enquiry and deleted after the case has been closed.

8. Safety measures

e-FOLLOW.cloud runs in an Azure Kubernetes service environment. Communication between MFP apps and the service takes place via HTTPS and LDAPS. Queued print jobs are stored in Azure Storage and encrypted by our application in addition to the platform encryption. Network protection is provided by the Azure platform. Management access to customer portals is Operator + Password by default, but can be configured to use the Entra ID (including MFA). Only the Azure administrators designated by Control Systems have access to the Azure/Kubernetes environment and storage.
The production environment is maintained under operational security practices (patches and updates of the Kubernetes platform and components, access with the least privileges for administrators and secure handling of credentials). Access to customer data by Control Systems employees is restricted to expressly authorised support or maintenance activities.

9. Updates and communication

This Data Policy may be updated periodically to reflect changes in legal requirements, product functionality or operational practices. Updated versions will be made available to customers before their effective date. The customer is responsible for checking the latest version.