

# HPE Aruba Networking Central

## Aneks II: Opis przetwarzania

1.	Opis przetwarzania	HPE Aruba Networking Central zapewnia nowoczesne, natywne dla chmury operacje sieciowe oraz zabezpieczenie dla przewodowych, opartych na Wi-Fi i SD-WAN sieci. HPE Aruba Networking Central poprawia tradycyjne zarządzanie za pomocą zintegrowanej, opartej na AI sieci oraz informacji od użytkownika, a także profilowania urządzenia IoT pod kątem bezpiecznego, ujednoliconego zarządzania i kontroli.
2.	Typ przetwarzanych danych osobowych	Dane osobowe gromadzone w ramach zarządzania siecią i powiązanych aplikacjami obejmują następujące informacje: a. Adres MAC urządzenia b. Adres IP urządzenia c. System operacyjny urządzenia d. Nazwa hosta urządzenia e. Nazwa użytkownika f. E-mail (w razie samodzielnej rejestracji gościa) g. Telefon (w razie samodzielnej rejestracji gościa) h. Identyfikator z mediów społecznościowych (w razie samodzielnej rejestracji gościa) i. Wyświetlana nazwa / Członkostwo w grupie / Tytuł (w razie wykorzystania uwierzytelniania za pośrednictwem chmury)
3.	Kategorie przetwarzanych danych osobowych	Klient Administratora danych, użytkownik końcowy, pracownik, wykonawca, pracownik tymczasowy.
4.	Okres przetwarzania	Informacje są gromadzone i przechowywane przez produkt w minimalnym zakresie potrzebnym do zapewniania bezpiecznego dostępu do portalu i niezbędnym do działania jego funkcji. Wszystkie dzienniki sesji dotyczące użytkownika będą automatycznie usuwane po 90 dniach.
5.	Środki techniczne i organizacyjne	Podmiot przetwarzający ma obowiązek utrzymywać program bezpieczeństwa informacji i bezpieczeństwa fizycznego do celów ochrony danych osobowych Administratora danych, jak wyszczególniono w Aneksie III poniżej.

# Aneks III: Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne do celów zabezpieczenia danych

## 1. Zabezpieczenia produktów:

- a. **Ochrona fizyczna:** HPE Aruba Networking Central jest rozwiązaniem hostowanym na powszechnie wykorzystywanych platformach IaaS – Amazon Web Services (AWS) oraz Microsoft Azure, które oferują najbardziej kompleksowe zabezpieczenia i funkcje zapewniania zgodności. Wdrożone przez AWS/Azure środki bezpieczeństwa obejmują wszystkie kluczowe obszary, w tym warstwy obwodu, infrastruktury, danych i środowiska.
- b. **Zabezpieczenia sieciowe:** Zabezpieczenia sieciowe podmiotu przetwarzającego zapewniają bezpieczeństwo sieci fizycznej i wirtualnej, w której rezydują aplikacja oraz dane. Wykorzystujemy usługi i narzędzia oferowane przez dostawcę usług IaaS oraz pewne rozwiązania innych producentów, aby zapewnić najwyższy możliwy poziom ochrony środowiska produkcyjnego przed zagrożeniami zewnętrznymi i wewnętrznymi lukami w zabezpieczeniach. Podmiot przetwarzający obsługuje oddzielne instancje środowiska wewnętrznego i produkcyjnego. Środowisko wewnętrzne przeznaczone jest do rozwijania i testowania, podczas gdy środowisko produkcyjne jest zarezerwowane wyłącznie dla naszych klientów (Administratora danych). Fizyczna i logiczna separacja naszego środowiska produkcyjnego od innych działających instancji umożliwia nam zapewnienie klientom (Administratorowi danych) najwyższej jakości wdrożeń oprogramowania i pomaga ograniczyć rezydowanie danych do jednego środowiska.
- c. **Architektura aplikacji i bezpieczeństwo:** Cały ruch, który odbywa się pomiędzy aplikacją Central oraz światem zewnętrznym, jest realizowany za pomocą standardu HTTPS opartego na SSL. Wszelki przepływający ruch jest szyfrowany z wykorzystaniem technologii szyfrowania AES. Różne poziomy aplikacji, takie jak sieć, aplikacja i baza danych, zostały opracowane z myślą o działaniu w ramach struktury z listą dozwolonych. Pomiędzy poziomami dozwolone są jedynie niezbędne i wymagane ścieżki komunikacyjne. Każda instancja wewnątrz poziomu jest chroniona przez reguły zapory ogniowej, aby zapobiegać nieautoryzowanym lub złośliwym próbom uzyskania dostępu.
- d. **Bezpieczeństwo danych:** Cała wymiana danych pomiędzy aplikacją i urządzeniami oraz użytkownikami odbywa się za pomocą standardu HTTPS. Dane w stanie spoczynku są szyfrowane i przechowywane. Kopie zapasowe danych są tworzone regularnie, a dane z kopii zapasowych są przechowywane w sposób nadmiarowy. Z perspektywy organizacyjnej dysponujemy zespołem DevOps, który zarządza kwestiami bezpieczeństwa i kwestiami operacyjnymi dotyczącymi aplikacji.
- e. **Dostępność geograficzna:** Rozwiązanie HPE Aruba Networking Central jest dostępne w wielu lokalizacjach na całym świecie, umożliwiając Administratorowi danych wybór regionu, w którym ma zostać utworzone konto. Wpływ na tę decyzję ma wiele czynników. Przykładowo, organizacja może wymagać, aby wszystkie dane były przechowywane w danym regionie lub narzucić ograniczenia regulacyjne na sposób przetwarzania i przechowywania danych.

