UMOWA

POWIERZENIA DALSZEGO PRZETWARZANIADANYCH OSOBOWYCH

Zawarta w dniu 2020-08-04 roku w Starogardzie Gdańskim pomiędzy:

Asist Spółką z ograniczoną odpowiedzialnością z siedzibą w Starogardzie Gdańskim przy ul. Owidzkiej 20, 83-200 Starogard Gdański, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000125085, numer NIP 5842468232, numer REGON 192760147, o kapitale zakładowym w wysokości 78.500,00 PLN, w całości opłaconym, działającą na podstawie umocowania zawartego w umowie z Towarzystwem Ubezpieczeń i Reasekuracji Allianz Polska Spółka Akcyjna, zwaną dalej**"Procesorem"**, reprezentowaną przez **Rafała Ćwiklińskiego - Prezesa Zarządu**,

oraz

CENTRUM FINANSOWE SŁOWIŃSCY SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w: Police, ul. Kosynierów Gdyńskich, NIP 8513249996, REGON 386508966
zwanym/ą dalej **„Subprocesorem”**, reprezentowanym/ą przez Anna Słowińska, PESEL 72041903563

Procesor i Subprocesor są zwani dalej łącznie "**Stronami",**a każdy z nich z osobna "**Stroną".**

Zważywszy, iż na dzień zawarcia niniejszej Umowy Strony są związane postanowieniami Umowy o współpracy, w związku z koniecznością dostosowania zasad wzajemnej współpracy do wymogów Rozporządzenia 2016/679, na podstawie zgodnej woli Stron ustala się co następuje:

§ 1

DEFINICJE

Użyte w niniejszej Umowie definicje oznaczają:

1) **RODO**: Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE. L. z 2016 r. Nr 119, str. 1);

2) **Przetwarzanie**: operacja lub zestaw operacji wykonywanych na Danych osobowych lub zestawach Danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie - w rozumieniu art. 4 pkt 2) RODO;

3) **Dane osobowe**: dane w rozumieniu art. 4 pkt 1) RODO tj. informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą");

4) **Naruszenie ochrony danych osobowych**: naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 2

OŚWIADCZENIA STRON

Strony oświadczają, co następuje:

1) Procesor oświadcza, iż na podstawie zawartej z Towarzystwem Ubezpieczeń i Reasekuracji Allianz Polska Spółka Akcyjna z siedzibą w Warszawie (02-685) przy ul. Rodziny Hiszpańskich 1, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy pod numerem KRS 0000028261, NIP 5251565015, o kapitale zakładowym 377.241.000 zł, który został opłacony w całości, umowy powierzenia przetwarzania danych osobowych, przetwarza dane osobowe, których Towarzystwo Ubezpieczeń i Reasekuracji Allianz Polska Spółka Akcyjna jest Administratorem.

2) Strony oświadczają, że celem niniejszej Umowy jest wykonanie obowiązków wynikających z przepisów powszechnych, w tym art. 28 RODO w związku z zawarciem Umowy o współpracy.

3) Procesor oświadcza, że jest Podmiotem Przetwarzającym w rozumieniu art. 4 pkt 8 RODO.

4) Subprocesor oświadcza, że jest Podmiotem Przetwarzającym w rozumieniu art. 4 pkt 8 RODO.

§ 3

OKRES OBOWIĄZYWANIA

Niniejsza Umowa wchodzi w życie z dniem zawarcia i pozostaje w mocy do czasu rozwiązania Umowy o współpracy lub do czasu rozwiązania niniejszej umowy przez Procesora.

§ 4

PRZEDMIOT UMOWY

1) Postanowienia niniejszej Umowy mają pierwszeństwo przed postanowieniami Umowy o współpracy w zakresie dotyczącym Przetwarzania Danych osobowych przez Subprocesora w imieniu Administratora i na podstawie dyspozycji Procesora lub Administratora.

2) Subprocesor dołoży należytej staranności w celu zapewnienia, aby wszystkie osoby, którym powierzył wykonywanie czynności będących przedmiotem Umowy o współpracy przestrzegały powszechnie obowiązujących na terytorium Rzeczypospolitej Polskiej przepisów w zakresie ochrony danych osobowych, oraz aby pozyskane informacje wewnętrzne Procesora lub Administratora nie były ujawniane nieuprawnionym osobom trzecim.

