

Platforma OChK a wymagania Cloud Sovereignty Framework

Styczeń 2026



1. Wprowadzenie

Niniejszy raport prezentuje, w jaki sposób Platforma OChK odpowiada na wymagania określone w dokumencie Cloud Sovereignty Framework (CSF) opublikowanym przez Komisję Europejską¹. Celem tego raportu jest przedstawienie dowodów i mechanizmów zapewniających wysoki poziom suwerenności cyfrowej Platformy OChK. Opracowanie ma charakter informacyjny, nie stanowi porady, ani opinii prawnej. Poniższa treść może wesprzeć klientów w procesie oceny zgodności z kryteriami opublikowanymi przez KE, przy czym OChK nie ponosi odpowiedzialności za wykorzystanie informacji zawartych w niniejszym materiale bez uprzedniej konsultacji z profesjonalnym doradcą prawnym lub biznesowym.

2. Kontekst usług Platformy OChK

Platforma OChK stanowi krajową usługę chmury obliczeniowej oferowaną w modelach: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) oraz Software as a Service (SaaS). Platforma OChK pozwala na udostępnienie mocy obliczeniowej wraz z elementami uzupełniającymi typu przestrzeń dyskowa, czy sieć.

Infrastruktura Platformy OChK jest zlokalizowana w Polsce i wykorzystywana do świadczenia usług na rzecz instytucji publicznych, spółek Skarbu Państwa oraz podmiotów komercyjnych.

Zakres raportu odnosi się wyłącznie do usług i procesów operacyjnych realizowanych w ramach Platformy OChK, obejmując ich organizację, zarządzanie i bezpieczeństwo operacyjne.

¹ European Commission, DG for Digital Services – Cloud Sovereignty Framework, Version 1.2.1, Oct 2025, źródło: https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en

3. Ramy odniesienia i certyfikacje

OChK prowadzi działalność zgodnie z międzynarodowymi standardami zarządzania bezpieczeństwem informacji, zarządzania usługami chmurowymi oraz ciągłością działania.

Spółka posiada wdrożony i utrzymywany zintegrowany System Zarządzania Bezpieczeństwem Informacji i Ciągłością Działania, zgodny z normami:

- ISO/IEC 27001:2022 – Systemy zarządzania bezpieczeństwem informacji,
- ISO 27017:2015 – Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze,
- ISO 27018:2019 – Praktyczne zasady ochrony danych identyfikujących osobę w chmurach publicznych działających jako przetwarzający dane osobowe,
- ISO 22301:2019 – Systemy zarządzania ciągłością działania.

Certyfikaty zgodności z wymienionymi wyżej normami są elementem systemowego podejścia OChK do zapewnienia bezpieczeństwa, niezawodności i odporności operacyjnej, stanowiąc podstawę realizacji wymagań w zakresie suwerenności i bezpieczeństwa informacji ocenianych w ramach niniejszego raportu.

4. Metodyka

Cloud Sovereignty Framework definiuje osiem celów suwerenności [Sovereignty Objectives SOV-1 – SOV-8] oraz odpowiadające im czynniki oceny dokonywanej w ramach tzw. poziomów efektywnego zapewnienia suwerenności [SEAL – *Sovereignty Effective Assurance Levels*].

Niniejsza analiza obejmuje weryfikację wymagań CSF w odniesieniu do usług świadczonych w ramach Platformy OChK. Dla każdego celu przedstawiono wymagania Komisji Europejskiej, odpowiedź oraz komentarz OChK. Mapowanie uwzględnia zarówno aspekty organizacyjne i prawne, jak i techniczne oraz operacyjne, które obejmują:

- lokalizację infrastruktury i danych,
- niezależność operacyjną i kompetencyjną,
- łańcuch dostaw i stosowane technologie,
- bezpieczeństwo informacji oraz zarządzanie zgodnością.

Analiza ma charakter informacyjny i porównawczy – nie stanowi deklaracji zgodności z ramami prawnymi UE, lecz prezentuje sposób, w jaki rozwiązania i procesy OChK wspierają realizację celów określonych w Cloud Sovereignty Framework. Formalna ocena poziomu spełnienia wymagań dla poszczególnych celów suwerenności (SOV-1 – SOV-8) dokonywana jest przez zamawiającego, na podstawie kryteriów SEAL zdefiniowanych przez Komisję Europejską.

Wszystkie sformułowania i definicje zaczerpnięte wprost z Cloud Sovereignty Framework zostały na potrzeby tego dokumentu przetłumaczone przez OChK na język polski, natomiast w nawiasach kwadratowych przytoczono ich oryginalne brzmienie.

SOV-1. Suwerenność strategiczna [*Strategic Sovereignty*]

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Zapewnienie, aby organy posiadające decydującą władzę nad usługami znajdowały się w jurysdykcji UE. <i>[Ensuring that bodies having decisive authority over your services are located within EU jurisdiction.]</i>	OChK jest polską firmą, a jej współwłaścicielami są spółki, w których dominującym akcjonariuszem jest Skarb Państwa (tj. PKO Bank Polski S.A. i Polski Fundusz Rozwoju S.A.). Spółka funkcjonuje w formie sp. z o.o. na podstawie ustawy Kodeks spółek handlowych.	Nadzór właścicielski nad OChK jest sprawowany z terenu RP, zgodnie z polskim prawem. Decyzje strategiczne i operacyjne podejmowane są w całości na terytorium RP.
Ocena zabezpieczeń przed zmianą kontroli. <i>[Evaluating the assurances against change of control.]</i>	Struktura właścicielska OChK opiera się na dwóch strategicznych instytucjach – PKO BP S.A. i PFR S.A., które posiadają po 50% udziałów w spółce. Ze względu na pośrednią kontrolę Skarbu Państwa, zmiany właścicielskie podlegają nadzorowi zgodnie z przepisami polskiego prawa oraz umową inwestycyjną, a nie wyłącznie mechanizmom rynku kapitałowego.	Struktura właścicielska OChK stanowi zabezpieczenie przed niekontrolowaną zmianą właścicieli lub przejęciem przez podmioty spoza UE. Wpływa to korzystnie na stabilność kapitałową i strategiczną ciągłość działalności, co w efekcie sprzyja długofalowemu rozwojowi usług Platformy OChK w ramach jurysdykcji UE.
Stopień, w jakim dostawca jest uzależniony od finansowania pochodzącego ze źródeł UE.	Spółka finansuje rozwój i utrzymanie własnej platformy chmurowej z wypracowanych dochodów generowanych z działalności komercyjnej; niezależnie od tego, wysoki kapitał zakładowy	OChK posiada wysoki kapitał zakładowy, a jej struktura właścicielska minimalizuje ryzyko uzależnienia od kapitału spoza UE. Model finansowy spółki opiera się na

