Warszawa, 9 października 2024 r.

ZWIĄZEK BANKÓW POLSKICH

Rekomendacje Zarządu Związku Banków Polskich z dnia 9 października 2024 r. ws. zgodnych z Rozporządzeniem DORA wzorów aneksów do umów o świadczenie usług ICT

Wersja 1.0

Niniejsze rekomendacje nie stanowią rekomendacji w rozumieniu artykułu 137 ust. 1 pkt 5 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, a stanowią dobre praktyki – samoregulację sektora bankowego w Polsce.

Spis treści

1. Wstęp

17 stycznia 2025 r. rozpocznie się okres stosowania wobec podmiotów finansowych, w tym wobec sektora bankowego, przepisów rozporządzenia DORA[1]. Nowy akt prawny wprowadza dla branży finansowej szereg wymogów, których celem jest zapewnienie wysokiego poziomu odporności cyfrowej na terenie UE. Jednym z elementów zapewnienia odporności finansowej podmiotów finansowych na gruncie DORA, jest wprowadzenie uregulowań dotyczących kształtowania relacji z zewnętrznymi dostawcami ICT. Zgodnie z przepisami rozporządzenia, podmioty finansowe zobowiązane będą m.in. do oceny ryzyka związanego z dostawcami ICT oraz do zapewnienia sobie w ramach zawieranych umów odpowiednich uprawnień gwarantujących właściwy poziom bezpieczeństwa w ramach ukształtowanych relacji.

W tym zakresie, artykuł 30 Rozporządzenia DORA wymaga włączenia do każdej umowy, która dotyczy korzystania przez podmiot finansowy z Usług ICT, określonych postanowień umownych regulujących m.in. zapewnienie określonego, minimalnego standardu świadczonych usług, zapewnienie odpowiednich uprawnień audytowych podmiotów finansowych wobec dostawców usług ICT oraz zapewnienie odpowiednich podstaw do wypowiedzenia umowy. Jednocześnie, zakres obowiązkowych klauzul umownych jest zróżnicowany w zależności od tego, czy dany dostawca wspiera funkcje krytyczne lub istotne związane z funkcjonowaniem danego podmiotu finansowego.

Zgodnie z artykułem 30 ust. 4 Rozporządzenia DORA, negocjując ustalenia umowne, podmioty finansowe i zewnętrzni dostawcy usług ICT powinni rozważać zastosowanie standardowych klauzul umownych opracowanych przez organy publiczne dla określonych usług. Ustawodawca unijny, wprowadzając ww. przepis zwrócił uwagę na potrzebę opracowywania w ramach sektora finansowego propozycji ustandaryzowanych klauzul umownych, które pozostawałyby zgodne z wymogami określonymi przez rozporządzenie DORA.

Wychodząc naprzeciw potrzebom rynkowym związanych z właściwym ukształtowaniem relacji przedstawicieli sektora bankowego z zewnętrznymi dostawcami usług ICT, Związek Banków Polskich podjął działania zmierzające do wypracowania wzorów aneksów, które mogłyby być stosowane jako standardowe klauzule umowne. W tym celu, została zorganizowana grupa robocza składająca się z przedstawicieli banków, reprezentujących komórki prawne oraz komórki bezpieczeństwa. Efektem prac grupy było opracowanie wzoru aneksu wdrażającego wymogi rozporządzenia DORA w relacjach z dostawcami wspierającymi krytyczne lub istotne funkcje (art. 30 ust. 2 rozporządzenia) oraz wzoru aneksu dotyczącego relacji z dostawcami wspierającymi pozostałe funkcje (art. 30 ust. 1 rozporządzenia).

Opracowany materiał stanowi formę wsparcia sektora bankowego w dostosowaniu wewnętrznych procedur oraz kształtu postanowień umownych łączących banki z dostawcami usług ICT do wymagań rozporządzenia DORA. Propozycje wzorów aneksów opracowane w ramach niniejszej Rekomendacji powinny być stosowane z uwzględnieniem zasady adekwatności oraz proporcjonalności – tj. mogą być stosowane w zakresie, w jakim dany podmiot finansowy uzna to za stosowne, uwzględniając specyfikę własnej działalności – w tym specyfikę relacji z zewnętrznymi dostawcami usług ICT. Ponadto, należy podkreślić, że opracowane wzory mogą nie odpowiadać specyfice niektórych relacji łączących podmioty finansowe z określonymi dostawcami zewnętrznymi – w szczególności dostawcami infrastruktury sektora bankowego, w odniesieniu do których konieczne może okazać się zmodyfikowanie niektórych elementów objętych przedmiotowymi wzorami.

Związek Banków Polskich, jak też żaden z jego Członków, nie ponoszą jakiejkolwiek odpowiedzialności za potencjalne szkody, które mogą wiązać się z wykorzystaniem niniejszej Rekomendacji do zmian jakichkolwiek postanowień umownych.

[1] 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. Zasady nadrzędne

2.1. Niniejsze rekomendacje i wytyczne należy traktować jako zbiór dobrych praktyk, które powinny być stosowane według zasady proporcjonalności, co oznacza, że zakres ich stosowania powinien być uzależniony od potrzeb danego podmiotu – w tym m.in. od specyfiki relacji łączących podmiot finansowy z zewnętrznym dostawcą usług ICT;

2.2. Niniejsze rekomendacje należy traktować jako zbiór dobrych praktyk, których stosowanie powinno być poprzedzone analizą ryzyka, której wyniki powinny być udokumentowane między innymi dla potrzeb nadzorczych;

2.3. Podmioty finansowe powinny wypracować i wdrożyć stosowne mechanizmy kontrolne, obejmujące etap wdrożenia i stosowania rekomendowanych rozwiązań, ich aktualizacji oraz dokumentowania;

2.4. Wprowadzenie przez podmioty finansowe przedmiotowych rekomendacji powinno mieć charakter solidarny, a jednocześnie prowadzić do niekonkurowania w obszarze bezpieczeństwa, współpracy i tworzenia najwyższych standardów w zakresie bezpieczeństwa;

2.5. W treści dokumentów wskazano kolorem żółtym fragmenty dokumentu, które powinny zostać uzupełnione przez strony zawierające aneks.

2.6. Instrukcje dotyczące wypełnienia niektórych elementów wzorów zostały umieszczone w treści wzorów *kursywą* oraz w ramach nawiasów [xyz],

2.7. Niektóre z proponowanych postanowień mają charakter opcjonalny – w takim przypadku strony powinny podjąć decyzję, czy decydują się na ich umieszczenie w treści aneksu. Fragmenty opcjonalne zostały wskazane *kursywą* wraz z informacją: [*postanowienie opcjonalne*].

2.8. Zaproponowany kształt klauzul może nie być adekwatny do każdej relacji łączącej podmiot finansowy z zewnętrznymi dostawcami usług ICT – wdrożenie przedmiotowych rekomendacji każdorazowo powinno być poprzedzone stosowną analizą.

2.9. Wraz z zawarciem aneksu, strony powinny również wspólnie opracować oraz dołączyć do umowy stosowne załączniki, których lista została wskazana w treści wzorów. Treść załączników pozostaje do opracowania przez strony, a ich uwzględnienie w ramach aneksów jest rekomendowane przez twórców dokumentu w celu osiągnięcia zgodności z rozporządzeniem DORA.

2.10. Uzyskanie edytowalnej wersji rekomendacji jest możliwe po skierowaniu stosownej prośby na adres: bcc@zbp.pl

3. Wzór aneksu w zakresie dostawców wspierających funkcje krytyczne lub istotne

Aneks nr [xxx] zawarty w dniu [xxx] (zwany dalej „Aneksem"),

pomiędzy:

(dalej **„Bank**"), reprezentowanym przez:

[imię i nazwisko] - [funkcja]

[imię i nazwisko] - [funkcja]

a

[Nazwa drugiej strony umowy] z siedzibą w [xxx] (kod pocztowy: [xxx]) przy ul. [xxx], wpisanym do rejestru przedsiębiorców Krajowego Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy [xxx], [xxx] Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: [xxx], NIP: [xxx], kapitał zakładowy: [xxx] PLN, kapitał w pełni opłacony (dalej „**Dostawca**"), reprezentowanym w przez:

[imię i nazwisko] - [funkcja]

[imię i nazwisko] - [funkcja]

łącznie zwani „Stronami", a każdego z osobna: „Stroną".

Preambuła:

1. Bank powierzył Dostawcy świadczenie określonych usług w umowie, a Dostawca zobowiązał się do ich świadczenia na warunkach określonych w umowie pomiędzy Bankiem a Dostawcą z dnia [xxx], z późniejszymi zmianami („**Umowa Główna**").

2. Bank jest zobowiązany do wypełniania obowiązków nałożonych na niego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 („**DORA**") jako „**podmiot finansowy**" oraz poprzez odpowiednie Wykonawcze Standardy Techniczne („**RTS**") do DORA. Bank identyfikuje usługi wykonywane przez Dostawcę na podstawie Umowy Głównej jako świadczenie „**Usług ICT**", w tym jako wspierające „**krytyczne lub istotne funkcje**" w rozumieniu DORA.

3. DORA wymaga włączenia do każdej umowy, która dotyczy korzystania przez Bank z Usług ICT określonych postanowień umownych. Umowa Główna zawiera część postanowień, które są wymagane dla zgodności z DORA, dlatego zamiarem Banku i Dostawcy jest wprowadzenie zmian do Umowy Głównej, aby zapewnić pełną zgodność jej warunków z wymogami DORA.

