DODATEK OUTSOURCINGOWY - Załącznik DORA

1. PRZEDMIOT ZAŁĄCZNIKA

1.1. Niniejszy załącznik („**Załącznik**”) reguluje obowiązki i zobowiązania Stron Umowy, uwzględniające wymagania wynikające z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 („**DORA**”).

1.2. Załącznik może zostać rozszerzony o regulacyjne standardy techniczne („**RTS**”) publikowane przez właściwe organy w oparciu o przepisy DORA.

1.3. Załącznik uwzględnia także następujące wytyczne organów nadzoru:

1.3.1. komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z 23 stycznia 2020 r. („**Komunikat Chmurowy**”);

1.3.2. wytyczne Europejskiego Urzędu Nadzoru Bankowego w sprawie outsourcingu z 25 lutego 2019 r., EBA/GL/2019/02 („**Wytyczne EBA**”).

1.4. Strony zdecydowały się przyjąć na siebie zobowiązania i obowiązki określone Załącznikiem, z uwagi na fakt, że NTT Poland sp. z o.o. z siedzibą w Warszawie (dalej “**NTT**”) świadczy na rzecz ZAMAWIAJĄCEGO usługi stanowiące „usługi ICT” w rozumieniu art. 3 pkt 21) DORA („**Usługi**”), odnoszące się do określonych funkcji realizowanych przez ZAMAWIAJĄCEGO, których szczegółowy i wyczerpujący opis (Usług i funkcji) znajduje się w Umowie/Zamówieniu.

1.5. W razie zaistnienia sprzeczności pomiędzy postanowieniami Umowy i Załącznika, decydujące znaczenie mają postanowienia Załącznika.

1.6. Strony oświadczają, że powierzenie NTT przez ZAMAWIAJĄCEGO świadczenia Usług nie wpłynie niekorzystnie na:

1.6.1. prowadzenie przez ZAMAWIAJĄCEGO działalności zgodnie z przepisami prawa,

1.6.2. ostrożne i stabilne zarządzanie ZAMAWIAJĄCYM,

1.6.3. skuteczność systemu kontroli wewnętrznej u ZAMAWIAJĄCEGO,

1.6.4. możliwość wykonywania obowiązków przez biegłego rewidenta upoważnionego do badania sprawozdań finansowych ZAMAWIAJĄCEGO na podstawie zawartej z ZAMAWIAJĄCYM umowy oraz

1.6.5. ochronę tajemnicy prawnie chronionej.

1.7. NTT oświadcza, że Usługi będą świadczone zgodnie z obowiązującymi ZAMAWIAJĄCEGO przepisami prawa.

1.8. NTT oświadcza, że w ramach Grupy NTT:

1.8.1. posiada następujące certyfikaty:

(a) PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT;

(b) PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji;

(c) PN-EN ISO 22301 dotyczące zarządzania ciągłością działania;

(d) ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej;

(e) ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej.

1.8.2. CPD, w którym NTT przetwarza dane dla potrzeb świadczenia Usług, spełnia wymagania normy PN-EN 50600 (Wyposażenie i infrastruktura centrów przetwarzania danych) minimum klasy 3 lub ANSI/TIA-942 minimum Tier III, lub innego normatywu odpowiedniego i uznanego do oceny CPD lub zawierającego wymagania z nim związane - dotyczy CPD: Google, AWS i Azure.

2. DEFINICJE

2.1. Pojęcia pisane w Załączniku wielką literą mają znaczenie nadane im w Umowie i innych załącznikach do Umowy, chyba, że w Załączniku – w szczególności w niniejszym rozdziale – zostały wprost zdefiniowane w sposób odmienny.

2.2. Niezależnie od powyższego, zapisanym poniżej małymi literami pojęciom Strony nadają wskazane przy nich znaczenie, zgodne z art. 3 DORA:

2.2.1. **operacyjna odporność cyfrowa** oznacza zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej operacyjnej integralności i niezawodności przez zapewnianie, bezpośrednio albo pośrednio – korzystając z usług zewnętrznych dostawców usług ICT – pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość, w tym w trakcie zakłóceń;

2.2.2. **sieci i systemy informatyczne** oznaczają (a) sieci łączności elektronicznej tj. systemy transmisyjne, niezależnie do tego, czy opierają się na stałej infrastrukturze lub scentralizowanym zarządzaniu zasobami, oraz, w stosownych przypadkach, urządzenia przełączające lub routingowe oraz inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają przekazywanie sygnałów przewodowo, za pomocą radia, środków optycznych lub innych rozwiązań wykorzystujących fale, w tym sieci satelitarnych, stacjonarnych (komutowanych i pakietowych, w tym internetu) i sieci ruchomych, elektroenergetycznych systemów kablowych, w zakresie, w jakim są one wykorzystywane do przekazywania sygnałów, w sieciach nadawania radiowego i telewizyjnego oraz sieciach telewizji kablowej, niezależnie od rodzaju przekazywanej informacji lub (b) urządzenie lub grupę wzajemnie połączonych lub powiązanych urządzeń, z których co najmniej jedno, na podstawie programu, automatycznie

przetwarza dane cyfrowe; lub (c) dane cyfrowe przechowywane, przetwarzane, pobierane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania;