3) Dane osobowe wymagane do realizacji Umowy o współpracy, kategorie osób, których Dane osobowe będą Przetwarzane, oraz szczegółowe informacje dotyczące czynności Przetwarzania określa Załącznik nr 1.

§ 5

OBOWIĄZKI SUBPROCESORA

1) W celu wykonania zobowiązań umownych wynikających z Umowy o współpracy, Subprocesor jest upoważniony do realizacji, w imieniu Administratora oraz zgodnie z niniejszą Umową, czynności Przetwarzania Danych osobowych wskazanych w Załączniku nr 1. Subprocesor będzie Przetwarzać Dane osobowe wyłącznie w celach określonych w Załączniku nr 1 w zakresie Umowy o współpracy oraz zgodnie ze szczegółowymi dyspozycjami Procesora i Administratora. Wszelkie takie dyspozycje wymagają pod rygorem nieważności formy pisemnej lub formy e-mail.

2) Subprocesor może poprawiać, usuwać lub blokować dane Przetwarzane w imieniu Procesora wyłącznie, jeżeli wynika to z dyspozycji wydanych przez Administratora za pośrednictwem Procesora. Jeżeli osoba, której dane dotyczą, zwróci się bezpośrednio do Subprocesora z wnioskiem o poprawienie lub usunięcie jej Danych osobowych, Subprocesor ma obowiązek niezwłocznie przekazać ten wniosek Administratorowi za pośrednictwem Procesora. Szczegółowe zasady dotyczące realizacji tego obowiązku reguluje osobno udostępniona **Procedura dotycząca realizacji uprawnień RODO**.

3) Wszelkie istotne zmiany stosowanych procesów lub organizacji pracy wykonywanej według procedur w imieniu Administratora, które mają wpływ na Przetwarzanie Danych osobowych, wymagają wcześniejszej wyraźnej zgody Administratora, wyrażonej za pośrednictwem Procesora pod rygorem nieważności w formie pisemnej lub w formie e-mail.

4) Wszelkie czynności związane z Przetwarzaniem Danych osobowych w imieniu Administratora, które mają zostać wykonane przez Subprocesora, muszą odbywać się w siedzibie Subprocesora wskazanej w Umowie o współpracy, chyba że Administrator za pośrednictwem Procesora udzieli wcześniej wyraźnej pisemnej zgody (pod rygorem nieważności), aby czynności te były wykonywane w innych miejscach.

5) Z zastrzeżeniem obowiązków określonych w § 6 Subprocesor zapewnia, aby dostęp do Danych osobowych posiadały jedynie osoby, których rola w procesie wykonywania przez Subprocesora Umowy o współpracy wymaga dostępu do takich danych.

6) Subprocesor nie może przekazywać Danych osobowych poza terytorium Europejskiego Obszaru Gospodarczego bez uprzedniej zgody Administratora wyrażonej pod rygorem nieważności w formie pisemnej lub w formie e-mail. Administrator może bez podania przyczyny odmówić udzielenia takiej zgody. Jeżeli Dane osobowe będą przekazywane poza terytorium Europejskiego Obszaru Gospodarczego, Subprocesor ma obowiązek zapewnić przekazywanym Danym osobowym odpowiedni poziom ochrony w celu zapewnienia zgodności z warunkami niniejszej Umowy.

7) Administrator lub Administrator za pośrednictwem Procesora może w dowolnym momencie nakazać Subprocesorowi zaprzestanie wykonywania czynności związanych z Przetwarzaniem Danych osobowych w jego imieniu z jakiegokolwiek powodu, w tym w związku ze stwierdzeniem lub podejrzeniem naruszenia przez Subprocesora postanowień niniejszej Umowy lub obowiązujących przepisów i regulacji w zakresie ochrony danych (w szczególności RODO).

§ 6

OBOWIĄZKI DOTYCZĄCE POWIADOMIEŃ I WSPARCIA

1) W wypadku podejrzenia naruszenia przepisów dotyczących ochrony Danych osobowych, naruszenia ochrony Danych osobowych, utraty Danych osobowych lub innych istotnych nieprawidłowości, Subprocesor ma obowiązek bez zbędnej zwłoki, nie później niż w ciągu 12 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony Danych osobowych, powiadomić o tym fakcie Administratora za pośrednictwem Procesora. Szczegółowe zasady dotyczące realizacji tego obowiązku reguluje osobno udostępniona **Procedura dotycząca zgłaszania naruszeń ochrony danych osobowych** .

