

1. PRZEDMIOT DODATKU OUTSOURCINGOWEGO

- 1.1. NTT Poland sp. z o.o. ("**NTT**" lub po prostu my) świadczy usługi teleinformatyczne na rzecz swoich Klientów będących podmiotami sektora finansowego w rozumieniu art. 2 DORA. DORA i odpowiednie przepisy krajowe nakładają obowiązki i promują dobre praktyki zarówno dla podmiotów sektora finansowego, jak i dostawców usług ICT.
- 1.2. Ze względu na to, że nasi dostawcy ("**Sprzedawca**" lub po prostu Ty) działają jako nasi podwykonawcy, pewne obowiązki regulacyjne i najlepsze praktyki są wiążące dla naszych stosunków umownych. Te obowiązki i najlepsze praktyki znajdują odzwierciedlenie w niniejszym dokumencie, wdrażającym przepisy outsourcingowe do naszego Odpowiedniego Zamówienia ("**Dodatek Outsourcingowy**").
- 1.3. Dodatek Outsourcingowy określa Wasze obowiązki wynikające z DORA i obowiązujących przepisów krajowych w związku z Obowiązującym Zamówieniem.
- 1.4. Niniejszy Dodatek Outsourcingowy i jego wiążące warunki są dołączone do Odpowiedniego Zamówienia zawartego na piśmie lub w równoważnej formie.
- 1.5. W przypadku jakichkolwiek rozbieżności pomiędzy Obowiązującym zamówieniem, Umową ramową i Dodatkiem Outsourcingowym, zastosowanie ma następująca kolejność pierwszeństwa:
 - 1.5.1. Odpowiednie Zamówienie;
 - 1.5.2. Dodatek Outsourcingowy;
 - 1.5.3. Umowa ramowa.

2. DEFINICJE

- 2.1. Poniższe terminy mają następujące znaczenie:
 - 2.1.1. **Umowa:** o ile ma zastosowania - Umowa ramowa ze Sprzedawcą, która reguluje relacje nawiązane między NTT a naszymi dostawcami poprzez podpisanie Odpowiedniego Zamówienia
 - 2.1.2. **Organ:** każdy organ władzy publicznej sprawujący nadzór nad działalnością NTT, w tym Komisja Nadzoru Finansowego (KNF), Narodowy Bank Polski (NBP), Generalny Inspektor Ochrony Danych Osobowych (GIODO), Generalny Inspektor Informacji Finansowej (GIIF) oraz Europejskie Organy Nadzoru (EUN) w rozumieniu pkt 7 DORA.
 - 2.1.3. **DORA:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 i (UE) 2016/1011.

- 2.1.4. **Komunikat KNF:** komunikat Biura Komisji Nadzoru Finansowego dotyczący przetwarzania informacji o podmiotach nadzorowanych w publicznej lub hybrydowej chmurze obliczeniowej z dnia 23 stycznia 2020 r.
 - 2.1.5. **ICT:** technologie informacyjne i komunikacyjne.
 - 2.1.6. **RTO:** Recovery Time Objective, czas od awarii systemu informatycznego do jego przywrócenia do działania.
 - 2.1.7. **RPO:** Recovery Point Objective, maksymalny czas od ostatniej kopii zapasowej danych do awarii usługi w chmurze. Oznacza to również potencjalne ryzyko (akceptowane przez nadzorowany podmiot), że wyniki przetwarzania informacji mogą zostać utracone na określony czas
- 2.2. Pozostałe terminy pisane wielką literą mają takie samo znaczenie jak w Umowie ramowej.

3. ODPOWIEDNIE PRZEPISY

- 3.1. Każda ze stron Odpowiedniego Zamówienia będzie przestrzegać przepisów prawa oraz odpowiednich wytycznych i zaleceń wydanych przez Organy w zakresie, w jakim mają one zastosowanie do Odpowiedniego Zamówienia, w szczególności:
 - 3.1.1. DORA
 - 3.1.2. wytyczne Europejskiego Urzędu Nadzoru Bankowego w sprawie outsourcingu z dnia 25 lutego 2019 r. (EBA/GL/2019/02);
 - 3.1.3. komunikat Biura Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 r. w sprawie przetwarzania informacji o podmiotach nadzorowanych w publicznej lub hybrydowej chmurze obliczeniowej.
- 3.2. Jeśli w okresie obowiązywania Odpowiedniego Zamówienia wejdą w życie nowe przepisy prawa lub zostaną wydane nowe wytyczne lub zalecenia Władz, strony zastosują się do nich. Jeśli będzie to wymagało zmiany Odpowiedniego Zamówienia lub sposobu jego realizacji, niezwłocznie rozpoczniemy negocjacje w dobrej wierze w celu wdrożenia odpowiednich zmian.

