



**Canon**

# SECURITATEA INFORMAȚIILOR CU CANON eMAINTENANCE

Canon eMaintenance se ocupă de gestionarea și administrarea tuturor multifuncționalelor și imprimantelor dumneavoastră Canon conectate în rețea, respectând în același timp protocoale stricte de securitate.

# PARTEA 1: ÎNTREBĂRI FRECVENTE

Acest document își propune să răspundă la principalele întrebări legate de securitate pe care le puteți avea referitor la eMaintenance. Pentru informații suplimentare despre securitatea încorporată în eMaintenance, vă rugăm să contactați reprezentantul Canon local.



## Cine deține datele mele?

În toate cazurile, datele dumneavoastră sunt deținute de dumneavoastră. Canon este doar un procesator de date agreat al datelor eMaintenance ale clienților.



## Cine îmi poate accesa datele?

### Canon oferă o abordare pe mai multe niveluri pentru controlul accesului la date, inclusiv:

- **Controale fizice de acces** – numai persoanele autorizate au permisiunea de a accesa fizic spațiile, clădirile sau încăperile în care sunt stocate Date cu caracter personal.
- **Controale de acces la sisteme** – sistemele care prelucrează Date cu caracter personal pot fi accesate numai cu autorizare pe baza rolurilor de utilizator și permisiunilor asociate.
- **Controlul accesului la date** – persoanele care au dreptul să utilizeze sistemele de prelucrare a datelor au acces numai la Datele cu caracter personal pe care au dreptul să le acceseze.
- **Controale de transmitere a datelor** – cu excepția cazului în care este necesar pentru furnizarea de servicii în conformitate cu acordul relevant, Datele cu caracter personal nu trebuie citite, copiate, modificate sau eliminate fără autorizație în timpul transferului.
- **Controale de introducere a datelor** – Canon implementează măsuri prin care se poate examina și stabili retrospectiv dacă și de către cine au fost introduse, modificate sau eliminate Datele cu caracter personal din sistemele Canon de prelucrare a datelor.
- **Controale la locul de muncă** – toți angajații Canon și subcontractanții contractuali sau alți furnizori de servicii sunt obligați prin contract să respecte confidențialitatea tuturor informațiilor sensibile.
- **Controale de separare a datelor** – Datele cu caracter personal sunt stocate și accesibile numai din entitatea găzduită individuală a fiecărui client eMaintenance.

### Accesul la date este controlat utilizând următoarele măsuri:

- Ca parte a Politicii de securitate Canon, Datele cu caracter personal necesită cel puțin același nivel de protecție ca și informațiile „confidențiale”.
- Accesul la Date cu caracter personal se acordă doar celor care trebuie să le cunoască. Personalul are acces la informațiile de care are nevoie pentru a-și îndeplini sarcinile.
- Măsurile de securitate care protejează aplicațiile care prelucrează Date cu caracter personal sunt verificate în mod regulat. În acest scop, Canon efectuează verificări de securitate interne și externe și teste de penetrare asupra sistemelor sale IT.
- Datele cu caracter personal nu trebuie citite, copiate, modificate sau eliminate fără autorizație în cursul prelucrării, utilizării și stocării.



## **Datele mele sunt criptate?**

Datele stocate în serviciul cloud AWS sunt criptate.

Atunci când datele sunt transferate între Canon și clienții săi, acest lucru se realizează întotdeauna folosind protocoalele de transport cu criptare securizată.

Datele cu caracter personal care pot fi stocate folosind Serviciul de backup al datelor sau Serviciul de asistență pentru instalare (disponibile opțional), cum ar fi datele din agenda dispozitivului, sunt criptate utilizând AES-256.



## **Cum sunt separate datele mele de datele altor clienți?**

Datele cu caracter personal sunt prelucrate utilizând următoarele controale de separare:

Canon utilizează controale tehnice adecvate pentru a realiza separarea logică a datelor clienților.