2) W wypadku podjęcia przez Organy Nadzoru ochrony Danych osobowych wobec Procesora lub Administratora jakichkolwiek kontroli, inspekcji lub czynności wyjaśniających bezpośrednio lub pośrednio dotyczących prac wykonywanych przez Subprocesora na podstawie niniejszej Umowy, Subprocesor zobowiązany będzie do udzielenia tym organom w wyznaczonym terminie odpowiedniego wsparcia zgodnie z żądaniem Procesora lub Administratora.

3) Jeżeli Subprocesor sam zostanie objęty przez właściwe dla niego Organy Nadzoru Ochrony Danych Osobowych kontrolą, inspekcją lub czynnościami wyjaśniającymi we wskazanym powyżej zakresie, Subprocesor ma obowiązek niezwłocznie powiadomić Administratora za pośrednictwem Procesora o tym fakcie, a także o zakresie kontroli oraz wszelkich ustaleniach, które mają bezpośredni lub pośredni wpływ na stosunek umowny pomiędzy Stronami. Subprocesor ma obowiązek niezwłocznie usunąć wszelkie nieprawidłowości stwierdzone w trakcie takiej kontroli.

4) Jeżeli Subprocesor uzna, że dyspozycja Administratora dotycząca Przetwarzania Danych osobowych narusza obowiązujące przepisy i regulacje w zakresie ochrony danych osobowych (w tym postanowienia RODO), Subprocesor ma obowiązek niezwłocznie powiadomić o tym Administratora za pośrednictwem Procesora.

5) Subprocesor poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych jest zobowiązany pomagać Procesorowi i Administratorowi wywiązać się z obowiązków określonych w art. 34 RODO, oraz obowiązku odpowiadania na żądania osoby, której Dane osobowe dotyczą, w zakresie wykonywania jej praw określonych w art. 12 - 23 RODO, w szczególności poprzez:

1. pomoc w zakresie informowania osoby, której Dane osobowe dotyczą o naruszeniu danych osobowych mogącym powodować wysokie ryzyko naruszenia praw lub wolności tej osoby,

2. prowadzenie rejestru naruszeń ochrony Danych osobowych,

3. pomoc w przekazywaniu osobie, której Dane osobowe dotyczą informacji określonych w art. 13, 14 i 15 RODO,

4. pomoc w informowaniu osoby, której Dane osobowe dotyczą o jej prawach określonych w art. 16 - 21 RODO, w szczególności poprzez niezwłoczne przekazanie Procesorowi i Administratorowi żądań osoby, której Dane osobowe dotyczą:
a) żądania sprostowania danych (o którym mowa w art. 16 RODO),

b) żądania usunięcia danych (o którym mowa w art. 17 RODO),

c) żądania ograniczenia Przetwarzania (o którym mowa w art. 18 RODO),

d) sprzeciwu wobec przetwarzania Danych osobowych (o którym mowa w art. 21 RODO).

Szczegółowe zasady dotyczące realizacji obowiązku Subprocesora określonego w pkt 4 reguluje osobno udostępniona**Procedura dotycząca realizacji uprawnień RODO.**

§ 7

ZACHOWANIE TAJEMNICY I POUFNOŚCI

1) Subprocesor zobowiązuje się do zachowania poufności danych w trakcie wykonywania czynności Przetwarzania Danych osobowych w imieniu Administratora. Do wykonywania czynności Przetwarzania Danych osobowych Subprocesor może wyznaczać wyłącznie osoby, które przeszły odpowiednie szkolenie i podlegają indywidualnemu obowiązkowi zachowania poufności danych. Na żądanie Procesora lub Administratora przestrzeganie obowiązku, o którym mowa powyżej, należy potwierdzić poprzez przekazanie oświadczenia podpisanego przez osobę zobowiązaną do zachowania poufności.

2) Strony zobowiązują się traktować jako ściśle poufne wszelkie informacje, które nie są publicznie dostępne, w szczególności tajemnice przedsiębiorstwa i tajemnice handlowe drugiej Strony i Administratora; zobowiązują się wykorzystywać takie informacje jedynie w zakresie objętym niniejszą Umową; a także zobowiązują się, że nie będą rejestrować, ujawniać ani wykorzystywać takich informacji, o ile nie będzie to konieczne do osiągnięcia celu Umowy.

