OKTAWAVE

Wersja: 20231214

Załącznik nr 3 do Regulaminu

Umowa o powierzenie danych osobowych do przetwarzania

(dalej również: „**Umowa Powierzenia**")

Definicje

Administrator	administrator Danych Osobowych powierzanych Oktawave, który ustala cele i sposoby przetwarzania Danych Osobowych;
Akty Prawne	przepisy prawa obowiązujące Oktawave jako podmiotu przetwarzającego Dane Osobowe w rozumieniu art. 28 RODO w związku z zawarciem Umowy Powierzenia, w tym w szczególności RODO;
Dane Osobowe	dane osobowe w rozumieniu RODO;
Miejsce Przetwarzania	lokalizacje, w których Oktawave przetwarza Dane Osobowe określone w Umowie Powierzenia;
Umowa Główna	umowa o świadczenie usług polegających w szczególności na udostępnieniu Użytkownikowi zasobów Chmury (wirtualne maszyny, moce obliczeniowe, usługi bazodanowe, wirtualne serwery), służących do przechowywania, współdzielenia i przetwarzania danych;
Podpowierzenie	sytuacja, w której Oktawave powierza Dane Osobowe do przetwarzania podmiotowi trzeciemu, który będzie zobowiązany do przetwarzania Danych Osobowych zgodnie z Umową Powierzenia oraz za którego działania w tym zakresie będzie odpowiadać Oktawave na takich samych zasadach jak za własne działania lub zaniechania;
RODO	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;

Preambuła

Zważywszy, że:

1) *Użytkownik przetwarza informacje stanowiące Dane Osobowe,*
2) *Użytkownik zawarł z Oktawave Umowę Główną;*
3) *dane przekazywane przez Użytkownika do Oktawave w związku z Umową Główną obejmują również Dane Osobowe;*

Strony zgodnie postanowiły zawrzeć Umowę Powierzenia o następującej treści:

§ 1
Przedmiot Umowy Powierzenia

1. Użytkownik powierza Oktawave do przetwarzania Dane Osobowe, w zakresie określonym Umową Powierzenia, a Oktawave zobowiązuje się do ich przetwarzania zgodnie z Umową Powierzenia.
2. Przetwarzanie Danych Osobowych przez Oktawave odbywa się w ramach wynagrodzenia ustalonego w Umowie Głównej. Pojęcia niezdefiniowane w niniejszej Umowie Powierzenia, a pisane z wielkiej litery, mają znaczenie nadane im w Umowie Głównej.

§ 2

Oświadczenia Stron

1. Użytkownik oświadcza, że z zastrzeżeniem ust. 2 poniżej jest Administratorem.
2. W każdym przypadku, w którym Dane Osobowe obejmują dane, których Użytkownik nie jest Administratorem, Użytkownik oświadcza, że ich Administratorem jest jego kontrahent, oraz że zgodnie z przepisami prawa oraz porozumieniem z tym kontrahentem jest uprawniony do dalszego powierzania Danych Osobowych do Oktawave, na zasadach określonych Umową Powierzenia.
3. Użytkownik, na żądanie Oktawave uzasadnione w szczególności ew. kontrolą prowadzoną przez właściwe organy nadzoru lub zmianą interpretacji przepisów prawa, niezwłocznie (tj. nie później niż w terminie 3 dni roboczych) doręczy Oktawave w formie elektronicznej aktualną listę Administratorów (kontrahentów), o których mowa w ust. 2 powyżej, zgodnie ze wzorem stanowiącym **Załącznik nr 1** do Umowy Powierzenia.
4. Użytkownik oświadcza, że powierzane Oktawave do przetwarzania Dane Osobowe zostały pozyskane w sposób legalny, a ich powierzenie lub dalsze powierzenie do Oktawave nie narusza przepisów prawa ani praw osób trzecich.
5. Oktawave zobowiązuje się do przetwarzania Danych Osobowych wyłącznie w zakresie niezbędnym do realizacji Umowy Powierzenia oraz Umowy Głównej i w celach w nich określonych.
6. Oktawave oświadcza, że zna i zobowiązuje się do przestrzegania Aktów Prawnych, z zastrzeżeniem ust. 7 poniżej.
7. Gdyby z uwagi na charakter Danych Osobowych lub szczególny status Użytkownika, w związku z zawarciem Umowy Powierzenia Oktawave miałoby podlegać pod szczególne Akty Prawne, które zwykle nie obowiązują przedsiębiorców podobnych do Oktawave i mających siedzibę w Polsce, Użytkownik zobowiązany jest zawiadomić o tym Oktawave na piśmie pod rygorem nieważności, z wyprzedzeniem co najmniej 30 dni, a Oktawave w terminie kolejnych 14 dni będzie uprawniona do rozwiązania Umowy Powierzenia z zachowaniem 7 dniowego okresu wypowiedzenia.

§ 3

Zakres powierzonych Danych Osobowych oraz kategorie przetwarzań

1. Z uwagi na charakter świadczonych przez Oktawave usług, rodzaj Danych Osobowych i kategorie osób, których one dotyczą określane są i kontrolowane przez Użytkownika. w zależności od przypadku Dane Osobowe powierzane Oktawave do przetwarzania mogą obejmować w szczególności: dane kontaktowe; dane pracownicze / współpracownicze; dane dot. rozliczeń i płatności, w tym również dane przetwarzane przez instytucje płatnicze; dane związane z marketingiem; szczególne kategorie danych; inne rodzaje danych zgodnie z umowami zawieranymi przez Oktawave z klientami. w zależności od przypadku Dane Osobowe powierzane Oktawave do przetwarzania mogą dotyczyć w szczególności następujących kategorii osób: pracownicy i współpracownicy Administratora lub podmiotów powiązanych z Administratorem, a także klientów lub dalszych klientów Administratora; klienci usług / produktów Administratora oraz ich dalsi klienci; kontrahenci Administratora lub klientów/dalszych klientów Administratora.
2. Kategorie przetwarzań Danych Osobowych dokonywanych przez Oktawave mogą obejmować w szczególności:
   a. przechowywanie Danych Osobowych w ramach zapewnianej przez Oktawave infrastruktury technicznej/sprzętu związanego ze świadczeniem Chmury, a także zapewnienie możliwości wykorzystywania mocy obliczeniowych tego sprzętu dla przetwarzania Danych Osobowych przez Użytkownika w sposób przez niego wybrany, zgodnie z Umową Główną;
   b. zabezpieczenie fizyczne i utrzymanie fizyczne infrastruktury technicznej/sprzętu związanego ze świadczeniem Chmury, na poziomie Chmury;

