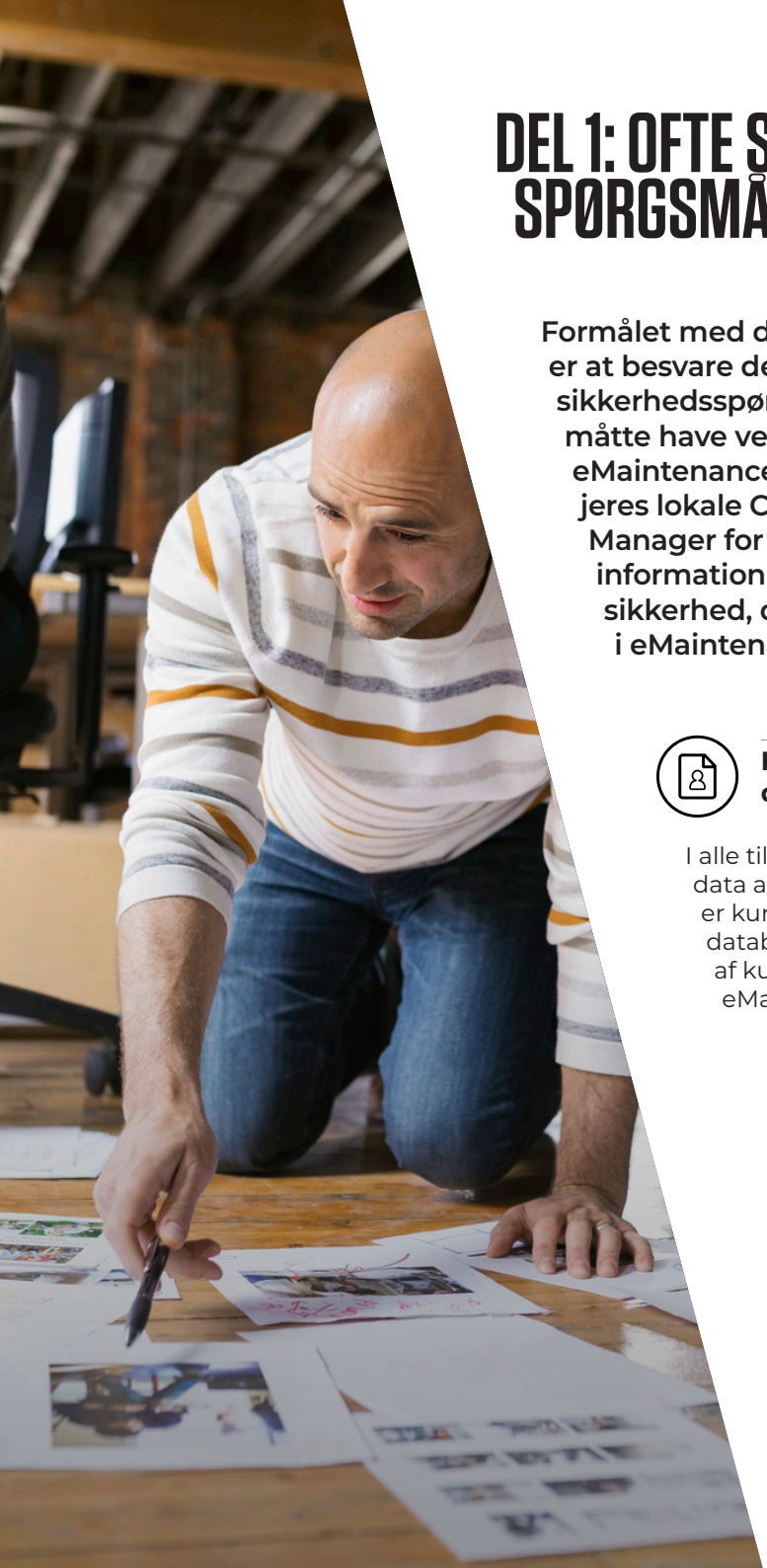
INFORMATIONSSIKKERHED MED CANON eMAINTENANCE

Canons eMaintenance tager sig af håndteringen og administrationen af alle jeres netværkstilsluttede MFP- og SFP-produkter fra Canon, samtidig med at strenge sikkerhedsprotokoller overholdes.



DEL 1: OFTE STILLEDE SPØRGSMÅL

Formålet med dette dokument er at besvare de vigtigste sikkerhedsspørgsmål, I måtte have vedrørende eMaintenance. Kontakt jeres lokale Canon Account Manager for at få yderligere information om den sikkerhed, der er indbygget i eMaintenance.

Hvem ejer vores data?

I alle tilfælde ejes jeres data af jer, og Canon er kun en godkendt databehandler af kundernes eMaintenance-data.

Hvem kan få adgang til vores data?