2.2.3. **dotychczasowy system ICT** oznacza system ICT, którego cykl życia dobiegł końca (koniec okresu użytkowania), którego ze względów technologicznych i komercyjnych nie można zmodernizować ani naprawić, lub który nie jest już obsługiwany przez dostawcę lub zewnętrznego dostawcę usług ICT, ale który nadal jest wykorzystywany i wspiera funkcje danego podmiotu finansowego;

2.2.4. **bezpieczeństwo sieci i systemów informatycznych** oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;

2.2.5. **ryzyko związane z ICT** oznacza każdą dającą się racjonalnie określić okoliczność związaną z użytkowaniem sieci i systemów informatycznych, która – jeżeli dojdzie do jej urzeczywistnienia – może zagrozić bezpieczeństwu sieci i systemów informatycznych, dowolnego narzędzia lub procesu zależnego od technologii, bezpieczeństwu operacji i procesów lub świadczeniu usług poprzez wywoływanie negatywnych skutków w środowisku cyfrowym lub fizycznym;

2.2.6. **zasoby informacyjne** oznaczają zbiór informacji, w formie materialnej albo niematerialnej, który jest wart ochrony;

2.2.7. **zasób ICT** oznacza oprogramowanie lub zasoby komputerowe w sieci i systemach informatycznych wykorzystywanych przez dany podmiot finansowy;

2.2.8. **incydent związany z ICT** oznacza pojedyncze zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które zagrażają bezpieczeństwu sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy;

2.2.9. **poważny incydent związany z ICT** oznacza incydent związany z ICT o dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego;

2.2.10. **cyberzagrożenie** oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób;

2.2.11. **znaczące cyberzagrożenie** oznacza cyberzagrożenie, którego charakterystyka techniczna wskazuje, że potencjalnie może spowodować poważny incydent związany

z ICT lub poważny incydent operacyjny lub poważny incydent w zakresie bezpieczeństwa związany z płatnościami;

2.2.12. **cyberatak** oznacza złośliwy incydent związany z ICT wywołany przez próbę zniszczenia, ujawnienia, zmiany, dezaktywacji, kradzieży lub uzyskania nieuprawnionego dostępu do składnika aktywów lub jego nieuprawnionego wykorzystania przez jakiegokolwiek agresora;

2.2.13. **analiza zagrożeń** oznacza informacje, które zostały zagregowane, przekształcone, przeanalizowane, zinterpretowane lub wzbogacone w celu zapewnienia niezbędnego kontekstu na potrzeby podejmowania decyzji i umożliwienia odpowiedniego i wystarczającego zrozumienia w celu złagodzenia skutków incydentu związanego z ICT lub cyberzagrożenia, w tym informacje dotyczące technicznych szczegółów cyberataku, osób odpowiedzialnych za atak oraz ich sposobu działania i motywacji;

2.2.14. **podatność** oznacza słabość, wrażliwość lub wadę zasobu, systemu, procesu lub kontroli, które można wykorzystać;

2.2.15. **testy penetracyjne pod kątem wyszukiwania zagrożeń (TLPT)** oznaczają ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które zapewniają kontrolowane, dostosowane do konkretnych zagrożeń, oparte na analizie zagrożeń (red team) testy działających na bieżąco krytycznych systemów produkcji podmiotu finansowego;

2.2.16. **ryzyko ze strony zewnętrznych dostawców usług ICT** oznacza ryzyko związane z ICT, które może wystąpić w przypadku podmiotu finansowego w związku z korzystaniem przez niego z usług ICT świadczonych przez zewnętrznych dostawców usług ICT lub przez ich podwykonawców, w tym w drodze uzgodnień dotyczących outsourcingu;

2.2.17. **zewnętrzny dostawca usług ICT** oznacza przedsiębiorstwo świadczące usługi ICT;

2.2.18. **dostawca usług ICT wewnątrz grupy** oznacza przedsiębiorstwo, które jest częścią grupy finansowej i które świadczy głównie usługi ICT na rzecz podmiotów finansowych należących do tej samej grupy lub podmiotów finansowych należących do tego samego systemu ochrony instytucjonalnej, w tym ich jednostek dominujących, jednostek zależnych, oddziałów lub innych podmiotów będących wspólną własnością lub pod wspólną kontrolą

2.2.19. **usługi ICT** oznaczają usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego, łącznie ze sprzętem komputerowym jako usługą i usługami w zakresie sprzętu komputerowego obejmującymi zapewnianie wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu, z wyłączeniem tradycyjnych usług telefonii analogowej;

2.2.20. **krytyczna lub istotna funkcja** oznacza funkcję, której zakłócenie w sposób istotny wpłynęłoby na wyniki finansowe podmiotu finansowego, na bezpieczeństwo lub ciągłość usług i działalności tego podmiotu lub której zaprzestanie lub wadliwe lub zakończone niepowodzeniem działanie w sposób istotny wpłynęłoby na dalsze wypełnianie przez podmiot finansowy warunków i obowiązków wynikających z udzielonego mu zezwolenia lub jego innych obowiązków wynikających z obowiązujących przepisów dotyczących usług finansowych;

2.2.21. **kluczowy zewnętrzny dostawca usług ICT** oznacza zewnętrznego dostawcę usług ICT wyznaczonego zgodnie z art. 31 DORA;

2.2.22. **zewnętrzny dostawca usług ICT z siedzibą w państwie trzecim** oznacza zewnętrznego dostawcę usług ICT, który jest osobą prawną mającą siedzibę w państwie trzecim i który zawarł z podmiotem finansowym ustalenie umowne o świadczenie usług ICT;