Rozwiązanie HPE Aruba Networking Central jest wdrażane w klastrach w wybranych Amazon Web Services (AWS) oraz centrach danych Microsoft Azure przy pomocy dostawców usług chmury zapewniających infrastrukturę obliczeniową i pamięci masowej. Poniższa tabela zapewnia szczegółową listę klastrów HPE Aruba Networking Central oraz obsługujących je regionów:

HPE Aruba Networking Klaster centralny	Region AWS (Miasto, w którym zlokalizowany jest klaster)	Adres url do rejestracji
US-1	Amerykański Zachód (Oregon), us-west-2	<a href="https://portal.central.arubanetworks.com/signup">portal.central.arubanetworks.com/signup</a>
US-2	Amerykański Zachód (Oregon), us-west-2	<a href="https://portal-prod2.central.arubanetworks.com/signup">portal-prod2.central.arubanetworks.com/signup</a> or <a href="https://console.greenlake.hpe.com">console.greenlake.hpe.com</a>
S-West-4	Amerykański Zachód (Oregon), us-west-2	<a href="https://portal-uswest4.central.arubanetworks.com/signup">portal-uswest4.central.arubanetworks.com/signup</a>
S-West-5	Amerykański Zachód (Oregon), us-west-2	<a href="https://common.cloud.hpe.com">common.cloud.hpe.com</a>
China-1	Chiny (Pekin), cn-north-1	<a href="https://portal.central.arubanetworks.com.cn/signup">portal.central.arubanetworks.com.cn/signup</a>
EU-1	UE (Frankfurt), eu-central-1	<a href="https://portal-eu.central.arubanetworks.com/signup">portal-eu.central.arubanetworks.com/signup</a>
EU-Central2	UE (Frankfurt), eu-central-1	<a href="https://common.cloud.hpe.com">common.cloud.hpe.com</a>
EU-Central3	UE (Frankfurt), eu-central-1	<a href="https://console.greenlake.hpe.com">console.greenlake.hpe.com</a>
Canada-1	Kanada (Centralna), ca-central-1	<a href="https://portal-ca.central.arubanetworks.com/signup">portal-ca.central.arubanetworks.com/signup</a>
APAC-1	Azja i Pacyfik (Mumbaj), ap-south-1	<a href="https://portal-apac.central.arubanetworks.com/signup">portal-apac.central.arubanetworks.com/signup</a>
APAC-East1	Azja i Pacyfik (Tokio), ap-northeast-1	<a href="https://portal-apaceast.central.arubanetworks.com/signup">portal-apaceast.central.arubanetworks.com/ signup</a>
APAC-South1	Azja i Pacyfik (Sydney), ap-southeast-2	<a href="https://console.greenlake.hpe.com">console.greenlake.hpe.com</a>
HPE Aruba Networking Klaster centralny	Region AWS (Miasto, w którym zlokalizowany jest klaster)	Adres url do rejestracji
UAE North1	ZEA North (Dubaj)	<a href="https://common.cloud.hpe.com">common.cloud.hpe.com</a>

Wszelki aktywność na urządzeniach przypisanych do Administratora danych kończy się w wybranym klastrze, włączając w to statystyki sieciowe i dane telemetryczne wypychane poprzez połączenia HTTPS. Dane konfiguracyjne dla wszystkich kont Administratora danych są również gromadzone w wybranym klastrze.