3) Subprocesor ma obowiązek zapewnić, aby jego podwykonawcy zobowiązali swoich pracowników oraz osoby, przy udziale których podwykonawca wykonuje umowę zawartą z Subprocesorem do zachowania poufności informacji w takim samym zakresie jaki obowiązuje Subprocesora, oraz ma obowiązek potwierdzić takie zobowiązanie na żądanie Procesora lub Administratora (w szczególności poprzez przekazanie oświadczenia podpisanego przez osobę zobowiązaną do zachowania poufności).

4) Subprocesor zobowiązany jest zapewnić, aby obowiązki określone w ust. 3 znalazły odpowiednie zastosowanie do podmiotów, którym podwykonawca powierzy wykonywanie czynności na rzecz Procesora lub Administratora.

§ 8

DOSTĘP DO ZASOBÓW IT

1) Jeżeli w trakcie trwania Umowy Subprocesor uzyska dostęp do zasobów IT Procesora lub Administratora (w tym sprzętu komputerowego, sieci, serwerów, systemów, baz danych itd.), wówczas zasoby takie muszą być traktowane z najwyższą ostrożnością oraz w każdym wypadku z zachowaniem rygorystycznie przestrzeganych standardowych procedur działania i instrukcji obsługi danego sprzętu lub systemu lub aplikacji przekazanych przez Procesora lub Administratora.

2) Przed przyznaniem dostępu, o którym mowa w ust. 1, wszyscy pracownicy Subprocesora wyznaczeni do korzystania ze sprzętu, lub systemu, lub aplikacji mają obowiązek podpisać stosowne indywidualne oświadczenia potwierdzające zobowiązanie do przestrzegania zasad ochrony danych osobowych określonych w niniejszej Umowie a w szczególności zachowania tajemnicy.

3) W przypadku, w którym Subprocesor otrzymał od Procesora lub Administratora dostęp do sprzętu lub systemu lub aplikacji dedykowanych do Przetwarzania Danych osobowych, wszelkie operacje na Danych osobowych muszą być wykonywane wyłącznie przy użyciu tego sprzętu, lub systemu lub aplikacji.

4) W przypadku, w którym Subprocesor otrzymał od Procesora lub Administratora dostęp do sprzętu lub systemu lub aplikacji dedykowanych do Przetwarzania Danych osobowych Subprocesor może wykonać operację na Danych osobowych poza sprzętem lub systemem lub aplikacją, o których mowa w ust. 2 wyłącznie w celu wprowadzenia Danych osobowych do systemu lub aplikacji i w zakresie niezbędnym do tego celu. Niezwłocznie po wprowadzeniu Danych osobowych wszelkie kopie (w tym kopie cyfrowe) Danych osobowych muszą być usunięte ze wszelkich nośników innych niż ten system, lub aplikacja, lub (w zależności od innych postanowień) przekazane Procesorowi lub Administratorowi.

§ 9

ZWROT DANYCH OSOBOWYCH

1) Subprocesor ma obowiązek:

1. zapewnić odpowiednią identyfikację i wyraźnie oznaczyć wszystkie dokumenty lub nośniki danych zawierające Dane osobowe należące do Administratora, w tym dokumentację pisemną, płyty CD-ROM, inne urządzenia pamięci masowej i podobne materiały;

2. przechowywać dokumenty, nośniki i dane, o których mowa w pkt 1) oddzielnie od innych dokumentów i danych Subprocesora;
3. chronić dokumenty, nośniki i dane, o których mowa w pkt 1) przed nieuprawnionym dostępem, podejmując odpowiednie techniczne i organizacyjne środki bezpieczeństwa w celu zabezpieczenia ich przed niewłaściwym wykorzystaniem, nieuprawnionym dostępem, powieleniem, ujawnieniem, lub utratą.

2) Subprocesor ma obowiązek zwrócić Procesorowi wszelkie dokumenty i nośniki zawierające Dane osobowe na żądanie Procesora lub Administratora lub po rozwiązaniu/wygaśnięciu Umowy o współpracy lub wypowiedzenia przez Procesora niniejszej umowy, w zależności od tego, która z tych okoliczności wystąpi wcześniej. Zwrot Danych osobowych Procesorowi oznacza przekazanie mu wszelkich dokumentów lub nośników Danych osobowych (zarówno oryginałów jak i wszystkich kopii) w taki sposób, aby Subprocesor nie był w posiadaniu tych Danych osobowych.