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
<i>[Degree to which the provider relies on financing coming from EU sources.]</i>	(155 mln PLN) wniesiony w całości przez udziałowców, tj. PKO BP S.A. i PFR S.A., stanowi gwarancję posiadania przez spółkę środków zabezpieczających spłatę jej zobowiązań.	zrównoważonej strukturze finansowej w postaci połączenia kapitału właścicielskiego (który umożliwił uruchomienie usług własnej platformy chmury obliczeniowej) oraz – w dalszej perspektywie czasowej – środków wypracowanych z działalności.
Zakres inwestycji, miejsca pracy i tworzenie wartości w UE. <i>[Extent of investment, jobs, and value creation within EU.]</i>	W ramach świadczenia usług Platformy OChK, spółka realizuje wszystkie inwestycje infrastrukturalne i technologiczne na terytorium Polski, w tym korzysta z centrów przetwarzania danych zlokalizowanych na terenie RP. Zatrudnienie oraz kluczowe kompetencje techniczne i operacyjne są w całości ulokowane w Polsce i obejmują zespoły dostarczania usług chmurowych (Platformy OChK), rozwoju produktu, cyberbezpieczeństwa i utrzymania. Spółka działa w zgodzie z wartościami i celami UE, wspierając cyfrową transformację oraz rozwój lokalnych kompetencji technologicznych m.in.	OChK wzmacnia suwerenność cyfrową Unii Europejskiej poprzez zlokalizowanie infrastruktury i kompetencji na terenie RP oraz prowadzenie działalności w duchu wartości spójnych z ładem prawnym i etycznym UE. Takie podejście wzmacnia autonomię operacyjną, zaufanie instytucjonalne oraz ukazuje transparentność funkcjonowania spółki.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
	poprzez współpracę z partnerami krajowymi i ośrodkami akademickimi. Spółka wdrożyła także Kodeks Etyki OChK, który określa zasady odpowiedzialności społecznej, transparentności i poszanowania prawa – wartości stanowiących integralny element europejskiego ładu prawnego i gospodarczego.	
Zaangażowanie w inicjatywy UE, spójność z celami w zakresie cyfryzacji, ekologii i suwerenności przemysłowej określonymi na szczeblu UE. <i>[Involvement in EU initiatives, Consistency with digital, green, and industrial sovereignty objectives defined at EU level.]</i>	Spółka wspiera cyfryzację lokalnych przedsiębiorstw, działa w zgodzie z celami ESG oraz oferuje podmiotom publicznym i prywatnym rozwiązania chmurowe w ramach ekosystemu autorskiej Platformy OChK, działającej na infrastrukturze zlokalizowanej w Polsce. Spółka angażuje się w działania na rzecz budowy europejskiego ekosystemu chmurowego, w tym inicjatywy dotyczące interoperacyjności, suwerenności danych oraz infrastruktury wspierającej rozwój sztucznej inteligencji w UE.	Strategia rozwoju, działalność operacyjna oraz wartości spółki są spójne z celami UE w zakresie cyfryzacji, ekologii oraz suwerenności.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Zdolność do utrzymania bezpiecznego działania pomimo wniosków o zaprzestanie lub zawieszenie świadczenia usług lub w przypadku wycofania lub zakłócenia wsparcia ze strony dostawcy. <i>[Ability to sustain secure operations against requests to cease or suspend the service, or if vendor support is withdrawn or disrupted.]</i>	Spółka posiada kontrolę nad procesami operacyjnym oraz infrastrukturą chmurową, która zlokalizowana jest na terytorium RP. OChK dysponuje zespołami technicznymi zdolnymi do samodzielnego zarządzania i utrzymania środowiska chmurowego, bez potrzeby angażowania zewnętrznych dostawców utrzymaniowych. Klient ma możliwość korzystania z usług Platformy OChK w jednym z dostępnych środowisk technologicznych – OpenStack (<i>open source</i>), które umożliwia niezależny rozwój i utrzymanie rozwiązania, lub VMware, w zależności od swoich potrzeb biznesowych i technicznych.	Lokalizacja infrastruktury oraz zarządzanie operacjami w granicach RP wzmacniają autonomię operacyjną i kontrolę nad świadczeniem usług chmurowych. Możliwość wykorzystania technologii <i>open source</i> obok środowisk komercyjnych, ogranicza ryzyko uzależnienia od jednego dostawcy i umożliwia niezależny rozwój oraz utrzymanie usług w zgodzie z postulatami suwerenności cyfrowej.

SOV-2. Suwerenność prawna i jurysdykcyjna [Legal & Jurisdictional Sovereignty]

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Krajowy system prawny regulujący działalność dostawcy i umowy. <i>[The national legal system governing the provider's operations and contracts.]</i>	OChK jest spółką prawa handlowego zarejestrowaną w Polsce. Działalność spółki podlega przepisom prawa polskiego oraz prawu UE, w szczególności regulacjom dotyczącym ochrony danych osobowych, cyberbezpieczeństwa oraz zasad świadczenia usług drogą elektroniczną. Umowy OChK zawierane z jej klientami określają prawo polskie jako prawo właściwe dla ich interpretacji i wykonania, a ewentualne spory podlegają rozstrzygnięciu przez sądy powszechne w Polsce.	Prowadzenie działalności i realizacja umów w ramach jurysdykcji państwa członkowskiego UE zapewnia przejrzystość regulacyjną i egzekwowalność zobowiązań w europejskim porządku prawnym. Usługi świadczone w ramach Platformy OChK nie podlegają jurysdykcjom spoza UE, co eliminuje ryzyko zastosowania zewnętrznych reżimów prawnych.
Stopień narażenia na przepisy spoza UE o zasięgu transgranicznym (np. amerykańska ustawa CLOUD Act, chińska ustawa o cyberbezpieczeństwie). <i>[Degree of exposure to non-EU laws with cross-border reach (e.g., US</i>	OChK jest spółką prawa handlowego zarejestrowaną w Polsce i funkcjonującą w ramach jurysdykcji państwa członkowskiego Unii Europejskiej. Spółka nie posiada powiązań właścicielskich z podmiotami spoza UE, w tym ze Stanów Zjednoczonych czy z Chin. Usługi w ramach Platformy OChK są świadczone wyłącznie w infrastrukturze zlokalizowanej	Usługi w ramach Platformy OChK nie podlegają jurysdykcjom państw trzecich, tym samym nie są objęte eksterytorialnym działaniem przepisów, takich jak ustawa CLOUD Act (US CLOUD Act) czy chińska ustawa o cyberbezpieczeństwie (Chinese Cybersecurity Law).

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
<i>CLOUD Act, Chinese Cybersecurity Law).</i>]	w Polsce, a dane klientów przetwarzane w ramach środowisk chmurowych Platformy OChK nie są przekazywane poza jej terytorium.	Pełna lokalizacja infrastruktury oraz decyzji operacyjnych w Polsce zapewnia ochronę danych klientów przed dostępem podmiotów spoza UE i wzmacnia zgodność z postulatami europejskiej suwerenności.
Istnienie kanałów prawnych, umownych lub technicznych, za pośrednictwem których organy spoza UE mogłyby wymusić dostęp do danych lub systemów. [Existence of legal, contractual, or technical channels through which non-EU authorities could compel access to data or systems.]	OChK nie udostępnia organom spoza Unii Europejskiej żadnych kanałów prawnych, umownych, ani technicznych umożliwiających uzyskanie dostępu do danych klientów lub ich systemów informatycznych. Dane klientów przetwarzane w ramach Platformy OChK znajdują się w infrastrukturze zarządzanej przez OChK na terytorium Rzeczypospolitej Polskiej i podlegają wyłącznie prawu polskiemu oraz prawu UE. OChK stosuje techniczne i organizacyjne środki bezpieczeństwa uniemożliwiające dostęp podmiotów trzecich do danych klientów, w tym szyfrowanie, kontrolę dostępu i separację środowisk.	OChK eliminuje ryzyko wymuszenia dostępu przez organy spoza UE dzięki pełnej lokalizacji danych klientów przetwarzanych w ramach Platformy OChK w krajowej infrastrukturze oraz zastosowaniu technicznych zabezpieczeń, które wykluczają możliwość udostępnienia informacji podmiotom z państw trzecich. Takie podejście zapewnia zgodność z postulatami suwerenności cyfrowej.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Zastosowanie międzynarodowych reżimów prawnych, które mogą ograniczać sposób użytkowania lub transfer. <i>[Applicability of international regimes, which may restrict usage or transfer.]</i>	OChK prowadzi działalność w ramach porządku prawnego Rzeczypospolitej Polskiej i Unii Europejskiej. Działalność spółki nie podlega reżimom prawnym państw trzecich, których przepisy mogłyby wpływać na sposób przetwarzania lub transfer danych klientów przetwarzanych w ramach usług Platformy OChK. OChK nie posiada powiązań kapitałowych z podmiotami spoza UE, które wpływałyby na jej decyzyjność, a także nie utrzymuje infrastruktury, ani zasobów wykorzystywanych do świadczenia usług Platformy OChK poza Europejskim Obszarem Gospodarczym. Umowy z klientami dotyczące świadczenia usług w ramach Platformy OChK uwzględniają stosowanie prawa polskiego jako prawa właściwego dla ich interpretacji i wykonania.	Ograniczenie działalności do terytorium UE minimalizuje ryzyko objęcia OChK reżimami prawnymi o eksterytorialnym zasięgu, które mogłyby wpływać na dostępność lub transfer danych przetwarzanych w ramach usług Platformy OChK. Brak zależności kapitałowych z podmiotami spoza UE zapewnia spółce większą przewidywalność regulacyjną i pozwala utrzymać kontrolę nad stosowanymi zasadami ochrony danych oraz relacjami umownymi z klientami.
Miejsce tworzenia, rejestracji i rozwoju własności intelektualnej (UE a kraje trzecie), jurysdykcja prawna,	Własność intelektualna dotycząca rozwiązań opracowywanych w ramach rozwoju usług Platformy OChK powstaje, jest rozwijana	Prowadzenie działalności operacyjnej w Polsce i zapewnienie nabycia przez spółkę autorskich praw majątkowych do rezultatów