Acolo unde este cazul, o structură ierarhică pe mai multe niveluri asigură accesul unei entități găzduite superioare la entitatea găzduită de nivel inferior, însă nivelurile inferioare nu pot avea acces la alte entități găzduite de la același nivel sau de la un nivel mai înalt (cele superioare).



## **Ce date sunt colectate de către eMaintenance?**

Majoritatea datelor colectate și utilizate de eMaintenance sunt date ale dispozitivului care nu identifică personal utilizatorii, cum ar fi clientul, numele dispozitivului, numărul de serie, locația, adresa IP, starea și alerte.

Următoarele informații nu sunt colectate de eMaintenance: informații legate de operațiile utilizatorului, cum ar fi numele de utilizator\*, data/ora, numele documentului, conținutul lucrării (date de imagine/date de imprimare) pentru COPIERE, IMPRIMARE, SCANARE și TRIMITERE.



## **Își verifică Canon securitatea cloud?**

Canon efectuează diverse audituri ca indicatori ai stării de implementare a securității informațiilor pentru serviciile cloud pe care le furnizează, pentru a se asigura că atât Canon, cât și clienții săi pot utiliza serviciile cu încredere.

Pentru a verifica măsurile de securitate eMaintenance, teste de penetrare sunt efectuate periodic de către o terță parte.

\* Atunci când utilizați Serviciul de backup al datelor sau Serviciul de asistență pentru instalare, disponibile opțional, date cu caracter personal, cum ar fi numele de utilizator și adresa de e-mail, pot fi colectate dacă sunt conținute în agenda dispozitivului, dar numai cu acordul specific al clientului.





## Este infrastructura cloud eMaintenance sigură?

Serviciul eMaintenance este găzduit pe platforma AWS, situată în Frankfurt, Germania.



## Are eMaintenance vre certificate conform unui standard important de securitate?

Centrul de dezvoltare a imprimării digitale Canon Inc. este certificat în conformitate cu standardul internațional ISO/IEC 27001. Certificarea obținută este legată de dezvoltarea de către Canon Inc. a Serviciului de monitorizare (inclusiv eMaintenance Suite) pentru dispozitive multifuncționale (MFD) și imprimante.

Prin îndeplinirea standardelor ISO/IEC 27001 și ISO/IEC 27017, Canon Inc. poate confirma că procesele sale de securitate au fost certificate de o terță parte conform unui standard recunoscut la nivel internațional.

Acest standard demonstrează angajamentul Canon Inc. față de securitatea informațiilor în cadrul companiei și oferta noastră de servicii online:

- **Confidențialitate** – asigurarea accesului la informații numai pentru persoanele autorizate să aibă acces.
- **Integritate** – protejarea acurateței și caracterului complet al informațiilor și metodelor de prelucrare.



- **Disponibilitate** – asigurarea accesului utilizatorilor autorizați la informații atunci când este necesar.

ISO/IEC 27001 necesită o revizuire periodică și înseamnă că funcțiile Serviciului de monitorizare sunt dezvoltate și livrate de o organizație sigură și securizată, care a fost confirmată printr-o certificare terță conform standardelor internaționale convenite.

O parte din ISO/IEC 27001 include ISO/IEC 27017, care definește controale de securitate suplimentare specifice furnizorilor de servicii cloud. Acesta prezintă un cadru de securitate a informațiilor pentru organizațiile care utilizează servicii cloud.

Canon a ales să respecte acest cod de practică pentru controalele de securitate a informațiilor, deoarece oferă mai multă siguranță clienților serviciilor cloud, asigurând o abordare unitară și cuprinzătoare a securității informațiilor.