3) Jeżeli Procesor lub Administrator zażąda nieodwracalnego zniszczenia lub usunięcia takich dokumentów i danych, Subprocesor ma obowiązek potwierdzić ich zniszczenie lub usunięcie.

4) Dane przechowywane na urządzeniach przenośnych należy fizycznie usunąć przed zbyciem lub likwidacją tych urządzeń. Subprocesor ma obowiązek zapewnić, aby żadne Dane osobowe Administratora nie zostały przekazane osobom trzecim, oraz aby przed wymianą sprzętu Dane osobowe, które się na nim znajdują, zostały nieodwracalnie usunięte przed przekazaniem takiego sprzętu osobom trzecim.

5) Zwrot Procesorowi dokumentów i danych określonych w niniejszym paragrafie lub usunięcie (stosownie do postanowień ust. 3) nastąpi nie później niż w ciągu 7 dni od rozwiązania/wygaśnięcia Umowy o współpracy lub wypowiedzenia przez Procesora niniejszej umowy, w zależności od tego, która z tych okoliczności wystąpi wcześniej.

6) Subprocesor ma obowiązek potwierdzić fakt zniszczenia Danych osobowych za pomocą pisemnego protokołu.

§ 10

PODWYKONAWCY

1) Subprocesor może wyznaczyć podwykonawców jedynie po uzyskaniu za pośrednictwem Procesora uprzedniej wyraźnej zgody Administratora. Zgoda Administratora, o której mowa w zdaniu poprzednim może być wyrażona na piśmie, lub w formie elektronicznej (e-mail).

Zakres podwykonawstwa obejmuje między innymi wykorzystanie osób trzecich wykonujących prace na zlecenie Subprocesora oraz środków zdalnego utrzymania systemów Przetwarzania danych.

2) Subprocesor informując Administratora za pośrednictwem Procesora o zamiarze wyznaczenia podwykonawcy przesyła następujące informacje:

1. nazwę potencjalnego podwykonawcy,

2. siedzibę potencjalnego podwykonawcy,

3. lokale potencjalnego podwykonawcy, w których będą Przetwarzane dane,

4. cele Przetwarzania danych Administratora przez potencjalnego podwykonawcę,

5. czynności Przetwarzania danych, które mają być wykonywane przez potencjalnego podwykonawcę,

6. kategorie Osób, których Dane Dotyczą,

7. kategorie Danych Osobowych,

8. dane kontaktowe Inspektora Ochrony Danych ze strony potencjalnego podwykonawcy,

9. planowany czas trwania podpowierzania.

3) Subprocesor nie może wyznaczyć podwykonawców mających siedzibę poza terytorium Europejskiego Obszaru Gospodarczego bez uprzedniej zgody Administratora wyrażonej pod rygorem nieważności w formie pisemnej lub w formie e-mail. Administrator może odmówić udzielenia takiej zgody bez uzasadnienia.

4) Jeżeli Subprocesor zamierza wyznaczyć podwykonawców mających siedzibę poza terytorium Europejskiego Obszaru Gospodarczego, wówczas przed rozpoczęciem jakichkolwiek prac dotyczących Danych osobowych Subprocesor podejmie kroki w celu zapewnienia odpowiedniej ochrony Danych osobowych zgodnie z RODO, np. poprzez zawarcie umów opartych na standardowych klauzulach umownych zatwierdzonych w Unii Europejskiej.

5) Subprocesor oświadcza, że dołoży należytej staranności przy wyborze podwykonawcy, oraz że upewni się, że podwykonawca przestrzega wymogów powszechnie obowiązujących na terytorium Rzeczypospolitej Polskiej przepisów dotyczących ochrony danych osobowych, a w szczególności, że podwykonawca dysponuje zasobami, doświadczeniem, wiedzą fachową i wykwalifikowanym personelem, które umożliwiają mu prawidłowe wykonywanie czynności Przetwarzania oraz wdrożenie odpowiednich środków technicznych i organizacyjnych tak, by Przetwarzanie przez niego Danych osobowych spełniało wymogi powszechnie obowiązującego na terytorium Rzeczypospolitej Polskiej prawa (w tym RODO) i chroniło prawa osób, których Dane osobowe dotyczą.