c. zapewnienie odpowiednich zabezpieczeń logicznych dostępu do Chmury, na poziomie Chmury (np. szyfrowana transmisja danych, używanie zaawansowanych protokołów komunikacyjnych, wieloetapowa autoryzacja);
d. zapewnienie dostępu do Usług, zgodnie z Umową Główną (w tym SLA), co obejmuje także monitorowanie ruchu z i do Chmury (na poziomie całej Chmury) w celu identyfikacji i ochrony przed działaniami typu ataki DDOS oraz zapewnienia stabilności działania Chmury;
e. udzielenie wsparcia technicznego w ramach wirtualnej maszyny Użytkownika – wyłącznie w przypadku skorzystania z pomocy technicznej, zgodnie z ust. 6 lit. a poniżej;
f. zarządzanie Usługami Użytkownika w ramach wskazanych przez Użytkownika wirtualnych maszyn – wyłącznie w przypadku korzystania z usługi „Cloud Operations", zgodnie z ust. 6 lit. b poniżej.

3. W celu uniknięcia wątpliwości, z zastrzeżeniem ust. 5 - 6 poniżej, Użytkownik samodzielnie administruje tzw. wirtualnymi maszynami, w ramach których przetwarza Dane Osobowe, w tym samodzielnie instaluje wybrane przez siebie oprogramowanie, wdraża zabezpieczenia, tworzy kopie zapasowe oraz realizuje inne obowiązki wynikające z Aktów Prawnych.
4. Użytkownik może zlecić Oktawave tworzenie i utrzymywanie kopii zapasowej Danych Użytkownika, co obejmuje utworzenie kopii zapasowej całej „wirtualnej maszyny" Użytkownika, na szczegółowych zasadach określonych dla tej dodatkowej Usługi.
5. Użytkownik może udzielić Oktawave dostępu do swoich wirtualnych maszyn (w zakresie określonym przez Użytkownika i stosując odpowiednie, dobrane przez siebie zabezpieczenia) poprzez:
   a. utworzenie na wirtualnej maszynie konta administracyjnego dla osoby działającej w imieniu Oktawave, w celu wykonania określonego, doraźnego działania; lub
   b. korzystanie z usługi „Cloud Operations".

   W takim przypadku Użytkownik przekazuje Oktawave instrukcje co do zakresu operacji, jakie mogą zostać wykonane przez osoby działające w imieniu Oktawave, w formie elektronicznej, a Oktawave, poza obowiązkami określonymi w §4 poniżej, zobowiązane jest także do dołożenia należytej staranności, w zakresie w jakim jest to możliwe dla Oktawave, do zapewnienia rozliczalności działań ww. osób w ramach wirtualnych maszyn Użytkownika (tj. logi dokonanych działań oraz możliwość ich przypisania do konkretnej osoby fizycznej) oraz do ich zobowiązania do działania zgodnie z Umową Powierzenia oraz przepisami prawa.

§ 4
Zasady przetwarzania Danych Osobowych

1. Dane Osobowe będą przetwarzane przez Oktawave wyłącznie w celu realizacji na rzecz Użytkownika Usług określonych w Umowie Głównej, zgodnie z Umową Główną oraz niniejszą Umową Powierzenia (charakter i cel przetwarzania), w zakresie kategorii czynności przetwarzania wskazanych w szczególności w § 3 ust. 3 powyżej.
2. Oktawave zobowiązuje się:
   a. przetwarzać Dane Osobowe wyłącznie na udokumentowane polecenie Użytkownika – co dotyczy też przekazywania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki wynika z Aktów Prawnych; w takim wypadku przed rozpoczęciem przetwarzania Oktawave informuje Użytkownika o tym obowiązku prawnym, jeśli Akty Prawne nie zabraniają udzielania takiej informacji z uwagi na ważny interes publiczny;
   b. zapewnić, by osoby upoważnione po stronie Oktawave do przetwarzania Danych Osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   c. podejmować środki wymagane na mocy art. 32 RODO, w zakresie związanym z realizacją niniejszej Umowy Powierzenia, których opis znajduje się w **Załączniku nr 2 oraz Załączniku nr 3** do Umowy Powierzenia;

d. przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego, zgodnie z ust. 5 oraz 6 poniżej;
e. w miarę możliwości i w granicach uzasadnionych charakterem czynności przetwarzania, pomagać Użytkownikowi, stosując odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
f. uwzględniając charakter przetwarzania oraz dostępne Oktawave informacje, pomagać Użytkownikowi wywiązać się z obowiązków określonych w art. 32-36 RODO w zakresie, w jakim jest to wymagane prawem;
g. po zakończeniu przetwarzania Danych Osobowych na podstawie niniejszej Umowy Powierzenia, zależnie od decyzji Użytkownika, usunąć lub zwrócić mu wszelkie Dane Osobowe, zgodnie z § 7 poniżej, usuwając przy tym wszelkie ich kopie, chyba że Akty Prawne nakazują przechowywanie Danych Osobowych;
h. udostępnić Użytkownikowi informacje niezbędne do wykazania spełnienia obowiązków Oktawave określonych w niniejszym ustępie, w granicach uzasadnionych charakterem czynności przetwarzania;
i. umożliwiać Użytkownikowi przeprowadzanie audytów i inspekcji, zgodnie z § 5 poniżej.