1. Definicje

O ile wyraźnie nie stwierdzono inaczej, wszystkie definicje użyte poniżej mają następujące znaczenie:

Dodatkowe Wymagania DORA	Znaczenie zdefiniowane w postanowieniu 5.1. Aneksu
Rozporządzenie DORA	oznacza 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
Właściwy Organ	Pod tym pojęciem należy rozumieć Komisję Nadzoru Finansowego
Incydent związany z ICT / Incydent ICT / Naruszenie Bezpieczeństwa / incydent bezpieczeństwa	Pojedyncze zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które naruszają bezpieczeństwo sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy.
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.
TLPT	Oznacza testy penetracyjne oparte na zagrożeniach zgodnie z art. 26 i 27 rozporządzenia DORA.
Organy ds. Restrukturyzacji i Uporządkowanej Likwidacji	Pod tym pojęciem należy rozumieć Bankowy Fundusz Gwarancyjny lub inne instytucje, których celem jest prowadzenie procedury restrukturyzacji i uporządkowanej likwidacji.

Postanowienia ogólne:

2. Zasady interpretacji zapisów Umowy Głównej oraz Aneksu

2.1. Słowa i wyrażenia zdefiniowane w Umowie Głównej mają takie samo znaczenie w Aneksie, o ile w Aneksie nie zaznaczono inaczej lub o ile kontekst nie stanowi inaczej.

2.2. Zasady interpretacji Umowy Głównej mają zastosowanie do Aneksu, tak jakby zostały w nim umieszczone (z uwzględnieniem zasady określonej w pkt. 3.3. poniżej).

3. Reguły kolizyjne

Z mocą obowiązującą od dnia podpisania Aneksu, Strony zgodnie postanawiają, że:

3.1. zmieniają treść Umowy Głównej poprzez dodanie postanowień umownych zawartych w Załączniku nr 1 do Aneksu,

3.2. w razie sprzeczności między postanowieniami ustalonymi w Umowie Głównej a postanowieniami umownymi zawartymi w Załączniku 1 do Aneksu, odpowiednie zastosowanie mają postanowienia określone w Załączniku nr 1 do Aneksu,

3.3. w razie stwierdzenia niezgodności z przepisami prawa, nieważności lub niewykonalności poszczególnego postanowienia Aneksu, postanowienie to, w zakresie, w jakim jest niezgodne z prawem, nieważne lub niemożliwe do wyegzekwowania, będzie bezskuteczne i traktowane jako niezawarte w Aneksie, bez wpływu na ważność i wykonalność pozostałych postanowień Aneksu.

4. Skuteczność Aneksu

4.1. Aneks i Umowa Główna (wraz ze zmianami wprowadzonymi Aneksem) stanowią całość porozumień i ustaleń Stron oraz zastępują wszystkie wcześniejsze umowy, ustalenia lub porozumienia (ustne lub pisemne) w przedmiocie Aneksu i Umowy Głównej.

4.2. Każda ze Stron jest zobowiązana wykonać wszystkie czynności, jakie mogą być zasadnie wymagane dla nadania pełnej skuteczności postanowieniom tego Aneksu.

5. Dodatkowe Wymagania DORA

5.1. Bez uszczerbku dla ogólnego charakteru klauzul zawartych w Umowie dotyczących wprowadzania zmian do Umowy, Dostawca przyjmuje do wiadomości i wyraża zgodę na dalsze zmiany Umowy w celu uwzględnienia wymogów wynikających z DORA, implementowanych w politykach/standardach Banku, w terminach uzgodnionych z Bankiem ("**Dodatkowe Wymagania DORA**"). Wprowadzenie zmian każdorazowo wymagać będzie zawarcia przez Strony stosownego aneksu.

5.2. Bank będzie działać w sposób racjonalny przy określaniu swoich wymogów w ramach DORA oraz ram czasowych dla Dodatkowych Wymagań DORA.

6. Postanowienia końcowe

6.1. Każda ze Stron jest zobowiązana pokryć koszty własne i wydatki związane z negocjowaniem, przygotowaniem, zawarciem i wykonaniem Aneksu.

6.2. Aneks został sporządzony w dwóch egzemplarzach, a w przypadku gdy jego zawarcie będzie dokonywane w formie elektronicznej – w jednym egzemplarzu udostępnionym elektronicznie.

6.3. Aneks zostanie zawarty w formie oświadczeń woli złożonych pisemnie albo w postaci elektronicznej w rozumieniu art. 78 in. 1 Kodeksu cywilnego. Za datę zawarcia Aneksu Strony uznają dzień złożenia podpisu przez osobę reprezentującą Stronę składającą podpis jako ostatnia.

6.4. Zmiany Umowy zawarte w Załączniku wchodzą w życie z dniem [XXX] ("**Data wejścia w życie**").

Podpisały osoby uprawnione do reprezentowania Stron w dacie oznaczonej na wstępie Aneksu.

(Bank):
Imię i nazwisko: [xxx]
Stanowisko: [xxx]
Podpis: [xxx]

[xxx] (Dostawca):
Imię i nazwisko: [XXX]
Stanowisko: [xxx]
Podpis: [xxx]

Załączniki:

Załącznik nr 1 - Klauzule umowne wymagane w świetle rozporządzenia DORA oraz odpowiednich RTS.

Załącznik nr 2 - Miejsca przechowywania i przetwarzania danych przez Dostawcę oraz jego podwykonawców.

Załącznik nr 3 – Wykaz raportów sporządzanych przez Dostawcę

Załącznik nr 4 – Standardy Bezpieczeństwa dotyczące usług świadczonych przez Dostawcę

Załącznik nr 5 – Opis gwarantowanego poziomu Usług (SLA)

Załącznik nr 6 – Opis Strategii Wyjścia

Załącznik nr 1 - Klauzule umowne wymagane w świetle rozporządzenia DORA oraz odpowiednich RTS

1. Opis usług

1.1 Opis Usług realizowanych przez Dostawcę

[*Należy uzupełnić o kompletny opis usług realizowanych przez Dostawcę. W przypadku umów, w których Przedmiot umowy w całości obejmuje usługi/funkcje ICT należy skopiować całe postanowienie ze wskazaniem odpowiedniego postanowienia Umowy (źródłowe miejsce) z podziałem na poszczególne Usługi.*
W przypadku umów, w których Przedmiot umowy w całości obejmuje nie tylko usługi/funkcje ICT należy z Przedmiotu umowy wyodrębnić usługi/funkcje ICT i opisać je (ze wskazaniem odpowiedniego postanowienia Umowy (źródłowe miejsce) z podziałem na poszczególne Usługi.

Funkcje muszą być zdefiniowane per usługa - jeśli w umowie realizowanych jest więcej usług ITC [np. dostawa sprzętu + licencja + wsparcie, dla każdej usługi należy zdefiniować funkcję]
Usługa 1
Usługa 2
Usługa 3
itp..]

1.2. Funkcje obsługiwane przez Usługę realizowaną przez Dostawcę

[Należy wskazać numery Usług wskazanych w 1.1 realizowanych przez daną Funkcję (zgodnie z powyższą numeracją) lub wpisać "ND"]

Identyfikator funkcji ICT	**Nazwa funkcji ICT**	**Opis**	**Usługi obsługujące funkcje**
S1	1. ICT project management	Świadczenie usług związanych z: Project Management Officer (PMO).	
S2	2. ICT Development	Świadczenie usług związanych z: analizą biznesową, projektowaniem i tworzeniem oprogramowania, testowaniem.	
S3	3. ICT help desk and first level support	Świadczenie usług związanych z: wsparciem helpdesk i wsparciem pierwszego poziomu w zakresie incydentów ICT	
S4	4. ICT security management services	Świadczenie usług związanych z: bezpieczeństwem ICT (ochrona, wykrywanie, reagowanie i odzyskiwanie), w tym obsługa incydentów bezpieczeństwa i śledztwa informatyczne.	
S5	5. Provision of data	Subskrypcja usług dostawców danych (usługa danych cyfrowych)	
S6	6. Data analysis	Świadczenie usług związanych z wsparciem analizy danych (usługa danych cyfrowych)	
S7	7. ICT facilities and hosting	Zapewnienie infrastruktury ICT, obiektów i usług hostingowych. Obejmuje to	

	services (excluding Cloud services)	dostarczanie mediów (energia, zarządzanie ciepłem...), dostęp telekomunikacyjny i bezpieczeństwo fizyczne. (z wyłączeniem usług w chmurze)		
S8	8. Computation	Zapewnienie możliwości przetwarzania cyfrowego (w tym obliczania danych). Nie obejmuje to usług obliczeniowych wykonywanych w kontekście środowiska chmury.		
S9	9. Non-Cloud Data storage	Zapewnienie platformy przechowywania danych (z wyłączeniem usług w chmurze).		
S10	10. Telecom carrier	Operacje dla systemów telekomunikacyjnych i zarządzanie przepływem. Tradycyjne analogowe usługi telefoniczne są wyraźnie wyłączone zgodnie z art. 3 ust. 21 rozporządzenia (UE) 2022/2554.		
S11	11. Network infrastructure	Zapewnienie infrastruktury sieciowej		
S12	12. Hardware and physical devices	Dostarczanie stacji roboczych, telefonów, serwerów, urządzeń do przechowywania danych, urządzeń itp. w formie usługi		
S13	13. Software licencing (excluding SaaS)	Dostarczanie oprogramowania działającego lokalnie.		
S14	14. ICT operation management (including maintenance)	Świadczenie usług związanych z: konfiguracją infrastruktury (systemów i sprzętu z wyjątkiem sieci), konserwacją, instalacją, zarządzaniem pojemnością, zarządzaniem ciągłością działania itp. W tym dostawcy usług zarządzanych (MSP).		
S15	15. ICT Consulting	Świadczenie usług w zakresie wiedzy intelektualnej / eksperckiej ICT.		
S16	16. ICT Risk management	Weryfikacja zgodności z wymogami zarządzania ryzykiem w zakresie ICT zgodnie z art. 6 ust. 10 rozporządzenia (UE) 2022/2554.		
S17	17. Cloud services: IaaS	Infrastructure-as-a-Service		
S18	18. Cloud services: PaaS	Platform-as-a-Service		
S19	19. Cloud services: SaaS	Software-as-a-Service		

1.3 Podwykonawstwo

[Należy wskazać wszystkich występujących Podwykonawców wraz z opisem realizowanych przez wskazanego Podwykonawcę Usług oraz numerem Funkcji obsługiwanej przez Usługę zgodnie z tabelą wskazaną w 1.2. Należy wskazać czy dozwolone jest podwykonawstwo usług ICT wspierających krytyczną lub ważną funkcję lub ich istotne części, a w takim przypadku warunki mające zastosowanie do takiego podwykonawstwa. W przypadku gdy brak jest podwykonawców - należy usunąć pkt 1.3 w całości.]