4. LOKALIZACJA

- 4.1. Zleczone lub podzleczone funkcje oraz usługi ICT, a także miejsca przetwarzania i przechowywania danych są określone w Obowiązującym Zamówieniu. Jeżeli lokalizacja nie jest określona w Obowiązującym Zamówieniu, usługi i przechowywanie danych objęte umową lub podwykonawcą powinny odbywać się na obszarze EOG.
- 4.2. W przypadku zamiaru zmiany miejsca świadczenia usług teleinformatycznych, przetwarzania danych lub ich przechowywania, musisz powiadomić nas o tym fakcie z wyprzedzeniem. Wypowiedzenie musi być złożone w formie pisemnej z zachowaniem co najmniej jednomiesięcznego okresu wypowiedzenia.

- 4.3. Zastrzegamy sobie prawo do sprzeciwienia się zmianie lokalizacji w ciągu 2 tygodni od otrzymania powiadomienia. W takiej sytuacji rozpoczniemy negocjacje dwustronne. Jeśli nie dojdziemy do porozumienia, NTT ma prawo do wypowiedzenia Odpowiedniego Zamówienia ze skutkiem natychmiastowym.

5. UPRAWNIENIA KONTROLNE I AUDYTOWE

- 5.1. NTT, Klienci i Organ są uprawnieni do przeprowadzania audytów i inspekcji w okresie obowiązywania Odpowiedniego Zamówienia.
- 5.2. Częstotliwość przeprowadzania audytów i inspekcji oraz obszary, które mają być audytowane, zostały określone w Obowiązującym Zarządzeniu.
- 5.3. W przypadku, gdy częstotliwość audytów nie jest określona w Obowiązującym Zamówieniu, audyt lub inspekcja mogą być przeprowadzane przez NTT lub Klienta raz na kwartał. Jednakże w przypadku uzasadnionego podejrzenia niewykonania lub nienależytego wykonania Odpowiedniego Zamówienia, w każdym czasie może zostać przeprowadzony audyt lub inspekcja.
- 5.4. Jeżeli zakres audytu nie jest określony w Obowiązującym Zamówieniu, NTT i Klient są uprawnieni do przeprowadzenia audytu i kontroli każdego obszaru usług świadczonych przez Ciebie w ramach Odpowiedniego Zamówienia.
- 5.5. W trakcie audytu lub inspekcji Organy są uprawnione do sprawdzenia pomieszczeń i dokumentacji dotyczącej przetwarzania informacji, procesów i procedur, organizacji, zarządzania oraz certyfikatów zgodności – w związku z Obowiązującym Zarządzeniem.
- 5.6. W przypadku audytu lub inspekcji zapewnicie pełną współpracę z NTT lub Klientem oraz osobami przez nich upoważnionymi, a także z Organami i osobami upoważnionymi przez Organy. Jesteś zobowiązany do przestrzegania instrukcji i wytycznych po audytowych lub pokontrolnych.
- 5.7. Jesteś zobowiązany do niezwłocznego informowania nas o wszelkich zmianach, które mogą mieć wpływ na prawidłowe wykonanie jego zobowiązań objętych Obowiązującym Zamówieniem.
- 5.8. W przypadku jeśli przeprowadzasz audyt wewnętrzny lub podlegasz audytowi zewnętrznemu (strony trzeciej), jesteś zobowiązany do niezwłocznego poinformowania nas o:
- 5.8.1. o wystąpieniu takiego audytu lub kontroli – nie później niż w terminie 7 dni od dnia rozpoczęcia audytu lub kontroli, oraz
 - 5.8.2. o wynikach audytu lub kontroli – nie później niż w terminie 7 dni od zakończenia audytu lub kontroli.
- 5.9. Jesteś zobowiązany do pełnej współpracy z właściwymi Organami, jak również z osobami wyznaczonymi przez Klienta lub NTT.