3. Oktawave oświadcza, że na dzień zawarcia Umowy Dane Osobowe przetwarzane są wyłącznie na terytorium Rzeczpospolitej Polskiej. Miejsca Przetwarzania mogą znajdować się wyłącznie na terytorium Rzeczpospolitej Polskiej lub Europejskiego Obszaru Gospodarczego.
4. Oktawave może Podpowierzyć Dane Osobowe wyłącznie na zasadach określonych w niniejszym ustępie. Oktawave informuje Użytkownika o zamiarze Podpowierzenia, wskazując podmiot trzeci oraz konkretne czynności przetwarzania, w zakresie jakich będzie korzystać z Podpowierzenia, w formie wiadomości mailowej, co najmniej 30 dni przed planowanym terminem Podpowierzenia. Użytkownik w ciągu 7 dni od otrzymania informacji, o której mowa w zdaniu poprzednim, może zgłosić uzasadniony sprzeciw wobec Podpowierzenia, który przekazuje Oktawave w formie zwrotnej wiadomości mailowej pod rygorem nieważności. W przypadku otrzymania sprzeciwu, Oktawave w okresie kolejnych 5 dni będzie uprawniona do złożenia oświadczenia o rozwiązaniu Umowy Powierzenia z Użytkownikiem, z zachowaniem 14 dniowego okresu wypowiedzenia. W przypadku braku sprzeciwu w ww. terminie, Oktawave może przystąpić do Podpowierzenia.
5. Użytkownik wyraża niniejszym zgodę na Podpowierzenie przetwarzania Danych Osobowych do spółki ATM S.A. z siedzibą w Warszawie, ul. Grochowska 21a, 04-186 Warszawa, tel. 22 51 56 100, info@atman.pl, do POLCOM S.A. z siedzibą w Skawinie, ul. Krakowska 43 (32-050) oraz do Netia S.A. z siedzibą w Warszawie przy ul. Poleczki 13, w zakresie czynności określonych w §3 ust. 3 lit. b powyżej.
6. Użytkownik oświadcza, że zakres Danych Osobowych oraz kategorie czynności przetwarzania objęte Umową nie wymagają i nie będą wymagać w trakcie trwania Umowy Powierzenia stosowania innych niż opisane w Załączniku nr 2 oraz Załączniku nr 3, szczególnych środków do ich przetwarzania albo spełnienia innych, szczególnych warunków (np. uzyskanie zgody, rejestracji, certyfikatu etc.), z zastrzeżeniem zdania następnego. Oktawave w ramach wynagrodzenia określonego w Umowie Głównej zobowiązuje się w terminie 21 dni roboczych od otrzymania zgłoszonego w formie wiadomości mailowej żądania Użytkownika, stosować również inne niż opisane w § 4 Umowy Powierzenia, szczególne środki bezpieczeństwa, jeśli są one dla Oktawave dostępne oraz biznesowo i ekonomicznie uzasadnione z perspektywy Oktawave.
7. Użytkownik zobowiązany jest do stosowania odpowiednich technik kryptograficznych (szyfrowania) względem wszelkich Danych Osobowych na etapie ich przesyłania do/z infrastruktury Oktawave oraz na etapie ich przechowywania w ramach infrastruktury Oktawave (obowiązek szyfrowania wirtualnej maszyny lub dysku, na którym przechowywane są Dane Osobowe), a także stosowania wszelkich innych zabezpieczeń wymaganych zgodnie z RODO w ramach tzw. wirtualnych maszyn, w celu odpowiedniego

zabezpieczenia Danych Osobowych i ich zgodnego z prawem przetwarzania. Oktawave nie odpowiada za skutki naruszenia ww. zobowiązań przez Użytkownika. Na podstawie odrębnych ustaleń Stron istnieje możliwość zapewnienia przez Oktawave w ramach Cloud Operations dedykowanych rozwiązań w zakresie bezpieczeństwa Usług, w tym szyfrowania informacji oraz zarządzania kluczami szyfrującymi.

8. W celu uniknięcia wątpliwości Strony potwierdzają, że realizacja obowiązków wynikających z Aktów Prawnych, w tym z RODO, względem Danych Osobowych przetwarzanych w ramach tzw. wirtualnych maszyn, w szczególności w zakresie zabezpieczeń organizacyjnych oraz technologicznych, a także wykonywania ich kopii bezpieczeństwa, jest obowiązkiem wyłącznie Użytkownika. z zastrzeżeniem §3 ust. 5 i 6 powyżej, Oktawave nie uzyskuje bezpośredniego dostępu do Danych Osobowych oraz nie wykonuje bezpośrednich operacji na tych danych, a jedynie wykonuje operacje na Chmurze jako zestawie technologii oraz danych bez możliwości bezpośredniego ich wyodrębnienia.
9. W każdym przypadku stwierdzenia przez Oktawave naruszenia ochrony Danych Osobowych powierzonych Oktawave do przetwarzania przez Użytkownika Oktawave, bez zbędnej zwłoki, jednak w miarę możliwości nie później niż w ciągu 48 godzin od wykrycia naruszenia, zgłasza je Użytkownikowi w formie wiadomości e-mail. Zawiadomienie będzie obejmowało znane Oktawave i uwzględniające charakter powierzenia informacje o:
   a. charakterze naruszenia, w tym w miarę możliwości będzie wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b. możliwych konsekwencjach naruszenia;
   c. środkach zastosowanych lub proponowanych do zastosowania w celu zaradzenia naruszeniu, w tym w stosownych przypadkach o środkach w celu zminimalizowania jego ewentualnych negatywnych skutków;

   Jeżeli – i w zakresie, w jakim – wyżej wskazanych informacji nie da się udzielić w tym samym czasie, będą udzielane sukcesywnie bez zbędnej zwłoki.