1.3.1 Pełna nazwa Podwykonawcy A

[Opis Usług realizowanych przez Podwykonawcę A

Funkcje obsługiwane przez Usługę ICT realizowaną przez Podwykonawcę A: Sx; Sy; Sz]

1.3.2 Pełna nazwa Podwykonawcy B

[Opis Usług realizowanych przez Podwykonawcę B

Funkcje obsługiwane przez Usługę realizowaną przez Podwykonawcę B: Sx; Sy; Sz]

Strony uzgadniają, że dozwolone jest / nie jest dozwolone podwykonawstwo usług ICT wspierających krytyczną lub ważną funkcję lub ich istotne części.

[Wariant, gdy dozwolone jest podwykonawstwo usług ICT wspierających krytyczną lub ważną funkcję lub ich istotne części:]

Dopuszcza podwykonawstwo następujących Usług ICT wspierających krytyczną lub ważną funkcję lub ich istotne części:

[do uzupełnienia]

na następujących warunkach:

[do uzupełnienia]

1.3.3. Dostawca zobowiązuje się do zapewnienia sobie w umowie z podwykonawcą możliwości dostępu i pozyskania kopii umów z jego dalszymi podwykonawcami, w tym na potrzeby przekazania jej Bankowi. Dotyczy to także zapewnienia, by podwykonawca w umowach z dalszymi swoimi podwykonawcami, poprzez stosowne postanowienia umowne posiadał zapewnioną możliwość dostępu i pozyskania kopii umów zawartych z dalszymi podwykonawcami, w tym na potrzeby przekazania jej Bankowi, celem zapewnienia monitorowania całego łańcucha podwykonawstwa Usługi ICT przez Bank.

2. Wypowiedzenie Umowy

2.1 **Okres wypowiedzenia**. Bank może, bez podania przyczyny, rozwiązać Umowę na piśmie przesłanym Dostawcy z zachowaniem minimum [xxx] okresu wypowiedzenia.

2.2 **Wypowiedzenie Umowy z podaniem przyczyny**. Bank może rozwiązać Umowę na piśmie ze skutkiem natychmiastowym, jeżeli:

(a) Właściwy Organ wyda stosowną rekomendację, komunikat, stanowisko lub decyzję;

(b) wynika to z wytycznych lub oczekiwań wyrażonych w innej formie wydanych przez Właściwy Organ lub Organy ds. Restrukturyzacji i Uporządkowanej likwidacji;

(c) Dostawca naruszy istotne zobowiązanie wynikające z postanowień Umowy lub dopuszcza się poważnego naruszenia przepisów ustawowych, wykonawczych lub wytycznych Właściwego Organu;

(d) w trakcie monitorowania ryzyka ze strony Dostawcy zostaną zidentyfikowane okoliczności, w przypadku wystąpienia których Bank uzna, że mogą one zmienić wykonywanie Usług ICT przewidzianych w Umowie, w tym istotne zmiany mające wpływ na Umowę lub sytuację Dostawcy;

(e) zostaną wykazane słabe strony Dostawcy w zakresie jego ogólnego zarządzania ryzykiem związanym z ICT, a w szczególności, w odniesieniu do sposobu, w jaki zapewnia on dostępność, autentyczność, integralność i poufność danych, niezależnie od tego, czy wykazane słabe strony dotyczą danych osobowych lub danych w inny sposób wrażliwych, czy danych nieosobowych; przed wypowiedzeniem Umowy z tej przyczyny, Bank wedle własnego uznania może poinformować Dostawcę o zakresie słabych stron, a także wyznaczyć [xxx] dniowy termin na wdrożenie stosownych działań naprawczych. W przypadku wyznaczenia tego terminu, wypowiedzenie Umowy z tej przyczyny jest możliwe po jego bezskutecznym upływie;

(f) gdy w wyniku warunków lub okoliczności związanych z Umową, Właściwy Organ nie może już skutecznie nadzorować Banku;

(g) Dostawca wprowadza istotne zmiany w umowie z podwykonawcą pomimo sprzeciwu Banku lub bez wyraźnej zgody Banku, albo przed upływem wskazanego w powiadomieniu przez Dostawcę terminu wprowadzenia zmiany;

(h) Dostawca zleca podwykonawstwo usługi wpierającej krytyczną lub ważną funkcję, której zlecanie podwykonawcom wyraźnie nie jest dozwolone na mocy Umowy;

(i) wymagania bezpieczeństwa Banku ulegną zmianie, a Dostawca nie wyrazi zgody na dostosowanie się do tych wymagań w terminie wyznaczonym przez Bank;

(j) gdy świadczenie usług nie odpowiada poziomowi usług uzgodnionemu z Bankiem. Przed wypowiedzeniem Umowy z tej przyczyny, Bank, wedle własnego uznania, może poinformować Dostawcę o zakresie Usług ICT nieodpowiadających uzgodnionemu poziomowi usług, a także wyznaczyć [xxx] dniowy termin na wdrożenie stosownych działań naprawczych. W razie wyznaczenia tego terminu, wypowiedzenie Umowy z tej przyczyny jest możliwe po jego bezskutecznym upływie.

3. Miejsce Świadczenia Usług

3.1 Usługi ICT i przedmiot Umowy będzie dostarczany wyłącznie z Miejsc Świadczenia Usług – tj. regionów lub krajów, w których mają być świadczone funkcje i Usługi ICT objęte Umową lub podwykonawstwem oraz w których mają być przetwarzane dane, w tym miejsce przechowywania. Miejsca Świadczenia Usług, w tym miejsca przechowywania danych i miejsca przetwarzania danych, w tym przez podwykonawców Dostawcy w ramach Umowy, zostały określone w Załączniku nr 2 do Aneksu. Jeżeli Dostawca zechce zmienić Miejsce Świadczenia Usług lub wykonywać Usługę z innego

miejsca, musi wcześniej powiadomić o tym Bank na piśmie z podaniem informacji o nowym, proponowanym miejscu w zakresie, jakiego Bank może zażądać, na co najmniej [xxx] dni roboczych przed proponowanym terminem rozpoczęcia Usług w nowym miejscu. Usługi nie mogą być dostarczane z innego Miejsca Świadczenia Usług bez uprzedniego uzyskania pisemnej zgody Banku oraz bez pisemnego zatwierdzenia przez Bank procedur bezpieczeństwa dla nowego Miejsca Świadczenia Usług. Wymóg ten dotyczy również Miejsca Świadczenia Usług podwykonawców Dostawcy.

[Postanowienie opcjonalne:]

3.2 Dostawca zwróci Bankowi uzasadnione koszty dodatkowe, poniesione przez Bank w wyniku zmiany Miejsca Świadczenia Usług z inicjatywy Dostawcy.

4. Bezpieczeństwo danych

4.1 Dostawca zobowiązuje się niezwłocznie informować Bank o wszelkich incydentach związanych z bezpieczeństwem danych, w tym danych osobowych, dotyczących świadczonej dla Banku Usługi ICT, mających wpływ na poufność, integralność, autentyczność lub dostępność do danych Banku, a w szczególności o przypadkach nieautoryzowanego dostępu lub przejęcia danych Banku lub naruszenia bezpieczeństwa systemu lub środowiska informatycznego używanego do przetwarzania, przesyłania lub przechowywania danych Banku. Incydenty powinny być zgłaszane do wskazanych w Umowie osób kontaktowych oraz na adres dedykowany do zgłaszania incydentów [xxx].

4.2 Dostawca zobowiązuje się do wdrożenia niezbędnych środków związanych z zapewnieniem bezpieczeństwa danych, w tym środków minimalizujących ryzyko wycieku, kradzieży i manipulacji danymi oraz do zapewnienia, w ramach wynagrodzenia z tytułu Umowy, pomocy Bankowi, w przypadku wystąpienia incydentu ICT dotyczącego świadczonej Usługi ICT.

4.3 Dostawca zobowiązuje się do zwrotu lub zniszczenia, powierzonych przez Bank informacji w uzgodnionym czasie w trakcie trwania Umowy lub po jej zakończeniu.

4.4 Dostawca jest zobowiązany do usuwania podatności, w szczególności krytycznych i istotnych, w swoich systemach, narzędziach i procesach oraz niezwłocznego reagowania na cyberzagrożenia, które mogą mieć negatywny wpływ na usługi świadczone dla Banku.

4.5 Dostawca w odpowiednim przypadku i na żądanie Banku będzie sporządzać raporty okresowe, raporty o incydentach, raporty o świadczeniu Usług ICT, raporty z obszaru bezpieczeństwa teleinformatycznego oraz środków i testów ciągłości działania. Szczegółowy wykaz raportów sporządzanych na podstawie Umowy przez Dostawcę określony jest w Załączniku nr 3.