## LEGENDĂ

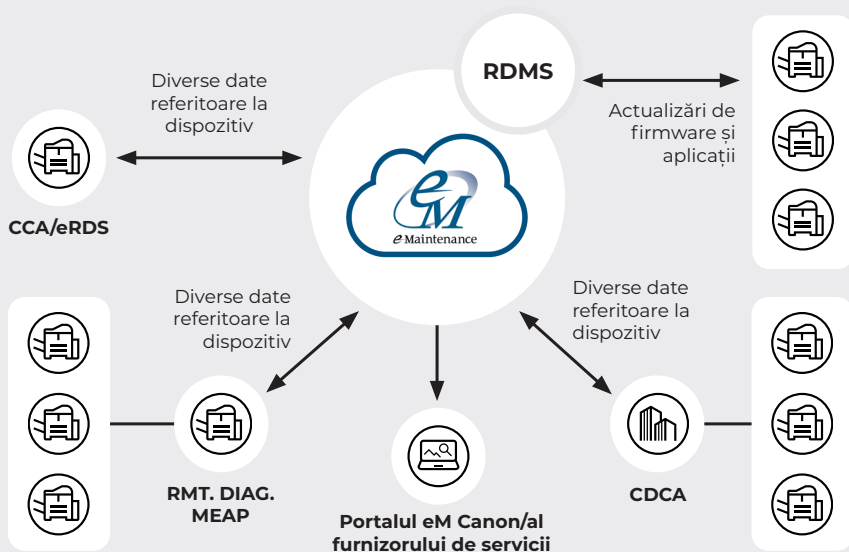
**CCA** – Cloud Connection Agent

**CDCA** – Canon Data Collection Agent

**RMT. DIAG. MEAP** – MEAP pentru diagnosticare de la distanță

**eRDS** – embedded Remote Diagnostic System (sistem de diagnosticare la distanță încorporat)

**RDMS** – Remote Distribution & Management Service (Serviciu de distribuție și gestionare de la distanță)



## PARTEA 2: CERINȚE PRIVIND INFRASTRUCTURA eM

eM utilizează un număr de agenți locali și aplicații software pentru a furniza comunicații între dispozitivele Canon și serviciul eM. În funcție de o serie de factori, cum ar fi tipul de dispozitiv, configurația infrastructurii locale și cerințele de service, fiecare client poate avea unul sau mai multe dintre acestea activate.

**Opțiunile sunt următoarele:**

---

### **CCA (Cloud Connection Agent)**

CCA este cel mai recent agent încorporat pe dispozitiv pentru eMaintenance, care funcționează intern pe dispozitiv, fără a fi nevoie de instalarea unui agent separat de colectare a datelor în rețeaua dumneavoastră. Deoarece poate colecta o gamă mai mare de date despre dispozitiv, conectivitatea CCA este necesară pentru a beneficia de cele mai recente (și de viitoare) funcționalități și servicii eMaintenance, inclusiv diagnosticarea și repararea predictive bazate pe AI. CCA poate fi adăugat la dispozitivele existente care rulează eRDS.

---

### **CDCA (Canon Data Collection Agent)**

Acesta este un agent instalat pe PC pentru eMaintenance. Acest software de monitorizare este instalat pe un PC local din rețeaua clienților.

---

### **RMT. DIAG. MEAP (MEAP pentru diagnosticare de la distanță)**

Acesta este un software de agent încorporat pe dispozitiv pentru eMaintenance ce utilizează platforma MEAP, care poate fi folosită pentru monitorizarea dispozitivului gazdă și a altor dispozitive Canon din rețea. Ideal pentru rețele mai mici care nu necesită un server CDCA.

---

### **eRDS (embedded Remote Diagnostic Service – serviciu de diagnosticare de la distanță încorporat)**

eRDS este un agent mai vechi încorporat pe dispozitiv pentru eMaintenance. Acest software de monitorizare rulează intern pe dispozitivul propriu-zis. eRDS trimite informații de gestionare a dispozitivului către serviciul eMaintenance și poate fi configurat pentru a primi actualizări de firmware și ale licențelor aplicațiilor MEAP.

---

### **RDMS (Remote Distribution & Management Service – Serviciu de distribuție și gestionare de la distanță)**

Permite furnizorilor de servicii Canon autorizați să gestioneze produsele și licențele pentru aplicațiile MEAP și opțiunile iR, precum și să actualizeze firmware-ul și licențele aplicațiilor MEAP.