Canon giver en lagdelt tilgang til regulering af adgang til data, herunder:

- Fysiske adgangskontroller – Kun autoriserede personer, der har tilladelse til fysisk at få adgang til lokaler, bygninger eller rum, hvor personlige data er gemt.
- Systemadgangskontroller – Systemer, der behandler personlige data, kan kun tilgås med godkendelse baseret på brugerroller og tilknyttede tilladelser.
- Dataadgangskontroller – Personer, der er berettiget til at bruge databehandlingssystemer, får kun adgang til de personoplysninger, de har ret til at få adgang til.
- Kontrol af datatransmission – Medmindre det er nødvendigt for levering af services i overensstemmelse med den pågældende aftale, må personlige data ikke læses, kopieres, ændres eller fjernes uden tilladelse under overførslen.
- Datainputstyring – Canon implementerer foranstaltninger, der gør det muligt retrospektivt at undersøge og fastslå, om og af hvem personlige data er blevet indtastet, ændret eller fjernet fra Canons databehandlingssystemer.
- Jobkontrol – Alle Canon-medarbejdere og kontraktmæssige underbehandlere eller andre serviceudbydere er kontraktligt forpligtet til at respektere fortroligheden af alle følsomme oplysninger.
- Dataadskillelseskontroller – Personlige data gemmes og er kun tilgængelige fra den enkelte kundes individuelle eMaintenance-tenant.

Dataadgang styres ved hjælp af følgende foranstaltninger:

- Som en del af Canons sikkerhedspolitik kræver personoplysninger mindst samme beskyttelsesniveau som "fortrolige" oplysninger.
- Adgang til personoplysninger gives på et need-to-know-grundlag. Personalet har adgang til de oplysninger, de skal bruge for at udføre deres opgaver.
- Sikkerhedsforanstaltninger, der beskytter programmer, der behandler personlige data, kontrolleres regelmæssigt. Med henblik herpå udfører Canon interne og eksterne sikkerhedskontroller og penetrationstest på sine IT-systemer.
- Personlige data må ikke læses, kopieres, ændres eller fjernes uden tilladelse i forbindelse med behandling, brug og lagring.

Er vores data krypterede?

Data, der er gemt i AWS-cloudtjenesten, krypteres.

Når data overføres mellem Canon og Canons kunder, udføres dette altid på tværs af sikre krypteringsoverførselsprotokoller.

Personlige data, der kan gemmes, når I bruger Data Backup Service (tilvalg) eller Installation Support Service (tilvalg), f.eks. data fra printerens adressekartotek, krypteres ved hjælp af AES-256.

Hvordan adskilles vores data fra andre kunders data?

Personlige data behandles ved hjælp af følgende adskillelseskontroller:

Canon anvender passende tekniske kontroller for at opnå logisk adskillelse af kundedata.

Hvor det er relevant, sikrer en flerlagsstruktur, at en overordnet tenant har adgang til deres underordnede tenant, men de underordnede kan ikke få adgang til andre tenants på samme niveau eller på et højere niveau (f.eks. de overordnedes niveau).

Hvilke data indsamles af eMaintenance?

Størstedelen af de data, der indsamles og anvendes af eMaintenance, er ikke-personligt identificerbare printerdata såsom kunde, produktnavn, serienummer, placering, IP-adresse, status og alarmer.

Følgende oplysninger indsamles ikke af eMaintenance: Oplysninger om brugerens handlinger, f.eks. brugernavn*, dato/klokkeslæt, dokumentnavn, jobindhold (billeddata/printdata) til KOPIERING, PRINT, SCANNING og AFSENDELSE.

Reviderer Canon sin cloud-sikkerhed?

Canon udfører forskellige audits som indikatorer for implementeringsstatus for informationssikkerhed for de cloud-services, de leverer, for at sikre, at Canon og Canons kunder trygt kan bruge disse services.

For at kontrollere sikkerhedsforanstaltningerne i eMaintenance udføres der jævnligt penetrationstest af en tredjepart.

* Ved brug af Data Backup Service (tilvalg) eller Installation Support Service (tilvalg) kan der indsamles personlige data som f.eks. brugernavn og e-mailadresse, hvis de findes i printerens adressekartotek, men kun med specifik aftale med kunden.

Er eMaintenance-cloudinfrastrukturen sikker?

eMaintenance-tjenesten hostes på AWS-platformen i Frankfurt, Tyskland.

Har eMaintenance nogen certificering i forhold til nogen af de vigtigste sikkerhedsstandarder?

Canon Inc.'s Digital Printing Development Center er certificeret i henhold til den internationale standard ISO/IEC 27001. Den opnåede certificering er relateret til Canon Inc.'s udvikling af overvågningsservicen (herunder eMaintenance Suite) til multifunktionsprintere (MFP'er) og printere.

