

Informationsblad

enligt artikel 3 i EU:s datalag

Tillhörande tjänst: e-FOLLOW.cloud och e-FOLLOW Essential/Professional

Tillverkare Control Systems GmbH & Co. KG

Leverantör: Toshiba TEC Germany Imaging Systems GmbH

1. Klassificering

e-FOLLOW Essential/Professional är en programvara som installeras och drivs av kunden. Control Systems är inte involverade i kundens verksamhet; därför tillhandahåller kunden den tillhörande tjänsten enligt förordning (EU) 2023/2854. Control Systems kommer endast att få tillgång till kunddata när de uttryckligen tillhandahålls för supportändamål och fungerar som dataprocessor.

e-FOLLOW.cloud drivs av Control Systems i deras Azure-miljö. Som operatör tillhandahåller Control Systems den tillhörande tjänsten enligt förordning (EU) 2023/2854 och kommer att offentliggöra den datapolicy som krävs enligt artikel 3.

2. Syften med behandlingen

Autentisera användare av multifunktionsskrivare (MFP) och godkänna åtkomst till utskrifts-, skannings- och kopieringsfunktionerna.

Spara, hantera och frigöra utskriftsjobb i kön.

Registrering av order- och transaktionsuppgifter för redovisning, fakturering, kvot- och saldohantering (användarsaldon gäller endast för lokalt installerade versioner).

Rapportering och övervakning för administratörer, inklusive användning per användare, MFP:er, avdelningar och projekt.

Molnversionen innehåller instrumentpanelsstatistik, t.ex. flest utskrivna och uppladdade sidor per användare och flest utskrivna sidor per enhet. Stöd vid driftskrav och felsökning (loggning, diagnostik och tillfällig åtkomst, om kunden uttryckligen beviljar detta).

Lagring av register som krävs för revision, efterlevnad av lagar eller avtal.

Användning av aggregerad och anonymiserad statistik för att övervaka systemstatus och förbättra produktens funktionalitet.

Inga personuppgifter säljs eller används för marknadsföring av tredje part.

Behandlingskonfigurationer (som definierar attribut som ska läsas, lagringsinställningar, raderingsregler och synlighet på instrumentpanelen) kontrolleras av kundadministratören.



3. Behandlingstyper

Attribut för användarkonton som hämtas från kundkatalogen (Entra ID, Active Directory eller annan LDAP-kompatibel katalog). Den exakta uppsättningen läsattribut (t.ex. fullständigt namn och e-postadress) kan konfigureras och definieras av kundadministratören.

De autentiseringsattribut som används för inloggning och autentisering inkluderar ett fast användarnamn och konfigurerbara attribut, t.ex. e-postadress, PIN-kod och kort-ID.

Order- och transaktionsregister med orderinformation och behandlingsresultat, bokförings- och saldojusteringar samt andra transaktionsmetadata som används för rapportering och fakturering. Användarsaldon (aktuell kredit/pengar) registreras för den lokala programvaruversionen.

Innehåll i utskriftsjobb i kön lagras tillfälligt för publicering; innehåll på e-FOLLOW.cloud lagras krypterat i leverantörmiljön medan innehåll i e-FOLLOW Essential/Professional finns kvar på kundservern.

Inloggnings- och aktivitetsloggar som används för övervakning och visas i administrativa instrumentpaneler (t.ex. inloggningshändelser och mätvärden med högst användning).

Drift- och supportloggar, inklusive standardsystemloggar, kan lagras och hanteras i enlighet med konfigurerade lagrings- och dimensioneringsregler. De får endast delas med leverantören av kunden i supportändamål.

4. Dataåtkomst och release

Kundadministratörer har primär åtkomst till och kontroll över sina data och kan konfigurera vilka katalogattribut som ska läsas och vem som ska kunna se instrumentpaneler och rapporter. Med e-FOLLOW Essential/Professional förblir data på kundens server och är endast tillgängliga för kundens administratörer och de som uttryckligen har behörighet. Kundens behöriga administratörer kan få tillgång till sina data via serviceportalen för e-FOLLOW.cloud. Control Systems driver tjänsten och lagrar kunddata i sin miljö för att tillhandahålla tjänsten.

Control Systems har inte tillgång till kunddata under normal drift. Åtkomst för Control Systems-personal kommer endast att ske i uttryckliga, kundinitierade supportscenarier (t.ex. när loggar tillhandahålls eller fjärråtkomst beviljas) och kommer att vara begränsad och omfattas av det gällande databehandlingsavtalet.

