



Canon

BEZPIECZEŃSTWO INFORMACJI Z CANON eMAINTENANCE

Usługa eMaintenance firmy Canon obejmuje zarządzanie i administrowanie wszystkimi sieciowymi urządzeniami wielofunkcyjnymi i drukarkami jednofunkcyjnymi firmy Canon z zachowaniem rygorystycznych protokołów bezpieczeństwa.

CZĘŚĆ 1. CZĘSTO ZADAWANE PYTANIA

Ten dokument ma zapewnić odpowiedzi na główne pytania dotyczące bezpieczeństwa, które mogą pojawić się w związku z korzystaniem z usługi eMaintenance (eM). Aby uzyskać więcej informacji na temat zabezpieczeń wbudowanych w usługę eMaintenance, należy skontaktować się z lokalnym przedstawicielem firmy Canon.



Kto jest właścicielem moich danych?

We wszystkich przypadkach, w których dane są własnością użytkownika, firma Canon jest tylko zatwierdzonym podmiotem przetwarzającym dane eMaintenance klientów.



Kto może uzyskać dostęp do moich danych?

Firma Canon stosuje wielowarstwowe podejście do kontroli dostępu do danych, w tym:

- **Fizyczne środki kontroli dostępu** – dostęp fizyczny do obiektów, budynków lub pomieszczeń, w których przechowywane są dane osobowe, mają wyłącznie upoważnione osoby.
- **Środki kontroli dostępu do systemów** – dostęp do systemów przetwarzających dane osobowe jest możliwy wyłącznie po uzyskaniu autoryzacji opartej na rolach użytkownika i powiązanych uprawnieniach.
- **Środki kontroli dostępu do danych** – osoby uprawnione do korzystania z systemów przetwarzania danych uzyskują dostęp tylko do tych danych osobowych, do których mają przyznane prawo dostępu.
- **Środki kontroli transmisji danych** – z wyjątkiem przypadków, gdy jest to konieczne do świadczenia usług zgodnie z odpowiednią umową, dane osobowe podczas przesyłania nie mogą być odczytywane, kopiowane, modyfikowane ani usuwane bez upoważnienia.
- **Środki kontroli wprowadzania danych** – firma Canon wprowadza środki umożliwiające retrospektywne badanie i ustalanie, czy i przez kogo dane osobowe zostały wprowadzone, zmodyfikowane lub usunięte z systemów przetwarzania danych firmy Canon.

- **Środki kontroli pracy** – wszyscy pracownicy firmy Canon oraz podwykonawcy przetwarzający dane na podstawie umowy lub inni dostawcy usług są zobowiązani umownie do przestrzegania poufności wszystkich informacji wrażliwych.
- **Środki kontroli separacji danych** – dane osobowe są przechowywane i dostępne tylko z poziomu indywidualnego konta dzierżawcy eMaintenance.

Dostęp do danych jest kontrolowany przy użyciu następujących środków:

- W ramach zasad bezpieczeństwa firmy Canon dane osobowe wymagają co najmniej takiego samego poziomu ochrony jak informacje „poufne”.
- Dostęp do danych osobowych jest przyznawany w oparciu o zasadę „potrzeby znajomości danych”. Pracownicy mają dostęp do informacji, których potrzebują do wypełnienia swoich obowiązków.
- Środki bezpieczeństwa chroniące aplikacje przetwarzające dane osobowe są regularnie sprawdzane. W tym celu firma Canon przeprowadza wewnętrzne i zewnętrzne kontrole bezpieczeństwa oraz testy penetracyjne swoich systemów IT.
- Dane osobowe nie mogą być odczytywane, kopiowane, modyfikowane ani usuwane bez upoważnienia w trakcie przetwarzania, użytkowania i przechowywania.



Czy moje dane są szyfrowane?

Dane przechowywane w usłudze chmury AWS są szyfrowane.

Gdy dane są przesyłane między firmą Canon a jej klientami, odbywa się to zawsze za pomocą bezpiecznych protokołów transportowych z szyfrowaniem.

Dane osobowe, które mogą być przechowywane podczas korzystania z opcjonalnej usługi Zapasowej Kopii Danych (Data Backup Service / DBS) lub Usługi Wsparcia Instalacji (InstallationSupport Service / ISS), takie jak dane z książki adresowej urządzenia, są szyfrowane za pomocą AES-256.