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
w której własność intelektualna jest tworzona i rozwijana. <i>[Location of intellectual property creation, registration, and development (EU vs. third countries), legal jurisdiction where IP is created and developed.]</i>	i chroniona zgodnie z przepisami prawa polskiego i unijnego. Autorskie prawa majątkowe do utworów wytwarzanych przez pracowników OChK przechodzą na spółkę z mocy przepisów prawa powszechnie obowiązującego, natomiast w przypadku współpracowników działających na podstawie umów B2B przeniesienie praw autorskich majątkowych na OChK jest przewidziane w umowach łączących te osoby ze spółką. Całość prac rozwojowych prowadzonych przez OChK, w tym w zakresie dokumentacji i kodu źródłowego, jest wytwarzana w Polsce i podlega ochronie zgodnie z przepisami prawa polskiego i unijnego.	pracy jej zespołu wzmacnia kontrolę OChK nad wytwarzaną własnością intelektualną i gwarantuje jej ochronę zgodnie z przepisami prawa krajowego. Brak transferu praw własności intelektualnej dotyczących utworów OChK poza Unię Europejską minimalizuje ryzyko przejęcia lub egzekucji tych praw przez podmioty spoza UE.

SOV-3. Suwerenność danych i sztucznej inteligencji [Data & AI Sovereignty]

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Zapewnienie, że tylko klient, a nie dostawca, ma skuteczną kontrolę nad kryptograficznym dostępem do swoich danych. <i>[Ensuring that only the customer, not the provider, has effective control over cryptographic access to their data.]</i>	OChK udostępnia klientom różne modele i mechanizmy zabezpieczeń, w szczególności możliwość skorzystania z kluczy zarządzanych w środowisku Platformy OChK lub zastosowania własnych kluczy kryptograficznych (<i>customer-managed keys</i>). Klienci uzyskują w ten sposób pełną kontrolę nad dostępem kryptograficznym do danych przetwarzanych w ramach Platformy OChk. Wybór modelu szyfrowania uzależniony jest od dostępnych funkcji technicznych dla poszczególnych usług Platformy OChK oraz indywidualnych potrzeb i wymagań bezpieczeństwa. Decyzja o sposobie szyfrowania oraz zarządzania kluczami należy do klienta.	Możliwość zastosowania różnych modeli szyfrowania oraz wykorzystania własnych kluczy kryptograficznych, w tym przechowywania kluczy lokalnie, wzmacnia autonomię kryptograficzną i kontrolę klientów nad ich danymi przetwarzanymi w ramach Platformy OChK. Klient w ramach funkcji danej usługi samodzielnie decyduje o sposobie szyfrowania i zarządzania kluczami, co ogranicza ryzyko nieautoryzowanego dostępu. Elastyczność techniczna Platformy OChK umożliwia dopasowanie stosowanych rozwiązań kryptograficznych do wymagań regulacyjnych oraz wewnętrznych polityk bezpieczeństwa organizacji.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Wgląd w to, kiedy, gdzie i przez kogo przeglądane są dane, w tym możliwość kontroli wykorzystania modelu sztucznej inteligencji, mechanizmy gwarantujące nieodwracalne usunięcie danych wraz z weryfikowalnymi dowodami. <i>[Visibility into when, where, and by whom data is accessed, including auditability of AI model usage, mechanisms guaranteeing irreversible removal of data, with verifiable evidence.]</i>	Platforma OChK zapewnia klientom dostęp do logów operacyjnych i audytowych, które umożliwiają identyfikację momentu zdarzenia, lokalizacji i użytkownika wykonującego operacje na danych. System rejestruje zdarzenia uwierzytelnienia, modyfikacji, odczytu oraz administracji środowiskiem. Ścieżki audytu pozwalają na pełną weryfikację dostępu do danych w czasie rzeczywistym oraz w trybie retrospektywnym. Dane logów są chronione i dostępne wyłącznie dla uprawnionych użytkowników. Platforma umożliwia również stosowanie mechanizmów trwałego usuwania danych (<i>secure-erase</i>) z generowaniem potwierdzeń wykonania procesu nieodwracalnego usunięcia danych w postaci logów systemowych. Aktualny zakres usług Platformy OChK nie obejmuje wbudowanych komponentów sztucznej inteligencji (AI). Spółka zapewnia jednak klientom możliwość wdrażania własnych rozwiązań AI	Zapewnienie klientom dostępu do logów operacyjnych i audytowych ich środowiska umożliwia pełną rozliczalność i przejrzystość działań wykonywanych na danych związanych z przetwarzaniem danych w ramach Platformy OChK oraz zarządzaniem środowiskiem chmurowym. Mechanizmy trwałego usuwania danych (<i>secure erase</i>) oraz możliwość weryfikacji ich wykonania stanowią potwierdzenie zgodności z zasadami cyklu życia informacji i ich trwałego usuwania. W zakresie potencjalnego wykorzystania sztucznej inteligencji, model odpowiedzialności i audytowalności przyjęty przez OChK umożliwia zachowanie kontroli po stronie klienta nad procesami ich przetwarzania i wdrożeniem odpowiednich polityk i mechanizmów nadzoru.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
	w ramach udostępnionych zasobów infrastrukturalnych. W takim przypadku odpowiedzialność za audyt i rejestrację procesów przetwarzania spoczywa na kliencie zgodnie z jego politykami bezpieczeństwa i zgodności.	
Ścisłe ograniczenie przechowywania i przetwarzania danych do jurysdykcji europejskiej, bez możliwości przeniesienia do państw trzecich. <i>[Strict confinement of storage and processing to European jurisdictions, with no fallback to third countries.]</i>	Dane klientów, przetwarzane w ramach korzystania z usług Platformy OChK, są przechowywane i przetwarzane wyłącznie w infrastrukturze zlokalizowanej na terytorium RP. OChK nie posiada centrów przetwarzania danych (CPD) poza Polską, co oznacza, że nie istnieje techniczna możliwość przeniesienia danych klientów poza granice UE bez ich wiedzy i zgody. Całość infrastruktury, operacji i procesów zarządzania środowiskami Platformy OChK znajduje się w Polsce i funkcjonuje w ramach obowiązującego porządku prawnego UE.	Pełna lokalizacja infrastruktury Platformy OChK w Polsce zapewnia kontrolę nad miejscem przetwarzania danych klientów i eliminuje ryzyko ich przekazywania do państw trzecich. Brak centrów przetwarzania danych w innych regionach technicznie uniemożliwia relokację danych poza jurysdykcję Unii Europejskiej (w ramach korzystania z usług Platformy OChK), wzmacniając tym samym suwerenność prawną i operacyjną.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Zakres, w jakim modele AI i strumienie danych są rozwijane, trenowane, hostowane i zarządzane pod kontrolą UE, minimalizując zależność od technologii spoza UE. <i>[Extent to which AI models and data pipelines are developed, trained, hosted, and governed under EU control, minimizing dependency on non-EU technology stacks.]</i>	Usługi Platformy OChK nie obejmują wbudowanych komponentów przeznaczonych do rozwijania lub trenowania modeli sztucznej inteligencji. Klienci mogą jednak uruchamiać i utrzymywać własne rozwiązania AI w środowisku Platformy OChK, wykorzystując udostępnione zasoby obliczeniowe, sieciowe i magazynowe zlokalizowane w Polsce.	Platforma OChK umożliwia rozwój i wykorzystanie rozwiązań AI w ramach infrastruktury utrzymywanej w UE, bez angażowania środowisk zewnętrznych spoza regionu. Klienci zachowują możliwość utrzymania pełnej kontroli nad narzędziami i technologiami używanymi do tworzenia lub trenowania modeli. Platforma OChK stanowi środowisko umożliwiające uruchamianie, rozwój i wykorzystanie rozwiązań AI w ramach infrastruktury utrzymywanej w Polsce.

