MATRYCA ZGODNOŚCI USŁUG OKTAWAVE S.A. Z KOMUNIKATEM KNF

Wersja z dnia 20.02.2024

Dokument stanowi potwierdzenie możliwości wdrażania i korzystania z rozwiązań opartych o chmurę obliczeniową, której dostawcą jest Oktawave S.A. z siedzibą w Warszawie (**Oktawave**) przez podmioty nadzorowane, zgodnie z Komunikatem Urzędu Komisji Nadzoru Finansowego dotyczącym przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z dnia 23 stycznia 2020 r.

W przypadku podmiotów objętych nadzorem bankowym matryca stanowi jedocześnie udokumentowanie możliwości korzystania z chmury Oktawave zgodnie ze Standardem wdrożenia usługi chmury obliczeniowej Związku Banków Polskich.

W DOKUMENCIE:

Lp.	Opis wymogu KNF	Rozwiązanie stosowane przez Oktawave
Obszar: informacje na potrzeby dokonania przez podmiot nadzorowany szacowania ryzyka		
1.	Lokalizacja CPD	Usługi świadczone są w CPD zlokalizowanych na terytorium Polski: 1. Warszawa – lokalizacja zespołu Cloud Operations Team oraz Cloud Migration Team; 2. centrum danych Thinx, zlokalizowane w Warszawie; 3. centrum danych ATM, zlokalizowane w Warszawie;

		4. centrum danych POLCOM, zlokalizowane w Skawinie; 5. centrum danych Netia, zlokalizowane w Jawczycach.
2.	Informowanie o zmianie lokalizacji CPD	Praktyka informowania podmiotów nadzorowanych o każdej zmianie lokalizacji CPD (na poziomie kraju, regionu). Każdorazowe potwierdzenie lokalizacji CPD na wniosek podmiotu nadzorowanego. Obowiązek wykonywany poprzez oświadczenie składane zgodnie z właściwą reprezentacją / umocowaniem.
3.	Zasady dostępu do przetwarzanych informacji przez pracowników / współpracowników / poddostawców	Pracownicy / współpracownicy: - wdrożono system gradacji dostępu do informacji. Zakres informacji, do których dostęp uzyskuje pracownik / współpracownik, każdorazowo odpowiada wykonywanym czynnościom w imieniu Oktawave na rzecz podmiotu nadzorowanego; - w strukturze wewnętrznej do przetwarzanych informacji dopuszczane są wyłącznie osoby posiadające odpowiednie upoważnienie; - osoby dopuszczane do przetwarzanych informacji zostają zobowiązane do zachowania poufności informacji oraz sposobów ich gromadzenia i zabezpieczania; - w przypadku zmiany zakresu kompetencji osoby dopuszczonej do informacji, każdorazowo przeprowadzana jest weryfikacja zakresu informacji, do których powinna mieć ona dostęp. . W przypadkach korzystania z usług poddostawców zapewniono: - standard zawierania umowy nakładającej na poddostawcę równoważne obowiązki ochrony informacji jak w umowie pomiędzy Oktawave a podmiotem nadzorowanym / Oktawave a podmiotem, którego łączy umowa z podmiotem nadzorowanym - w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia środków technicznych i organizacyjnych, w tym zasad dostępu do informacji; - obowiązek poddostawców zobowiązania osób dopuszczonych do informacji do zachowania poufności; - mechanizm kontroli / audytów poddostawców w celu oceny rzetelności wywiązywania się z obowiązków. Konkretne działania kontrolne, które są podejmowane wymagają weryfikacji per projekt. Jeśli będzie taka potrzeba, zostaną odrębnie przedstawione.
4.	Dostęp do przetwarzanych informacji gwarantowany przez przepisy kraju, w którym odbywa się przetwarzanie	Fizycznie przetwarzanie (lokalizacja CPD) odbywa się na terenie Polski (patrz pkt 1) – zastosowanie znajdują standardowe regulacje krajowe umożliwiające w konkretnych sytuacjach dostęp do przetwarzanych informacji przede wszystkim organom administracji / ścigania. W przypadku podmiotu nadzorowanego mającego siedzibę poza terytorium Polski - na żądanie przedstawiona zostanie opinia prawna w zakresie dostępu do przetwarzanych informacji gwarantowanego przez jurysdykcję krajową (w szczególności w