Ved at opnå ISO/IEC 27001 og ISO/IEC 27017 kan Canon Inc. bekræfte, at sikkerhedsprocesser er blevet tredjepartscertificeret i henhold til en internationalt anerkendt standard.

Denne standard demonstrerer Canon Inc.'s engagement i informationssikkerhed i virksomheden og vores online servicetilbud:

- **Fortrolighed** – Sikre, at oplysningerne kun er tilgængelige for autoriseret personale, der har adgang.
- **Integritet** – Sikre nøjagtigheden og fuldstændigheden af oplysninger og behandlingsmetoder.

- **Tilgængelighed** – Sikre, at autoriserede brugere har adgang til oplysninger, når det er nødvendigt.

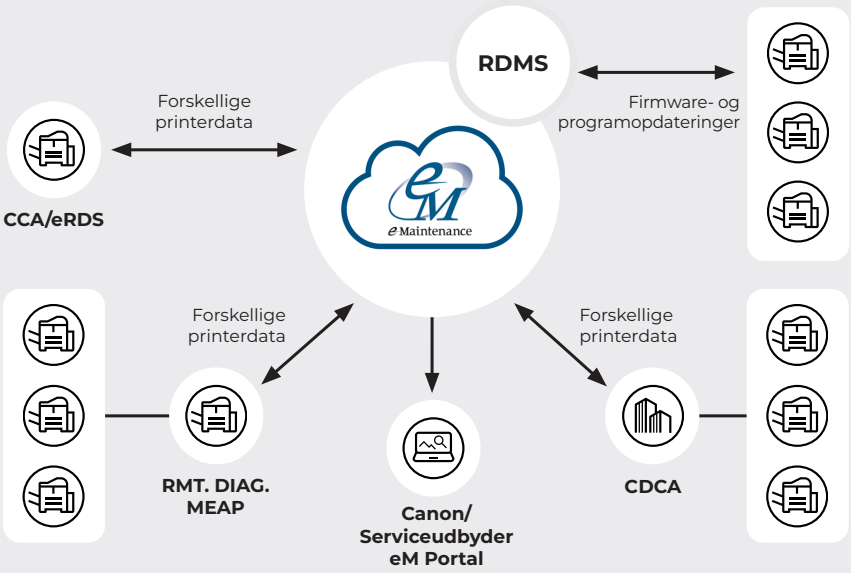
ISO/IEC 27001 kræver regelmæssig gennemgang og betyder, at overvågningsservicens funktioner udvikles og leveres af en sikker organisation, som er blevet bekræftet af tredjepartscertificering i henhold til aftalte internationale standarder.

En del af ISO/IEC 27001 omfatter ISO/IEC 27017, som definerer yderligere sikkerhedskontroller specielt for cloud-serviceudbydere. Den skitserer en ramme for informationssikkerhed for organisationer, der bruger cloud-services.

Canon har valgt at overholde denne adfærdskodeks for kontrol af informationssikkerhed, fordi det gør deres cloud-services mere sikre ved at levere en ensartet og omfattende tilgang til informationssikkerhed.

FORTEGNELSE

CCA – Cloud Connection Agent
CDCA – Canon Data Collection Agent
RMT. DIAG. MEAP – Remote Diagnostics MEAP
eRDS – embedded Remote Diagnostic System
RDMS – Remote Distribution & Management Service



DEL 2: eM INFRASTRUKTURKRAV

eM bruger en række lokale agenter og softwareprogrammer til kommunikation mellem Canon-printere/MFP'er og eM-services. Afhængigt af en række faktorer, f.eks. printertype, opsætning af lokal infrastruktur og servicekrav, kan hver kunde have et eller flere af disse aktiveret.

Mulighederne er som følger:

CCA (Cloud Connection Agent)

CCA er den nyeste enhedsintegrerede agent for eMaintenance, som kører internt på printeren uden behov for at installere en separat dataindsamlingsagent på jeres netværk. Da den kan indsamle en bredere vifte af printerdata, er CCA-tilslutning nødvendig for at drage fordel af alle de seneste (og fremtidige) eMaintenance-funktioner og -services, herunder AI-baseret forebyggende diagnosticering og reparation. CCA kan føjes til eksisterende printere, der kører eRDS.

CDCA (Canon Data Collection Agent)

Dette er en PC-installeret agent til eMaintenance. Denne overvågningssoftware installeres på en lokal pc på kundens netværk.

RMT. DIAG. MEAP (Remote Diagnostics MEAP)

Dette er en enhedsintegreret agentsoftware til eMaintenance ved hjælp af MEAP-platform, som kan bruges til at overvåge værtsenheden og andre Canon-produkter på netværket. Ideel til mindre netværk, der ikke kræver en CDCA-server.

eRDS (embedded Remote Diagnostic Service)

eRDS er en ældre enhedsintegreret agent til eMaintenance. Denne overvågningssoftware kører internt på selve printeren. eRDS sender information om enhedsadministration til eMaintenance-services og kan konfigureres til at modtage firmware- og MEAP-programlicensopdateringer.