SOV-4. Suwerenność operacyjna *[Operational Sovereignty]*

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Łatwość migracji obciążeń lub integracji z alternatywnymi rozwiązaniami kontrolowanymi w UE	Platforma OChK została zaprojektowana z wykorzystaniem otwartych technologii i standardów, umożliwiających interoperacyjność oraz migrację środowisk pomiędzy rozwiązaniami chmurowymi.	Wykorzystanie otwartych technologii i standardowych protokołów minimalizuje ryzyko uzależnienia od pojedynczego dostawcy (tzw. <i>vendor lock-in</i>). Klienci mogą swobodnie migrować swoje zasoby lub

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
bez uzależnienia od pojedynczego dostawcy. <i>[Ease of migrating workloads or integrating with alternative EU -controlled solutions without vendor lock-in.]</i>	Usługi oferowane w ramach Platformy OChK wykorzystują m.in. OpenStack i standardowe interfejsy API, co pozwala klientom przenosić lub integrować zasoby (aplikacje, dane, usługi) z innymi środowiskami chmurowymi, w tym z rozwiązaniami utrzymywanymi w Unii Europejskiej. OChK nie stosuje mechanizmów ograniczających eksport danych ani konfiguracji, a struktura usług umożliwia klientom zachowanie kontroli nad własnymi zasobami i architekturą.	integrować środowiska z innymi platformami działającymi w UE, zachowując niezależność operacyjną i elastyczność technologiczną. Jako dostawca usług przetwarzania danych OChK podlega przepisom Data Act, co obejmuje m.in. obowiązek ułatwienia migracji danych i unikania nieuzasadnionych ograniczeń technicznych, umownych lub komercyjnych w tym zakresie.
Zdolność operatorów z UE do zarządzania, utrzymywania i wspierania technologii bez konieczności angażowania dostawców spoza UE. <i>[Capacity for EU operators to manage, maintain, and support the technology without requiring non-EU vendor involvement.]</i>	OChK dysponuje własnymi zespołami technicznymi, inżynieryjnymi i operacyjnymi, które realizują zadania w zakresie utrzymania, rozwoju i wsparcia Platformy OChK. Wszystkie kluczowe funkcje operacyjne, w tym zarządzanie infrastrukturą, bezpieczeństwem, siecią i usługami Platformy OChK, są wykonywane przez zespół OChK działający w Polsce. Spółka zapewnia ciągły rozwój kompetencji wewnętrznych poprzez szkolenia i współpracę	Samodzielne utrzymanie i rozwój środowiska przez zespół OChK w zakresie działań operacyjnych, utrzymaniowych i rozwojowych zapewniają niezależność operacyjną oraz wzmacnia odporność na zakłócenia wynikające z czynników zewnętrznych. Taki model operacyjny OChK eliminuje potrzebę angażowania podmiotów spoza UE i sprzyja rozwojowi kompetencji lokalnych specjalistów

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
	z organizacjami branżowymi oraz systemowe wsparcie dla procesu stałego doskonalenia zespołu OChK.	w obszarze infrastruktury chmurowej, automatyzacji i bezpieczeństwa.
Istnienie bazy kompetencji zlokalizowanej w UE, obejmującej wiedzę niezbędną do utrzymania i rozwoju usług. <i>[Existence of an EU-based talent pool with the expertise to operate and sustain the service.]</i>	Zespół OChK działa w Polsce i posiada aktualną wiedzę oraz praktyczne doświadczenie w zakresie projektowania, wdrażania i utrzymania środowisk chmurowych. Spółka rozwija kompetencje techniczne poprzez stałe szkolenia specjalistyczne oraz współpracę z organizacjami branżowymi i środowiskiem eksperckim.	Dostępność i rozwój lokalnych kompetencji technicznych wzmacniają niezależność operacyjną OChK i umożliwiają samodzielne utrzymanie oraz rozwój usług Platformy OChK bez potrzeby pozyskiwania wsparcia spoza regionu. Aktywność szkoleniowa i współpraca z organizacjami branżowymi przyczyniają się do budowania bazy ekspertów chmurowych w UE.
Gwarancja, że wsparcie operacyjne jest świadczone z terytorium UE i podlega wyłącznie ramom prawnym UE. <i>[Assurance that operational support is delivered from within the EU and</i>	Działania w zakresie utrzymania i wsparcia operacyjnego Platformy OChK są realizowane przez zespół OChK zlokalizowany w Polsce. Zespoły operacyjne i administracyjne wykonują zadania związane z konfiguracją oraz obsługą środowisk w infrastrukturze należącej do OChK,	Organizacja wsparcia operacyjnego w ramach struktur OChK zlokalizowanych w Polsce umożliwia utrzymanie bezpośredniego nadzoru nad procesami utrzymania i eksploatacji usług. Taki model pracy wzmacnia kontrolę nad realizacją działań operacyjnych i zapewnia ich wykonywanie w ramach porządku prawnego

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
<i>subject exclusively to EU legal frameworks.]</i>	działając zgodnie z przepisami prawa polskiego i unijnego.	obowiązującego w UE, obejmującego m.in. przepisy odnoszące się do ochrony danych oraz bezpieczeństwa informacji.
Dostępność pełnej dokumentacji technicznej, kodu źródłowego i wiedzy operacyjnej umożliwiającej długoterminową samodzielność. <i>[Availability of full technical documentation, source code, and operational know-how enabling long-term autonomy.]</i>	OChK posiada pełną dokumentację techniczną i operacyjną środowisk Platformy OChK. Obejmuje ona architekturę, konfigurację, procesy utrzymaniowe oraz procedury operacyjne. Dokumentacja jest utrzymywana przez OChK w sposób systemowy w ramach zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania. Wiedza techniczna jest budowana i utrwalana dzięki wewnętrznym standardom, szkoleniom oraz działaniom usprawniającym procesy operacyjne i automatyzację infrastruktury.	Dostępność aktualnej dokumentacji i utrwalaonych procedur technicznych pozwala na efektywne utrzymanie oraz rozwój Platformy OChK w dłuższej perspektywie. Systemowe działania prowadzone przez spółkę w zakresie dokumentowania i przekazywania wiedzy ograniczają zależność od zewnętrznych dostawców oraz wspierają długoterminową samodzielność operacyjną.
Lokalizacja i kontrola prawna nad kluczowymi dostawcami i podwykonawcami zaangażowanymi w świadczenie usług.	OChK prowadzi działalność na podstawie umów z kluczowymi dostawcami i podwykonawcami działającymi na terytorium UE lub na warunkach podlegających prawu polskiemu bądź unijnemu.	Lokalizacja działalności kluczowych dostawców (w szczególności operatorów centrów danych) w Polsce umożliwia skuteczny nadzór nad realizacją usług