5. Dostęp do danych

5.1 W razie rozwiązania Umowy, bez względu na powód, lub upływu czasu jej trwania, Dostawca niezwłocznie bez konieczności wezwania zwróci lub usunie (wedle wyboru Banku) wszystkie składniki majątkowe, informacje, dane (w tym Dane Osobowe) i materiały (w tym kopie) – dalej jako: „Dane" należące do Banku, które w owym czasie znajdują się w posiadaniu, władzy lub pod kontrolą Dostawcy. W przypadku zwrotu Danych, może on zostać dokonany wedle wyboru Banku, Bankowi lub zastępczemu dostawcy, w formacie i na nośnikach uzgodnionych przez Strony. Na wyraźne polecenie Banku i w terminie wskazanym przez Bank lub innym uzgodnionym przez Strony, Dostawca zniszczy takie Dane. Fakt ich zniszczenia zostanie udokumentowany w formie protokołu przez osobę upoważnioną przez Dostawcę.

[Postanowienie opcjonalne]
W przypadku danych zapisanych w systemach informatycznych w sposób automatyczny, w ramach kopii zapasowych, gdy obowiązujące przepisy prawa pozwalają na przechowywanie tych danych, Dostawca nie będzie podejmował celowych działań zmierzających do odzyskania Danych oraz nadal będą one traktowane przez Dostawcę jako poufne oraz zostaną usunięte nie później niż do ustania przydatności kopii zapasowej, z zastrzeżeniem, że Dane nie mogą być użyte dla celów innych niż związanych z Umową lub wynikających z obowiązujących przepisów prawa. Usunięcie danych zostanie potwierdzone przez Dostawcę w formie protokołu sporządzonego przez osobę upoważnioną przez Dostawcę.

5.2 W czasie trwania Umowy Dostawca jest zobowiązany do sporządzania kopii zapasowych wszystkich danych należących do Banku, z częstotliwością przynajmniej [XXX]. W razie rozwiązania Umowy wskutek niewypłacalności Dostawcy lub zakończenia działalności gospodarczej przez Dostawcę, wówczas – bez wpływu na punkt 5.1 – Dostawca udostępni Bankowi ostatnie kopie zapasowe Danych w ciągu 7 Dni Roboczych po rozwiązaniu Umowy.

6. Współpraca z Organem Właściwym lub Organami ds. Restrukturyzacji i Uporządkowanej Likwidacji

6.1 Dostawca będzie współpracować z Bankiem i jego personelem oraz przedstawicielami, Właściwym Organem, Organami ds. Przymusowej Restrukturyzacji i Uporządkowanej Likwidacji i osobą wyznaczoną przez Właściwy Organ lub Organy ds. Przymusowej Restrukturyzacji i Uporządkowanej Likwidacji w sprawach, w których będzie to wymagane, w tym w związku z wykonywaniem obowiązku lub prawa wynikającego z przepisów prawnych lub dochodzenia prowadzonego przez Bank lub inny podmiot w jego imieniu lub przez Właściwy Organ lub Organy ds. Przymusowej Restrukturyzacji i Uporządkowanej Likwidacji . Forma współpracy może polegać na udostępnieniu lub zapewnieniu dostępu do dokumentacji, informacji, danych, systemów, pomieszczeń i sieci telekomunikacyjnych, jakie znajdują się w posiadaniu, pieczy lub pod kontrolą Dostawcy, jego podwykonawców lub agentów.

6.2 Bank oraz jego Dostawcy podlegają nadzorowi sprawowanemu przez Właściwy Organ, w ramach którego Właściwy Organ jest uprawniony do przeprowadzania badań i sprawowania nadzoru nad Dostawcami wykonującymi pewne funkcje lub operacje, tak jakby dane funkcje lub operacje wykonywał Bank w pomieszczeniach Banku. Dostawca będzie współpracować i niezwłocznie spełniać wszystkie żądania Właściwego Organu.

7. Programy zwiększania świadomości w zakresie bezpieczeństwa teleinformatycznego

7.1. Dostawca zobowiązuje się do zwiększania świadomości swojego personelu, zaangażowanego do realizacji Umowy w zakresie bezpieczeństwa teleinformatycznego oraz do przeprowadzania szkoleń dla swojego personelu w zakresie operacyjnej odporności cyfrowej. W stosownych przypadkach i na żądanie Banku Dostawca będzie również uczestniczyć w opracowanych przez Bank programach zwiększania świadomości w zakresie bezpieczeństwa teleinformatycznego i szkoleniach w zakresie operacyjnej odporności cyfrowej.

8. Testy TLPT

8.1. Dostawca, w ramach realizacji Umowy jest zobowiązany do:

a) przeprowadzania analizy ryzyka związanego z własną działalnością pod kątem cyberzagrożeń w zakresie usług krytycznych i istotnych, świadczonych dla Banku,
b) regularnego testowania swoich systemów, narzędzi i procesów, które wykorzystuje do świadczenia Usług ICT dla Banku – w tym do analizy dokumentacji, weryfikacji zgłaszanych błędów lub incydentów, przeprowadzania testów penetracyjnych, a także do wprowadzania odpowiednich zabezpieczeń w sytuacji, gdy zostaną wykryte nieprawidłowości,
c) wspierania Banku w opracowaniu programu testów TLPT, w tym w opracowaniu regulacji wewnętrznych,
d) przekazania na żądanie Banku informacji bądź raportu z testów TLPT przeprowadzanych przez Dostawcę, w tym ich częstotliwości, wyniku testów oraz działań naprawczych jakie zostały podjęte.

8.2. Dostawca będzie uczestniczyć w testach penetracyjnych pod kątem wyszukiwania zagrożeń Banku (TLPT) oraz zobowiązuje się do pełnej współpracy w tym zakresie. W tym celu Dostawca jest zobowiązany do:

a) podjęcia niezbędnych działań (w tym przekazania odpowiednich informacji do Banku oraz wyznaczenia personelu Dostawcy do współpracy z Bankiem) w terminie 5 dni roboczych, aby przeprowadzenie testów TLPT było możliwe,
b) wprowadzenia działań naprawczych w ustalonym z Bankiem zakresie i terminie w przypadku wykazania w ramach testów TLPT słabości systemów, narzędzi lub procesów Dostawcy.

9. Audyt

9.1. Bank, jego audytorzy, Właściwy Organ lub osoby wyznaczone przez Bank, jego audytorów lub Właściwy Organ mają prawo do przeprowadzenia audytu Dostawcy w celu zapewnienia przestrzegania warunków Umowy. W razie przeprowadzenia audytu, wewnętrzni lub zewnętrzni audytorzy Banku przekażą Dostawcy stosowne upoważnienie udzielone przez Bank. W celu przeprowadzenia audytu:

(a) Dostawca będzie współpracował ze wskazanymi w poprzednim zdaniu osobami lub podmiotami,
(b) Dostawca uwzględni wymogi wskazane w ramach niniejszego punktu w uzgodnieniach dokonywanych przez niego z każdym podwykonawcą, w tym z usługodawcami świadczącymi usługi w zakresie ciągłości działalności i tworzenia kopii zapasowych,
(c) Dostawca umożliwi Bankowi, jego audytorom lub Właściwemu Organowi:

(i) otrzymanie dokumentów i informacji przekazanych Dostawcy oraz przechowywanych lub przetwarzanych przez Dostawcę związanych z Usługami ICT świadczonymi Bankowi;

(ii) dostęp do każdego raportu i ustalenia dotyczącego Dostawcy i związanego z Usługami ICT świadczonymi Bankowi;

(iii) dostęp do obiektów i pomieszczeń biznesowych wykorzystywanych przez Dostawcę w wykonaniu jego praw określonych w Umowie oraz

(iv) kontrolę, badanie i audyt operacji i dokumentacji Dostawcy w zakresie, w jakim dotyczą one Usług ICT świadczonych przez Dostawcę na podstawie Umowy, w tym między innymi środków kontroli wewnętrznej stosowanych przez Dostawcę w zakresie zachowania poufności i bezpieczeństwa danych oraz, w szczególności, informacji Banku (w odpowiednich przypadkach);

d) Bank niezwłocznie zawiadomi Dostawcę o każdym związanym z Usługami audycie rozpoczętym przez zewnętrzne organy nadzoru lub upoważnione instytucje.

9.2. Oprócz prawa do audytu przestrzegania warunków Umowy, Bankowi przysługuje prawo do dokonywania:

a) audytów środków kontroli wewnętrznej; lub
b) audytów finansowych.

9.3. W przypadku banku będącego uczestnikiem systemu ochrony, o którym mowa w art. 22 a ustawy z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, Bank jest uprawniony do wskazania jednostki zarządzającej systemem ochrony, o której mowa w art. 22 d ustawy z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, lub innego podmiotu, jako podmiotu uprawnionego do przeprowadzenia audytu w imieniu Banku, o którym mowa w pkt. 9.1. oraz 9.2. Skorzystanie przez jednostkę zarządzającą systemem ochrony z tego uprawnienia nie wymaga dodatkowego upoważnienia Banku.

9.4. Dostawca potwierdza, że w ramach prawa dostępu, kontroli i audytu przez Bank, jego audytorów lub przez Właściwy Organ, umożliwi sporządzanie kopii stosownej dokumentacji na miejscu.

9.5. O audytach przeprowadzanych przez audytorów w trybie postanowienia 9.1, 9.2 lub 9.3 (Prawo do przeprowadzania audytu) Dostawca musi być powiadomiony z odpowiednim wyprzedzeniem (pod warunkiem, że nie zabraniają tego stosowne przepisy prawa powszechnie obowiązującego). Audyty będą przeprowadzane z częstotliwością wynikającą z oceny ryzyka prowadzonej przez Bank lub wymaganą przez przepisy prawa lub Właściwy Organ. Dostawca udostępni swoje pomieszczenia, personel, ewidencję w każdym czasie bez wcześniejszego powiadomienia, jeżeli:

a) zażąda tego Właściwy Organ w ramach audytu Banku,
b) zażądają tego upoważnieni wewnętrzni lub zewnętrzni audytorzy Banku, w ramach audytu, którego przedmiotem jest konkretny Incydent ICT lub podejrzenie Incydentu ICT stanowiącego poważne ryzyko dla działalności lub reputacji Banku.