§ 5
Uprawnienia kontrolne

1. Użytkownik jest uprawniony do samodzielnej, a Administratorzy wskazani w Załączniku nr 1 łącznej z Użytkownikiem, kontroli przetwarzania przez Oktawave Danych Osobowych zgodnie z Umową Powierzenia, w postaci audytu lub inspekcji, nie częściej jednak niż w sumie raz na 6 miesięcy. Użytkownik może zlecić na własny koszt przeprowadzenie kontroli profesjonalnemu audytorowi, za którego ponosi odpowiedzialność. w każdym przypadku kontroli Użytkownik powiadamia Oktawave o zamiarze przeprowadzania kontroli, przesyłając jednocześnie plan kontroli, z wyprzedzeniem, nie krótszym niż 14 dni roboczych, a Oktawave zobowiązana jest umożliwić przeprowadzenie kontroli, w szczególności poprzez udostępnienie właściwej dokumentacji i pomieszczeń, w zakresie niezbędnym dla realizacji kontroli oraz udzielić wszelkich niezbędnych informacji dotyczących realizacji postanowień Umowy Powierzenia, z zastrzeżeniem obowiązków Oktawave wynikających z przepisów prawa lub umów zawartych z innymi Administratorami oraz tajemnicy przedsiębiorstwa Oktawave. w przypadku, gdy kontrola mogłaby negatywnie wpłynąć na bieżące funkcjonowanie Oktawave lub podmiotów, którym Oktawave podpowierza wykonywanie określonych czynności, Strony zobowiązują się wspólnie wyznaczyć inny, odpowiedni termin kontroli.
2. Kontrola może być wykonywana w dni robocze w godzinach od 9:30 do 17:30 w sposób nieutrudniający pracy Oktawave lub Miejsca Przetwarzania. Jedna kontrola w tych miejscach nie może trwać dłużej niż łącznie 3 dni robocze. w przypadku gdyby przeprowadzenie kontroli w terminie wskazanym przez Użytkownika zgodnie z ust. 1 powyżej było z obiektywnych przyczyn niemożliwe (np. zbieg terminu z kontrolą prowadzoną przez innego użytkownika), Oktawave niezwłocznie powiadomi o tym Użytkownika i Strony niezwłocznie uzgodnią najbliższy możliwy termin kontroli.

3. Z kontroli Strony sporządzą protokół. Użytkownik może przedstawić zalecenia dotyczące jakości zabezpieczenia Danych Osobowych oraz sposobu ich przetwarzania, sporządzonych w wyniku kontroli, w terminie uzgodnionym przez Strony.
4. Wszelkie koszty kontroli ponosi Użytkownik.
5. Oktawave jest zobowiązana powiadomić Użytkownika o każdej przeprowadzanej u Oktawave kontroli uprawnionych organów państwowych, jeżeli ma ona związek z przetwarzaniem powierzonych przez Użytkownika Danych Osobowych, w terminie do 3 dni roboczych od dnia otrzymania odpowiedniego pisma, wezwania lub informacji o planowanej kontroli.
6. W przypadku, o którym mowa w § 2 ust. 2 Umowy Powierzenia, Oktawave ma prawo do żądania udokumentowania przez Użytkownika uprawnienia do dalszego powierzania Danych Osobowych w każdym czasie, a Użytkownik jest zobowiązany dostarczyć Oktawave stosowne pisemne lub elektroniczne oświadczenie Administratora pod rygorem nieważności, w terminie 5 dni roboczych od dnia otrzymania żądania w formie wiadomości mailowej.

§ 6
Czas trwania Umowy Powierzenia

1. Umowa Powierzenia zostaje zawarta na czas obowiązywania zawartej przez Strony Umowy Głównej, z zastrzeżeniem ust. 2.
2. Rozwiązanie Umowy Głównej w każdym czasie i trybie przez którąkolwiek ze Stron, skutkuje rozwiązaniem Umowy Powierzenia.
3. W przypadku oświadczenia przez Użytkownika, że zaprzestał przetwarzania w ramach Usług Danych Osobowych, Użytkownikowi przysługuje prawo rozwiązania Umowy Powierzenia z zachowaniem jednomiesięcznego okresu wypowiedzenia.

§ 7
Usunięcie Danych Osobowych

1. Użytkownik w każdym czasie może usunąć Dane Osobowe przetwarzane w ramach Usług przykładowo poprzez:
   a. odpowiednie nadpisanie, w ramach samodzielnie wybranego oprogramowania zainstalowanego i wykorzystywanego przez Użytkownika w ramach wirtualnej maszyny oraz określonej przez niego procedury - usunięcie następuje w chwili i na zasadach określonych samodzielnie przez Użytkownika;
   b. usunięcie zaszyfrowanej wirtualnej maszyny Użytkownika – w takim przypadku uniemożliwienie dostępu do danych następuje natychmiast, a ich usunięcie następuje najpóźniej w przeciągu 48h.
2. Użytkownik przez cały okres trwania Umowy Powierzenia ma możliwość dowolnego eksportowania Danych Osobowych, poprzez:
   a. eksport poszczególnych baz danych / programów, które samodzielnie tworzy i którymi zarządza Użytkownik, w formatach właściwych dla tych baz danych / programów (funkcjonalności zarządzane przez Użytkownika);
   b. eksport zestawu danych składających się na całą wirtualną maszynę Użytkownika, w formacie VMware (funkcjonalność zapewniana przez Usługodawcę).
3. Najpóźniej do chwili:
   a. rozwiązania Umowy Powierzenia lub Umowy Głównej;
   b. wyczerpania się posiadanych przez Użytkownika Jednostek Taryfowych (dotyczy Użytkowników Pre-Paid);

   Użytkownik zobowiązany jest do eksportu Danych Osobowych zgodnie z ust. 2 powyżej oraz zapewnienia, aby wszelkie Dane Osobowe zostały usunięte z Chmury zgodnie z ust. 1 powyżej.