6. PLANY AWARYJNE

- 6.1. Po zawarciu Odpowiedniego Zamówienia NTT dostarczy Ci biznesowy plan awaryjny ustalony między NTT a Klientem. W przypadku zmiany/aktualizacji planu, NTT niezwłocznie poinformuje Cię o tym.
- 6.2. Jesteś zobowiązany do wdrożenia i testowania swojego biznesowego planu awaryjnego, który jest zgodny z planami NTT i Klienta oraz posiada środki, narzędzia i polityki bezpieczeństwa teleinformatycznego, które zapewniają odpowiedni poziom bezpieczeństwa świadczenia usług przez Klienta zgodnie z jego ramami regulacyjnymi.
- 6.3. Twój biznesowy plan awaryjny będzie obejmował pełen zakres usług świadczonych w ramach Odpowiedniego Zamówienia.
- 6.4. Jesteś zobowiązany do uczestnictwa, na żądanie, w testach biznesowego planu awaryjnego NTT lub Klienta.
- 6.5. OŚWIADCZASZ, ŻE POSIADASZ DOBRĄ SYTUACJĘ FINANSOWĄ, UMOŻLIWIAJĄCĄ NIEPRZERWANE PROWADZENIE DZIAŁALNOŚCI OBJĘTEJ OBOWIĄZUJĄCYM ZAMÓWIENIEM.
- 6.6. Na żądanie, bez zbędnej zwłoki, dostarczysz kopię swojego biznesowego planu awaryjnego. O wynikach testów biznesowego planu awaryjnego informujesz NTT niezwłocznie po ich przeprowadzeniu.

7. BEZPIECZEŃSTWO IT

- 7.1. Jesteś zobowiązany do przestrzegania odpowiednich, najbardziej aktualnych i najwyższej jakości standardów bezpieczeństwa informacji.
- 7.2. Zrealizujesz Odpowiednie Zamówienie należycie uwzględniając zapewnienie dostępności, autentyczności, integralności i poufności w związku z ochroną danych NTT i Klientów.
- 7.3. Przez cały okres obowiązywania Odpowiedniego Zamówienia jesteś zobowiązany do utrzymywania aktualnych i odpowiednich planów działania, szczególnie opisujących strategie odzyskiwania danych przechowywanych lub przetwarzanych zgodnie z warunkami Odpowiedniego Zamówienia w celu ograniczenia ryzyka utraty danych w wyniku nieprzewidzianych okoliczności. Oczekuje się, że na żądanie niezwłocznie dostarczysz zaktualizowane plany.
- 7.4. W przypadku wystąpienia incydentu teleinformatycznego związanego z usługą teleinformatyczną świadczoną przez Ciebie na rzecz NTT, jesteś zobowiązany do udzielenia pomocy NTT i Klientowi NTT bez dodatkowych kosztów.
- 7.5. Gwarantujesz, że personel oddelegowany do realizacji Odpowiedniego Zamówienia weźmie udział w programach uświadamiających w zakresie bezpieczeństwa teleinformatycznego oraz szkoleniach w zakresie operacyjnej odporności cyfrowej organizowanych przez NTT lub Klienta. NTT poinformuje Cię o szkoleniu z wyprzedzeniem i ułatwi udział oddelegowanemu personelowi.

8. KORZYSTANIE Z PODWYKONAWCÓW

- 8.1. We wniosku do NTT o wyrażenie zgody na korzystanie z usług podwykonawcy jesteś zobowiązany do:
 - 8.1.1. oznaczenia podwykonawcy w sposób umożliwiający NTT przeprowadzenie procedur weryfikacyjnych;
 - 8.1.2. przedłożenia NTT kopię umowy o zachowaniu poufności zawartej z podwykonawcą;
 - 8.1.3. jasnego określenia zakresu usług, które mają być wykonane przez podwykonawcę, specyfikacji tych usług, w które podwykonawca będzie zaangażowany oraz szczegółowego opisanie czynności, które podwykonawca ma wykonać;
 - 8.1.4. przedłożyć NTT projekt umowy z podwykonawcą, jeśli taki istnieje.
- 8.2. NTT może zażądać dodatkowych informacji w dowolnym momencie, a Ty jest zobowiązany do udzielenia żądanych informacji bez zbędnej zwłoki.
- 8.3. Powiadomisz nas o każdej zmianie lub rozwiązaniu umowy z podwykonawcą, a także o każdym przypadku zaprzestania świadczenia usług przez podwykonawcę. Zawiadomienie powinno zostać przekazane niezwłocznie, nie później jednak niż w terminie 1 dnia od zaistnienia zdarzenia.

9. POZIOM USŁUG

- 9.1. Opisy poziomów usług, w tym aktualizacje i poprawki, są opisane w Obowiązującym Zamówieniu.