Wszystkie dane (włączając w to dane osobowe) odpowiadające urządzeniom sieciowym (tj. punktom dostępu, przełącznikom, bramkom), urządzeniom Administratora danych oraz inne dane użytkownika są przechowywane w bazach danych w tym samym klastrze. Wszelkie dodatkowe przetwarzanie, które może być wymagane, jest również przeprowadzane w instancjach obliczeniowych w ramach tego samego klastra lub w innym miejscu, zgodnie z DPSA dla usług produktu HPE Aruba Networking.

## — Środki bezpieczeństwa:

- Podmiot przetwarzający ma obowiązek utrzymywać program bezpieczeństwa informacji i bezpieczeństwa fizycznego do celów ochrony danych osobowych Administratora danych („Program bezpieczeństwa podmiotu przetwarzającego”):
  - Infrastruktura Podmiotu przetwarzającego obejmuje rozsądne aktualne wersje oprogramowania systemu bezpieczeństwa, które może obejmować zaporę firewall, ochronę antywirusową oraz aktualne łatki i definicje wirusów. Podmiot przetwarzający utrzymuje dzienniki zdarzeń dotyczących infrastruktury, w tym systemów wykrywania włamań w celu monitorowania, wykrywania i raportowania wzorców niewłaściwego użycia, podejrzanych działań, nieautoryzowanych użytkowników i innych zagrożeń w zakresie bezpieczeństwa.
  - Pracownicy i podwykonawcy są przeszkoleni w zakresie polityki prywatności i bezpieczeństwa Podmiotu przetwarzającego i są świadomi swoich obowiązków w zakresie praktyk dotyczących prywatności i bezpieczeństwa. Pracownicy i podwykonawcy Podmiotu przetwarzającego są umownie zobowiązani do zachowania poufności danych osobowych Administratora danych i przestrzegania obowiązujących polityk, standardów lub wymogów Podmiotu przetwarzającego w odniesieniu do przetwarzania danych osobowych Administratora. Nieprzestrzeganie tych polityk, standardów lub wymogów będzie przedmiotem dochodzenia, które może skutkować podjęciem działań dyscyplinarnych, łącznie z rozwiązaniem stosunku pracy lub zaangażowania przez Podmiot przetwarzający.
- Jeśli Administrator danych wejdzie w posiadanie informacji o incydencie związanym z naruszeniem danych, który ma wpływ na usługi, niezwłocznie powiadomi o tym Podmiot przetwarzający i poinformuje Podmiot przetwarzający o zakresie naruszenia danych osobowych. Powiadomienie należy dostarczyć do Centrum operacji bezpieczeństwa podmiotu przetwarzającego za pośrednictwem wiadomości e-mail wysłanej na adres [security@hpe.com](mailto:security@hpe.com).

Odwiedź [HPE.com](https://www.hpe.com)

## [Porozmawiaj teraz na czacie](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. Niniejsze informacje mogą ulec zmianie bez powiadomienia. Jedyne gwarancje, jakich udziela Hewlett Packard Enterprise na swoje produkty i usługi, są określone w wyraźnych oświadczeniach gwarancyjnych dostarczanych wraz z takimi produktami i usługami. Żadne informacje przedstawione w niniejszym dokumencie nie powinny być interpretowane jako dodatkowa gwarancja. Hewlett Packard Enterprise nie ponosi odpowiedzialności za ewentualne błędy techniczne lub redakcyjne bądź pominięcia w niniejszym dokumencie.

Azure i Microsoft są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach. Wszystkie znaki towarowe innych firm należą do ich właścicieli.

a50009439PLE, wer. 3

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