9.6. Dostawca oświadcza, że żadne z postanowień Umowy lub innych umów z jego podwykonawcami, nie utrudniają oraz nie ograniczają skutecznego korzystania z praw do dostępu i audytu przez Bank, Organ Właściwy lub osoby trzecie wyznaczone przez te instytucje do wykonywania takich praw.

10. Alternatywne poziomy zabezpieczeń

10.1. Bank zastrzega sobie prawo do uzgodnienia alternatywnych poziomów zabezpieczenia w przypadku naruszenia praw innych klientów Dostawcy, tj. w szczególności:

a) zwiększenia przez Dostawcę środków organizacyjnych lub technicznych, przeznaczonych na dostarczenie Usług,
b) przeprowadzenia przez Dostawcę dodatkowego audytu lub udziału w dodatkowym audycie przeprowadzonym przez Bank lub upoważnionego przez Bank audytora zewnętrznego,
c) zobowiązanie do udziału w szkoleniu wskazanym przez Bank,
d) pozyskania dodatkowych certyfikatów.

11. Obowiązki Dostawcy w kontekście umowy z podwykonawcami

11.1 Dostawca przed zawarciem umowy z podwykonawcą wspierającym świadczenie usługi dla Banku przez Dostawcę, dokona oceny podwykonawcy, uwzględniającej reputację biznesową podwykonawcy, jego zasoby, w tym wiedzę fachową oraz odpowiednie zasoby finansowe, ludzkie i techniczne, bezpieczeństwo informacji zapewniane przez podwykonawcę oraz jego strukturę organizacyjną, w tym proces zarządzania ryzykiem i kontroli wewnętrznych.

11.2 Dostawca dokona oceny wszelkich rodzajów ryzyka, ze szczególnym uwzględnieniem rodzajów ryzyka z obszaru bezpieczeństwa teleinformatycznego, związanych z lokalizacją potencjalnego podwykonawcy i jego spółki dominującej oraz lokalizacji, z których świadczona jest usługa.

11.3 Dostawca w umowie z podwykonawcą określi obowiązki monitorowania i raportowania wobec Dostawcy lub Banku odpowiadające wymogom Umowy.

11.4 Standardy bezpieczeństwa ICT oraz, w stosownych przypadkach, wszelkie dodatkowe zabezpieczenia, które muszą spełnić podwykonawcy stanowią Załącznik nr 4 do Aneksu.

11.5 Dostawca zobowiązuje się w umowie z podwykonawcą przyznać Bankowi oraz Właściwym Organom co najmniej takie same prawa do audytu, informacji i dostępu, jak przyznane Bankowi i odpowiednim Właściwym Organom przez Dostawcę.

11.6 Dostawca jest zobowiązany zapewnić ciągłe świadczenie usług, nawet w przypadku niespełnienia przez podwykonawcę poziomu usług lub jakichkolwiek innych zobowiązań umownych.

11.7 Dostawca powiadomi Bank o wprowadzeniu istotnej zmiany do umów z podwykonawcami na [xxx] Dni Roboczych przed planowanym wprowadzeniem zmiany. Dostawca wprowadzi istotne zmiany dopiero po zatwierdzeniu zmian przez Bank lub braku sprzeciwu do końca okresu powiadomienia.

11.8 Bank ma prawo żądać od Dostawcy modyfikacji proponowanych zmian w umowie z podwykonawcą przed ich wprowadzeniem, jeżeli z oceny ryzyka dokonanej przez Bank okaże się, że planowane podwykonawstwo lub zmiany w podwykonawstwie planowane przez Dostawcę, narażają Bank na ryzyko. Bank jest uprawniony wycofać zgodę na korzystanie przez Dostawcę z podwykonawcy w przypadku np. decyzji Właściwego Organu nakazującego zakończenie świadczenia Usług ICT przez Podwykonawcę lub innych ważnych przyczyn po stronie podwykonawcy w szczególności niewłaściwej realizacji Usług ICT.

11.9 Dostawca jest zobowiązany do regularnego monitorowania wykonywania przez podwykonawcę obowiązków Dostawcy wynikających z Umowy, by zapewnić ciągłość wypełniania wszystkich obowiązków umownych łączących Strony.

11.10 Dostawca odpowiedzialny jest jak za własne działanie lub zaniechanie za działania i zaniechania osób za pomocą których wykonuje Umowę, jak również osób którym wykonanie zobowiązania wynikającego z Umowy powierza. Żadne z postanowień Umowy nie ustanawia stosunku umownego pomiędzy Bankiem a podwykonawcą lub zobowiązania Banku do zapłaty wynagrodzenia podwykonawcy lub zapewnienia jego zapłaty.

11.11 Dostawca jest zobowiązany do monitorowania wszystkich podzlecanych usług ICT wspierających krytyczną lub ważną funkcję lub jej istotną część, aby zapewnić ciągłe wypełnianie jego zobowiązań umownych wobec Banku.

11.12 Dostawca zobowiązuje się w trakcie trwania Umowy identyfikować oraz niezwłocznie informować Bank o wszelkich podwykonawcach w łańcuchu podwykonawców świadczących usługi ICT wspierające krytyczne lub ważne funkcje. Dostawca zobowiązuje się każdorazowo uzyskiwać zgodę Banku na zawarcie umowy z podwykonawcami, o których mowa w zdaniu pierwszym.

11.13 Na żądanie Banku i w terminie ustalonym z Dostawcą, Dostawca zobowiązuje się przekazać dokumentację umowną z jego podwykonawcami świadczącymi usługi ICT wspierające krytyczne lub ważne funkcje oraz na temat odpowiednich wskaźników efektywności.

12. Plany reagowania na incydenty i plany ciągłości działania

12.1. Dostawca zobowiązuje się do zgłoszenia do Banku potwierdzonych incydentów ICT, zaistniałych po stronie Dostawcy /lub podwykonawcy (jeśli dotyczy) lub podwykonawcy chmurowego (jeśli dotyczy), zgodnie z procedurą, opisaną w punktach 12.2. – 12.6.:

12.2. Niniejszej procedurze podlegają zdarzenia dotyczące usług świadczonych przez Dostawcę w ramach Umowy, a w szczególności:

a) naruszenie co najmniej jednego z atrybutów: poufności, integralności, autentyczności, rozliczalności lub dostępności informacji chronionych, np. nieautoryzowany dostęp do tych informacji (wyciek poza infrastrukturę informatyczną lub nieuprawniony dostęp do dokumentacji przechowywanej poza infrastrukturę informatyczną),

b) podszywanie się pod Dostawcę z wykorzystaniem technik informatycznych (np. phishing, pharming) lub socjotechniki, o ile ma to wpływ na realizację usług świadczonych przez Dostawcę w ramach Umowy,

c) nadużycia personelu Dostawcy zagrażające bezpieczeństwu informacji prawnie chronionych Banku, realizacji usług świadczonych przez Dostawcę w ramach Umowy,

d) naruszenie bezpieczeństwa informacji prawnie chronionych Banku przetwarzanych u podwykonawców chmurowych w usługach chmury obliczeniowej bądź dotyczących infrastruktury wykorzystywanej w usłudze chmurowej, jeśli dotyczy.

12.3. W przypadku wystąpienia Incydentu ICT Dostawca jest zobowiązany do niezwłocznego, ale nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, poinformowania Banku o takim zdarzeniu oraz do ścisłej współpracy z Bankiem, a także do dostarczenia materiałów niezbędnych do skutecznej obsługi tego rodzaju incydentu.

12.4. Incydenty ICT, związane ze świadczeniem usług w ramach Umowy, zidentyfikowane przez:

a) Dostawcę – należy niezwłocznie zgłaszać do Banku, mailowo na adres: [adres email Banku] oraz ewentualnie telefonicznie pod numerem [nr tel. Banku],

b) Bank – należy niezwłocznie zgłaszać do Dostawcy, mailowo na adres: [należy wpisać adres e-mail Dostawcy] oraz ewentualnie telefonicznie pod numerem [należy wpisać nr telefonu Dostawcy].

12.5. Każde zgłoszenie incydentu ICT powinno zawierać przynajmniej:

a) unikalny identyfikator Incydentu ICT (tj. sygnatura, nadawana przez Bank i Dostawcy niezależnie od siebie) incydentu ICT, jednoznacznie identyfikująca dane zdarzenie),

b) datę wystąpienia lub powzięcia informacji o incydencie ICT,

c) opis zdarzenia wraz z okolicznościami i przyczyną jego zaistnienia (o ile jest znany na etapie zgłaszania incydentu ICT),

d) zakres incydentu ICT(zakres osób, danych oraz systemów, których dotyczy),

e) opis podjętych działań w ramach obsługi incydentu ICT,

f) opis planowanych lub już podjętych czynności w celu zapobieżenia takim sytuacjom w przyszłości, o ile mogą być określone na etapie zgłaszania incydentu ICT.

12.6. Dostawca jest zobowiązany do przekazania Bankowi ewentualnych dodatkowych informacji wymaganych przepisami obowiązującego prawa, związanych z Incydentem ICT.

12.7. Dostawca, w przypadku zgłoszenia Incydentu ICT zobowiązany jest aktualizować zgłoszenie okresowo, stosownie do pozyskiwania kolejnych danych aż do czasu zamknięcia obsługi Incydentu ICT.