10. FUNKCJE I USŁUGI ICT

- 10.1. Pełny i jasny opis wszystkich funkcji i usług ICT, które świadczysz, jest zawarty w Obowiązującym Zamówieniu.

11. ODPOWIEDZIALNOŚĆ

- 11.1. Ponosisz pełną odpowiedzialność za wszelkie szkody poniesione przez klientów Klienta w związku z realizacją przez Ciebie Odpowiedniego Zamówienia. W takich przypadkach nie ma zastosowania żadne ograniczenie Twojej odpowiedzialności.

12. WAŻNOŚĆ, ZAKOŃCZENIE I PLAN WYJŚCIA

- 12.1. Niniejszy Dodatek Outsourcingowy wchodzi w życie z chwilą jego dostarczenia Tobie jako załącznika do odpowiedniego Zamówienia, przy czym data odpowiedniego Zamówienia staje się datą wejścia w życie Dodatku Outsourcingowego.
- 12.2. Zastrzegamy sobie prawo do wypowiedzenia Odpowiedniego Zamówienia w dowolnym momencie bez dodatkowego okresu wypowiedzenia w każdej z następujących okoliczności:

- 12.2.1. istotne naruszenie obowiązujących przepisów prawa, regulacji lub warunków umownych Odpowiedniego Zamówienia, Umowy (o ile ma zastosowanie) lub niniejszego Dodatku Outsourcingowego;
 - 12.2.2. okoliczności zidentyfikowane w trakcie monitorowania ryzyka związanego z ICT, które uznaje się za mogące wpłynąć na działanie funkcji świadczonych w ramach odpowiedniego Zamówienia, w tym istotne zmiany, które mają wpływ na Odpowiednie Zamówienie lub Sprzedawcę;
 - 12.2.3. uchybienia związane z ogólnym zarządzaniem ryzykiem związanym z ICT, a w szczególności ze sposobem, w jaki zapewniają dostępność, autentyczność, integralność i poufność danych, niezależnie od tego, czy są to dane osobowe lub inne dane szczególnie chronione, czy też dane nieosobowe;
 - 12.2.4. w przypadku, gdy właściwy Organ nie może już skutecznie nadzorować Klienta ze względu na warunki lub okoliczności związane z Odpowiednim Zamówieniem;
 - 12.2.5. rozwiązania umowy (dotyczącej Odpowiedniego Zamówienia) pomiędzy NTT a Klientem przez Organ, NTT lub Klienta.
- 12.3. Strategie wyjścia, w tym obowiązkowy odpowiedni okres przejściowy, zostały określone w odpowiednim Zamówieniu lub dodatkowym porozumieniu Stron.
- 12.4. W obowiązkowym okresie przejściowym będziesz nadal świadczył odpowiednie funkcje lub usługi ICT w celu zmniejszenia ryzyka zakłóceń w świadczeniu usług na rzecz i przez NTT oraz Klienta lub w celu zapewnienia skutecznego rozwiązania i restrukturyzacji.
- 12.5. W trakcie obowiązkowego okresu przejściowego, na żądanie, jesteś zobowiązany do udostępnienia nam danych NTT, w formacie zwyczajowo używanym przez Stronę lub w łatwo dostępnej formie, a także umożliwienia nam migracji do innego usługodawcy lub zmiany na rozwiązanie wewnętrzne zgodne ze złożonością świadczonych usług. Na żądanie NTT usuniesz nasze dane.

13. USŁUGI ICT WSPIERAJĄCE KRYTYCZNE LUB ISTOTNE FUNKCJE

- 13.1. Poniższe postanowienia mają zastosowanie do Sprzedawcy, jeżeli Odpowiednie Zamówienie określa lub z innych okoliczności wynika, że usługi teleinformatyczne wspierają krytyczne lub istotne funkcje Klienta. Jeśli zastosowanie mają poniższe postanowienia i istnieją jakiegokolwiek rozbieżności między niniejszą sekcją 13 oraz pozostałych warunków niniejszego Dodatku Outsourcingowego, zastosowanie mają poniższe postanowienia.
- 13.2. Opisy poziomów usług, w tym zaktualizowane i skorygowane z precyzyjnymi ilościowymi i jakościowymi celami w zakresie wydajności w ramach uzgodnionych poziomów usług, są zawarte w Odpowiednim Zamówieniu.
- 13.3. Jesteś zobowiązany do niezwłocznego powiadamiania NTT o wszelkich zmianach, które mogą mieć istotny wpływ na Twoją zdolność do skutecznego świadczenia usług teleinformatycznych wspierających krytyczne lub ważne funkcje Klienta zgodnie z uzgodnionymi poziomami usług. Konkretny okres wypowiedzenia mogą być opisane w Odpowiednim Zamówieniu.