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
<i>[Location and legal control of critical suppliers or subcontractors involved in service delivery.]</i>	Operatorzy centrów przetwarzania danych (CPD) wykorzystywanych do świadczenia usług Platformy OChK działają na terytorium Polski, i są objęci nadzorem oraz wymaganiami kontraktowymi określonymi przez OChK w zakresie bezpieczeństwa i zgodności. Spółka utrzymuje kontrolę nad zakresem i charakterem prac realizowanych przez kluczowe podmioty zewnętrzne, a relacje kontraktowe określają obowiązki dotyczące bezpieczeństwa i ochrony informacji. OChK monitoruje wykonanie umów oraz okresowo ocenia ryzyka związane z łańcuchem dostaw.	i bezpieczeństwem infrastruktury. Model współpracy z podmiotami działającymi w ramach prawa UE wspiera przejrzystość i możliwość kontroli nad łańcuchem dostaw oraz ogranicza ryzyka operacyjne związane z utrzymaniem infrastruktury.

SOV-5. Suwerenność łańcucha dostaw [Supply Chain Sovereignty]

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Źródło geograficzne kluczowych części fizycznych, miejsce produkcji – kraje, w których sprzęt jest produkowany lub montowany. <i>[Geographic source of key physical parts, manufacturing location - countries where hardware is manufactured or assembled.]</i>	Sprzęt wykorzystywany w infrastrukturze Platformy OChK pochodzi od uznanych producentów spełniających europejskie i międzynarodowe normy jakości oraz bezpieczeństwa. Dostawcy sprzętu wytworzonego poza UE mają główne siedziby w: • USA (95%) • Japonii (5%) Dostawy i montaż infrastruktury serwerowej realizowane są przez podmioty działające na terenie Unii Europejskiej, w tym w Polsce, natomiast jej komponenty (np. procesory, pamięci, podzespoły sieciowe) są wytwarzane w krajach trzecich, zgodnie z globalnym modelem produkcji sprzętu IT.	Infrastruktura Platformy OChK jest oparta na sprzęcie pochodzącym od globalnych producentów o ugruntowanej pozycji na rynku. Świadomość pochodzenia komponentów i nadzór nad wyborem dostawców, obejmujący proces ich weryfikacji, ograniczają ryzyka związane z globalnym łańcuchem produkcji, w tym z pochodzeniem komponentów spoza UE.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Jurysdykcja i pochodzenie kodu wbudowanego sterującego sprzętem (<i>firmware</i>). <i>[Jurisdiction and provenance of embedded code controlling hardware, firmware.]</i>	Kod wbudowany (<i>firmware</i>) urządzeń używanych w infrastrukturze Platformy OChK jest dostarczany przez uznanych producentów sprzętu z lokalizacją w USA oraz Japonii. Aktualizacje <i>firmware</i> są kontrolowane i zatwierdzane przez zespół bezpieczeństwa OChK, a ich integralność jest weryfikowana za pomocą podpisów cyfrowych producenta.	Świadomość pochodzenia i kontroli nad kodem wbudowanym (<i>firmware</i>) stanowi istotny element zarządzania bezpieczeństwem łańcucha dostaw sprzętu wykorzystywanego w infrastrukturze Platformy OChK.
Pochodzenie oprogramowania – miejsce i podmiot odpowiedzialny za projektowanie i programowanie, lokalizacja i jurysdykcja, której poddane są procesy pakowania, dystrybucji i aktualizacji oprogramowania. <i>[Origin of Software: where and by whom software is architected and programmed, location and jurisdiction]</i>	Komercyjne oprogramowanie wykorzystywane w infrastrukturze Platformy OChK w całym cyklu życia – od jego opracowania po aktualizacje – jest dostarczane przez uznanych globalnych producentów. Dostawcy oprogramowania wytworzonego poza UE mają główne siedziby w USA, Japonii i Indiach. Ponadto, klienci Platformy OChK mają możliwość wyboru środowiska technologicznego, korzystając z oprogramowania komercyjnego (VMware) lub technologii <i>open source</i> (OpenStack), w zależności od swoich potrzeb i polityk bezpieczeństwa.	Możliwość wyboru przez klienta pomiędzy oprogramowaniem pochodzącym od globalnego producenta a <i>open source</i> pozwala zachować równowagę między stabilnością komercyjnych rozwiązań a elastycznością otwartych standardów. Świadomość pochodzenia oprogramowania oraz możliwość stosowania otwartych modeli licencyjnych wzmacnia przejrzystość oraz niezależność operacyjną usług Platformy OChK.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
<i>governing software packaging, distribution, and updates.]</i>	W przypadku środowisk OpenStack obowiązują postanowienia licencyjne typowe dla modeli otwartego oprogramowania, umożliwiające wgląd w kod, jego audyt i modyfikację zgodnie z zasadami licencji w modelu open source Apache License 2.0.	
Stopień zależności od dostawców, infrastruktury i technologii spoza Unii Europejskiej. <i>[Degree of reliance on non-EU vendors, facilities, or proprietary technologies.]</i>	OChK świadczy usługi Platformy OChK na infrastrukturze zlokalizowanej w Polsce. Wykorzystanie do budowy i utrzymania infrastruktury Platformy OChK komponentów lub oprogramowania pochodzącego od dostawców spoza UE dotyczy elementów standardowych dla globalnego rynku sprzętu i systemów operacyjnych. Jednocześnie spółka umożliwia klientom korzystanie z usług Platformy OChK w ramach technologii opartych na otwartych standardach (środowisko OpenStack). OChK wdrożyła także proces weryfikacji i monitoringu dostawców, z uwzględnieniem oceny	Zlokalizowane infrastruktury Platformy OChK na terenie Polski, świadome zarządzanie relacjami z dostawcami oraz monitorowanie ryzyk związanych z globalnym łańcuchem technologicznym pozwala ograniczać wpływ podmiotów spoza UE na działalność operacyjną OChK.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
	zależności od dostawców – także w kontekście ryzyk geopolitycznych i operacyjnych.	
Wgląd w cały łańcuch dostawców i poddostawców, w tym prawa do audytu. <i>[Visibility into the entire supplier and sub-supplier chain, including audit rights.]</i>	OChK utrzymuje przejrzystość w zakresie łańcucha dostaw (w odniesieniu do kluczowych dostawców) związanego z usługami Platformy OChK, obejmującą przede wszystkim operatorów centrów przetwarzania danych. Wszyscy dostawcy i poddostawcy, którzy mają dostęp do infrastruktury Platformy OChK, objęci są procesem weryfikacji i okresowego monitoringu bezpieczeństwa, a odpowiednie obowiązki regulujące kwestie poufności, zgodności oraz bezpieczeństwa są określone we właściwych umowach. Operatorzy centrów przetwarzania danych działają na terytorium Polski i w ramach prawa polskiego. Przeprowadzane są cykliczne audyty ich bezpieczeństwa, w tym inspekcje.	Skoncentrowanie nadzoru na lokalnych elementach łańcucha dostaw – w szczególności centrach przetwarzania danych - pozwala OChK skutecznie kontrolować krytyczne procesy operacyjne oraz reagować na ryzyka związane z bezpieczeństwem i ciągłością działania. Uregulowanie właściwych obowiązków dostawców w umowach oraz stosowanie procedur ich weryfikacji i monitoringu zapewnia przejrzystość współpracy i możliwość kontroli zgodności w obszarach kluczowych dla świadczenia usług w ramach Platformy OChK.