6) Niezależnie od postanowień ust. 5, Subprocesor zapewni zgodność z postanowieniami dotyczącymi zgody na przekazywanie Danych osobowych, uprawnień kontrolnych przysługujących Procesorowi i Administratorowi, oraz obowiązków opisanych w § 5 również w odniesieniu do podwykonawców zgodnie z niniejszą umową. Subprocesor ponosi wobec Procesora i Administratora pełną odpowiedzialność za wykonywanie obowiązków przez swoich podwykonawców.

7) Subprocesor powiadomi Administratora za Pośrednictwem Procesora o rozwiązaniu umowy z podwykonawcą w terminie 7 dni od dnia zaistnienia tego faktu.

§ 11

INNE ZOBOWIĄZANIA

1) Wszelkie dokumenty niezbędne do weryfikacji prawidłowego wykonania czynności Przetwarzania Danych osobowych zostaną przez Subprocesora w bezpieczny sposób (w szczególności w sposób zapobiegający ich zniszczeniu, uszkodzeniu lub utracie) zarchiwizowane i przekazane na wyraźne żądanie Administratora lub po rozwiązaniu/zakończeniu Umowy o współpracy lub wypowiedzenia niniejszej Umowy, w zależności od tego, która z tych okoliczności wystąpi wcześniej.

2) Po rozwiązaniu/zakończeniu Umowy o współpracy lub wypowiedzenia niniejszej umowy każda ze Stron zobowiązuje się do bezterminowego zachowania poufności Danych osobowych zgodnie z powyższymi ustaleniami.

§12

INSPEKTOR OCHRONY DANYCH WYZNACZONY PRZEZ SUBPROCESORA

1) W przypadku, w którym Subprocesor nie ma - zgodnie z powszechnie obowiązującymi na terytorium Rzeczypospolitej Polskiej przepisami prawa (w tym RODO) - obowiązku powoływania Inspektora Ochrony Danych, Subprocesor zapewni, aby wykonywanie Umowy o współpracy przebiegało zgodnie z postanowieniami niniejszej Umowy (np. poprzez wyznaczenie innej niż Inspektor Ochrony Danych osoby dedykowanej do przestrzegania postanowień niniejszej Umowy, oraz wskazanie kontaktu w sprawach dotyczących ochrony Danych Osobowych).

2) W przypadku powołania przez Subprocesora Inspektora Ochrony Danych, Subprocesor:

1. udostępni Procesorowi i Administratorowi wszelkie raporty z kontroli ochrony danych zebrane przez Inspektora Ochrony Danych, istotne w kontekście wykonywania czynności związanych z Przetwarzaniem Danych osobowych przez Subprocesora w imieniu Administratora na podstawie niniejszej Umowy (Subprocesor ma obowiązek niezwłocznie usunąć wszelkie nieprawidłowości wskazane w takich raportach),

2. niezwłocznie zawiadomi Procesora o wszelkich zmianach personalnych i kontaktowych dotyczących wyznaczonego przez niego Inspektora Ochrony Danych.

§13

PRAWA OSÓB TRZECICH. ZABEZPIECZENIE NA WYPADEK ROSZCZEŃ

1) Prawa osób, których dotyczą czynności Przetwarzania Danych osobowych prowadzone przez Subprocesora w imieniu Administratora, będą wykonywane i egzekwowane przez Procesora i Administratora.

2) Subprocesor ma obowiązek bez zbędnej zwłoki przekazywać Administratorowi za pośrednictwem Procesora wszelkie zapytania zgłaszane przez takie osoby i udzielać im w miarę swoich możliwości wsparcia, szczególnie w odniesieniu do powiadamiania, przekazywania informacji, zatwierdzania, blokowania i usuwania Danych osobowych, a także wsparcia w obronie przed nieuzasadnionymi roszczeniami.

3) W przypadku odpowiedzialności solidarnej Subprocesora, Procesora oraz Administratora, Subprocesor niezwłocznie i całkowicie zabezpieczy Procesora i Administratora na wypadek roszczeń osób, których dotyczą czynności Przetwarzania Danych osobowych prowadzone przez Subprocesora, lub kar pieniężnych nałożonych przez Organy Nadzoru Ochrony Danych Osobowych w związku z określonymi czynnościami Przetwarzania prowadzonymi przez Subprocesora lub jego podwykonawców, bądź naruszeniami postanowień umownych lub przepisów ustawowych przez Subprocesora lub jego podwykonawców.