4. Niezależnie od postanowień ust. 3 powyżej, Oktawave w terminie do 14 dni od rozwiązania Umowy Głównej lub wyczerpania się posiadanych przez Użytkownika Jednostek Taryfowych (dotyczy Użytkowników Pre-Paid), usuwa wirtualne maszyny Użytkownika, które nie zostały uprzednio usunięte przez Użytkownika, co powoduje natychmiastową utratę dostępu do przechowywanych tam danych oraz ich usunięcie w przeciągu najpóźniej kolejnych 14 dni.
5. Oktawave oświadcza, że w przypadku prawidłowego wykonania przez Użytkownika czynności określonych w ust. 1 powyżej, Oktawave z chwilą tam określoną nie posiada i nie przetwarza kopii usuniętych Danych Osobowych, co w okresie trwania Umowy Powierzenia lub 30 dni po jej rozwiązaniu potwierdzi, na żądanie Użytkownika, w formie wiadomości e-mail.
6. Strony mogą określić w Umowie Głównej odrębne zasady zakończenia współpracy niż opisane w niniejszym paragrafie.

§ 8
Odpowiedzialność

1. Oktawave odpowiada za szkody wyrządzone Użytkownikowi oraz osobom trzecim (w tym zwłaszcza inni Administratorzy) w związku z wykonywaniem Umowy Powierzenia wyłącznie na zasadach i w granicach określonych w Umowie Głównej. Powyższa odpowiedzialność obejmuje także odpowiedzialność Oktawave za podmioty, którym Oktawave Podpowierzył przetwarzanie Danych Osobowych zgodnie z Umową Powierzenia.
2. Użytkownik zobowiązany jest do zapewnienia realizacji postanowienia wynikającego z ust. 1 powyżej, w ramach odpowiednich umów z właściwymi podmiotami trzecimi, w granicach dopuszczalnych prawem.

§ 9
Postanowienia końcowe

1. Oktawave jest uprawniona do jednostronnej aktualizacji treści Załączników nr 2 lub 3 w formie wiadomości e-mail pod rygorem nieważności, w przypadku zmiany przez Oktawave lub przez podmiot, któremu Oktawave Podpowierzyła Dane Osobowe do przetwarzania, zakresu stosowanych rozwiązań / zabezpieczeń, pod warunkiem że będą one spełniały wymogi określone w RODO. Użytkownik, w przypadku uznania, że zmiany wprowadzone przez Oktawave zgodnie ze zdaniem poprzednim są niezgodne z RODO, zawiadomi o tym Oktawave w terminie 14 dni od aktualizacji, w formie zwrotnej wiadomości e-mail.
2. W sprawach nieuregulowanych Umową Powierzenia znajdują zastosowanie odpowiednie przepisy powszechnie obowiązującego prawa oraz postanowienia Umowy Głównej.
3. W przypadku gdy te same kwestie zostały odmiennie uregulowane w Umowie Powierzenia oraz Umowie Głównej, stosuje się postanowienia Umowy Powierzenia.

Lista załączników:

1. Załącznik Nr 1 – WZÓR: lista Administratorów;
2. Załącznik Nr 2 – Stosowane procedury bezpieczeństwa w Oktawave S.A.;
3. Załącznik Nr 3 – Opis organizacji i sposobów zabezpieczenia zasobów informacyjnych u poddostawców.

Załącznik nr 1 – WZÓR: lista Administratorów

Lp.	Nazwa / imię i nazwisko Administratora i jego reprezentanta (jeśli posiada)	Adres siedziby Administratora	Adres e-mail Administratora	Imię i nazwisko, e-mail inspektora ochrony danych (jeśli posiada)

OKTAWAVE

Załącznik nr 2 Stosowane procedury bezpieczeństwa

Oktawave świadczy usługi objęte zakresem Umowy Powierzenia nieprzerwanie od 2014 roku. Aktualnie pośród dziesiątek podmiotów, które zleciły Oktawave świadczenie usług chmurowych, są klienci z tak wymagających branż jak ochrona zdrowia czy ubezpieczenia.

W działalności Oktawave stosowane są w szczególności następujące środki prawne, techniczne i organizacyjne, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa dla zakresu usług świadczonych przez Oktawave:

1. rozwiązania prawne:

    a. Oktawave jest spółką akcyjną zarejestrowaną w Polsce. Oktawave jest właścicielem (pełna, wyłączna kontrola) całej infrastruktury wykorzystywanej do świadczenia Usług, w tym serwerów, systemów pamięci masowej, przełączników sieciowych, szkieletowych oraz sieci danych, jak również routerów i okablowania;

    b. wszystkie osoby działające w imieniu Oktawave przy przetwarzaniu danych osobowych, których administratorem lub podmiotem przetwarzającym jest Oktawave, zobowiązały się do zachowania tych informacji w tajemnicy oraz niewykorzystywania w jakimkolwiek celu innym niż związany z realizacją ich obowiązków służbowych;

    c. naruszenie zobowiązania do poufności, o którym mowa w lit. a powyżej, co do zasady będzie stanowiło przestępstwo przeciwko ochronie informacji (art. 266 i następne ustawy z dnia 6 czerwca 1997 r. Kodeks karny) i osoby, których to zobowiązanie dotyczy, zostały o tym fakcie pouczone;

    d. Oktawave zna i stale dąży do pełnej realizacji obowiązków nakładanych na nią przez właściwe przepisy, w tym w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, w tym także na bieżąco monitoruje oraz uwzględnia w niezbędnym zakresie opinie i wytyczne właściwych organów nadzoru, takich jak Europejska Rada Ochrony Danych;

    e. wszelkie umowy dotyczące powierzenia przez Oktawave danych osobowych do przetwarzania podmiotowi trzeciemu, gdzie Oktawave działa jako administrator lub jako procesor, spełniają wymogi RODO i są zawierane wyłącznie z podmiotami, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO, w tym posiadają odpowiednie doświadczenie oraz renomę;

    f. Oktawave nieprzerwanie posiada polisę ubezpieczeniową od roszczeń z tytułu odpowiedzialności zawodowej konsultantów komputerowych, obejmującą swoim zakresem usługi świadczone przez Oktawave oraz działania personelu Oktawave.