12.8. Dostawca jest zobowiązany do prowadzenia rejestru incydentów ICT związanych z realizacją Umowy, które wystąpiły w trakcie trwania Umowy, a także do jego udostępnienia na każde żądanie Banku.

13. Strategie wyjścia

13.1. W razie rozwiązania Umowy, bez względu na powód, lub upływu czasu jej trwania, Załącznik nr 6 (Opis Strategii Wyjścia) będzie regulować Usługi ICT, których dotyczy rozwiązanie Umowy.

13.2. Z chwilą rozwiązania Umowy z jakiejkolwiek przyczyny (w tym z powodu uchybienia popełnionego przez którąkolwiek ze Stron) każda ze Stron zapewni drugiej Stronie informacje, współpracę i pomoc, których druga Strona zażąda w celu zapewnienia prawidłowego zwrotu lub przekazania (bez nieuzasadnionego opóźnienia i nie później niż w terminie [xxx] dni po takim rozwiązaniu) Stronie zgłaszającej żądanie lub wyznaczonej przez nią osobie wszystkich danych (oraz związanych z nimi dokumentów i plików) oraz materiałów Strony zgłaszającej żądanie.

13.3. W przypadku rozwiązania Umowy z przyczyny innej niż okoliczność mogąca (w uzasadnionej ocenie Dostawcy) narazić Dostawcę na trwałe szkody lub zobowiązania, Dostawca zapewni Bankowi pomoc, której Bank może zażądać, w celu wsparcia Banku w przejściu do innego dostawcy wybranego przez Bank z zastrzeżeniem zapłaty przez Bank na rzecz Dostawcy uzasadnionych kosztów i wydatków związanych z taką pomocą. Dostawca jest zobowiązany do świadczenia Bankowi pomocy w okresie przejściowym przez czas minimum [xxx] dni od rozwiązania Umowy, w trakcie których Dostawca nadal będzie świadczył Usługi ICT bez ryzyka zakłóceń dla funkcji realizowanych w Banku.

14. **Gwarantowany Poziom Jakości Usług (SLA)**

14.1. Strony uzgadniają opis gwarantowanego poziomu jakości Usług w ramach dokumentu stanowiącego Załącznik nr 5.

Załącznik nr 2 - Miejsca przechowywania i przetwarzania danych przez Dostawcę oraz jego podwykonawców

	Miejsca świadczenia usług (region lub państwo)	Miejsca przechowywania i przetwarzania danych (region lub państwo)
Nazwa Dostawcy		
Nazwa podwykonawcy*		

*przy większej liczbie podmiotów należy dodać kolejne wiersze

Załącznik nr 3 – Wykaz raportów sporządzanych przez Dostawcę

L.p.	**Nazwa raportu**	**Opis treści raportu**

Załącznik nr 4 – Standardy Bezpieczeństwa dotyczące Usług świadczonych przez Dostawcę

[TREŚĆ UZGODNIONA PRZEZ STRONY]

Załącznik nr 5 – Opis gwarantowanego poziomu Usług (SLA)

[TREŚĆ UZGODNIONA PRZEZ STRONY]

Załącznik nr 6 – Opis Strategii Wyjścia

[TREŚĆ UZGODNIONA PRZEZ STRONY]

W imieniu Banku:

[podpisy osób uprawnionych do reprezentacji]

W imieniu Dostawcy:

[podpisy osób uprawnionych do reprezentacji]

4. Wzór aneksu w zakresie dostawców wspierających pozostałe funkcje

Aneks nr [xxx] zawarty w dniu [xxx] (zwany dalej „Aneksem"),

pomiędzy:

(dalej **„Bank**"), reprezentowanym przez:

[imię i nazwisko] - [funkcja]

[imię i nazwisko] - [funkcja]

a

[Nazwa drugiej strony umowy] z siedzibą w [xxx] (kod pocztowy: [xxx]) przy ul. [xxx], wpisanym do rejestru przedsiębiorców Krajowego Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy [xxx], [xxx] Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: [xxx], NIP: [xxx], kapitał zakładowy: [xxx] PLN, kapitał w pełni opłacony (dalej „**Dostawca**"), reprezentowanym w przez:

[imię i nazwisko] - [funkcja]

[imię i nazwisko] - [funkcja]

Preambuła:

1. Bank powierzył Dostawcy świadczenie określonych usług, a Dostawca zobowiązał się do ich świadczenia na warunkach określonych w umowie pomiędzy Bankiem a Dostawcą z dnia [xxx], z późniejszymi zmianami („**Umowa Główna**").

2. Bank jest zobowiązany do wypełniania obowiązków nałożonych na niego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 („**DORA**") jako „**podmiot finansowy**". Bank identyfikuje usługi wykonywane przez Dostawcę na podstawie Umowy Głównej jako świadczenie „**usług ICT**" w rozumieniu DORA.

3. DORA wymaga włączenia do każdej umowy, która dotyczy korzystania przez Bank z usług ICT określonych postanowień umownych. Umowa Główna zawiera część postanowień, które są wymagane dla zgodności z DORA, dlatego zamiarem Banku i Dostawcy jest wprowadzenie zmian do Umowy Głównej, aby zapewnić pełną zgodność jej warunków z wymogami DORA.

2. Definicje

O ile wyraźnie nie stwierdzono inaczej, wszystkie definicje użyte poniżej mają następujące znaczenie:

Dodatkowe Wymagania DORA	Znaczenie zdefiniowane w postanowieniu 5.1. Aneksu

Rozporządzenie DORA	oznacza 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
Właściwy Organ	Pod tym pojęciem należy rozumieć Komisję Nadzoru Finansowego
Incydent związany z ICT / Incydent ICT / Naruszenie Bezpieczeństwa / incydent bezpieczeństwa	Pojedyncze zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które naruszają bezpieczeństwo sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy.
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.
TLPT	Oznacza testy penetracyjne oparte na zagrożeniach zgodnie z art. 26 i 27 rozporządzenia DORA.
Organy ds. Restrukturyzacji i Uporządkowanej Likwidacji	Pod tym pojęciem należy rozumieć Bankowy Fundusz Gwarancyjny lub inne instytucje, których celem jest prowadzenie procedury restrukturyzacji i uporządkowanej likwidacji.

Postanowienia ogólne:

3. Zasady interpretacji zapisów Umowy Głównej oraz Aneksu

2.1. Słowa i wyrażenia zdefiniowane w Umowie Głównej mają takie samo znaczenie w Aneksie, o ile nie zaznaczono inaczej lub o ile kontekst nie stanowi inaczej.

2.2. Zasady interpretacji Umowy Głównej mają zastosowanie do Aneksu, tak jakby zostały w nim umieszczone (z uwzględnieniem zasady określonej w pkt. 1.3. poniżej).

3. Reguły kolizyjne

Z mocą obowiązującą od dnia podpisania Aneksu, Strony zgodnie postanawiają, że:

Strony zgodnie postanawiają, że zmieniają treść Umowy Głównej poprzez dodanie Postanowień umownych zawartych w Załączniku nr 1 do niniejszego Aneksu

w razie sprzeczności między postanowieniami ustalonymi w Umowie Głównej a postanowieniami umownymi zawartymi w Załączniku 1 do Aneksu odpowiednie zastosowanie mają warunki określone w Załączniku 1 do Aneksu,

w razie stwierdzenia niezgodności z przepisami prawa, nieważności lub niewykonalności poszczególnego postanowienia niniejszego Aneksu, postanowienie to, w zakresie, w jakim jest niezgodne z prawem,

nieważne lub niemożliwe do wyegzekwowania, będzie bezskuteczne i traktowane jako niezawarte w Aneksie, bez wpływu na ważność i wykonalność pozostałych postanowień Aneksu.

4. Skuteczność Aneksu

4.1. Aneks i Umowa Główna (wraz ze zmianami wprowadzonymi Aneksem) stanowią całość porozumień i ustaleń Stron oraz zastępują wszystkie wcześniejsze umowy, ustalenia lub porozumienia (ustne lub pisemne) w przedmiocie niniejszego Aneksu i Umowy Głównej.

4.2. Każda ze Stron jest zobowiązana wykonać wszystkie czynności, jakie mogą być zasadnie wymagane dla nadania pełnej skuteczności postanowieniom tego Aneksu.

5. Postanowienia końcowe

5.1. Każda ze Stron jest zobowiązana pokryć koszty własne i wydatki związane z negocjowaniem, przygotowaniem, zawarciem i wykonaniem Aneksu.

5.2. Aneks został sporządzony w dwóch egzemplarzach, a w przypadku gdy jego zawarcie będzie dokonywane w formie elektronicznej – w jednym egzemplarzu udostępnionym elektronicznie.

5.3. Aneks zostanie zawarty w formie oświadczeń woli złożonych pisemnie albo w postaci elektronicznej w rozumieniu art. 78 in. 1 Kodeksu cywilnego. Za datę zawarcia Aneksu Strony uznają dzień złożenia podpisu przez osobę reprezentującą Stronę składającą podpis jako ostatnia.

5.4. Zmiany Umowy zawarte w Załączniku wchodzą w życie z dniem [XXX] ("**Data wejścia w życie**").

Podpisali należycie upoważnieni przedstawiciele stron w dacie oznaczonej na wstępie niniejszego Aneksu.

(Bank):
Imię i nazwisko: [xxx]
Stanowisko: [xxx]
Podpis: [xxx]

[xxx] (Dostawca):
Imię i nazwisko: [xxx]
Stanowisko: [xxx]
Podpis: [xxx]

Załączniki:

1. Załącznik nr 1 - Klauzule umowne wymagane w świetle rozporządzenia DORA oraz odpowiednich RTS.
2. Załącznik nr 2 - Miejsca przechowywania i przetwarzania danych przez Dostawcę oraz jego podwykonawców.
3. Załącznik nr 3 – Wykaz raportów sporządzanych przez Dostawcę.
4. Załącznik nr 4 – Opis gwarantowanego poziomu Usług (SLA).