SOV-6. Suwerenność technologiczna [Technology Sovereignty]

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Zdolność integracji z innymi technologiami przy użyciu udokumentowanych i niezależnych API lub protokołów, stopień zgodności z publicznymi i powszechnie stosowanymi standardami ograniczającymi zależność od pojedynczych dostawców. <i>[Ability to integrate with other technologies through well-documented and non-proprietary APIs or protocols, extent to which the solution adheres to publicly governed and widely adopted standards, reducing dependency on single vendors.]</i>	OChK dysponuje własnymi zespołami – deweloperskim, technicznym, inżynierskim i operacyjnym, które realizują zadania w zakresie rozwoju, utrzymania i wsparcia Platformy OChK, w tym możliwości jej integracji z użyciem API. OChK udostępnia dokumentację kodu Terraform potrzebnego do zarządzania Platformą OChK. Spółka zapewnia ciągły rozwój kompetencji wewnętrznych poprzez szkolenia i współpracę z organizacjami branżowymi.	Zdolność integracji z innymi technologiami jest możliwa dzięki udostępnianiu dokumentacji i kodu Terraform umożliwiającego zarządzanie Platformą OChK za pomocą powszechnie stosowanego standardu <i>Infrastructure as Code</i>, który wykorzystuje otwarte specyfikacje providerów na bazie publicznych API. Dzięki ciągłemu rozwojowi kompetencji zespołów OChK poprzez szkolenia i współpracę z organizacjami branżowymi, spółka stosuje najlepsze standardy branżowe, w tym w zakresie możliwości integracji.
Dostępność oprogramowania na licencjach otwartych z prawem do audytu, modyfikacji i redystrybucji,	Platforma OChK wykorzystuje m.in. technologie oparte na otwartym oprogramowaniu, w tym m.in. OpenStack, Kubernetes.	Możliwość korzystania przez klienta z usług Platformy OChK opartych na technologii <i>open source</i> zapewnia przejrzystość i możliwość

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
zapewniających przejrzystość i elastyczność. <i>[Whether software is accessible under open licenses, with rights to audit, modify, and redistribute, ensuring transparency and adaptability.]</i>	Oprogramowanie to jest rozwijane w ramach projektów o publicznie dostępnych repozytoriach kodu, co umożliwia wgląd w jego strukturę oraz audyt bezpieczeństwa. Oprogramowanie komercyjne wykorzystywane w środowisku jest objęte umowami licencyjnymi, które umożliwiają OChK prawo utrzymania i aktualizacji.	audytu kodu, a także pozwala na niezależny rozwój i modyfikację komponentów. Połączenie rozwiązań otwartych z możliwością korzystania z oprogramowania komercyjnego ogranicza ryzyko uzależnienia od pojedynczego dostawcy i wspiera elastyczność rozwoju poszczególnych usług Platformy OChK.
Przejrzystość projektu i funkcjonowania usługi, w tym dokumentacji architektonicznej, przepływów danych i zależności. <i>[Visibility into the design and functioning of the service, including architectural documentation, data flows, and dependencies.]</i>	OChK posiada aktualną dokumentację architektury technicznej, przepływów danych oraz zależności pomiędzy komponentami środowiska Platformy OChK. Dokumentacja ta jest opracowywana i utrzymywana w ramach systemowych procesów wytwarzania oprogramowania, zarządzania zmianą i bezpieczeństwem informacji. Weryfikacja zależności technologicznych stanowi element przeglądów bezpieczeństwa i jest uwzględniana w ramach procesu oceny ryzyka.	Przejrzystość architektury i utrzymywanie aktualnej dokumentacji technicznej ułatwia identyfikację zależności pomiędzy komponentami środowiska oraz kontrolę nad zmianami w infrastrukturze. Dostępność informacji o przepływach danych i powiązaniach technologicznych wspiera procesy oceny ryzyka, planowania rozwoju oraz utrzymania bezpieczeństwa Platformy OChK.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Stopień niezależności UE w zakresie wysokowydajnych zasobów obliczeniowych, w tym procesorów, akceleratorów i ekosystemów oprogramowania. <i>[Degree of EU independence in high-performance computing capabilities, including processors, accelerators, and software ecosystems.]</i>	Infrastruktura Platformy OChK jest zlokalizowana w Polsce. Wykorzystanie komponentów lub oprogramowania pochodzącego od dostawców spoza UE dotyczy elementów typowych dla globalnego rynku sprzętu i systemów operacyjnych np. procesorów graficznych (GPU).	OChK wykorzystuje powszechnie stosowane technologie rynkowe. Utrzymywanie infrastruktury obliczeniowej w Polsce daje większą kontrolę nad jej eksploatacją i bezpieczeństwem, nawet jeśli część komponentów pochodzi spoza UE.

SOV-7.Suwerenność bezpieczeństwa i zgodności *[Security & Compliance Sovereignty]*

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Uzyskanie certyfikatów uznawanych w UE i na arenie międzynarodowej (np. systemy ISO, ENISA). <i>[Attainment of EU and internationally recognized certifications (e.g., ISO, ENISA schemes).]</i>	OChK posiada certyfikaty potwierdzające zgodność z uznanymi międzynarodowymi normami w zakresie bezpieczeństwa informacji, usług chmurowych oraz ciągłości działania. System zarządzania bezpieczeństwem informacji OChK jest certyfikowany zgodnie z normą ISO/IEC 27001 oraz jej rozszerzeniami ISO/IEC 27017	Utrzymywanie Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania zgodnie z wymaganiami norm ISO potwierdza dojrzałość organizacyjną OChK w obszarze bezpieczeństwa informacji, ciągłości działania oraz zarządzania ryzykiem. Certyfikacje

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
	i ISO/IEC 27018, które dotyczą środowisk chmurowych i ochrony danych osobowych. OChK utrzymuje również certyfikację ISO 22301, obejmującą zarządzanie ciągłością działania. Wszystkie certyfikaty są wydane przez niezależne jednostki akredytujące.	obejmują procesy kluczowe dla świadczenia usług chmurowych i wspierają ich dalszy rozwój w zgodzie z międzynarodowymi standardami jakości i bezpieczeństwa.
Zgodność z RODO, NIS2, DORA i innymi ramami prawnymi UE. <i>[Adherence to GDPR, NIS2, DORA, and other EU frameworks.]</i>	OChK realizuje swoje obowiązki w zakresie ochrony danych osobowych, w tym wynikające z roli podmiotu przetwarzającego w rozumieniu RODO (GDPR). Relacje z klientami Platformy OChK są uregulowane odpowiednimi umowami powierzenia przetwarzania danych, które określają prawa i obowiązki stron oraz środki organizacyjne i techniczne stosowane w celu zabezpieczenia danych. W obszarze bezpieczeństwa systemów informacyjnych OChK utrzymuje System Zarządzania Bezpieczeństwem Informacji (SZBI), który uwzględnia wymagania NIS2 w zakresie cyberbezpieczeństwa, zarządzania ryzykiem	Uwzględnianie w praktykach OChK zasad wynikających z kluczowych regulacji unijnych w obszarze odporności cyfrowej i cyberbezpieczeństwa wzmacnia przejrzystość relacji z klientami oraz zaufanie do usług chmurowych. Stosowanie umów dostosowanych do wymagań regulacyjnych, utrzymywanie Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłością Działania (SZBI/CD) oraz uwzględnianie wymagań sektorowych, w tym DORA, stanowi element dojrzałego podejścia OChK do zarządzania bezpieczeństwem informacji