W jaki sposób moje dane są oddzielone od danych innych klientów?

Dane osobowe są przetwarzane przy użyciu następujących środków kontroli separacji:

Firma Canon stosuje odpowiednie techniczne środki kontroli w celu uzyskania logicznej separacji danych klientów.

W stosownych przypadkach wielowarstwowa struktura drzewa zapewnia dzierżawie nadrzędnej dostęp do dzierżaw podrzędnych, jednak dzierżawy podrzędne nie mogą uzyskać dostępu do innych dzierżaw na tym samym lub wyższym poziomie (np. do dzierżaw nadrzędnych).



Jakie dane są gromadzone przez usługę eMaintenance?

Większość danych gromadzonych i używanych przez eMaintenance nie umożliwia identyfikacji użytkownika. Są to takie dane, jak klient, nazwa urządzenia, numer seryjny, lokalizacja, adres IP, stan i alerty.

Następujące informacje nie są gromadzone przez usługę eMaintenance: informacje związane z działaniem użytkownika, takie jak nazwa użytkownika*, data/godzina, nazwa dokumentu, zawartość zadania (dane obrazu / dane wydruku), w operacjach KOPIOWANIA, DRUKOWANIA, SKANOWANIA i WYSYŁANIA.



Czy Canon sprawdza swoje zabezpieczenia rozwiązań w chmurze?

Canon przeprowadza różne audyty jako wskaźniki stanu wdrożenia zabezpieczeń informacji w świadczonych usługach przetwarzania w chmurze, aby firma i jej klienci mogli bezpiecznie korzystać z usług.

W celu weryfikacji środków bezpieczeństwa eMaintenance regularnie przeprowadzane są testy penetracyjne przez podmiot zewnętrzny.



* W przypadku korzystania z opcjonalnych usług DBS oraz ISS, dane osobowe, takie jak nazwa użytkownika i adres e-mail, mogą być gromadzone, jeśli są zawarte w książce adresowej urządzenia, ale tylko za wyraźną zgodą klienta.



Czy infrastruktura chmury dla usługi eMaintenance jest bezpieczna?

Usługa eMaintenance jest hostowana na platformie AWS zlokalizowanej we Frankfurcie w Niemczech.



Czy usługa eMaintenance ma certyfikaty zgodności z którymkolwiek spośród głównych standardów bezpieczeństwa?

Centrum rozwoju druku cyfrowego firmy Canon Inc. ma certyfikat zgodności z międzynarodową normą ISO/IEC 27001. Uzyskany certyfikat jest związany z opracowaniem przez firmę Canon Inc. usługi monitorowania (w tym pakietu eMaintenance Suite) dla urządzeń wielofunkcyjnych (MFD) i drukarek.

Dzięki zgodności z normami ISO/IEC 27001 i ISO/IEC 27017 firma Canon Inc. może potwierdzić, że jej procesy bezpieczeństwa są certyfikowane przez podmiot zewnętrzny pod kątem zgodności z międzynarodową normą.

Ten standard pokazuje zaangażowanie firmy Canon Inc. w ochronę informacji w firmie oraz w naszej ofercie usług online:

- **Poufność** – dbałość o to, aby informacje były dostępne tylko dla upoważnionych osób.
- **Integralność** – zagwarantowanie dokładności i kompletności informacji oraz metod przetwarzania.
- **Dostępność** – zapewnienie stałego dostępu do informacji autoryzowanym użytkownikom.



Norma ISO/IEC 27001 wymaga regularnego przeglądu i stosowania środków zapewniających, że funkcje usługi monitorowania są opracowywane i dostarczane przez bezpieczną organizację, która uzyskała od podmiotu zewnętrznego certyfikat zgodności z normami międzynarodowymi.

Część normy ISO/IEC 27001 obejmuje normę ISO/IEC 27017, która określa dodatkowe środki kontroli bezpieczeństwa stosowane przez poszczególnych dostawców usług w chmurze. Przedstawia ona ramy bezpieczeństwa informacji dla organizacji korzystających z usług w chmurze.