Załącznik nr 1 - Klauzule umowne wymagane w świetle rozporządzenia DORA oraz odpowiednich RTS

1.1 Opis Usług realizowanych przez Dostawcę

[*Należy uzupełnić o kompletny opis usług realizowanych przez Dostawcę. W przypadku umów, w których Przedmiot umowy w całości obejmuje usługi/funkcje ICT należy skopiować całe postanowienie ze wskazaniem odpowiedniego postanowienia Umowy (źródłowe miejsce) z podziałem na poszczególne Usługi.*
W przypadku umów, w których Przedmiot umowy w całości obejmuje nie tylko usługi/funkcje ICT należy z Przedmiotu umowy wyodrębnić usługi/funkcje ICT i opisać je (ze wskazaniem odpowiedniego postanowienia Umowy (źródłowe miejsce) z podziałem na poszczególne Usługi.

Funkcje muszą być zdefiniowane per usługa - jeśli w umowie realizowanych jest więcej usług ITC [np. dostawa sprzętu + licencja + wsparcie, dla każdej usługi należy zdefiniować funkcję]
Usługa 1
Usługa 2
Usługa 3
itp..]

1.2. Funkcje obsługiwane przez Usługę realizowaną przez Dostawcę

[Należy wskazać numery Usług wskazanych w 1.1 realizowanych przez daną Funkcję (zgodnie z powyższą numeracją) lub wpisać "ND"]

Identyfikator funkcji ICT	**Nazwa funkcji ICT**	**Opis**	**Usługi obsługujące funkcje**
S1	1. ICT project management	Świadczenie usług związanych z: Project Management Officer (PMO).	
S2	2. ICT Development	Świadczenie usług związanych z: analizą biznesową, projektowaniem i tworzeniem oprogramowania, testowaniem.	
S3	3. ICT help desk and first level support	Świadczenie usług związanych z: wsparciem helpdesk i wsparciem pierwszego poziomu w zakresie incydentów ICT	
S4	4. ICT security management services	Świadczenie usług związanych z: bezpieczeństwem ICT (ochrona, wykrywanie, reagowanie i odzyskiwanie), w tym obsługa incydentów bezpieczeństwa i śledztwa informatyczne.	
S5	5. Provision of data	Subskrypcja usług dostawców danych (usługa danych cyfrowych)	
S6	6. Data analysis	Świadczenie usług związanych z wsparciem analizy danych (usługa danych cyfrowych)	
S7	7. ICT facilities and hosting services (excluding Cloud services)	Zapewnienie infrastruktury ICT, obiektów i usług hostingowych. Obejmuje to dostarczanie mediów (energia, zarządzanie ciepłem...), dostęp telekomunikacyjny i bezpieczeństwo	

		fizyczne. (z wyłączeniem usług w chmurze)	
S8	8. Computation	Zapewnienie możliwości przetwarzania cyfrowego (w tym obliczania danych). Nie obejmuje to usług obliczeniowych wykonywanych w kontekście środowiska chmury.	
S9	9. Non-Cloud Data storage	Zapewnienie platformy przechowywania danych (z wyłączeniem usług w chmurze).	
S10	10. Telecom carrier	Operacje dla systemów telekomunikacyjnych i zarządzanie przepływem. Tradycyjne analogowe usługi telefoniczne są wyraźnie wyłączone zgodnie z art. 3 ust. 21 rozporządzenia (UE) 2022/2554.	
S11	11. Network infrastructure	Zapewnienie infrastruktury sieciowej	
S12	12. Hardware and physical devices	Dostarczanie stacji roboczych, telefonów, serwerów, urządzeń do przechowywania danych, urządzeń itp. w formie usługi	
S13	13. Software licencing (excluding SaaS)	Dostarczanie oprogramowania działającego lokalnie.	
S14	14. ICT operation management (including maintenance)	Świadczenie usług związanych z: konfiguracją infrastruktury (systemów i sprzętu z wyjątkiem sieci), konserwacją, instalacją, zarządzaniem pojemnością, zarządzaniem ciągłością działania itp. W tym dostawcy usług zarządzanych (MSP).	
S15	15. ICT Consulting	Świadczenie usług w zakresie wiedzy intelektualnej / eksperckiej ICT.	
S16	16. ICT Risk management	Weryfikacja zgodności z wymogami zarządzania ryzykiem w zakresie ICT zgodnie z art. 6 ust. 10 rozporządzenia (UE) 2022/2554.	
S17	17. Cloud services: IaaS	Infrastructure-as-a-Service	
S18	18. Cloud services: PaaS	Platform-as-a-Service	
S19	19. Cloud services: SaaS	Software-as-a-Service	

1.4 Podwykonawstwo

[Należy wskazać wszystkich występujących Podwykonawców wraz z opisem realizowanych przez wskazanego Podwykonawcę Usług oraz numerem Funkcji obsługiwanej przez Usługę zgodnie z tabelą wskazaną w 1.2. Należy wskazać czy dozwolone jest podwykonawstwo usług ICT wspierających krytyczną lub ważną funkcję lub ich istotne części, a w takim przypadku warunki mające zastosowanie do takiego podwykonawstwa. W przypadku gdy brak jest podwykonawców - należy usunąć pkt 1.3 w całości.]

1.3.1 Pełna nazwa Podwykonawcy A

[Opis Usług realizowanych przez Podwykonawcę A

Funkcje obsługiwane przez Usługę ICT realizowaną przez Podwykonawcę A: Sx; Sy; Sz]

1.3.2 Pełna nazwa Podwykonawcy B

[Opis Usług realizowanych przez Podwykonawcę B

Funkcje obsługiwane przez Usługę realizowaną przez Podwykonawcę B: Sx; Sy; Sz]

Strony uzgadniają, że dozwolone jest / nie jest dozwolone podwykonawstwo usług ICT wspierających krytyczną lub ważną funkcję lub ich istotne części.

[Wariant, gdy dozwolone jest podwykonawstwo usług ICT wspierających krytyczną lub ważną funkcję lub ich istotne części:]

Dopuszcza podwykonawstwo następujących Usług ICT wspierających krytyczną lub ważną funkcję lub ich istotne części:

[do uzupełnienia]

na następujących warunkach:

[do uzupełnienia]

1.3.3. Dostawca zobowiązuje się do zapewnienia sobie w umowie z podwykonawcą możliwości dostępu i pozyskania kopii umów z jego dalszymi podwykonawcami, w tym na potrzeby przekazania jej Bankowi. Dotyczy to także zapewnienia, by podwykonawca w umowach z dalszymi swoimi podwykonawcami, poprzez stosowne postanowienia umowne posiadał zapewnioną możliwość dostępu i pozyskania kopii umów zawartych z dalszymi podwykonawcami, w tym na potrzeby przekazania jej Bankowi, celem zapewnienia monitorowania całego łańcucha podwykonawstwa Usługi ICT przez Bank.

2. Wypowiedzenie Umowy

2.1. **Okres wypowiedzenia**. Bank może, bez podania przyczyny, rozwiązać Umowę na piśmie przesłanym Dostawcy z zachowaniem minimum [xxx] okresu wypowiedzenia.

2.2. **Wypowiedzenie Umowy z podaniem przyczyny**. Bank może rozwiązać Umowę na piśmie ze skutkiem natychmiastowym, jeżeli:

(k) Właściwy Organ wyda stosowną rekomendację, komunikat, stanowisko lub decyzję;

(l) wynika to z wytycznych lub oczekiwań wyrażonych w innej formie wydanych przez Właściwy Organ lub Organy ds. Restrukturyzacji i Uporządkowanej likwidacji;

(m) Dostawca naruszy istotne zobowiązanie wynikające z postanowień Umowy lub dopuszcza się poważnego naruszenia przepisów ustawowych, wykonawczych lub wytycznych Właściwego Organu;

(n) w trakcie monitorowania ryzyka ze strony Dostawcy zostaną zidentyfikowane okoliczności, w przypadku wystąpienia których Bank uzna, że mogą one zmienić

wykonywanie Usług ICT przewidzianych w Umowie, w tym istotne zmiany mające wpływ na Umowę lub sytuację Dostawcy;

(o) zostaną wykazane słabe strony Dostawcy w zakresie jego ogólnego zarządzania ryzykiem związanym z ICT, a w szczególności, w odniesieniu do sposobu, w jaki zapewnia on dostępność, autentyczność, integralność i poufność danych, niezależnie od tego, czy wykazane słabe strony dotyczą danych osobowych lub danych w inny sposób wrażliwych, czy danych nieosobowych; przed wypowiedzeniem Umowy z tej przyczyny, Bank wedle własnego uznania może poinformować Dostawcę o zakresie słabych stron, a także wyznaczyć [xxx] dniowy termin na wdrożenie stosownych działań naprawczych. W przypadku wyznaczenia tego terminu, wypowiedzenie Umowy z tej przyczyny jest możliwe po jego bezskutecznym upływie;

(p) gdy w wyniku warunków lub okoliczności związanych z Umową, Właściwy Organ nie może już skutecznie nadzorować Banku;

(q) Dostawca wprowadza istotne zmiany w umowie z podwykonawcą pomimo sprzeciwu Banku lub bez wyraźnej zgody Banku, albo przed upływem wskazanego w powiadomieniu przez Dostawcę terminu wprowadzenia zmiany;

(r) Dostawca zleca podwykonawstwo usługi wpierającej krytyczną lub ważną funkcję, której zlecanie podwykonawcom wyraźnie nie jest dozwolone na mocy Umowy;

(s) wymagania bezpieczeństwa Banku ulegną zmianie, a Dostawca nie wyrazi zgody na dostosowanie się do tych wymagań w terminie wyznaczonym przez Bank;

(t) gdy świadczenie usług nie odpowiada poziomowi usług uzgodnionemu z Bankiem. Przed wypowiedzeniem Umowy z tej przyczyny, Bank, wedle własnego uznania, może poinformować Dostawcę o zakresie Usług ICT nieodpowiadających uzgodnionemu poziomowi usług, a także wyznaczyć [xxx] dniowy termin na wdrożenie stosownych działań naprawczych. W razie wyznaczenia tego terminu, wypowiedzenie Umowy z tej przyczyny jest możliwe po jego bezskutecznym upływie.