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
	i ciągłości działania, pomimo braku krajowej implementacji tej dyrektywy. W odniesieniu do rozporządzenia DORA spółka przeanalizowała jego wymagania i dostosowała procesy operacyjne oraz zapisy umowne do oczekiwań klientów z sektora finansowego, którzy podlegają tej regulacji. Ponadto OChK uwzględnia inne istotne ramy prawne Unii Europejskiej mające znaczenie dla świadczenia usług chmurowych (np. Data Act, DSA, AI Act) oraz monitoruje rozwój unijnych regulacji w obszarze chmury, danych i cyberbezpieczeństwa oraz uwzględnia ich kierunki w rozwoju usług, procesów wewnętrznych i relacji kontraktowych z klientami.	i odpowiedzialnego świadczenia usług chmury obliczeniowej. OChK uwzględnia także postanowienia Digital Services Act (DSA) dotyczące możliwości zgłaszania nielegalnych treści oraz zasad postępowania z tego rodzaju zgłoszeniami.
Centra operacji bezpieczeństwa (SOC) i zespoły reagowania działające wyłącznie w jurysdykcji UE; kontrola nad monitoringiem i rejestrowaniem zdarzeń – możliwość wglądu klientów	Działania w zakresie bezpieczeństwa informacji, monitorowania i reagowania na incydenty są prowadzone przez Security Operations Center (SOC) OChK, działające w trybie 24/7.	Funkcjonowanie całodobowego SOC w strukturach OChK zapewnia ciągłość nadzoru nad bezpieczeństwem środowisk i szybką reakcję na incydenty.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
lub organów UE w logi, alerty i funkcje nadzoru. <i>[Security Operations Centres and response teams operating exclusively under EU jurisdiction, control over security monitoring/logging - customer or EU authority ability to oversee logs, alerts, and monitoring functions directly.]</i>	Zlokalizowany w Polsce zespół SOC OChK realizuje zadania w zakresie nadzoru nad zdarzeniami bezpieczeństwa, analizy logów, korelacji alertów oraz reagowania na incydenty w środowisku OChK. W działaniach realizowanych przez SOC OChK, wykorzystywane są narzędzia <i>open source</i> służące do monitorowania i analizy bezpieczeństwa. Narzędzia te są utrzymywane w modelu zapewniającym kontrolę konfiguracji i wyników po stronie OChK. Zakres dostępu klientów do informacji o bezpieczeństwie oraz sposób raportowania incydentów są określone w umowach o świadczenie usług oraz właściwej dokumentacji technicznej. W przypadku konieczności udostępnienia informacji organom Unii Europejskiej, OChK działa zgodnie z przepisami powszechnie obowiązującego prawa. OChK oferuje również usługę SOC as a Service, która umożliwia klientom korzystanie	Prowadzenie działań monitorujących i analitycznych przez zespół zlokalizowany w Polsce ogranicza ryzyko zaangażowania podmiotów spoza UE w procesy bezpieczeństwa oraz umożliwia utrzymanie kontroli nad danymi i logami. Jasno określone w umowach zasady raportowania incydentów oraz możliwość korzystania przez klientów z usługi SOC as a Service ułatwiają klientom bieżącą współpracę z OChK w zakresie monitorowania bezpieczeństwa i reagowania na incydenty.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
	z dedykowanego monitoringu i reagowania na incydenty w ich środowiskach chmurowych z wykorzystaniem oprogramowania komercyjnego lub <i>open source</i> .	
Przejrzyste, terminowe i zgodne z przepisami UE raportowanie incydentów lub podatności; autonomia utrzymaniowa – możliwość samodzielnego opracowania, testowania i stosowania poprawek bezpieczeństwa niezależnie od dostawców spoza UE. <i>[Transparent, timely, and EU-compliant reporting of breaches or vulnerabilities, maintenance Autonomy - ability to develop, test, and apply security patches independently of non-EU vendors.]</i>	OChK posiada formalnie określone procedury zgłaszania i raportowania incydentów bezpieczeństwa oraz podatności, realizowane zgodnie z powszechnie obowiązującymi przepisami prawa i właściwymi ustaleniami umownymi. Zespoły cyberbezpieczeństwa, dostarczania usług i utrzymania infrastruktury są odpowiedzialne za analizę, testowanie i wdrażanie poprawek w środowisku Platformy OChK – tam, gdzie jest to technologicznie możliwe. Procesy te są prowadzone przez zespół OChK zlokalizowany w Polsce i nie wymagają udziału podmiotów spoza Unii Europejskiej. Informacje o incydentach są przekazywane klientom lub właściwym organom zgodnie	Utrzymywanie właściwych procedur raportowania incydentów oraz podatności umożliwia sprawne reagowanie i skuteczną komunikację w sytuacjach wymagających podjęcia działań w zakresie cyberbezpieczeństwa. Realizacja tych procesów przez zespół OChK zlokalizowany w Polsce wzmacnia kontrolę nad analizą, testowaniem i wdrażaniem poprawek.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
	z obowiązującymi przepisami prawa oraz postanowieniami umownymi.	
Możliwość przeprowadzania niezależnych audytów bezpieczeństwa i zgodności przez podmioty z UE z zapewnieniem pełnego dostępu. <i>[Capacity for EU entities to perform independent security and compliance audits with full access.]</i>	Umowy zawierane z klientami OChK przewidują możliwość realizacji audytów klienckich, prowadzonych na zasadach i warunkach określonych w umowie o świadczenie usług. W przypadkach, gdy obowiązek przeprowadzenia audytu lub kontroli wynika z przepisów prawa – na przykład w związku z wymaganiami rozporządzenia DORA – OChK zapewnia współpracę z klientem lub właściwymi organami nadzoru w zakresie przewidzianym zawartą umową (jeśli dotyczy) oraz powszechnie obowiązującymi przepisami prawa. Zakres, forma i tryb realizacji audytów są każdorazowo uzgadniane z klientem lub organem, z uwzględnieniem zasad poufności i bezpieczeństwa środowisk chmurowych.	Określenie zasad realizacji audytów w umowach z klientami oraz współpracy z organami nadzoru w przypadkach przewidzianych przepisami umożliwia przeprowadzanie kontroli w sposób uporządkowany, przewidywalny oraz z zachowaniem zasad bezpieczeństwa informacji. Takie podejście zapewnia przejrzystość działań audytowych oraz pozwala zachować równowagę między potrzebą weryfikacji usług a ochroną integralności, poufności i mechanizmów bezpieczeństwa Platformy OChK.

SOV-8. Zrównoważony rozwój środowiskowy [*Environmental Sustainability*]

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Wdrażanie energooszczędnej infrastruktury (np. o niskim wskaźniku PUE) oraz mierzalnych celów poprawy. <i>[Adoption of energy-efficient infrastructure (e.g., low PUE) and measurable improvement targets.]</i>	OChK utrzymuje infrastrukturę Platformy OChK w centrach przetwarzania danych zarządzanych przez wyspecjalizowanych operatorów stosujących rozwiązania spełniające standardy UE, m.in. dyrektywy EED (Energy Efficiency Directive). Współpraca OChK z operatorami centrów przetwarzania danych obejmuje monitorowanie efektywności energetycznej. Spółka analizuje raporty tych dostawców pod kątem wydajności energetycznej elementów infrastruktury Platformy OChK oraz weryfikuje możliwości jej poprawy. Podjęte działania energooszczędne w infrastrukturze CPD obejmują m.in.: - montaż czujek ruchu oraz stosowanie oświetlenia LED, - zastosowanie free coolingu w systemach klimatyzacji CPD, - montaż instalacji fotowoltaicznej.	Wykorzystywanie nowoczesnych centrów przetwarzania danych, działających zgodnie z branżowymi standardami efektywności energetycznej, pozwala OChK ograniczać ślad węglowy. Monitorowanie i współpraca z operatorami w zakresie zużycia energii umożliwia dalszą optymalizację środowisk przetwarzania danych i wpisują się w cele zrównoważonego rozwoju Unii Europejskiej.