Kunderna kontrollerar vidare överföring av sina data (t.ex. export av rapporter eller integration med andra system). All information som krävs enligt lag kommer att hanteras i enlighet med lagstadgade krav och, där så är möjligt, kommer kunden att underrättas.



5. Datalagring

Autentiseringsdata: Användarnamnet definieras för varje användare. Andra autentiseringsattribut som t.ex. e-post, PIN eller kort-ID sparas i enlighet med kundens konfiguration och kan raderas av kundadministratören. Om en användare tas bort från katalogen kan kundadministratören bestämma om användarkontot också ska tas bort från e-FOLLOW vid nästa synkronisering.

Användning och fakturerings-/rapporteringsdata: Transaktions- och användningsdata (orderhistorik, orderdetaljer, saldobytt, bokföringsunderlag, inloggningsaktivitet) sparas för operativa och rapporteringsändamål. Lagring beror på tillhandahållande och konfiguration: e-FOLLOW.cloud lagrar data i leverantörmiljön. Vid användning av e-FOLLOW Essential/Professional förblir data på kundens server. Kundadministratören kan konfigurera automatisk radering av gamla data (t.ex. radering av dataposter som är äldre än ett år) och permanent radera rapportdata när som helst.

Utskriftsjobb: För e-FOLLOW.cloud lagras utskriftsjobb i kön krypterade i leverantörmiljön tills de frigörs eller raderas enligt den konfigurerade lagringspolicyn.

Utskriftsjobb i e-FOLLOW Essential/Professional förblir i kön på plats på kundens server och följer de lagringsinställningar som kunden har angett. Pausade utskriftsjobb kan raderas automatiskt efter en tid som kunden har ställt in tidigare.

Support- och systemloggar: Loggfiler genereras som standard och lagras i systemet. Loggar raderas endast automatiskt om loggkatalogen överskrider en konfigurerad storleksgräns. Loggfiler eller tillfälliga data som kunden tillhandahåller Control Systems för supportändamål kommer att raderas efter att supportärendet har lösts.

Anteckningar och restriktioner: Inställningar för lagring och radering styrs av kundadministratören. Control Systems kan inte garantera att lokalt lagrade data raderas, såvida inte kundens administratör utför raderingen eller instruerar oss att göra det som en del av en överenskommen process. Data i e-FOLLOW.cloud raderas enligt den konfigurerade lagringspolicyn och avtalsinställningarna.

6. Användarrättigheter

Användarna har rätt att få tillgång till, korrigera eller radera sina personuppgifter. Kundadministratören kontrollerar hur dessa rättigheter implementeras. Control Systems kan endast hjälpa till i supportärenden om kunden uttryckligen har godkänt detta.



7. Data som stöds

Som en del av supportärenden kan kunder tillhandahålla loggfiler eller bevilja tillfällig fjärråtkomst. Loggfiler genereras som standard på kundens system och förblir där så länge loggkatalogen inte överskrider den konfigurerade maximala storleken. De data som överförs till Control Systems för supportändamål kommer endast att användas för att behandla supportförfrågan och raderas efter att ärendet har avslutats.

8. Säkerhetsåtgärder

e-FOLLOW.cloud körs i en Azure Kubernetes-tjänstmiljö. Kommunikationen mellan MFP-appar och tjänsten äger rum via HTTPS och LDAPS. Utskriftsjobb i kön lagras i Azure Storage och krypteras av vår applikation utöver plattformskrypteringen. Nätverksskyddet tillhandahålls av Azure-plattformen. Administratörsåtkomst till kundportaler är som standard operatör + lösenord, men kan konfigureras för att använda Entra ID (inklusive MFA). Endast de Azure-administratörer som utsetts av Control Systems har tillgång till miljön och lagringen i Azure/Kubernetes.

Produktionsmiljön underhålls enligt operativa säkerhetsrutiner (patchar och uppdateringar av Kubernetes-plattformen och dess komponenter, åtkomst med minsta möjliga behörighet för administratörer och säker hantering av inloggningsuppgifter). Tillgången som anställda på Control Systems har till kunddata är begränsad till uttryckligen godkända support- eller underhållsaktiviteter.

9. Uppdateringar och kommunikation

Denna datapolicy kan uppdateras regelbundet för att återspegla förändringar i lagstadgade krav, produktfunktionalitet eller operativa rutiner. Uppdaterade versioner kommer att göras tillgängliga för kunderna före deras ikraftträdandedatum. Kunden ansvarar för att kontrollera den senaste versionen.