2.2.23. **jednostka zależna** oznacza jednostkę kontrolowaną przez jednostkę dominującą, w tym dowolną jednostkę zależną jednostki dominującej najwyższego szczebla (tj. jednostkę, która kontroluje co najmniej jedną jednostkę zależną) tj. jednostkę zależną w rozumieniu art. 2 pkt 10 i art. 22 dyrektywy Parlamentu Europejskiego i Rady 2013/34/UE w sprawie rocznych sprawozdań finansowych, skonsolidowanych sprawozdań finansowych i powiązanych sprawozdań niektórych rodzajów jednostek, zmieniającej dyrektywę Parlamentu Europejskiego i Rady 2006/43/WE oraz uchylającej dyrektywy Rady 78/660/EWG i 83/349/EWG

2.2.24. **grupa** oznacza jednostkę, która kontroluje co najmniej jedną jednostkę zależną i wszystkie jej jednostki zależne tj. grupę zdefiniowaną w art. 2 pkt 11 dyrektywy Parlamentu Europejskiego i Rady 2013/34/UE z dnia 26 czerwca 2013 r. w sprawie rocznych sprawozdań finansowych, skonsolidowanych sprawozdań finansowych i powiązanych sprawozdań niektórych rodzajów jednostek, zmieniającej dyrektywę Parlamentu Europejskiego i Rady 2006/43/WE oraz uchylającej dyrektywy Rady 78/660/EWG i 83/349/EWG;

2.2.25. **jednostka dominująca** oznacza jednostkę, która kontroluje co najmniej jedną jednostkę zależną tj. jednostkę dominującą w rozumieniu art. 2 pkt 9 i art. 22 dyrektywy Parlamentu Europejskiego i Rady 2013/34/UE z dnia 26 czerwca 2013 r. w sprawie rocznych sprawozdań finansowych, skonsolidowanych sprawozdań finansowych i powiązanych sprawozdań niektórych rodzajów jednostek, zmieniającej dyrektywę Parlamentu Europejskiego i Rady 2006/43/WE oraz uchylającej dyrektywy Rady 78/660/EWG i 83/349/EWG;

2.2.26. **podwykonawca usług ICT z siedzibą w państwie trzecim** oznacza podwykonawcę usług ICT, który jest osobą prawną mającą siedzibę w państwie trzecim i który zawarł ustalenie umowne z zewnętrznym dostawcą usług ICT albo z zewnętrznym dostawcą usług ICT mającym siedzibę w państwie trzecim;

2.2.27. **ryzyko koncentracji w obszarze ICT** oznacza ekspozycję na poszczególnych lub wielu powiązanych ze sobą kluczowych zewnętrznych dostawców usług ICT, która prowadzi do takiego stopnia uzależnienia od takich dostawców, że niedostępność, awaria lub innego rodzaju braki po stronie tych ostatnich mogą potencjalnie zagrozić zdolności podmiotu finansowego do wypełniania krytycznych lub istotnych funkcji lub przyczynić się do poniesienia przez ten podmiot innego rodzaju negatywnych skutków, w tym dużych strat, lub zagrozić stabilności finansowej Unii jako całości;

2.2.28. **organ zarządzający** oznacza organ zarządzający zdefiniowany w art. 4 ust. 1 pkt 36 dyrektywy 2014/65/UE, art. 3 ust. 1 pkt 7 dyrektywy 2013/36/UE, art. 2 ust. 1 lit. s) dyrektywy 2009/65/WE, art. 2 ust. 1 pkt 45 rozporządzenia (UE) nr 909/2014, art. 3 ust. 1 pkt 20 rozporządzenia (UE) 2016/1011, oraz w odpowiednim przepisie rozporządzenia w sprawie rynków kryptoaktywów lub równorzędne osoby, które faktycznie zarządzają podmiotem lub pełnią kluczowe funkcje zgodnie z odpowiednimi przepisami unijnymi lub krajowymi.

2.3. Następujące pojęcia zapisane wielką literą otrzymują nadane im poniżej znaczenie:

2.3.1. **CPD** – centrum przetwarzania danych.

2.3.2. **Organ nadzoru** – każdy organ władzy publicznej, sprawujący nadzór nad działalnością ZAMAWIAJĄCEGO, w szczególności Europejski Urząd Nadzoru Bankowego (EUNB), Komisja Nadzoru Finansowego (KNF), Prezes Urzędu Ochrony Danych Osobowych (PUODO), Generalny Inspektor Informacji Finansowej (GIIF), jak również „organ publiczny" w rozumieniu art. 3 pkt 65) DORA.

2.3.3. **Podwykonawca** – zewnętrzny dostawca usług ICT, niebędący pracownikiem NTT lub osobą fizyczną, prowadzącą jednoosobową działalność gospodarczą stale współpracującą z NTT, któremu NTT powierza realizację Usługi w całości lub części.

2.3.4. **RTO (*recovery time objective*)** – czas od chwili wystąpienia awarii systemu IT do momentu przywrócenia funkcjonowania systemu IT.

2.3.5. **RPO (*recovery point objective*)** – maksymalny czas od wykonania ostatniej kopii zapasowej danych do wystąpienia awarii usługi chmurowej. Oznacza to akceptację przez ZAMAWIAJĄCEGO potencjalnego ryzyka utraty wyników przetwarzania informacji powstałych w określonym czasie.