---

### **Serviciul de backup al datelor**

Acest serviciu opțional efectuează periodic o copie de siguranță programată a setărilor stocate pe dispozitivul de stocare intern într-o formă criptată în cloud. În cazul unei defecțiuni a unității HDD/SSD/controlerului care necesită înlocuire, Serviciul de backup al datelor poate restaura datele pe dispozitiv, reducând semnificativ timpul de reparație.

---

### **Acces la rețea necesar**

Pentru ca eMaintenance să funcționeze, clienților li se va solicita să permită accesul la adresele URL corespunzătoare prin rețeaua lor pentru dispozitivele Canon. Vă rugăm să solicitați reprezentantului Canon lista adreselor URL specifice necesare pentru medii dumneavoastră.

# ADRESE URL INDIVIDUALE DE CONECTARE PENTRU eMAINTENANCE

Canon recomandă utilizarea metacaracterelor în excluziunile de la firewall, cum ar fi:

\*.srv.ygles.com \*amazonaws.com  
\*c-cdsknn.net \*.ugwdevice.net

CCA	
hbp-ecl.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-ecl.srv.ygles.com - Port 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com - Port 443 sau Port 8883	hbpm-ecl.srv.ygles.com - Port 443
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX și versiunile ulterioare (modul standard)	CDCA v2.XX și versiunile ulterioare (modul CCA)
rgt.srv.ygles.com	hbp-ecl.srv.ygles.com
hbpm-ecl.srv.ygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ecl.srv.ygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ecl.srv.ygles.com	a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com
camapi.srv.ygles.com	rgt.srv.ygles.com
camapis.srv.ygles.com	hbpm-ecl.srv.ygles.com
mds-ecl.srv.ygles.com	camapi-ecl.srv.ygles.com
gdlp01.c-wss.com	camapis-ecl.srv.ygles.com
www-ecl.srv.ygles.com	camapi.srv.ygles.com
cam-ecl.srv.ygles.com	camapis.srv.ygles.com
	mds-ecl.srv.ygles.com
	gdlp01.c-wss.com
	www-ecl.srv.ygles.com
	cam-ecl.srv.ygles.com
Pentru RMT, DIAG, MEAP (modul CCA v4.0 și versiunile ulterioare)	Pentru RMT, DIAG, MEAP (modul HTTP)
hbp-ecl.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	
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srv.ygles.com	
hbpm-ecl.srv.ygles.com	
camapis-ecl.srv.ygles.com	
camapis.srv.ygles.com	
camapi-ecl.srv.ygles.com	
camapi.srv.ygles.com	
mds-ecl.srv.ygles.com	
eRDS	
a01.ugwdevice.net - Port 443	
b01.ugwdevice.net - Port 443	
cnvextdata-anls.srv.ygles.com - Port 443 este necesar numai pentru activarea de la distanță a CCA pe dispozitivele existente cu eRDS	
Pentru RDMS	
device.c-cdsknn.net - Port 443	a02.c-cdsknn.net - Port 443
device02.c-cdsknn.net - Port 443	
Pentru Serviciul de backup al datelor	
hbp-ecl.srv.ygles.com - Port 443	b01.ugwdevice.net - Port 443
kinesis.eu-central-1.amazonaws.com - Port 443	cnvextdata-anls.srv.ygles.com - Port 443
cognito-identity.eu-central-1.amazonaws.com - Port 443	camapi-ecl.srv.ygles.com - Port 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com - Port 443 sau Port 8883	camapis-ecl.srv.ygles.com - Port 443
rgt.srv.ygles.com - Port 443	camapi.srv.ygles.com - Port 443
hbpm-ecl.srv.ygles.com - Port 443	camapis.srv.ygles.com - Port 443
a01.ugwdevice.net - Port 443	dcf-ecl.srv.ygles.com - Port 443

Februarie 2025 - V.01



Canon Inc.  
canon.com

Canon Europe  
canon-europe.com

Romanian edition  
© Canon Europa N.V. 2025

Canon Romania  
Clădirea Euro Tower, Etaj 16,  
Strada Dinu Vintila, nr. 11, sector 2,  
Cod postal 021101, Bucuresti, Romania  
Tel: +40 21 318 38 56  
www.canon.ro