Stand: 05.01.2026

Informationsblatt

gemäß Artikel 3 EU Data Act

Verbundener Dienst: e-FOLLOW.cloud & e-FOLLOW Essential/Professional

Hersteller: Control Systems GmbH & Co. KG

Anbieter: Toshiba TEC Germany Imaging Systems GmbH

---

1. Klassifikation

e-FOLLOW Essential/Professional wird als Software bereitgestellt, die vom Kunden installiert und betrieben wird. Control Systems betreibt im Normalbetrieb keine Kundeninstanzen und greift nicht darauf zu; daher ist der Kunde der Anbieter der damit verbundenen Dienstleistung im Sinne der Verordnung (EU) 2023/2854.
Control Systems greift nur dann auf Kundendaten zu, wenn dies ausdrücklich für den Support zur Verfügung gestellt wird, und wird in diesen Fällen als Datenverarbeiter fungieren.
e-FOLLOW.cloud wird von Control Systems in der eigenen Azure-Umgebung betrieben. Als Betreiber ist Control Systems der Anbieter der damit verbundenen Dienstleistung gemäß der Verordnung (EU) 2023/2854 und wird die gemäß Artikel 3 erforderliche Datenrichtlinie veröffentlichen.

2. Zweck der Verarbeitung

Authentifizieren von Benutzern am Multifunktionsdrucker (MFP) sowie autorisieren des Zugriffs auf die Druck-, Scan- und Kopierfunktionen.
Speichern, Verwalten und Freigeben von Druckaufträgen in der Warteschlange.
Erfassen von Auftrags- und Transaktionsdetails für Buchhaltung, Abrechnung, Kontingent- und Saldenverwaltung (Benutzersalden werden nur für lokal installierten Versionen verwendet).
Bereitstellung von Berichten und Überwachung für Administratoren, einschließlich der Nutzung durch Benutzer, MFPs, Abteilungen und Projekte; Die Cloud-Version umfasst Dashboard-Metriken wie die am häufigsten gedruckten Seiten nach Benutzer, die am häufigsten hochgeladenen Seiten nach Benutzer und die am häufigsten gedruckten Seiten nach Gerät.
Unterstützung bei betrieblichen Anforderungen und Fehlerbehebung (Protokollerfassung, Diagnose und temporärer Zugriff, sofern vom Kunden ausdrücklich gewährt).
Aufbewahren von Aufzeichnungen die für die Audit-, Rechts- oder Vertragskonformität erforderlich sind.
Verwenden von aggregierten und anonymisierten Statistiken, um den Systemzustand zu überwachen und die Produktfunktionalität zu verbessern. Es werden keine personenbezogenen Daten verkauft oder für Marketing Dritter verwendet.
Alle Verarbeitungskonfigurationen (welche Attribute gelesen werden, Aufbewahrungseinstellungen, Löschregeln, Dashboard-Sichtbarkeit) werden vom Kundenadministrator gesteuert.

3. Arten der Verarbeitung

Benutzerkontoattribute, die aus dem Kundenverzeichnis (Entra ID, Active Directory oder ein beliebiges LDAP-kompatibles Verzeichnis) abgerufen werden. Der genaue Satz der gelesenen Attribute (z. B. vollständiger Name und E-Mail-Adresse) kann vom Kundenadministrator konfiguriert und festgelegt werden.
Zu den Authentifizierungsattributen, die für die Anmeldung und Freigabe verwendet werden, gehören ein fester Benutzername sowie konfigurierbare Attribute wie E-Mail-Adresse, PIN und Karten-ID.
Auftrags- und Transaktionsaufzeichnungen mit Auftragsdetails und Verarbeitungsergebnissen, Buchhaltungs- und Saldoanpassungen sowie anderen Transaktionsmetadaten, die für Berichte und Abrechnungen verwendet werden.
Benutzersalden (aktuelle Guthaben/Geldmittel) werden für lokale Softwareversion aufgezeichnet.
Inhalt von Druckaufträgen in der Warteschlange, der für die Freigabe vorübergehend gespeichert wird: e-FOLLOW.cloud dieser Inhalt verschlüsselt in der Provider-Umgebung gespeichert wird; Bei e-FOLLOW Essential/Professional verbleiben die Inhalte auf dem Kundenserver.
Anmelde- und Aktivitäts-Traces, die für die Überwachung verwendet und in administrativen Dashboards angezeigt werden (z. B. Anmeldeereignisse und Metriken mit der höchsten Nutzung).
Betriebs- und Supportprotokolle, einschließlich Systemprotokolle, die standardmäßig generiert werden; Diese können gemäß konfigurierten Aufbewahrungs- und Größenregeln aufbewahrt und verwaltet werden und dürfen nur dann an den Anbieter weitergegeben werden, wenn sie vom Kunden zu Supportzwecken bereitgestellt werden.