		odniesieniu do sytuacji, w których możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu nadzorowanego).
5.	Mechanizmy izolacji zasobów używanych do świadczenia usług chmury obliczeniowej, w tym informacje o incydentach bezpieczeństwa wiązanych z naruszeniem mechanizmów izolacji	Mechanizm izolacji: - stosowany system pozwala na uruchamianie odseparowanych od siebie instancji serwerów gwarantując bezpieczeństwo i izolację zasobów tej samej fizycznej infrastruktury oferowanej różnym odbiorcom usług. - możliwe jest również definiowanie poziomów dostępu do zasobów serwera; (konkretne mechanizmy izolacji, które są stosowane wymagają weryfikacji per projekt; jeśli będzie taka potrzeba, zostaną odrębnie przedstawione). Incydenty bezpieczeństwa – wdrożone w ramach posiadanej przez Oktawave certyfikacji ISO 22301, ISO 27001, ISO 27017, 27018, 22301 oraz CSA STAR procedury zapewniają: - odpowiednie schematy postępowania wewnątrz organizacji dotyczące reagowania na incydenty, związane również z naruszeniem mechanizmów izolacji; - system reagowania wewnętrznego, aby zdarzenia związane z naruszeniem ochrony informacji były zgłaszane wewnątrz struktur w sposób umożliwiający podjęcie szybkich działań korygujących; - prawidłową realizację obowiązków dotyczących zgłaszania naruszeń bezpieczeństwa (w tym obowiązek niezwłocznego poinformowania podmiotu nadzorowanego o wszelkich incydentach mogących mieć dla niego znaczenie, w szczególności pod kątem obowiązku ich raportowania / zgłaszania odpowiednim organ); *** W dokumencie nie zostają przedstawione konkretne mechanizmy izolacji oraz procedury postępowania z incydentami. Udostępnianie na zewnątrz takich informacji może osłabić ich skuteczność, a przez to zagrozić właściwej ochronie informacji.
6.	Możliwość migracji usługi / danych do innych dostawców w celu mitygacji przywiązania do jednego dostawcy chmury	W miarę możliwości i zgodnie z przyjętym modelem biznesowym zapewniana jest zgodności technologiczna pomiędzy usługami Oktawave, a usługami innych dostawców chmury obliczeniowej. Ma to pomóc podmiotowi nadzorowanemu uniknąć sytuacji vendor lock-in. W szczególności w zakresie usługi IaaS wykorzystywany jest rynkowy standard OVF, w zakresie usług object storage – protokół komunikacyjny REST/API oparty o OpenstackSwift Konkretne mechanizmy, które zostały zastosowane w celu zapewnienia zgodności technologicznej pomiędzy usługami Oktawave, a usługami innych dostawców, wymagają weryfikacji per projekt. Jeśli będzie taka potrzeba, zostaną odrębnie przedstawione. Nie są stosowane mechanizmy prawne ani technologiczne, których wyłącznym celem byłoby przywiązanie podmiotu nadzorowanego do Oktawave jako jednego dostawcy usług chmury obliczeniowej.

		Ocena możliwości dokonania konkretnej migracji usługi / informacji do innego dostawcy zależy od specyfiki konkretnego przypadku (w szczególności technologii stosowanej przez takiego dostawcę usług). W przypadku takiej potrzeby podmiot nadzorowany może uzyskać niezbędne wsparcie w określeniu działań koniecznych do dokonania migracji usługi / informacji do innego dostawcy.
7.	Informacje o podatnościach interfejsów zarządzających usługami, które są udostępniane przez dostawcę	Przeprowadzono wymaganą przez przepisy prawa analizę ryzyka. W jej ramach dokonano określenia podatności zastosowanych rozwiązań technologicznych służących do przetwarzania informacji (określono występujące zagrożenia dla bezpieczeństwa informacji oraz potencjalne następstwa ich zaistnienia). W wyniku przeprowadzanej analizy ryzyka podjęto niezbędne działania w celu wyeliminowania ryzyk dla bezpieczeństwa informacji, lub ich zmniejszenia do akceptowalnego poziomu, zgodnie z obowiązującymi przepisami. Podjęte działania dotyczące podatności rozwiązań technologicznych podlegają okresowym przeglądom i aktualizacji. *** W dokumencie nie zostają przedstawione konkretne podatności zidentyfikowane dla interfejsów (wyniki badania podatności / testy bezpieczeństwa). Ich udostępnienie na zewnątrz mogłoby osłabić skuteczność przyjętych środków bezpieczeństwa. Wszelkie podatności są zabezpieczane z dochowaniem najwyższych standardów rynkowych oraz zgodnie z obowiązującymi przepisami.
8.	Możliwości kontrolowania dostawcy oraz jego podwykonawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej	Podmioty nadzorowane (a w przypadku korzystania z usług Oktawave za pośrednictwem innych podmiotów – te podmioty) mają zapewnianą na mocy umowy z Oktawave możliwość samodzielnego lub przy pomocy audytora zewnętrznego przeprowadzania audytów, w tym inspekcji, w zakresie potwierdzenia wdrożenia przez Oktawave wystarczających gwarancji i środków technicznych / organizacyjnych, w celu ochrony bezpieczeństwa informacji. Szczegółowe zasady kontroli określa zawierana umowa.
9.		