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
Praktyki gospodarki o obiegu zamkniętym zapewniające ponowne wykorzystanie, odnawianie i odpowiedzialną utylizację sprzętu po jego wycofaniu z eksploatacji. [Circular economy practices ensuring reuse, refurbishment, and responsible end-of-life treatment of hardware.]	OChK prowadzi działalność operacyjną uwzględniając zasady zrównoważonego rozwoju i gospodarki o obiegu zamkniętym (<i>circular economy</i>), szczególnie w zakresie infrastruktury IT oraz zarządzania centrami przetwarzania danych. Podejście to zakłada maksymalne wydłużenie cyklu życia sprzętu, ograniczenie odpadów elektronicznych (<i>e-waste</i>) oraz ograniczanie negatywnego wpływu na środowisko poprzez ponowne wykorzystanie, naprawę i certyfikowaną utylizację komponentów. Sprzęt wykorzystywany do świadczenia usług po zakończeniu głównego cyklu eksploatacji jest weryfikowany pod kątem możliwości ponownego użycia w mniej krytycznych środowiskach IT (np. środowiska testowe, szkoleniowe, backupowe).	Wdrażanie zasad gospodarki o obiegu zamkniętym (<i>circular economy</i>) w obszarze infrastruktury IT ogranicza wpływ na środowisko oraz pozwala efektywnie wykorzystywać zasoby sprzętowe w całym cyklu ich życia. Takie podejście wspiera realizację celów zrównoważonego rozwoju i postulatów ESG oraz wpisuje się w unijne inicjatywy dotyczące odpowiedzialnej gospodarki cyfrowej.
Przejrzyste pomiary i ujawnianie emisji dwutlenku węgla, zużycia wody i innych wskaźników zrównoważonego rozwoju.	OChK nie jest objęte obowiązkiem raportowania wynikającym z dyrektywy o sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (CSRD) i w związku z tym nie prowadzi	Obszary związane ze środowiskiem i zrównoważonym rozwojem stanowią jeden z elementów, które spółka zamierza uwzględnić w swojej działalności

Czynnik wpływu	Odpowiedź OChK	Komentarz OChK
<i>[Transparent measurement and disclosure of carbon emissions, water usage, and other sustainability indicators.]</i>	takich pomiarów oraz nie udostępnia sprawozdań w tym zakresie. Niezależnie od powyższego, OChK analizuje raporty operatorów centrów przetwarzania danych pod kątem wydajności energetycznej.	i podejmowanych inicjatywach, kierując się zasadą odpowiedzialnego biznesu. OChK uruchomiło projekt dostosowania się do wymagań CSRD oraz na bieżąco monitoruje zmiany legislacyjne w tym obszarze.
Pozyskiwanie energii odnawialnej lub niskoemisyjnej do zasilania infrastruktury i działalności operacyjnej. <i>[Sourcing of renewable or low-carbon energy to power infrastructure and operations.]</i>	Ponad 20% energii elektrycznej wykorzystywanej do zasilania infrastruktury Platformy OChK pochodzi z odnawialnych źródeł energii (OZE).	OChK monitoruje i zachęca operatorów CPD do zwiększenia udziału energii odnawialnej lub niskoemisyjnej.

5. Podsumowanie – samoocena OChK

Platforma OChK spełnia kluczowe kryteria suwerenności cyfrowej w ośmiu obszarach Cloud Sovereignty Framework. Najsilniejsze z nich to: suwerenność danych, suwerenność prawa i jurysdykcji oraz suwerenność strategiczna, co odzwierciedla solidne fundamenty organizacyjne, prawne i bezpieczeństwa informacji przetwarzanych z wykorzystaniem usług Platformy OChK.

Dzięki lokalizacji infrastruktury w Polsce, niezależności technologicznej kluczowych komponentów, a także stosowaniu ram regulacyjnych UE w zakresie chmury i bezpieczeństwa, OChK plasuje się jako dostawca chmury o wysokim poziomie zaufania i suwerenności.

Poniższe zestawienie przedstawia samoocenę poziomu dojrzałości Platformy OChK dla poszczególnych celów suwerenności:

Cel suwerenności	Waga celu w ocenie	Osiągnięty poziom SEAL	Wynik
SOV-1 Suwerenność strategiczna	15%	SEAL-4	94%
SOV-2 Suwerenność prawna i jurysdykcyjna	10%	SEAL-4	96%
SOV-3 Suwerenność danych i sztucznej inteligencji	10%	SEAL-4	100%
SOV-4 Suwerenność operacyjna	15%	SEAL-4	93%
SOV-5 Suwerenność łańcucha dostaw	20%	SEAL-3	65%
SOV-6 Suwerenność technologiczna	15%	SEAL-3	73%
SOV-7 Suwerenność bezpieczeństwa i zgodności	10%	SEAL-4	93%
SOV-8 Zrównoważony rozwój środowiskowy	5%	SEAL-2	39%
Całkowity wynik suwerenności			82.79%

Biorąc pod uwagę poziomy suwerenności zdefiniowane w Cloud Sovereignty Framework, tzn.:

- **SEAL-0. Brak suwerenności:** usługa, technologia lub działania operacyjne znajdują się pod wyłączną kontrolą stron trzecich spoza UE i podlegają w całości jurysdykcjom państw trzecich;
- **SEAL-1. Suwerenność jurysdykcyjna:** prawo UE ma formalne zastosowanie, lecz jego praktyczna egzekwowalność jest ograniczona; usługa, technologia lub działania operacyjne znajdują się pod wyłączną kontrolą stron trzecich spoza UE;
- **SEAL-2. Suwerenność danych:** prawo UE ma zastosowanie i jest egzekwowalne, przy czym utrzymują się istotne zależności od podmiotów spoza UE; usługa, technologia lub działania operacyjne znajdują się pod pośrednią kontrolą stron trzecich spoza UE;
- **SEAL-3. Odporność cyfrowa:** prawo UE ma zastosowanie i jest egzekwowalne; podmioty z UE sprawują znaczący, lecz niepełny wpływ; usługa, technologia lub działania operacyjne znajdują się pod marginalną kontrolą stron trzecich spoza UE;
- **SEAL-4. Pełna suwerenność cyfrowa:** technologia i działania operacyjne znajdują się pod pełną kontrolą UE i podlegają wyłącznie prawu UE, bez krytycznych zależności od podmiotów spoza UE;

w ocenie OChK, uwzględniając wszystkie określone przez KE cele suwerenności oraz kryteria oceny ich spełnienia, **Platforma OChK jest rozwiązaniem chmurowym w pełni suwerennym cyfrowo (SEAL-4).**

Końcowa ocena poziomu suwerenności, zgodnie z metodyką zalecaną przez Komisję Europejską, powinna zostać przeprowadzona przez zamawiającego, który ocenia dostawcę usługi chmurowej w kontekście własnych wymagań regulacyjnych, organizacyjnych i bezpieczeństwa.



OChK

ulica Grzybowska 62
00-844 Warszawa

kontakt@ochk.pl
www.ochk.cloud



o@hK
we know **the cloud**