4. Datenzugriff und-freigabe

Kundenadministratoren haben primären Zugriff und Kontrolle über ihre Daten und können konfigurieren, welche Verzeichnisattribute gelesen werden und wer Dashboards und Berichte sehen kann. Bei e-FOLLOW Essential/Professional verbleiben alle Daten auf dem Kundenserver und sind nur für die Administratoren des Kunden und alle von ihnen ausdrücklich autorisierten Personen zugänglich. Zum e-FOLLOW.cloud können die autorisierten Administratoren des Kunden über das Serviceportal auf ihre Daten zugreifen; Control Systems betreibt den Service und speichert Kundendaten in der eigenen Umgebung, um den Service bereitzustellen.
Control Systems greift im Normalbetrieb nicht auf Kundendaten zu. Der Zugriff durch das Personal von Control Systems erfolgt nur in expliziten, vom Kunden initiierten Supportszenarien (z. B. wenn Protokolle bereitgestellt oder Fernzugriff gewährt werden) und ist begrenzt und unterliegt der geltenden Datenverarbeitungsvereinbarung.

Kunden haben die Kontrolle über die weitere Weitergabe ihrer Daten (z. B. Export von Berichten oder Integration mit anderen Systemen). Jede gesetzlich vorgeschriebene Offenlegung wird gemäß den gesetzlichen Anforderungen gehandhabt und, wenn möglich, der Kunde benachrichtigt.

5. Aufbewahrung von Daten

Authentifizierungsdaten: Der Benutzername ist für jeden Benutzer festgelegt. Andere Authentifizierungsattribute wie E-Mail, PIN oder Karten-ID werden wie vom Kunden konfiguriert gespeichert und können vom Kundenadministrator gelöscht werden. Wird ein Benutzer aus dem Verzeichnis entfernt, kann der Kundenadministrator entscheiden, ob das Benutzerkonto bei der nächsten Synchronisation auch aus e-FOLLOW entfernt wird.

Nutzungs- und Abrechnungs-/Berichtsdaten: Transaktions- und Nutzungsdaten (Auftragshistorie, Auftragsdetails, Saldenänderungen, Buchhaltungsaufzeichnungen, Anmeldeaktivitäten) werden für Betriebs- und Berichtszwecke aufbewahrt. Die Aufbewahrung hängt von der Bereitstellung und Konfiguration ab: e-FOLLOW.cloud werden die Daten in der Anbieterumgebung gespeichert. Mit Verwendung von e-FOLLOW Essential/Professional verbleiben die Daten auf dem Kundenserver. Der Kundenadministrator kann das automatische Löschen alter Daten konfigurieren (z. B. das Löschen von Datensätzen, die älter als ein Jahr sind) und Berichtsdaten jederzeit dauerhaft löschen.

