

OKTAWAVE A KOMUNIKAT CHMUROWY KNF

W DOKUMENCIE:

[O komunikacie KNF](#)

[ZGODNOŚĆ OKTAWAVE Z KOMUNIKATEM KNF](#)

[AUDYTY MIĘDZYNARODOWYCH INSTYTUCJI CERTYFIKUJĄCYCH](#)

FAQ:

- [JAK W PRAKTYCE MAM WDROŻYĆ KOMUNIKAT KNF \(STEP BY STEP\)?](#)
- [CZY OKTAWAVE ZAPEWNI MI WSPARCIE ADMINISTRACYJNE WŁASNYCH ZESPOŁÓW?](#)
- [CZY CHMURA OKTAWAVE ZLOKALIZOWANA JEST W CAŁOŚCI W POLSCE?](#)

1. O KOMUNIKACIE KNF

Branża finansowa w Polsce od stycznia 2020 r. posiada mapę drogową dla wdrażania modelu chmurowego w postaci [Komunikatu Urzędu Komisji Nadzoru Finansowego dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej \(Komunikat KNF\)](#).

Sektor finansowy podlega szczególnym regulacjom i nie może zdecydować się na skorzystanie z jakiegokolwiek chmury, jak każdy inny podmiot. Bank czy ubezpieczyciel musi zadbać, aby dostawca takich usług spełniał restrykcyjne wymogi formalne i techniczne. Komunikat KNF wyjaśnia o jakie wymogi w praktyce chodzi.

2. ZGODNOŚĆ OKTAWAVE Z KOMUNIKATEM KNF

Chmura Oktawave odpowiada rygorystycznym wymogom Komunikatu KNF.

Aby pomóc Ci wdrożyć i korzystać z rozwiązań opartych o chmurę Oktawave w zgodzie z Komunikatem KNF przygotowaliśmy dedykowaną w tym celu matrycę:

[Matryca zgodności chmury Oktawave z Komunikatem KNF](#)

W przypadku podmiotów objętych nadzorem bankowym matryca stanowi jednocześnie udokumentowanie spełniania przez Oktawave wymagań dostawcy usług chmury obliczeniowej zgodnie ze [Standardem wdrożenia usługi chmury obliczeniowej Związku Banków Polskich](#).

3. AUDYTY MIĘDZYNARODOWYCH INSTYTUCJI CERTYFIKUJĄCYCH

Ochrona przetwarzania informacji istotnych dla procesów i działalności naszych Klientów jest dla nas priorytetem. Mając to na względzie zapewniamy zgodność naszych usług także z poniższymi normami:

- ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji) [potwierdzone certyfikatem](#);
- ISO/IEC 27017 (bezpieczeństwo informacji w chmurze obliczeniowej) [potwierdzone certyfikatem](#);
- ISO/IEC 27018 (dobre praktyki zabezpieczania danych osobowych w chmurze obliczeniowej) [potwierdzone certyfikatem](#);



Dane spółki:

Adres biura:

Kontakt:

Oktawave S.A. | Poleczki 13 | 02-822 Warszawa | NIP 5213633306

Oktawave S.A. | Puławska 464 (Baletowa Business Park) | 02-844 Warszawa

www.oktawave.com | customer@oktawave.com | +48 22 10 10 555

- ISO/IEC 22301 (zarządzanie ciągłością działania) [potwierdzone certyfikatem](#);
- CSA STAR [potwierdzone certyfikatem](#).

Dokumentacja bezpieczeństwa Oktawave związana ze świadczeniem usług chmurowych podlega tym samym szczegółowym, okresowym audytom międzynarodowych instytucji certyfikujących (wspomniana certyfikacja ISO oraz STAR audytowana przez BSI).

4. FAQ

JAK W PRAKTYCE MAM WDROŻYĆ KOMUNIKAT KNF (STEP BY STEP)?

Dla komfortu naszych Klientów przygotowaliśmy dedykowany poradnik stanowiący esencję wiedzy dla podmiotów nadzorowanych na temat outsourcingu chmury. Są to praktyczne wskazówki dotyczące wymogów formalnych w procesie migracji, opracowane przez specjalistów.

[Praktyczny poradnik dla klientów Oktawave jak wdrożyć Komunikat KNF](#)

CZY OKTAWAVE ZAPEWNI MI WSPARCIE ADMINISTRACYJNE WŁASNYCH ZESPOŁÓW?

Ważną kwestią podkreśloną w Komunikacie KNF są wymagania co do kompetencji pracowników – obszaru IT, cyberbezpieczeństwa jak i ochrony danych osobowych. Zapewnienie i udokumentowanie odpowiednich kompetencji jest kluczowym czynnikiem finalnego sukcesu i jednocześnie wyzwaniem często bardziej złożonym od samej technologii.

Chmura Oktawave obok infrastruktury zapewnia również wsparcie administracyjne własnych, wysoko wykwalifikowanych zespołów. Nasze doświadczenie i obecność na rynku od 2014 r. nabrały znaczenia formalnego, które pomaga naszym Klientom spełnić wymogi komunikatu KNF.

O naszej usłudze Cloud Operations Support przeczytasz [tutaj](#).

CZY CHMURA OKTAWAVE ZLOKALIZOWANA JEST W CAŁOŚCI W POLSCE?

KNF rekomenduje chmurę, której centra danych zlokalizowane są na terenie państw należących do Europejskiego Obszaru Gospodarczego. Bardziej restrykcyjne wytyczne dotyczą operatorów usług kluczowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa. Taki status nierzadko mają chociażby banki. W tych przypadkach podmiot nadzorowany powinien w pierwszej kolejności korzystać z usług tych dostawców chmury, których centra danych znajdują się na terenie Polski.

Wszystkie centra danych chmury Oktawave zlokalizowane są w Polsce.