2. rozwiązania organizacyjne:

a. Oktawave posiada i wdrożyła w szczególności następujące polityki związane z bezpieczeństwem przetwarzania danych osobowych:
   - polityka bezpieczeństwa danych osobowych;
   - instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
   - polityka bezpieczeństwa informacji zgodna ze standardem ISO 27001;
   - polityka zarządzania dostępem zgodna ze standardem ISO 27001.

   Wyciągi z powyższych polityk (nie obejmujące informacji ściśle poufnych, których ujawnienie mogłoby obniżyć poziom bezpieczeństwa danych) dostępne są dla administratorów danych osobowych lub wskazanych przez nich audytorów do wglądu w siedzibie Oktawave, po uprzednim uzgodnieniu terminu.

b. Oktawave posiada aktualny Certyfikat Systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001:2013 wydany przez British Standards Institution z numerem certyfikatu IS 630529 oraz Certyfikat CSA STAR wydany przez British Standards Institution z numerem certyfikatu STAR 657851. Oktawave posiada również certyfikaty ISO/IEC 27017 (bezpieczeństwo informacji w chmurze obliczeniowej) oraz ISO/IEC 27018 (dobre praktyki zabezpieczania danych osobowych w chmurze obliczeniowej;

c. Oktawave uzyskało certyfikat zgodności Systemu Zarządzania Ciągłością Działania ze standardem ISO 22301. Oznacza to, że Oktawave w ramach chmury:
   - prowadzi nadzór i zarządzanie obszarem ciągłości działania w sposób usystematyzowany, zdefiniowany i udokumentowany;
   - wdrożyła odpowiednie systemy i zabezpieczenia w celu zapewnienia nieprzerwanego działania krytycznych zasobów i procesów;
   - systematyczne testuje wdrożone rozwiązania i plany awaryjne, uwzględniając różnorodne scenariusze incydentów;
   - przeprowadza audyty wewnętrzne i zewnętrzne, mające na celu niezależną i obiektywną ocenę skuteczności Systemu Zarządzania Ciągłością Działania;
   - realizuje ciągłe doskonalenie, poprzez analizę wyników testów i audytów oraz wdrożenie działań naprawczych i korygujących;

d. Oktawave od dnia 14 maja 2013 roku posiada Administratora Bezpieczeństwa Informacji, który po wejściu w życie RODO został zastąpiony Inspektorem Ochrony Danych;

e. wdrożona jest procedura aktualizacji systemów/programów - systemy aktualizowane są cyklicznie, zgodnie z ustalonym harmonogramem. w przypadku, kiedy wystąpi błąd/podatność, która znacząco wpływa na bezpieczeństwo środowiska, aktualizacje wykonywane są bezzwłocznie, z pominięciem ustalonego harmonogramu;

f. stosowane są rozwiązania z zakresu tzw. utwardzania systemów (ang. hardening), zgodnie z przyjętymi zasadami best best practice, zarządzane przy pomocy serwera automatycznej konfiguracji;

g. Każda osoba należąca do personelu Oktawave posiada własny identyfikator (login+hasło) oraz imienny certyfikat SSL, którym posługuje się w ramach organizacji. Dostęp dla każdej

osoby i poziom jej uprawnień przyznawany jest zgodnie z polityką najmniejszych uprawnień i wyłącznie celu w realizacji zadań służbowych;

h. wszystkie osoby działające w imieniu Oktawave uczestniczą w okresowych szkoleniach z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji;

3. rozwiązania techniczne:

a. w zakresie danych autoryzacyjnych Użytkownika, nie są one przechowywane przez Oktawave – stosowany jest mechanizm Active Directory, przechowywany jest wyłącznie hash hasła;

b. wszelkie dane przesyłane pomiędzy serwerami Oktawave na poziomie Chmury są przesyłane w postaci zaszyfrowanej – SSL;

c. konfiguracja systemów wykorzystywanych na poziomie Chmury wykonywana jest z centralnego systemu zarządzającego konfiguracją, dodatkowo serwery posiadają lokalnie mechanizm umożliwiający śledzenie zmian w konfiguracji;

d. infrastruktura Oktawave umożliwia wykorzystywanie przez Użytkowników w ramach ich maszyn wirtualnych wszelkich znanych rozwiązań technologicznych mogących służyć zapewnieniu bezpieczeństwa przechowywanych danych osobowych, w tym możliwość pseudonimizacji lub szyfrowania przechowywanych danych, stosowania rozwiązań typu VPN itp. Każdy Użytkownik przechowujący dane osobowe w ramach maszyn wirtualnych zobowiązany jest do szyfrowania tych maszyn (stosowania rozwiązań kryptograficznych);

e. dostęp do wewnętrznej sieci Oktawave służącej do zarządzania Chmurą oparty jest o autoryzację wieloetapową, dodatkowo występuje segmentacja sieci, gdzie dany użytkownik wewnętrzny ma dostęp jedynie do wydzielonej części infrastruktury;

f. infrastruktura podlega testom bezpieczeństwa - stosowane są mechanizmy automatycznego wykrywania podatności, wszystkie systemy skanowane są na bieżąco (testy uruchamiane zgodnie z harmonogramem), pod kątem aktualnie opublikowanych podatności (CVE). Oktawave korzysta również z usług firm zewnętrznych, które cyklicznie przeprowadzają audyt bezpieczeństwa infrastruktury (DSS) oraz niezwłocznie wdraża ew. rekomendacje;

g. stosowany jest monitoring funkcjonowania infrastruktury w trybie 24/7/365 w celu wykrywania awarii – wykorzystywane są zarówno wewnętrzne jak i zewnętrzne, zautomatyzowane narzędzia do monitorowania sieci, a w przypadku wystąpienia awarii inżynier Oktawave dostępny jest całą dobę.

Załącznik nr 3 - opis organizacji i sposobów zabezpieczenia zasobów informacyjnych u poddostawców.

Załącznik zawiera spis zabezpieczeń mających wpływ na utrzymanie bezpieczeństwa w procesach, w których dochodzi do przetwarzania danych osobowych w ATM S.A., POLCOM S.A. i NETIA S.A.