RDMS (Remote Distribution & Management Service)

Giver autoriserede Canon-serviceudbydere mulighed for at administrere produkter og licenser til MEAP-programmer og iR-funktioner samt opdatere firmware og MEAP-programlicenser.

Data Backup Service

Denne valgfri service tager en regelmæssig planlagt backup af de indstillinger, der er gemt på den interne lagringsenhed i krypteret form, til clouden. I tilfælde af HDD/SSD/Controller-fejl, der kræver udskiftning, kan datasikkerhedskopieringsservice gendanne dataene til printeren/MFP'en, hvilket reducerer reparationstiden betydeligt.

Påkrævet netværksadgang

For at gøre eMaintenance i stand til at fungere vil kunderne blive bedt om at give adgang til de relevante URL'er, der er tilgængelige via deres netværk for Canon-printere/MFP'er. Kontakt jeres Canon Account Manager for at få en liste over specifikke URL-adresser, der kræves til jeres miljø.

INDIVIDUELLE eMAINTENANCE-FORBINDELSES-URL'er

Canon anbefaler brug af jokertegn i firewall-undtagelser som f.eks.:
*.srv.ygles.com *.amazonaws.com
*.c-cdsknn.net *.ugwdevice.net

CCA	
hbp-ec1l.srv.ygles.com – Port 443	rgt.srv.ygles.com – Port 443
kinesis.eu-central-1.amazonaws.com – Port 443	camapi.srv.ygles.com – Port 443
cognito-identity.eu-central-1.amazonaws.com – Port 443	camapi-ec1.srv.ygles.com – Port 443
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com – Port 443 eller Port 8883	hbpm-ec1l.srv.ygles.com – Port 443
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX og nyere (standardtilstand)	**CDCA v2.XX og nyere (CCA-tilstand)**
rgt.srv.ygles.com	hbp-ec1l.srv.ygles.com
hbpm-ec1l.srv.ygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ec1.srv.ygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ec1.srv.ygles.com	a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com
camapi.srv.ygles.com	rgt.srv.ygles.com
camapis.srv.ygles.com	hbpm-ec1l.srv.ygles.com
mds-ec1.srv.ygles.com	camapi-ec1.srv.ygles.com
gdlp01.c-wss.com	camapis-ec1.srv.ygles.com
www-ec1.srv.ygles.com	camapi.srv.ygles.com
cam-ec1.srv.ygles.com	camapis.srv.ygles.com
	mds-ec1.srv.ygles.com
	gdlp01.c-wss.com
	www-ec1.srv.ygles.com
	cam-ec1.srv.ygles.com
Til RMT. DIAG. MEAP (CCA-tilstand v4.0 og nyere)	**Til RMT. DIAG. MEAP (HTTP-tilstand)**
hbp-ec1l.srv.ygles.com	a01.ugwdevice.net – Port 443
kinesis.eu-central-1.amazonaws.com	b01.ugwdevice.net – Port 443
cognito-identity.eu-central-1.amazonaws.com	
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srv.ygles.com	
hbpm-ec1l.srv.ygles.com	
camapis-ec1.srv.ygles.com	
camapis.srv.ygles.com	
camapi-ec1.srv.ygles.com	
camapi.srv.ygles.com	
mds-ec1.srv.ygles.com	
eRDS	
a01.ugwdevice.net – Port 443	
b01.ugwdevice.net – Port 443	
cnvextdata-an1s.srv.ygles.com – Port 443 er kun påkrævet til fjernbetjent aktivering af CCA på eksisterende printere med eRDS	
Til RDMS	
device.c-cdsknn.net – Port 443	a02.c-cdsknn.net – Port 443
device02.c-cdsknn.net – Port 443	
Til Data Backup Service	
hbp-ec1l.srv.ygles.com – Port 443	b01.ugwdevice.net – Port 443
kinesis.eu-central-1.amazonaws.com – Port 443	cnvextdata-an1s.srv.ygles.com – Port 443
cognito-identity.eu-central-1.amazonaws.com – Port 443	camapi-ec1.srv.ygles.com – Port 443
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com – Port 443 eller Port 8883	camapis-ec1.srv.ygles.com – Port 443
rgt.srv.ygles.com – Port 443	camapi.srv.ygles.com – Port 443
hbpm-ec1l.srv.ygles.com – Port 443	camapis.srv.ygles.com – Port 443
a01.ugwdevice.net – Port 443	dcf-ec1.srv.ygles.com – Port 443

Februar 2025 - V.01

Canon Inc.
canon.com

Canon Europe
canon-europe.com

Danish edition

Canon Danmark
Østmarken 3A
2860 Søborg
Tlf.: 70 15 50 05
canon.dk