Druckaufträge: Für e-FOLLOW.cloud werden Druckaufträge in der Warteschlange verschlüsselt in der Anbieterumgebung gespeichert, bis sie gemäß der konfigurierten Aufbewahrungsrichtlinie freigegeben oder gelöscht werden.
Bei e-FOLLOW Essential/Professional verbleiben Druckaufträge in der Warteschlange vor Ort auf dem Kundenserver und folgen den vom Kunden definierten Aufbewahrungseinstellungen. Pausierte Druckaufträge können nach einer vom Kunden definierten Zeit automatisch gelöscht werden.

Support- und Systemprotokolle: Protokolldateien werden standardmäßig generiert und im System aufbewahrt. Das automatische Löschen von Protokollen erfolgt nur, wenn das Protokollverzeichnis eine konfigurierte Größenbeschränkung überschreitet. Alle Protokolldateien oder temporären Daten, die der Kunde Control Systems für den Support zur Verfügung stellt, werden nach Klärung des Supportfalls gelöscht.

Hinweise und Einschränkungen: Aufbewahrungseinstellungen und Löschaktionen werden vom Kundenadministrator gesteuert. Control Systems kann die Löschung von lokalen gespeicherten Daten nicht garantieren, es sei denn, der Administrator des Kunden führt die Löschung durch oder weist uns an, dies im Rahmen eines vereinbarten Prozesses zu tun. Bei e-FOLLOW.cloud werden Daten gemäß der konfigurierten Aufbewahrungsrichtlinie und den vertraglichen Einstellungen gelöscht.

6. Rechte der Nutzer

Die Nutzer können den Zugang, die Berichtigung oder die Löschung ihrer personenbezogenen Daten verlangen. Der Kundenadministrator steuert, wie diese Rechte implementiert werden. Control Systems kann in Supportfällen nur dann helfen, wenn der Kunde dies ausdrücklich autorisiert hat.

7. Support-Daten

Im Rahmen von Supportfällen können Kunden Protokolldateien bereitstellen oder temporären Fernzugriff gewähren. Protokolldateien werden standardmäßig auf dem Kundensystem generiert und verbleiben dort, es sei denn, das Protokollverzeichnis überschreitet die konfigurierte maximale Größe. Die zu Supportzwecken an Control Systems übermittelten Daten werden nur zur Bearbeitung der Supportanfrage verwendet und nach Abschluss des Falls gelöscht.

8. Sicherheitsmaßnahmne

e-FOLLOW.cloud wird in einer Azure Kubernetes Service-Umgebung ausgeführt. Die gesamte Kommunikation zwischen MFP-Apps und dem Dienst erfolgt über HTTPS und LDAPS. Druckaufträge in der Warteschlange werden in Azure Storage gespeichert und zusätzlich zur Plattformverschlüsselung von unserer Anwendung verschlüsselt. Der Netzwerkschutz wird von der Azure-Plattform bereitgestellt. Der Verwaltungszugriff auf Kundenportale ist standardmäßig Operator + Passwort, kann aber für die Verwendung der Entra ID (einschließlich MFA) konfiguriert werden. Nur die von Control Systems designierten Azure-Administratoren haben Zugriff auf die Azure-/Kubernetes-Umgebung und den Speicher.
Die Produktionsumgebung wird gemäß den betrieblichen Sicherheitspraktiken gepflegt (Patches und Updates der Kubernetes-Plattform und -Komponenten, Zugriff mit den geringsten Rechten für Administratoren und sicherer Umgang mit Anmeldeinformationen). Der Zugriff auf Kundendaten durch Mitarbeiter von Control Systems ist auf ausdrücklich autorisierte Support- oder Wartungstätigkeiten beschränkt.

9. Updates und Kommunikation

Diese Datenrichtlinie kann regelmäßig aktualisiert werden, um Änderungen der gesetzlichen Anforderungen, der Produktfunktionalität oder der betrieblichen Praktiken widerzuspiegeln. Aktualisierte Versionen werden den Kunden vor dem Datum ihres Inkrafttretens zur Verfügung gestellt. Der Kunde ist dafür verantwortlich, die neueste Version zu überprüfen.