ATM S.A

W kontekście klasyfikacji zabezpieczeń dla procesów, w których przetwarzane są dane osobowe, szczególną uwagę w ***ATM*** zwraca się na zgodność z przepisami Rozporządzenia o Ochronie Danych Osobowych (RODO), co oznacza ciągłe monitorowanie i identyfikowanie wszystkich wynikających zobowiązań prawnych, nadzorczych, umownych oraz systemowego podejścia do ich przestrzegania. Przy doborze sposobów zabezpieczenia uwzględnia się najlepsze praktyki i technologie dostępne dla danej kategorii zabezpieczeń w celu ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów służących do przetwarzania danych osobowych oraz usług przetwarzania. Skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych poddawana jest regularnym testowaniem, mierzeniem i ocenianiem.

1. Zabezpieczenia organizacyjne
   a. ***ATM*** posiada dokumentację, która reguluje sposób organizacji systemu ochrony danych osobowych – Polityka Ochrony Danych Osobowych w ATM S.A.,
   b. ***ATM*** posiada Procedurę Zarządzania Incydentami gwarantującą możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   c. ***ATM*** posiada wyznaczonego Inspektora Ochrony Danych,
   d. ***ATM*** posiada certyfikowany Zintegrowany System Zarządzania spełniający wymogi normy ISO 27001 oraz ISO 9001 mający bezpośredni wpływ na bezpieczeństwo usług,
   e. wszyscy pracownicy i współpracownicy ***ATM*** zostali upoważnieni do przetwarzania danych osobowych,
   f. dla pracowników i współpracowników ***ATM*** przeprowadza szkolenia wstępne i okresowe z ochrony danych osobowych.

2. Bezpieczeństwo fizyczne i środowiskowe
   a. ***ATM*** zapewnia całkowitą kontrolę przepływu osób i pojazdów na terenie całego obszaru administracyjnego - nadzór realizowany jest przez zewnętrzną, koncesjonowaną firmę ochrony mienia,
   b. obiekty ***ATM*** podzielone są na strefy bezpieczeństwa a przemieszczanie w strefach wspierane jest Systemem Kontroli Dostępu zapewniającym całkowitą rozliczalność i kontrolę uprawnień dostępu,
   c. obiekty ***ATM*** monitorowane są przez System Telewizji Dozorowej CCTV,
   d. obiekty ***ATM*** posiadają System Sygnalizacji Włamania i Napadu włączony w system monitoringu koncesjonowanej firmy ochrony mienia gwarantujący dojazd uzbrojonych patroli interwencyjnych,
   e. obiekty ***ATM*** posiadają System Przeciwpożarowy oraz wyposażone są w wielostrefową instalację gaśniczą typu INERGEN®,

f. sygnały z systemów bezpieczeństwa są odbierane i monitorowane w trybie ciągłym (w tym dotyczące infrastruktury sieciowej, zasilania energetycznego i bezpieczeństwa serwerowni, obiektów administracyjno-biurowych i innych ważnych zasobów wykorzystywanych do świadczenia usług przez ATM) – systemy te są regularnie testowane,

g. ciągłość działania procesów w serwerowniach realizowana jest poprzez kaskadowy i redundantny system zasilania rezerwowego obejmujący m.in. UPS, dedykowane agregaty prądotwórcze i redundantne stacje zasilania.

h. następujące służby zabezpieczenia infrastruktury i bezpieczeństwa pracują w trybie ciągłym, tj. 24/7/365:
   - obsługa techniczna i recepcyjna,
   - ochrona terenu i budynków centrum danych (koncesjonowana firma ochrony mienia),
   - Customer Service oraz NOC (Centrum Operacyjne Sieci).

i. fizyczny dostęp do platformy sprzętowej, na bazie której świadczona jest usługa ograniczony jest tylko do wybranej grupy opiekunów-inżynierów. Dostęp zarówno osób trzecich jak i pracowników ***ATM*** spoza tej grupy jest zabroniony i podlega ścisłej kontroli.

POLCOM S.A.

Zabezpieczenie przetwarzania danych osobowych

1. W celu ochrony przetwarzania danych osobowych zastosowano następujące organizacyjne środki bezpieczeństwa:
   a) dopuszczane do przetwarzania danych osobowych są jedynie osoby, które uzyskały indywidualne upoważnienie do przetwarzania danych osobowych;
   b) dane osobowe przetwarzane są jedynie na terenie Europejskiego Obszaru Gospodarczego i nie mogą być przekazywane do państw spoza tego obszaru;
   c) obszar, na którym dochodzi do przetwarzania danych osobowych, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych poprzez zamykanie drzwi wejściowych do danego obszaru;
   d) zabezpieczenie powyższe, odbywa się poprzez zamknięcie danego obszaru przez ostatnią osobę opuszczającą dany obszar danego dnia oraz otwarcie go przez pierwszą osobę wchodzącą do danego obszaru danego dnia, a także zamykanie go w ciągu dnia w przypadku, gdy na danym obszarze nikt nie przebywa;
   e) przebywanie osób nieuprawnionych do przetwarzania danych osobowych na chronionym obszarze, jest możliwe jedynie w przypadkach:
      - posiadanie imiennego upoważnienia, wydanego przez członka Zarządu Spółki lub Inspektora Ochrony Danych lub jego zastępcę;
      - w obecności osoby upoważnionej do przetwarzania danych osobowych;
      - pod ciągłym nadzorem wizyjnym;
   f) każda osoba, która ma zostać upoważniona do przetwarzania danych osobowych zostaje zapoznana z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami dotyczącymi danych osobowych, a także innymi kwestiami związanymi z ochroną danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych;

g) uprawnienie do przetwarzania danych osobowych nadaje indywidualnie członek Zarządu Spółki, Inspektor Ochrony Danych lub inna osoba upoważniona przez Zarząd Spółki;
h) z podmiotami, którym Spółka powierza przetwarzanie danych osobowych, podpisywane są umowy na piśmie o powierzeniu przetwarzania danych osobowych;
i) całodobowa ochrona fizyczna 24/7 Polcom Data Center: koncesjonowani pracownicy ochrony, koncesjonowanej agencji ochrony mienia, grupa interwencyjna 24/7.