2.3.6. **Siła Wyższa** – wydarzenie, występujące po podpisaniu Umowy i mimo dochowania należytej staranności niedające się przewidzieć, będące poza kontrolą STRONY, uniemożliwiające danej STRONIE wykonywanie jej obowiązków objętych Umową. Takie wydarzenia mogą obejmować w szczególności wojny, rewolucje, pożary, powodzie, epidemie, embarga przewozowe lub ogłoszone strajki generalne w gałęziach gospodarki.

2.3.7. **TLPT** – testy penetracyjne pod kątem wyszukiwania zagrożeń, w rozumieniu art. 3 pkt 17) DORA, oznaczające ramy naśladujące taktykę, techniki i procedury stosowane w

rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które zapewniają kontrolowane, dostosowane do konkretnych zagrożeń, oparte na analizie zagrożeń (red team) testy działających na bieżąco krytycznych systemów produkcji podmiotu finansowego.

2.3.8. **Grupa NTT** – grupa kapitałowa w skład której wchodzi NTT, spółki dominujące wobec NTT i takie wobec których NTT jest spółką dominującą, a także spółki powiązane z NTT – w rozumieniu art. 4 § 1 pkt. 4 i 5 Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (t.j. Dz. U. z 2024 r. poz. 18 z późn. zm.).

3. PODWYKONAWSTWO

3.1. NTT jest uprawnione do powierzenia Podwykonawcom wykonywania, w części lub w całości, wyłącznie Usług określonych w Umowie/Zamówieniu.

3.2. W przypadku zamiaru powierzenia przez NTT Podwykonawcy świadczenia Usługi, o której mowa w pkt. 3.1 Załącznika NTT jest zobowiązane do:

3.2.1. poinformowania ZAMAWIAJĄCEGO o Podwykonawcy, który rozpocznie świadczenie danej Usługi, nie później niż na 14 dni przed dopuszczeniem tego Podwykonawcy do realizacji prac objętych tą Usługą – niniejsze zobowiązanie nie dotyczy Podwykonawców wskazanych bezpośrednio w Zamówieniu ;

3.2.2. przekazania, na żądanie ZAMAWIAJĄCEGO, umowy na podstawie której Podwykonawca będzie realizował prace objęte Usługą lub odpowiedniego wyciągu z umowy, jeśli NTT współpracuje z Podwykonawcą w szerszym zakresie niż dotyczący danej Usługi, z zastrzeżeniem, że NTT nie jest zobowiązane do ujawniania wynagrodzenia należnego Podwykonawcy;

3.2.3. poinformowania ZAMAWIAJĄCEGO o zaprzestaniu realizacji przez Podwykonawcę prac objętych Usługą, w terminie 14 dni po wygaśnięciu umowy łączącej Podwykonawcę z NTT lub faktycznego, trwałego zaprzestania przez Podwykonawcę wykonywania umowy. W przypadku konieczności zastąpienia jednego Podwykonawcy innym, zastosowanie ma pkt. 3.2.1 Załącznika.

3.3. W razie poinformowania ZAMAWIAJĄCEGO przez NTT o zamiarze powierzenia realizacji danej Usługi Podwykonawcy, w tym o zamiarze zastąpienia jednego Podwykonawcy innym, ZAMAWIAJĄCY jest uprawniony do wyrażenia sprzeciwu w terminie 7 dni od dnia otrzymania takiego powiadomienia. Brak wyrażenia sprzeciwu w terminie, o którym mowa w zdaniu poprzednim STRONY uznają za akceptację przez ZAMAWIAJĄCEGO powierzenia przez NTT realizacji danej Usługi Podwykonawcy lub zastąpienia jednego Podwykonawcy innym.

3.4. W razie, gdy korzystanie przez NTT z określonego Podwykonawcy zagraża lub narusza istotny interes ZAMAWIAJĄCEGO, ZAMAWIAJĄCY zwróci się do NTT z wnioskiem o zmianę lub rozwiązanie przez NTT umowy z tym Podwykonawcą i wówczas STRONY przystąpią do negocjacji, dotyczących warunków rezygnacji z określonego Podwykonawcy.

3.5. W przypadku, gdy ZAMAWIAJĄCY wyrazi sprzeciw zgodnie z pkt. 3.3 Załącznika, STRONY przystąpią do negocjacji w zakresie powierzenia realizacji danej Usługi Podwykonawcy.

3.6. NTT jest uprawnione do udzielenia Podwykonawcy, zaakceptowanemu przez ZAMAWIAJĄCEGO zgodnie z niniejszym rozdziałem 3 Załącznika, dostępu do informacji przetwarzanych w związku z realizacją Umowy, w zakresie potrzebnym z uwagi na zakres Usług, w których świadczeniu dany Podwykonawca uczestniczy.

4. LOKALIZACJA I BEZPIECZEŃSTWO DANYCH

4.1. NTT zobowiązuje się świadczyć Usługi, w tym przetwarzać dane w związku ze świadczeniem Usług, wyłącznie w lokalizacjach wskazanych w Umowie/Zamówieniu.