	Możliwości kontrolowania jakości usług chmury obliczeniowej	Gwarantowane w przypadku zawarcia SLA – określa parametry świadczenia usług chmury obliczeniowej pozwalające na monitorowanie przez podmioty nadzorowane usługi. Dodatkowo - Oktawave Watch umożliwia kompleksową kontrolę działania usług udostępnionych w chmurze (o ile podmiot nadzorowany korzysta z tej usługi). Możliwe uwzględnienie w SLA dedykowanych zasad raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej. Konkretne mechanizmy wymagają weryfikacji per projekt. Jeśli będzie taka potrzeba, zostaną odrębnie przedstawione. Podmioty nadzorowane mają zagwarantowaną techniczną możliwość wpływania na zakres, kształt i zmiany usług, w tym na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług.
10.	Informacje o podziale odpowiedzialności za bezpieczeństwo przetwarzanych informacji	Szczegółowy podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji wynika z zakresu usług z jakich korzysta podmiot nadzorowany. Co do zasady Oktawave odpowiada za: 1) zapewnienie infrastruktury technicznej/sprzętu, w ramach którego będą przetwarzane informacje oraz za zapewnienie możliwości wykorzystywania mocy obliczeniowych tego sprzętu dla przetwarzania tych informacji, w sposób wybrany przez podmiot nadzorowany; 2) zabezpieczenie fizyczne i utrzymanie fizyczne infrastruktury technicznej/sprzętu związanego ze świadczeniem chmury, na poziomie chmury oraz zapewnienie jej połączenia z siecią Internet; 3) zapewnienie odpowiednich zabezpieczeń logicznych dostępu do chmury, na poziomie chmury; 4) zapewnienie dostępu do usług, zgodnie z umową (w tym SLA), co obejmuje także monitorowanie ruchu z i do chmury w celu identyfikacji i ochrony przed działaniami typu ataki DDOS oraz zapewnienia stabilności działania chmury; 5) udzielenie wsparcia technicznego w ramach wirtualnej maszyny klienta – wyłącznie w przypadku skorzystania z pomocy technicznej, na żądanie klienta i po udzieleniu przez niego odpowiednich dostępów; 6) zarządzanie usługami klienta w ramach wskazanych przez klienta wirtualnych maszyn – wyłącznie w na żądanie klienta i po udzieleniu przez niego odpowiednich dostępów. W zakresie pkt 5 i 6 powyżej, klient standardowo przekazuje Oktawave instrukcje, co do zakresu operacji, jakie mogą zostać wykonane przez osoby działające w imieniu Oktawave, a Oktawave, w zakresie, w jakim jest to możliwe dla Oktawave, do zapewnienia rozliczalność działań ww. osób w ramach wirtualnych maszyn klienta (tj. logi dokonanych działań oraz możliwość ich przypisania do konkretnej osoby fizycznej) oraz zapewnia ich zobowiązanie do działania zgodnie z umową oraz przepisami prawa. O ile co innego nie wynika z umowy klient samodzielnie administruje tzw. wirtualnymi maszynami, w ramach, których przetwarza informacje, w tym samodzielnie instaluje wybrane przez siebie oprogramowanie, wdraża zabezpieczenia, szyfruje dane (na etapie