2. W celu ochrony przetwarzania danych osobowych zastosowano następujące techniczne środki bezpieczeństwa w Polcom Data Center:
a) rozbudowany system kontroli dostępu i antywłamaniowy;
b) wielostopniowa kontrola dostępu;
c) system telewizji dozorowej;
d) stały monitoring CCTV;
e) system monitorowania budynku (BMS) kontrolujący pracę wszystkich urządzeń w centrum danych;
f) redundantny system gaszenia, podwójny zestaw butli;
g) wydzielone strefy pożarowe o odpowiedniej odporności ogniowej;
h) wykrywanie pożaru oparte na systemie wczesnej detekcji dymu;
i) system gaszenia gazem neutralnym dla ludzi, sprzętu i środowiska;
j) dwa podziemne przyłącza energetyczne średniego napięcia;
k) dystrybucja zasilania w układzie 2N;
l) rezerwowe agregaty prądotwórcze;
m) system podtrzymania zasilania UPS;
n) zbiorniki paliwa zapewniające nieprzerwane zasilanie agregatów prądotwórczych;
o) rozbudowany system monitorowania parametrów zasilania;
p) dwa niezależne źródła chłodu;
q) redundantny system klimatyzacji precyzyjnej;
r) systemy informatyczne i aplikacje służące do przetwarzania danych osobowych są regularnie aktualizowane, weryfikowane pod kątem podatności na ataki oraz zabezpieczone przez systemy antywirusowe;
s) stosuje się ochronę przed nieuprawnionym dostępem do systemów i sieci przez zaporę ogniową (firewall);
t) stosuje się systemy monitorujące ruch sieciowy, a wykrywane anomalie są logowane i raportowane.

NETIA S.A.

Data center jest certyfikowane klasie trzeciej zgodnie z normą EN/PN50600
(europejski standard obejmujący szczegółowe wymagania wobec infrastruktury krytycznej i systemów bezpieczeństwa centrów danych, opracowany przez Europejski Komitet Normalizacyjny Elektrotechniki – CENELEC - zatwierdzony przez Komisję Europejską)

Jednocześnie w obiekcie wdrożone są odpowiednie środki organizacyjne i techniczne w celu zabezpieczenia danych, w tym danych osobowych.

1. **W celu ochrony przetwarzania danych zastosowano następujące organizacyjne środki bezpieczeństwa:**
   a. dostęp do obiektu opiera się na Systemie Kontroli Dostępu (SKD), wliczając w to przyznawanie pracownikom i osobom autoryzowanym karty dostępu;
   b. dostęp do obiektu osób, które nie mają kart dostępu jest szczegółowo uregulowany w wewnętrznych procedurach obiektu;
   c. cały obiekt wraz z przylegającym placem są otoczone ogrodzeniem.
   d. kontroli podlegają pojazdy wjeżdżające, jak i wyjeżdżające z obiektu;
   e. wszyscy pracownicy obiektu zostali przeszkoleni z zakresu ochrony danych (w tym danych osobowych), a jednocześnie przechodzą cykliczne szkolenia aktualizacyjne w tym zakresie;
   f. wszyscy pracownicy oraz współpracownicy w ramach obiektu zobowiązani są do zachowania poufności informacji związanych z bezpieczeństwem obiektu oraz do niewykorzystania tych informacji w żadnym innym celu poza obowiązkami służbowymi;
   g. zabronione jest samowolne fotografowanie lub jakiekolwiek utrwalanie na dowolnych nośnikach jakichkolwiek elementów znajdujących się z obiekcie;
   h. podmioty korzystające z obiektu mogą instalować urządzenia, które:
      - są w pełni sprawne i mogą być eksploatowane na terenie Rzeczpospolitej Polskiej oraz do których zapewnione jest posiadanie tytułu prawnego pozwalającego na zainstalowanie w obiekcie;
      - posiadają wymagane prawem pozwolenia, opinie techniczne i ekspertyzy, które podmiot korzystający musi udostępnić na żądanie operatora obiektu;
      - posiadają trwałe oznaczenia pozwalające na ich jednoznaczną identyfikację.

2. **W celu ochrony przetwarzania danych zastosowano następujące techniczne środki bezpieczeństwa:**
   a. klimatyzacja precyzyjna (pracuje w układzie N+1), która składa się z niezależnych zespołów klimatyzacyjnych; każdy z zespołów jest wyposażony we własny układ regulacyjny; przez serwerownie nie przebiegają żadne instalacje niezwiązane z obsługą tych pomieszczeń;
   b. układ zasilania 3N/2, z wykorzystaniem 3 niezależnych torów, zgodny z zasadą nadmiarowości 2N; pojedynczy tor może być w każdej chwili wyłączony (np. dla celów serwisowych);
   c. system zasilania bezprzerwowego UPS (*Uninterruptible Power Supply*) oraz w agregaty prądotwórcze; systemy te tworzą redundantne źródło zasilania;
   d. podtrzymywanie awaryjne wykorzystujące system DRUPS;
   e. 2 niezależne obwody zasilające;
   f. 2 przyłącza zasilające z miejskiej sieci energetycznej;
   g. system wczesnej detekcji dymu;
   h. sygnalizacja pożarowa z monitoringiem sygnału do Państwowej Straży Pożarnej;
   i. stałe urządzenia gaśnicze;
   j. monitoring (CCTV);
   k. system sygnalizacji włamania i napadu (SSWiN);
   l. obiekt opiera się na współdziałaniu systemów ochrony technicznej (m.in. SSWiN, SKD, CCTV) z ochroną fizyczną;
   m. system BMS, który integruje alarmy systemów detekcyjnych, w tym czujek obecności wody, czujek obecności gazu, czujek przekroczenia granicy temperatury, czujek pożarowych, zasilania.