4.2. W razie potrzeby zmiany lokalizacji świadczenia Usługi lub przetwarzania i przechowywania danych związanych z Usługą, NTT zobowiązane jest do poinformowania ZAMAWIAJĄCEGO o planowanej zmianie z odpowiednim wyprzedzeniem, jednak nie później niż 14 dni przed zmianą. ZAMAWIAJĄCY jest uprawniony do sprzeciwienia się zmianie w terminie 7 dni od otrzymania powiadomienia i w takim wypadku Strony wspólnie ustalą lokalizację dalszego świadczenia Usługi lub przetwarzania i przechowywania danych związanych z Usługą. Brak zgłoszenia przez ZAMAWIAJĄCEGO sprzeciwu w terminie, o którym mowa w zdaniu poprzednim uznaje się za zgodę ZAMAWIAJĄCEGO na zmianę lokalizacji świadczenia Usługi lub przetwarzania i przechowywania danych związanych z Usługą.

4.3. NTT zobowiązuje się do zachowania dostępności, autentyczności, integralności i poufności danych przetwarzanych w związku ze świadczeniem Usług, w tym danych osobowych. Szczegółowy opis stosowanych przez NTT mechanizmów, procedur, zasad, środków i polityk, mających na celu zachowanie bezpieczeństwa danych został zawarty w **Dodatku nr 1 – Bezpieczeństwo danych**.

4.4. Strony oświadczają, że dane osobowe, których przetwarzanie zostanie powierzone NTT przez ZAMAWIAJĄCEGO w związku z realizacją niniejszej Umowy, będę przetwarzane za zasadach szczegółowo określonych w odrębnej umowie o powierzeniu przetwarzania danych osobowych, zgodnych z prawem Unii Europejskiej, w tym z RODO.

4.5. Każda ze STRON zachowuje własność informacji przetwarzanych w toku wykonywania Umowy, w tym informacji przez daną STRONĘ wytworzonych, chyba że STRONY wyraźnie postanowią inaczej, na piśmie pod rygorem nieważności.

5. SZCZEGÓŁOWE ZASADY WSPÓŁPRACY STRON

OBSŁUGA INCYDENTÓW I SLA

5.1. Umowa/Zamówienie określa szczegółowe zasady realizacji przez NTT wsparcia w obsłudze incydentów ICT dotyczących Usług, w tym gwarantowane poziomy świadczenia Usług (SLA) oraz zasady wymiany informacji pomiędzy personelem NTT (w tym Podwykonawców) i ZAMAWIAJĄCEGO w razie zaistnienia incydentu ICT.

5.2. Umowa /Zamówienie określa RPO i RTO, gwarantowane przez NTT, w odniesieniu do danych przetwarzanych w związku ze świadczeniem Usług, jeśli taka gwarancja jest objęta zakresem Usług.

PRAWO DO AUDYTU I WSPÓŁPRACA Z ORGANAMI NADZORU

5.3. W toku realizacji Umowy, ZAMAWIAJĄCY jest uprawniony do przeprowadzenia – na własny koszt – audytu należytego wykonywania Umowy, w tym inspekcji w lokalizacji przetwarzania przez NTT lub jej Podwykonawcę, informacji w związku ze świadczeniem Usług, przy czym:

5.3.1. ZAMAWIAJĄCY jest zobowiązany do poinformowania NTT o planowanej inspekcji w terminie 14 dni przed jej planowanym terminem wraz z przekazaniem danych osób, mających przeprowadzić inspekcję;

5.3.2. ZAMAWIAJĄCY zapewnia, że osoby przeprowadzające inspekcję w imieniu ZAMAWIAJĄCEGO będą przestrzegały wszelkich zasad obowiązujących w NTT w związku z dostępem do określonych pomieszczeń, w których prowadzona będzie inspekcja, a także, jeśli będzie to wymagane przez NTT, zobowiązać się do zachowania poufności informacji pozyskanych w związku z dopuszczeniem takiej osoby do przeprowadzenia inspekcji. W razie niedochowania zapewnień, o których mowa w niniejszym podpunkcie, NTT jest uprawnione odsunąć daną osobę od wykonywanej inspekcji;

5.3.3. ZAMAWIAJĄCY zobowiązuje się podjąć wszelkie rozsądne działania w celu zminimalizowania wpływu prowadzonej inspekcji na działalność NTT i do współdziałania w tym zakresie z NTT w dobrej wierze.

5.4. W toku realizacji Umowy, NTT zobowiązuje się do udzielania Organom nadzoru wszelkich żądanych przez nie informacji, dotyczących świadczonych Usług, jak również – na żądanie Organu nadzoru – do umożliwienia Organowi nadzoru kontroli pomieszczeń, w których świadczone są Usługi i udostępnienia Organowi nadzoru dokumentacji związanej z przetwarzaniem informacji ZAMAWIAJĄCEGO, procesów i procedur, organizacji i zarządzania oraz potwierdzeń zgodności.

5.5. Prawo do audytu lub kontroli wykonywanych przez ZAMAWIAJĄCEGO bądź odpowiedni Organ nadzoru obejmuje uprawnienie dostępu do pełnego zakresu odpowiednich urządzeń, systemów, sieci, informacji i danych wykorzystywanych do świadczenia przez NTT Usług, w tym do powiązanych informacji finansowych, dotyczących personelu i audytorów zewnętrznych NTT.

5.6. W przypadku, gdy wykonywanie uprawnienia do audytu przez ZAMAWIAJĄCEGO lub Organ nadzoru będzie miało negatywny wpływ na świadczenie przez NTT Usług, NTT poinformuje ZAMAWIAJĄCEGO o wpływie prowadzonego audytu na świadczone Usługi i będzie zwolnione w tym zakresie z odpowiedzialności wobec ZAMAWIAJĄCEGO, w razie niewykonania lub nienależytego wykonania Umowy.