		ich przesyłania oraz w spoczynku), tworzy kopie zapasowe oraz realizuje inne czynności wymagane przez jego procedury lub przepisy prawa. Konkretne mechanizmy, które zostały przewidziane w umowie wymagają weryfikacji per projekt. Jeśli będzie taka potrzeba, zostaną odrębnie przedstawione.
11.	Możliwości kontroli dostępu i urządzeń dostępowych użytkowników końcowych	Zapewniono odpowiednie mechanizmy w zakresie kontroli dostępu do usługi chmurowej, jak również kontroli urządzeń użytkowników końcowych, które są wykorzystywane w tym celu, w tym możliwość zarządzania dostępem do zasobów w chmurze w oparciu o role (RBAC). Zarządzanie usługami odbywa się z poziomu konta użytkownika wyposażanego z zabezpieczenia dostępowe. Na żądanie przedstawiony zostanie szczegółowy opis powyższych mechanizmów. O ile z umowy wynika, że Oktawave administruje maszynami wirtualnymi podmiotu nadzorowanego, mogą zostać wdrożone dodatkowe mechanizmy dostępowe w zakresie zarządzania takimi maszynami (konkretne rozwiązania do weryfikacji per projekt).
12.	Zasady zmiany warunków umowy	Zasady zmiany warunków umowy zależą od zakresu usług wykorzystywanych przez podmiot nadzorowany. Usługodawca wyraża gotowość do indywidualnego ustalania zakresu warunków, jakich zmiana będzie zawsze wymagała zgody podmiotu nadzorowanego.
13.	Informacje o wykorzystywanych poddostawcach i zakresie świadczonych przez nich usług; informacja o ich dostępie do danych	1. W przypadku usług IaaS, OCS, OKS, ODF, OCK, kopie zapasowe, poddostawcami są: - ATM S.A. z siedzibą w Warszawie, ul. Grochowska 21a, 04-186 Warszawa – centrum kolokacyjne, zakres czynności powierzonych obejmuje te wskazane w pkt 10.2 powyżej; - Polcom S.A., Skawina, ul. Krakowska 43 – zakres czynności jw.; - Netia S.A. z siedzibą w Warszawie przy ul. Poleczki 13 – zakres czynności jw. 2. W przypadku usługi Oktawave Watch: – Monit24 Sp. z o.o. ul. Prosta 70, 00-838 Warszawa Na żądanie podmiotu nadzorowanego przedstawiona zostanie aktualna lista poddostawców wraz z zakresem świadczonych przez nich zadań oraz informacją o dostępie do informacji.

Obszar: informacje na potrzeby dokonania przez podmiot nadzorowany oceny występowania ewentualnych zagrożeń związanych z zasobami podmiotu nadzorowanego		
14.	Określenie wymaganych kompetencji przy korzystaniu z usługi, określenie ścieżek szkoleniowych i certyfikacyjnych	Określenie wymaganych kompetencji, ścieżek szkoleniowych i certyfikacyjnych zależy od zakresu usług, z których korzysta podmiot nadzorowany. W przypadku takiej potrzeby Oktawave przedstawi informacje pomocne przy określaniu zalecanych wymogów z uwzględnieniem zakresu współpracy.
15.	Zgodność technologiczna posiadanego środowiska teleinformatycznego oraz środowiska chmury obliczeniowej (w szczególności mechanizmy integracji)	Na żądanie podmiotu nadzorowanego przedstawione zostaną dedykowane informacje dotyczące architektury usługi, które będą niezbędne do dokonania przez podmiot nadzorowany oceny zgodności technologicznej posiadanego środowiska teleinformatycznego ze środowiskiem chmury.
Obszar: uwzględnienie stanowiska nadzoru w sprawie szyfrowania informacji		
16.	Bezpieczeństwo usług	Zapewniono na poziomie chmury możliwość: - szyfrowania informacji, gdy to jest technologicznie możliwe (przy jednoczesnym uwzględnieniu oceny Oktawave lub podmiotu nadzorowanego ekonomicznego uzasadnienia takiego działania); - szyfrowania informacji prawnie chronionych „at rest" oraz „in transit"; - weryfikacji algorytmów szyfrowania pod kątem wykluczenia ryzyka zastosowanie rozwiązań uznanych powszechnie za skompromitowane; - zarządzania kluczami szyfrującymi w sposób zapobiegający ujawnieniu informacji; - możliwość przekazywania logów do SIEM; Zastosowanie (zakres) powyższych rozwiązań zależy od konkretnych ustaleń pomiędzy stronami umowy, w szczególności od zakresu usług, z których korzysta podmiot nadzorowany. Na żądanie (adekwatnie do potrzeby) przekazywane są: - informacje o zalecanych przez dostawcę ustawieniach konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług;