Firma Canon zdecydowała się stosować się do tego kodeksu postępowania w zakresie środków kontroli bezpieczeństwa informacji, ponieważ zapewnia on bezpieczeństwo jej klientom korzystającym z usług w chmurze, umożliwiając spójne i kompleksowe podejście do bezpieczeństwa informacji.

KLUCZ

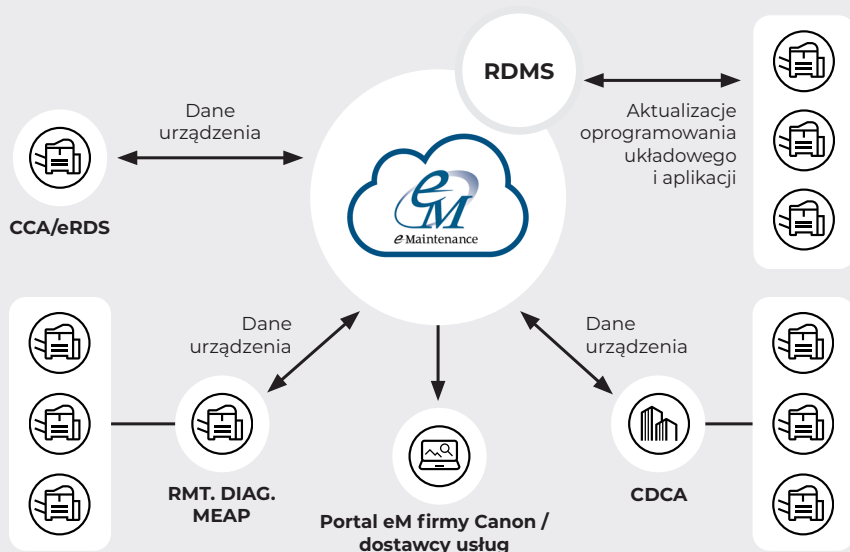
CCA – Cloud Connection Agent

CDCA – Canon Data Collection Agent

RMT, DIAG, MEAP – Remote Diagnostics MEAP

eRDS – embedded Remote Diagnostic System

RDMS – Remote Distribution & Management Service



CZĘŚĆ 2. WYMAGANIA DOTYCZĄCE INFRASTRUKTURY eM

Usługa eM korzysta z kilku lokalnych agentów i aplikacji, aby zapewnić komunikację między urządzeniami Canon a usługą eM. W zależności od takich czynników jak typ urządzenia, konfiguracja lokalnej infrastruktury i wymagania serwisowe każdy klient może mieć różne opcje (jedną lub kilka).

Dostępne są następujące opcje:

CCA (Cloud Connection Agent)

CCA to najnowszy, wbudowany w urządzenie agent eMaintenance, który działa wewnętrznie na urządzeniu, więc nie trzeba instalować oddzielnego agenta gromadzenia danych. Ponieważ może on gromadzić szerszy zakres danych urządzenia, łączność CCA jest niezbędna do korzystania ze wszystkich najnowszych (i przyszłych) funkcji i usług eMaintenance, w tym diagnostyki predykcyjnej i naprawy opartej na AI. CCA można dodać do istniejących urządzeń z eRDS.

CDCA (Canon Data Collection Agent)

Jest to agent eMaintenance zainstalowany na komputerze. To oprogramowanie monitorujące jest instalowane na lokalnym komputerze w sieci klienta.

RMT. DIAG. MEAP (Remote Diagnostics MEAP)

Jest to wbudowane w urządzenie oprogramowanie agenta eMaintenance korzystające z platformy MEAP, które może być używane do monitorowania urządzenia głównego i innych urządzeń firmy Canon w sieci. Jest ono idealne do mniejszych sieci, które nie wymagają serwera CDCA.

eRDS (embedded Remote Diagnostic Service)

eRDS jest starszym, wbudowanym agentem do eMaintenance. To oprogramowanie monitorujące działa wewnętrznie na samym urządzeniu. System eRDS wysyła informacje o zarządzaniu urządzeniami do usługi eMaintenance i może być skonfigurowany do odbierania aktualizacji oprogramowania układowego i licencji aplikacji MEAP.

RDMS (Remote Distribution & Management Service)

Umożliwia autoryzowanym dostawcom usług firmy Canon zarządzanie produktami i licencjami na aplikacje MEAP i opcje IR, a także aktualizowanie oprogramowania układowego i licencji aplikacji MEAP.