5.7. W przypadku, gdy wykonywanie uprawnienia do audytu przez ZAMAWIAJĄCEGO lub Organ nadzoru będzie wymagało istotnego zaangażowania ze strony NTT, NTT poinformuje ZAMAWIAJĄCEGO o szacowanych kosztach takiego zaangażowania, a ZAMAWIAJĄCY – w razie przeprowadzenia audytu – zobowiązany jest zwrócić NTT poniesione koszty, zgodnie z przekazaną i udokumentowaną informacją, w terminie 7 dni.

SZKOLENIA Z BEZPIECZEŃSTWA ICT

5.8. Na żądanie ZAMAWIAJĄCEGO, zgłoszone nie później niż 14 dni przed wyznaczonym terminem szkolenia, NTT zobowiązane jest delegować odpowiedni personel NTT lub Podwykonawcy – uczestniczący przy świadczeniu Usług – do udziału w organizowanym przez ZAMAWIAJĄCEGO lub podmiot przez niego wyznaczony szkoleniu z zakresu operacyjnej odporności cyfrowej lub w innym wydarzeniu, mającym na celu zwiększenie świadomości w zakresie bezpieczeństwa ICT.

5.9. Udział w szkoleniu lub wydarzeniu, o którym mowa, delegowanych członków personelu NTT lub Podwykonawcy, odbywa się na koszt ZAMAWIAJĄCEGO, na warunkach szczegółowo uzgodnionych przez STRONY przed rozpoczęciem szkolenia lub wydarzenia.

RAPORTOWANIE I MONITOROWANIE WYNIKÓW ŚWIADCZENIA USŁUG

5.10. NTT zobowiązane jest do przekazywania ZAMAWIAJĄCEMU określonych w Umowie raportów ze świadczenia Usług, we wskazanych w Umowie terminach.

5.11. Niezależnie od otrzymywanych raportów, ZAMAWIAJĄCY jest uprawniony do monitorowania we własnym zakresie wyników świadczenia Usług przez NTT, w szczególności ich zgodności z Umową. W razie potrzeby NTT zobowiązane jest do współpracy z ZAMAWIAJĄCYM w celu umożliwienia efektywnego monitorowania poziomu świadczonych Usług, na warunkach szczegółowo uzgodnionych pomiędzy STRONAMI.

UBEZPIECZENIE

5.12. NTT oświadcza, że posiada ubezpieczenie prowadzonej działalności gospodarczej do sumy ubezpieczenia nie niższej niż 5.000.000,00 PLN i zobowiązuje się do utrzymania ubezpieczenia na nie niższym poziomie przez cały okres świadczenia Usług.

STANDARDY ŚWIADCZONYCH USŁUG

5.13. W przypadku zmian w standardach świadczonych Usług:

5.13.1. w przypadku, gdy zmiana dotyczy Usługi świadczonej bezpośrednio przez NTT – NTT jest zobowiązane do poinformowania ZAMAWIAJĄCEGO o planowanej zmianie na co najmniej 14 dni przed jej wdrożeniem;

5.13.2. w przypadku, gdy zmiana dotyczy Usługi świadczonej przez Podwykonawcę – NTT jest zobowiązane do poinformowania ZAMAWIAJĄCEGO o zmianie w terminie 14 dni od otrzymania takiej informacji od Podwykonawcy,

– przy czym NTT będzie informowało ZAMAWIAJĄCEGO w formie dokumentowej, z wyraźnym wskazaniem, że informacja dotyczy zmiany w standardach świadczonych Usług.

TESTY I PLANY AWARYJNE (CIĄGŁOŚCI DZIAŁANIA)

5.14. NTT zobowiązane jest posiadać i testować – nie rzadziej niż co 12 miesięcy – plan awaryjny, dotyczący świadczonych Usług. W przypadku, gdy ZAMAWIAJĄCY posiada szczegółowe wymagania, dotyczące planów awaryjnych, przekaże je NTT, a STRONY wspólnie uzgodnią termin oraz warunki ich wdrożenia. Przez plan awaryjny STRONY rozumieją również plan ciągłości działania.

5.15. Na żądanie ZAMAWIAJĄCEGO, zgłoszone z co najmniej 14 dniowym wyprzedzeniem, NTT zobowiązane jest do wzięcia udziału w TLPT i zapewnienia ZAMAWIAJĄCEMU wsparcia w tym zakresie na warunkach szczegółowo uzgodnionych przez STRONY.

DOKUMENTACJA

5.16. Umowa /Zamówienie określa miejsce przechowywania i aktualizowania dokumentacji technicznej – wraz z instrukcjami konfiguracji, jeśli znajduje to zastosowanie – dotyczącej świadczonych Usług wraz z zasadami dostępu STRON do tej dokumentacji.

5.17. Umowa /Zamówienie precyzyjnie określa zakres dokumentacji oraz wszelkich informacji jakie NTT zobowiązane jest udostępniać ZAMAWIAJĄCEMU w związku ze świadczeniem Usług.