		- instrukcje konfiguracji usług oraz metod weryfikacji poprawności ich konfiguracji i działania; - opis mechanizmów logowania; - wytyczne, wzorcowe konfiguracje, opisy zasad itp., które definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji; - opisy mechanizmów dostępu zdalnego do środowiska chmurowego (przy czym zapewnia się, że stosowane mechanizmy spełniają wymogi komunikatu chmurowego KNF, opisane w pkt 28-31 matrycy);
Obszar: wymogi dla umowy z dostawcą usług chmury obliczeniowej		
17.	Treść umowy	Do indywidualnych uzgodnień zastosowanie dedykowanych rozwiązań w umowie (w przypadku oceny stron konieczności zmian w celu dostosowania do wymogów komunikatu chmurowego KNF).
18.	Informacja o prawie właściwym dla umowy (w tym sąd właściwy)	Standardowo: - prawem właściwym dla umowy jest prawo polskie; - spory podlegają jurysdykcji sądów polskich (właściwych ze względu na siedzibę usługodawcy – Warszawa). Rozwiązanie przyjęte w konkretnym przypadku - do potwierdzenia na poziomie podpisanej umowy.
Obszar: opracowanie planu przetwarzania informacji w chmurze obliczeniowej		
19.	Informacje o architekturze i konfiguracji usługi stanowiące wkład do opracowania planu przetwarzania przez podmiot nadzorowany	W przypadku potrzeby uzyskania dodatkowych informacji niezbędnych do sporządzenia planu przetwarzania - podmiotom nadzorowanym zapewniany jest dostęp do wybranych informacji w zakresie (adekwatnie do potrzeby): - zastosowania pseudonimizacji lub anonimizacji; - sposobu szyfrowania informacji oraz miejsca (lub sposobu) zarządzania kluczami szyfrującymi; - podmiotów mających dostęp do przetwarzanych informacji, sposobu nadawania i odbierania dostępu oraz zarządzania nim, w tym kontrolowania; - innych informacji, które mają umożliwić podmiotowi nadzorowanemu zrozumienie konsekwencji stosowania określonej architektury chmury obliczeniowej; - zasad konfiguracji usług.

Obszar: zgodność usług dostawcy z normami (ISO)		
20.	, Normy ISO	Świadczone usługi spełniają następujące wymagania w całości, potwierdzone certyfikatami: – 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; – 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).
Obszar: wymogi ochrony przetwarzanych informacji dla dostawcy usług		
21.	Wymagania w zakresie ochrony informacji	Zapewniono zgodność świadczonych usług z wymogami ochrony informacji przed nieautoryzowanym dostępem lub użyciem przez pracowników / współpracowników / poddostawców, poprzez: - domyślną zasadę braku dostępu do przetwarzanych informacji przez dostawcę w zakresie w jakim mogłoby to wykraczać poza działania konieczne w ramach świadczonych usług; - domyślną zasadę braku konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego lub w innych uruchamianych usługach chmury obliczeniowej; - zasadę „minimum koniecznego” dla uprawnień serwisowych (nadawane wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez stronę umowy, w tym usunięcia usterek) oraz na czas ich trwania; - wytyczne, wzorcowe konfiguracje, opisy zasad, itp., które definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji; - domyślne uruchamianie nowego środowiska (lub usługi chmury) separowanego od innych tenantów, z ustawieniami „secure-by-default”; Konkretne mechanizmy, które zostały zastosowane w danym przypadku zależą od zakresu usług i wymagają weryfikacji per projekt. W przypadku potrzeby uzyskania dalej idących gwarancji co do spełniania wymagań w zakresie ochrony informacji, udostępniany jest bardziej szczegółowy opis wspomnianych mechanizmów lub wskazanie zapisów umownych / proceduralnych zapewniających powyższe funkcjonalności.