- 13.4. Jesteś zobowiązany do uczestniczenia i pełnej współpracy w testach penetracyjnych prowadzonych przez Klienta NTT, o których mowa w art. 26 i 27 DORA.
- 13.5. NTT i Klient mają prawo do bieżącego monitorowania wykonania przez Ciebie obowiązków, co wiąże się z następującymi kwestiami:
- 13.5.1. nieograniczone prawa dostępu, kontroli i audytu przez NTT i Klienta lub wyznaczoną stronę третią oraz przez właściwy Organ, a także prawo do sporządzania kopii odpowiedniej dokumentacji na miejscu, jeśli ma ona kluczowe znaczenie dla działania usługi Klienta, której skuteczne wykonywanie nie jest utrudnione ani ograniczone przez inne ustalenia umowne lub polityki wdrożeniowe;
 - 13.5.2. prawo do uzgodnienia alternatywnych poziomów gwarancji, jeśli obecne naruszają prawa klientów Klienta;
 - 13.5.3. zobowiązanie do pełnej współpracy podczas kontroli na miejscu i audytów przeprowadzanych przez właściwe Organy, Klienta lub wyznaczoną stronę третią; oraz
 - 13.5.4. obowiązek podania szczegółowych informacji na temat zakresu, procedur, których należy przestrzegać, oraz częstotliwości takich inspekcji i audytów.
- 13.6. Jesteś zobowiązany do posiadania środków, narzędzi i polityk bezpieczeństwa teleinformatycznego, które zapewniają odpowiedni poziom bezpieczeństwa przy świadczeniu usług.

14. USŁUGI W CHMURZE

- 14.1. Poniższe postanowienia mają zastosowanie i są dla Ciebie wiążące, jeśli Odpowiednie Zamówienie określa, że Komunikat KNF ma zastosowanie do świadczonych przez Ciebie usług.
- 14.2. Jasny podział odpowiedzialności za bezpieczeństwo informacji, z uwzględnieniem modelu usługi, ciągłości świadczenia usług (w tym parametrów RTO i RPO, w stosownych przypadkach) oraz deklarowanego SLA wraz ze sposobem pomiaru i raportowania ma zastosowanie, gdy jest to określone w Odpowiednim Zamówieniu.
- 14.3. W okresie obowiązywania Odpowiedniego Zamówienia oraz po jego zakończeniu (wygaśnięciu, rozwiązaniu) prawo własności do informacji pozostaje odpowiednio własnością NTT lub Klienta.
- 14.4. Odpowiednie Zamówienie określa obowiązki Sprzedawcy w zakresie przekazywania informacji na temat spodziewanych zmian w standardach mających zastosowanie do odpowiednich usług w chmurze (w tym zmian technicznych).
- 14.5. Odpowiednie Zamówienie określa obowiązki Sprzedawcy w zakresie dostarczenia dokumentacji technicznej, instrukcji konfiguracji usług w chmurze oraz deklaracji zgodności.