WŁASNOŚĆ INTELEKTUALNA

5.18. Umowa /Zamówienie określa szczegółowo zakres uprawnień ZAMAWIAJĄCEGO do korzystania z utworów udostępnianych mu przez NTT w związku ze świadczeniem Usług, a także zasady wykonywania aktualizacji bezpieczeństwa oprogramowania wykorzystywanego przy świadczeniu Usług.

6. ODPOWIEDZIALNOŚĆ, KARY UMOWNE I SIŁA WYŻSZA

ODPOWIEDZIALNOŚĆ

6.1. Odpowiedzialność NTT wobec ZAMAWIAJĄCEGO, w tym klientów ZAMAWIAJĄCEGO, w związku z realizacją Umowy jest ograniczona do wysokości limitu oznaczonego w Umowie /Zamówieniu, jako limit odpowiedzialności NTT.

6.2. STRONY wyłączają odpowiedzialność NTT z tytułu rękojmi za wady fizyczne i prawne rezultatów prac dostarczanych ZAMAWIAJĄCEMU w toku wykonywania Umowy.

KARY UMOWNE

6.3. W razie niewykonania lub nienależytego wykonania Umowy przez jedną ze STRON, druga STRONA jest uprawniona do naliczenia STRONIE naruszającej Umowę karę umowną – w wypadkach i w wysokości szczegółowo określonych w Umowie. Kara umowna będzie płatna na pierwsze żądanie, w terminie 14 dni od dnia doręczenia pisemnego wezwania STRONIE zobowiązanej do zapłaty przez drugą STRONĘ.

SIŁA WYŻSZA

6.4. Żadna ze STRON nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich obowiązków w ramach Umowy, jeśli niewykonanie lub nienależyte wykonanie tych obowiązków jest wynikiem Siły Wyższej.

6.5. Jeśli niemożność wykonania przez jedną ze STRON jej zobowiązań w wyniku Siły Wyższej w istotny sposób wpływa na możliwość wykonania przez drugą STRONĘ jej zobowiązań w ramach Umowy, ta STRONA również nie będzie odpowiedzialna za niewykonanie swoich zobowiązań. STRONA, która zawiadomiła o zaistnieniu okoliczności Siły Wyższej nie ponosi odpowiedzialności wobec drugiej STRONY za jakiekolwiek straty lub szkody, poniesione przez tę drugą STRONĘ, od daty wystąpienia Siły Wyższej, pod warunkiem, że zawiadomienie zostanie dokonane na piśmie, najpóźniej w terminie 14 dni od ustania okoliczności Siły Wyższej, pod rygorem utraty uprawnień wynikających z niniejszego postanowienia.

6.6. Niezależnie od zobowiązania wynikającego z pkt. 6.5 Załącznika, STRONA, której dotyczy Siła Wyższa, zobowiązana jest powiadomić drugą STRONĘ o wystąpieniu Siły Wyższej niezwłocznie po jej wystąpieniu, gdy tylko będzie to możliwe i wraz z takim powiadomieniem, przekazać następujące informacje (o ile są one danej STRONIE znane lub możliwe do ustalenia):

6.6.1. informacja o tym na czym polega zdarzenie Siły Wyższej;

6.6.2. informacja o chwili rozpoczęcia i szacowanym czasie trwania Siły Wyższej;

6.7. Jeśli wykonanie części lub całości jakiegokolwiek zobowiązania wynikającego z Umowy jest opóźnione z powodu Siły Wyższej o okres przekraczający 60 dni względem terminów wynikających z Umowy, Strony spotkają się i w dobrej wierze rozpatrzą celowość i warunki rozwiązania Umowy.

7. ZAKOŃCZENIE OBOWIĄZYWANIA UMOWY I STRATEGIA WYJŚCIA (EXIT PLAN)

7.1. Każda ze STRON jest uprawniona do wypowiedzenia Umowy /Zamówienie, jeżeli Umowa przewiduje takie uprawnienie i z zachowaniem okresu wypowiedzenia w niej wskazanego.

7.2. Niezależnie od innych postanowień Umowy /Zamówienie, ZAMAWIAJĄCY jest uprawniony do wypowiedzenia Umowy:

7.2.1. z zachowaniem 3 miesięcznego okresu wypowiedzenia – w przypadku, gdy Organ nadzoru wyda decyzję nakazującą ZAMAWIAJĄCEMU rozwiązanie Umowy. W takim wypadku wypowiedzenie jest skuteczne z chwilą doręczenia NTT oświadczenia o wypowiedzeniu wraz z kopią wydanej przez Organ nadzoru decyzji dotyczącej rozwiązania Umowy;

7.2.2. z zachowaniem 1 miesięcznego okresu wypowiedzenia – w przypadku, gdy ZAMAWIAJĄCY zwrócił się do NTT z wnioskiem o rozwiązanie lub zmianę umowy z określonym Podwykonawcą z uwagi na naruszenie lub zagrożenie istotnego interesu ZAMAWIAJĄCEGO (zgodnie z pkt. 3.3 Załącznika) i STRONY w terminie 30 dni nie doszły do porozumienia w zakresie zmiany takiej umowy z Podwykonawcą lub jej rozwiązania;

7.2.3. z zachowaniem 1 miesięcznego okresu wypowiedzenia – w przypadku, gdy NTT powierzył świadczenie Usług Podwykonawcy, który nie uzyskał akceptacji ZAMAWIAJĄCEGO zgodnie z rozdziałem 3 Załącznika;