DBS (Data Backup Service)

Ta opcjonalna usługa regularnie tworzy według harmonogramu kopię zapasową ustawień przechowywanych w pamięci masowej urządzenia w postaci zaszyfrowanej w chmurze. W przypadku awarii dysku HDD/SSD lub kontrolera i konieczności jego wymiany usługa tworzenia kopii zapasowych danych może przywrócić dane do urządzenia, znacznie skracając czas naprawy.

Wymagany dostęp do sieci

Aby usługa eMaintenance mogła działać, klienci są proszeni o udostępnienie w sieci odpowiednich adresów URL na potrzeby urządzeń firmy Canon. Aby uzyskać listę adresów URL wymaganych w danym środowisku, należy skontaktować się z przedstawicielem firmy Canon.

ADRESY URL POSZCZEGÓLNYCH POŁĄCZEŃ eMAINTENANCE

Firma Canon zaleca stosowanie symboli wieloznacznych w wyjątkach zapory, na przykład:
*.srvygles.com *.amazonaws.com
*.c-cdsknn.net *.ugwdevice.net

CCA	
hbp-ec1.srvygles.com – port 443	rgt.srvygles.com – port 443
kinesis.eu-central-1.amazonaws.com – port 443	camapi.srvygles.com – port 443
cognito-identity.eu-central-1.amazonaws.com – port 443	camapi-ec1.srvygles.com – port 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com – port 443 lub 8883	hbp-ec1.srvygles.com – port 443
CDCA wersja 1.XX	
b01.ugwdevice.net	
CDCA wersja 2.XX lub nowsza (tryb standardowy)	CDCA wersja 2.XX lub nowsza (tryb CCA)
rgt.srvygles.com	hbp-ec1.srvygles.com
hbp-ec1.srvygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ec1.srvygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ec1.srvygles.com	a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com
camapi.srvygles.com	rgt.srvygles.com
camapis.srvygles.com	hbp-ec1.srvygles.com
mds-ec1.srvygles.com	camapi-ec1.srvygles.com
gdlp01.c-wss.com	camapis-ec1.srvygles.com
www-ec1.srvygles.com	camapi.srvygles.com
cam-ec1.srvygles.com	camapis.srvygles.com
	mds-ec1.srvygles.com
	gdlp01.c-wss.com
	www-ec1.srvygles.com
	cam-ec1.srvygles.com
Dla RMT, DIAG, MEAP (tryb CCA w wersji 4.0 lub nowszej)	Dla RMT, DIAG, MEAP (tryb HTTP)
hbp-ec1.srvygles.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.srvygles.com	
hbp-ec1.srvygles.com	
camapis-ec1.srvygles.com	
camapis.srvygles.com	
camapi-ec1.srvygles.com	
camapi.srvygles.com	
mds-ec1.srvygles.com	
eRDS	
a01.ugwdevice.net – port 243	
b01.ugwdevice.net – port 443	
cnvextdata-anls.srvygles.com – port 443 jest wymagany tylko do zdalnej aktywacji CCA na istniejących urządzeniach z eRDS	
Dla RDMS	
device.c-cdsknn.net – port 443	a02.c-cdsknn.net – port 443
device02.c-cdsknn.net – port 443	
Dla usługi Data Backup Service	
hbp-ec1.srvygles.com – port 443	b01.ugwdevice.net – port 443
kinesis.eu-central-1.amazonaws.com – port 443	cnvextdata-anls.srvygles.com – port 443
cognito-identity.eu-central-1.amazonaws.com – port 443	camapi-ec1.srvygles.com – port 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com – port 443 lub 8883	camapis-ec1.srvygles.com – port 443
rgt.srvygles.com – port 443	camapi.srvygles.com – port 443
hbp-ec1.srvygles.com – port 443	camapis.srvygles.com – port 443
a01.ugwdevice.net – port 443	dcf-ec1.srvygles.com – port 443

Luty 2025 – wersja 01



Canon Inc.
canon.com

Canon Europe
canon-europe.com

Polish edition
© Canon Europa N.V. 2025

Canon Polska Sp. z o.o.
ul. Gottlieba Daimlera 2
02-460 Warszawa
tel. +48 22 430 60 00
canon.pl