- 14.6. Niezależnie od uprawnień NTT i Klienta do przeprowadzania audytów i inspekcji (określonych w punkcie 5 niniejszego Dodatku Outsourcingowego), NTT i Klient mają prawo do przeprowadzania kontroli w miejscach, w których przetwarzane są dane w związku z Odpowiednim Zamówieniem, w tym prawo do przeprowadzenia audytu drugiej strony lub osoby trzeciej na żądanie Klienta lub NTT.
- 14.7. W stosownych przypadkach zasady licencjonowania (w tym prawo do aktualizacji zabezpieczeń oprogramowania lub jego komponentów) oraz prawa własności intelektualnej, w tym prawo do obsługi przetwarzanych informacji, są określone w Odpowiednim Zamówieniu.
- 14.8. Parametry techniczne usług wykonywanych w ramach Odpowiedniego Zamówienia mogą być modyfikowane wyłącznie w przypadkach i zgodnie z procedurą określoną w Odpowiednim Zamówieniu.
- 14.9. Zasady i terminy usuwania informacji, które są przetwarzane, są określone w Odpowiednim Zamówieniu. Jeśli zasady i terminy nie zostaną określone, informacje zostaną usunięte zgodnie z zasadami i w terminach wskazanych przez NTT.
- 14.10. Odpowiednie Zamówienie określa standardy i normy, których przestrzega Sprzedawca, takie jak PN-ISO/IEC ISO 20000, PN-EN ISO/IEC 27001, PN-EN ISO 22301, ISO/IEC 27017, ISO/IEC 27018 lub inne.
- 14.11. Sprzedawca wdroży zasady chroniące przed nieuprawnionym dostępem do informacji przez swoich pracowników i podwykonawców, w tym:
 - 14.11.1. domyślna zasada braku dostępu do informacji przetwarzanych przez NTT lub Klienta,
 - 14.11.2. domyślna zasada braku konta administratora lub użytkownika na maszynach wirtualnych dedykowanych dla NTT lub Klienta lub w uruchamianych usługach chmurowych,
 - 14.11.3. zasada "niezbędnego minimum" wymagań dotyczących uprawnień do konta w usłudze, ma być przyznawana tylko wtedy, gdy jest to niezbędne do wykonania operacji wymaganych przez NTT lub Klienta (np. usuwanie usterek) i tylko na czas trwania takich operacji, na podstawie zgłoszenia serwisowego złożonego przez NTT lub Klienta; cały proces zarządzania i realizacji może odbywać się po zalogowaniu; Odpowiednie procedury operacyjne mogą być również potwierdzone odpowiednim certyfikatem (np. SOC7 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną zgodnie z europejskimi standardami akredytacyjnymi.
- 14.12. Sprzedawca będzie również chronić informacje przed nieautoryzowanym dostępem stosując się do dostępnych wytycznych, konfiguracji modelu, opisów reguł itp., które powinny jasno określać separację w przetwarzaniu informacji i wskazywać metody weryfikacji poprawności konfiguracji, a także poprzez uruchomienie nowego domyślnego środowiska (lub usługi w chmurze) oddzielnego od innych użytkowników, z ustawieniami „domyślnie bezpiecznymi” ('secure-by-default').

- 14.13. Informacje przetwarzane w chmurze muszą być szyfrowane zgodnie z poniższymi zasadami:
- 14.13.1. zapewnisz NTT dostęp do aktualnych, szczegółowych instrukcji konfiguracji chmury oraz metod weryfikacji poprawności konfiguracji i działania, w szczególności w obszarze szyfrowania;
 - 14.13.2. Twój personel powinien posiadać odpowiednie kompetencje do skonfigurowania prawidłowej konfiguracji usług chmurowych zgodnie z wytycznymi przekazanymi przez dostawcę usług chmurowych, w tym w zakresie szyfrowania;
 - 14.13.3. będziesz korzystać z dedykowanych ustawień konfiguracyjnych – lub ustawień zalecanych przez dostawcę usług chmurowych – które zwiększają bezpieczeństwo danych usług chmurowych;
 - 14.13.4. Informacje chronione prawem muszą być szyfrowane zarówno jako dane "w spoczynku", jak i jako dane "w transzycie".
- 14.14. przekażesz następujące informacje do NTT:
- 14.14.1. aktualne szczegółowe instrukcje konfiguracji chmury oraz metody weryfikacji poprawności konfiguracji i działania, w szczególności w obszarze szyfrowania;
 - 14.14.2. wytyczne dotyczące prawidłowej konfiguracji usług w chmurze;
 - 14.14.3. zalecenia dotyczące ustawień konfiguracyjnych zwiększających bezpieczeństwo usług w chmurze.
- 14.15. Będziesz chronił logi przed nieuprawnionym dostępem, modyfikacją lub usunięciem przez czas określony w zasadach bezpieczeństwa wynikających z oceny ryzyka oraz obowiązujących zasad szczególnych.
- 14.16. Jeśli masz zdalny dostęp do usług w chmurze używanych przez NTT lub Klienta, upewnij się, że:
- 14.16.1. wyłącznie upoważniony personel ma dostęp do określonych systemów informatycznych lub określonych części struktury informatycznej;
 - 14.16.2. Twój personel korzysta z uwierzytelniania wieloskładnikowego (MFA), którego rodzaj i zakres są określane na podstawie wyników oceny ryzyka;
 - 14.16.3. dostęp administracyjny i uprzywilejowanych użytkowników jest ograniczony do zaufanych sieci NTT lub Klienta i/lub Ciebie i kontrolowany (w tym poprzez rejestrowanie sesji i parametrów sesji, a następnie poprzez analizę poprawności i celu każdej operacji), chyba że ocena ryzyka wykazała, że nie jest to konieczne.