Obszar: kryptografia		
22.	Wymagania dla szyfrowania informacji w chmurze obliczeniowej	W przypadku takiej potrzeby i na żądanie podmiotu nadzorowanego, dostarczane są aktualne instrukcje konfiguracji usług chmury oraz metod weryfikacji poprawności ich konfiguracji i działania, w tym w zakresie szyfrowania przetwarzanych informacji.
23.	Klucze	Umożliwia się szyfrowanie kluczami generowanymi lub dostarczonymi i zarządzanymi przez podmiot nadzorowany / stronę umowy z Oktawave. W zależności od konkretnych ustaleń pomiędzy stronami umowy, w szczególności od zakresu usług, z których korzysta podmiot nadzorowany (m.in. Premium Support), możliwe jest również szyfrowanie kluczami generowanymi lub zarządzanymi przez Oktawave.
24.	Utrzymywanie i zarządzanie kluczami szyfrującymi przy wykorzystaniu rozwiązań sprzętowych (HSM)	Zapewniona gotowość udostępnienia rozwiązań sprzętowych (HSM) spełniających wymagania FIPS 140-2 Level 2 (lub równoważne) na wypadek konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu HSM.
25.	Proces zarządzania kluczami szyfrującymi	W przypadkach wygenerowania lub zarządzania kluczami przez Oktawave – zapewniona jest możliwość przechowywania przez podmiot nadzorowany / stronę umowy z Oktawave kopii kluczy szyfrujących w ramach własnej infrastruktury.
Obszar: logowanie zdarzeń		
26.	Logowanie zdarzeń	Wdrożono: - mechanizmy logowania zdarzeń; - możliwość dostępu podmiotu nadzorowanego / strony umowy z Oktawave do logów; - możliwość przekazywania logów do podmiotu nadzorowanego / strony umowy z Oktawave, np. do SIEM.
27.	Zabezpieczenie	Wdrożono zabezpieczania logów przed nieautoryzowanym dostępem, modyfikacją oraz usunięciem.

	.	
Obszar: zdalny dostęp do środowiska chmurowego przez dostawcę* **Wymagania i wdrożone środki dotyczą sytuacji zlecenia dostawcy wykonania działań na zasobach podmiotu nadzorowanego / strony umowy z Oktawave umieszczonych w chmurze (np. aktualizacja oprogramowania, prace serwisowe). Wymagania nie dotyczą usług wsparcia w zakresie standardów obsługi wynikających z umowy na świadczenie usług chmury.*		
28.	Personel dostawcy	Zapewnia się dostęp do wskazanych systemów teleinformatycznych lub ich wybranych zakresów wyłącznie przez uprawniony personel.
29.	Uwierzytelnianie (przynajmniej dwuskładnikowe)	Wdrożono uwierzytelnienia MFA.
30.	Bezpieczne lokalizacje sieciowe	Możliwość zapewnienia dostępu zdalnego wyłącznie z bezpiecznych lokalizacji sieciowych (zaufane sieci podmiotu nadzorowanego lub dostawcy usług), np. w zakresie dostępu administracyjnego lub innego dostępu o charakterze uprzywilejowanym.
31.	Kontrola podmiotu nadzorowanego nad zdalnym dostępem	Możliwość zapewnienia podmiotowi nadzorowanemu / stronie umowy z Oktawave kontroli nad zdalnym dostępem do środowiska chmurowego, w tym sesji administracyjnych (np. poprzez nagrywanie sesji).

Dokładamy starań, aby dokument uwzględniał aktualne informacje. Może się jednak zdarzyć, że kwestie techniczne lub organizacyjne spowodują pewne opóźnienia. Stąd jeśli chcesz potwierdzić aktualność informacji według stanu późniejszego niż wersja niniejszego dokumentu, skontaktuj się z naszym Biurem Obsługi Klienta.

Ze względów bezpieczeństwa część zapisów ma charakter ogólny. W przypadku chęci podjęcia współpracy, bardziej szczegółowe informacje mogą zostać przedstawione na wniosek klienta.

Zastosowanie konkretnych rozwiązań z dokumentu wymaga weryfikacji per projekt.