3. Miejsce Świadczenia Usług

3.1. Usługi ICT i przedmiot Umowy będzie dostarczany wyłącznie z Miejsc Świadczenia Usług – tj. regionów lub krajów, w których mają być świadczone funkcje i Usługi ICT objęte Umową lub podwykonawstwem oraz w których mają być przetwarzane dane, w tym miejsce przechowywania. Miejsca Świadczenia Usług, w tym miejsca przechowywania danych i miejsca przetwarzania danych, w tym przez podwykonawców Dostawcy w ramach Umowy, zostały określone w Załączniku nr 2 do Aneksu. Jeżeli Dostawca zechce zmienić Miejsce Świadczenia Usług lub wykonywać Usługę z innego miejsca, musi wcześniej powiadomić o tym Bank na piśmie z podaniem informacji o nowym, proponowanym miejscu w zakresie, jakiego Bank może zażądać, na co najmniej [xxx] dni roboczych przed proponowanym terminem rozpoczęcia Usług w nowym miejscu. Usługi nie mogą być dostarczane z innego Miejsca Świadczenia Usług bez uprzedniego uzyskania pisemnej zgody Banku oraz bez pisemnego zatwierdzenia przez Bank procedur bezpieczeństwa dla nowego Miejsca

Świadczenia Usług. Wymóg ten dotyczy również Miejsca Świadczenia Usług podwykonawców Dostawcy.

[Postanowienie opcjonalne:]

3.2. *Dostawca zwróci Bankowi uzasadnione koszty dodatkowe, poniesione przez Bank w wyniku zmiany Miejsca Świadczenia Usług z inicjatywy Dostawcy.*

4. Bezpieczeństwo danych

4.1. Dostawca zobowiązuje się niezwłocznie informować Bank o wszelkich incydentach związanych z bezpieczeństwem danych, w tym danych osobowych, dotyczących świadczonej dla Banku Usługi ICT, mających wpływ na poufność, integralność, autentyczność lub dostępność do danych Banku, a w szczególności o przypadkach nieautoryzowanego dostępu lub przejęcia danych Banku lub naruszenia bezpieczeństwa systemu lub środowiska informatycznego używanego do przetwarzania, przesyłania lub przechowywania danych Banku. Incydenty powinny być zgłaszane do wskazanych w Umowie osób kontaktowych oraz na adres dedykowany do zgłaszania incydentów [xxx].

4.2. Dostawca zobowiązuje się do wdrożenia niezbędnych środków związanych z zapewnieniem bezpieczeństwa danych, w tym środków minimalizujących ryzyko wycieku, kradzieży i manipulacji danymi oraz do zapewnienia, w ramach wynagrodzenia z tytułu Umowy, pomocy Bankowi, w przypadku wystąpienia incydentu ICT dotyczącego świadczonej Usługi ICT.

4.3. Dostawca zobowiązuje się do zwrotu lub zniszczenia, powierzonych przez Bank informacji w uzgodnionym czasie w trakcie trwania Umowy lub po jej zakończeniu.

4.4. Dostawca jest zobowiązany do usuwania podatności, w szczególności krytycznych i istotnych, w swoich systemach, narzędziach i procesach oraz niezwłocznego reagowania na cyberzagrożenia, które mogą mieć negatywny wpływ na usługi świadczone dla Banku.

4.5. Dostawca w odpowiednim przypadku i na żądanie Banku będzie sporządzać raporty okresowe, raporty o incydentach, raporty o świadczeniu Usług ICT, raporty z obszaru bezpieczeństwa teleinformatycznego oraz środków i testów ciągłości działania. Szczegółowy wykaz raportów sporządzanych na podstawie Umowy przez Dostawcę określony jest w Załączniku nr 3.

5. Dostęp do danych

5.1 W razie rozwiązania Umowy, bez względu na powód, lub upływu czasu jej trwania, Dostawca niezwłocznie bez konieczności wezwania zwróci lub usunie (wedle wyboru Banku) wszystkie składniki majątkowe, informacje, dane (w tym Dane Osobowe) i materiały (w tym kopie) – dalej jako: „Dane" należące do Banku, które w owym czasie znajdują się w posiadaniu, władzy lub pod kontrolą Dostawcy. W przypadku zwrotu Danych, może on zostać dokonany wedle wyboru Banku, Bankowi lub zastępczemu dostawcy, w formacie i na nośnikach uzgodnionych przez Strony. Na wyraźne polecenie Banku i w terminie wskazanym przez Bank lub innym uzgodnionym przez Strony, Dostawca zniszczy takie Dane. Fakt ich zniszczenia zostanie udokumentowany w formie protokołu przez osobę upoważnioną przez Dostawcę.

[Postanowienie opcjonalne]
W przypadku danych zapisanych w systemach informatycznych w sposób automatyczny, w ramach kopii zapasowych, gdy obowiązujące przepisy prawa pozwalają na przechowywanie tych danych,

Dostawca nie będzie podejmował celowych działań zmierzających do odzyskania Danych oraz nadal będą one traktowane przez Dostawcę jako poufne oraz zostaną usunięte nie później niż do ustania przydatności kopii zapasowej, z zastrzeżeniem, że Dane nie mogą być użyte dla celów innych niż związanych z Umową lub wynikających z obowiązujących przepisów prawa. Usunięcie danych zostanie potwierdzone przez Dostawcę w formie protokołu sporządzonego przez osobę upoważnioną przez Dostawcę.

5.2 W czasie trwania Umowy Dostawca jest zobowiązany do sporządzania kopii zapasowych wszystkich danych należących do Banku, z częstotliwością przynajmniej [XXX]. W razie rozwiązania Umowy wskutek niewypłacalności Dostawcy lub zakończenia działalności gospodarczej przez Dostawcę, wówczas – bez wpływu na punkt 5.1 – Dostawca udostępni Bankowi ostatnie kopie zapasowe Danych w ciągu 7 Dni Roboczych po rozwiązaniu Umowy.

6. Współpraca z Organami Regulacyjnymi

6.1 Dostawca będzie współpracować z Bankiem i jego personelem oraz przedstawicielami, Właściwym Organem, Organami ds. Przymusowej Restrukturyzacji i Uporządkowanej Likwidacji i osobą wyznaczoną przez Właściwy Organ lub Organy ds. Przymusowej Restrukturyzacji i Uporządkowanej Likwidacji w sprawach, w których będzie to wymagane, w tym w związku z wykonywaniem obowiązku lub prawa wynikającego z przepisów prawnych lub dochodzenia prowadzonego przez Bank lub inny podmiot w jego imieniu lub przez Właściwy Organ lub Organy ds. Przymusowej Restrukturyzacji i Uporządkowanej Likwidacji . Forma współpracy może polegać na udostępnieniu lub zapewnieniu dostępu do dokumentacji, informacji, danych, systemów, pomieszczeń i sieci telekomunikacyjnych, jakie znajdują się w posiadaniu, pieczy lub pod kontrolą Dostawcy, jego podwykonawców lub agentów.

6.2 Bank oraz jego Dostawcy podlegają nadzorowi sprawowanemu przez Właściwy Organ, w ramach którego Właściwy Organ jest uprawniony do przeprowadzania badań i sprawowania nadzoru nad Dostawcami wykonującymi pewne funkcje lub operacje, tak jakby dane funkcje lub operacje wykonywał Bank w pomieszczeniach Banku. Dostawca będzie współpracować i niezwłocznie spełniać wszystkie żądania Właściwego Organu.

7. Programy zwiększania świadomości w zakresie bezpieczeństwa teleinformatycznego

7.1. Dostawca zobowiązuje się do zwiększania świadomości swojego personelu, zaangażowanego do realizacji Umowy w zakresie bezpieczeństwa teleinformatycznego oraz do przeprowadzania szkoleń dla swojego personelu w zakresie operacyjnej odporności cyfrowej. W stosownych przypadkach i na żądanie Banku Dostawca będzie również uczestniczyć w opracowanych przez Bank programach zwiększania świadomości w zakresie bezpieczeństwa teleinformatycznego i szkoleniach w zakresie operacyjnej odporności cyfrowej.

8. Opisy gwarantowanych poziomów usług w tym ich aktualizacje i zmiany

8.1 Strony uzgadniają opis gwarantowanego poziomu jakości Usług w ramach dokumentu stanowiącego Załącznik nr 4.

Załącznik nr 2 - Miejsca przechowywania i przetwarzania danych przez Dostawcę oraz jego podwykonawców

	Miejsca świadczenia usług (region lub państwo)	Miejsca przechowywania i przetwarzania danych (region lub państwo)
Nazwa Dostawcy		
Nazwa podwykonawcy*		

*przy większej liczbie podmiotów należy dodać kolejne wiersze

Załącznik nr 3 – Wykaz raportów sporządzanych przez Dostawcę

L.p.	**Nazwa raportu**	**Opis treści raportu**

Załącznik nr 4– Opis gwarantowanego poziomu Usług (SLA)

[TREŚĆ UZGODNIONA PRZEZ STRONY]

W imieniu Banku:

[podpisy osób uprawnionych do reprezentacji]

W imieniu Dostawcy:

[podpisy osób uprawnionych do reprezentacji]