7.2.4. z zachowaniem 1 miesięcznego okresu wypowiedzenia – w przypadku, gdy NTT w związku ze świadczeniem Usług narusza obowiązujące ZAMAWIAJĄCEGO przepisy prawa lub regulacje a ZAMAWIAJĄCY wezwał NTT do zaniechania naruszeń, wyznaczając w tym celu odpowiedni termin, który bezskutecznie upłynął;

7.2.5. z zachowaniem 1 miesięcznego okresu wypowiedzenia – w przypadku, gdy NTT naruszy Umowę w sposób powodujący zagrożenie bezpieczeństwa informacji ZAMAWIAJĄCEGO i nie zaprzestanie naruszenia w wyznaczonym przez ZAMAWIAJĄCEGO, odpowiednim terminie;

7.3. Niezależnie od innych postanowień Umowy, NTT jest uprawnione do wypowiedzenia Umowy:

7.3.1. z zachowaniem 1 miesięcznego okresu wypowiedzenia – w przypadku braku osiągnięcia przez STRONY porozumienia co do dopuszczenia określonego Podwykonawcy do świadczenia Usług, zgodnie z pkt. 3.4 Załącznika;

7.3.2. z zachowaniem 1 miesięcznego okresu wypowiedzenia – w przypadku braku osiągnięcia przez STRONY porozumienia co do lokalizacji świadczenia Usług bądź przetwarzania lub przechowywania danych związanych z Usługą, zgodnie z pkt. 4.2 Załącznika;

OKRES PRZEJŚCIOWY

7.4. Z chwilą wypowiedzenia Umowy przez którąkolwiek ze STRON, jak również ogłoszenia przez NTT upadłości lub postawienia NTT w stan likwidacji, rozpoczyna się okres przejściowy („**Okres**

przejściowy"). Okres przejściowy trwa przez czas trwania okresu wypowiedzenia, a jeśli Umowa została rozwiązana w trybie natychmiastowym – przez okres 1 miesiąca.

7.5. W Okresie przejściowym NTT świadczy Usługi w pełnym zakresie i zgodnie z Umową, chyba że STRONY postanowią inaczej na piśmie, pod rygorem nieważności.

7.6. W Okresie przejściowym NTT jest zobowiązane do:

7.6.1. umożliwienia ZAMAWIAJĄCEMU, na jego żądanie, dostępu do danych – w tym danych osobowych – powierzonych NTT przez ZAMAWIAJĄCEGO w związku ze świadczeniem Usług oraz

7.6.2. wydania ZAMAWIAJĄCEMU, na jego żądanie, danych – w tym danych osobowych – powierzonych NTT przez ZAMAWIAJĄCEGO w związku ze świadczeniem Usług, w łatwo dostępnym formacie i w formie ustalonej przez STRONY,

– nie później niż w terminie 1 miesiąca od zgłoszenia NTT takiego żądania przez ZAMAWIAJĄCEGO.

7.7. Z chwilą wydania danych NTT jest uprawnione do zwrotu kosztów realizacji prac poświęconych na wydanie danych zgodnie z niniejszym postanowieniem, w tym zwrotu kosztów nośników, na których dane zostały ZAMAWIAJĄCEMU wydane.

7.8. W Okresie przejściowym mają zastosowanie następujące, szczegółowe zasady współpracy:

7.8.1. NTT zobowiązane jest wspierać ZAMAWIAJĄCEGO w umożliwieniu ZAMAWIAJĄCEMU lub podmiotowi trzeciemu przejęcia świadczenia Usług, w zamian za wynagrodzenie określone w odrębnym porozumieniu.

7.9. W Okresie przejściowym NTT, na żądanie ZAMAWIAJĄCEGO wyrażone w formie pisemnej pod rygorem nieważności, zobowiązane jest trwale usunąć wszystkie informacje powierzone NTT przez ZAMAWIAJĄCEGO w związku ze świadczeniem Usług, będące w posiadaniu NTT oraz do zobowiązania Podwykonawców do ich usunięcia. Usunięcie informacji zostanie wykonane nie później niż w terminie 14 dni od zgłoszenia takiego żądania przez ZAMAWIAJĄCEGO i będzie potwierdzone stosownym protokołem wydanym ZAMAWIAJĄCEMU przez NTT.

7.10. Niezależnie od innych postanowień Umowy lub Załącznika, NTT jest uprawnione do zachowania pojedynczej kopii danych ZAMAWIAJĄCEGO przetwarzanych lub przechowywanych w związku z zawarciem i wykonywaniem Umowy dla dochodzenia przysługujących NTT roszczeń lub dla obrony przed ewentualnymi roszczeniami dochodzonymi przeciwko NTT, z zastrzeżeniem, że NTT nie jest uprawnione do wykorzystania tych danych w żadnym innym celu niż ochrona przysługujących NTT praw.

8. POSTANOWIENIA KOŃCOWE

8.1. Umowa jest zawarta pod prawem polskim.

8.2. Wszelkie spory wynikające z tej umowy lub pozostające w związku z nią będą rozstrzygane ostatecznie na podstawie Regulaminu Arbitrażowego Sądu Arbitrażowego przy Krajowej Izbie Gospodarczej w Warszawie, obowiązującego w dniu wszczęcia postępowania, przez arbitra lub arbitrów powołanych zgodnie z tym Regulaminem.

8.3. Umowa określa szczegółową procedurę jej zmiany przez STRONY, w tym zmiany parametrów świadczonych przez NTT Usług.