§14

PRAWO DO WYPOWIEDZENIA UMOWY W SYTUACJACH NADZWYCZAJNYCH

1) Procesor może z ważnych przyczyn wypowiedzieć niniejszą Umowę lub Umowę o współpracy ze skutkiem natychmiastowym, w całości lub w części, jeżeli Subprocesor nie przestrzega swoich zobowiązań wynikających z niniejszej Umowy, w tym m.in. narusza czy to umyślnie, czy wskutek niedbalstwa - powszechnie obowiązujące na terytorium Rzeczypospolitej Polskiej przepisy dotyczące ochrony danych osobowych (w tym RODO) lub przepisy dotyczące bezpieczeństwa informacji. W szczególności Strony uzgadniają, że wszczęcie wobec Subprocesora postępowania upadłościowego stanowić będzie ważną przyczynę w tym kontekście. W celu usunięcia ewentualnych wątpliwości Strony wskazują, iż rozwiązanie Umowy o współpracy skutkuje rozwiązaniem niniejszej Umowy i odwrotnie.

§15

UPRAWNIENIA KONTROLNE

1) Procesor i Administrator mają prawo kontrolować stosowane przez Subprocesora zabezpieczenia techniczne i organizacyjne, które dotyczą czynności Przetwarzania Danych osobowych podlegających niniejszej Umowie, przed rozpoczęciem jakichkolwiek czynności Przetwarzania Danych osobowych na rzecz Procesora i Administratora oraz w trakcie ich wykonywania. W tym celu Procesor i Administrator mogą w szczególności zażądać przedłożenia odpowiednich dokumentów, w tym raportów dotyczących bezpieczeństwa informatycznego lub raportów z kontroli ochrony prywatności przeprowadzonych przez kontrolerów Subprocesora lub podmiotów zewnętrznych.

2) Procesor i Administrator mogą przeprowadzać kontrole, o których powinien powiadamiać z wyprzedzeniem co najmniej 3 dni, w celu stwierdzenia, czy Subprocesor przestrzega wymogów określonych w niniejszej Umowie. Na żądanie Subprocesor przekaże Procesorowi i Administratorowi wszelkie niezbędne informacje w tym zakresie i zachowa odpowiednie potwierdzenia.

3) W przypadku powzięcia przez Procesora lub Administratora wiadomości o rażącym naruszeniu przez Subprocesora zobowiązań wynikających z niniejszej Umowy, Subprocesor umożliwi Procesorowi lub Administratorowi dokonanie niezapowiedzianej kontroli w przedmiocie objętym niniejszą Umową.

4) Kontrole, o których mowa w niniejszym paragrafie Procesor i Administrator mogą wykonywać samodzielnie, lub za pośrednictwem podmiotów trzecich.

§16

BEZPIECZEŃSTWO INFORMACJI

1) Subprocesor oświadcza, że dysponuje zasobami, doświadczeniem, wiedzą fachową i wykwalifikowanym personelem, które umożliwiają mu prawidłowe wykonanie niniejszej Umowy oraz wdrożenie odpowiednich środków technicznych i organizacyjnych tak, by Przetwarzanie przez niego Danych osobowych spełniało wymogi powszechnie obowiązującego na terytorium Rzeczypospolitej Polskiej prawa i chroniło prawa osób, których Dane osobowe dotyczą. Subprocesor zapewni przestrzeganie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa niezbędnych w celu prawidłowej ochrony i zabezpieczenia Danych Osobowych Przetwarzanych w imieniu Administratora. Subprocesor musi kontrolować przestrzeganie tych środków, przekazując Procesorowi i Administratorowi dokumentację potwierdzającą wykonywanie tego obowiązku.

2) Środki bezpieczeństwa wdrożone przez Subprocesora muszą zapewniać bezpieczeństwo co najmniej w następujących obszarach:
1. ochrona przed nieuprawnionym dostępem do systemów Przetwarzania danych w celu Przetwarzania Danych osobowych (kontrola

dostępu),

2. ochrona przed nieuprawnionym korzystaniem z systemów Przetwarzania danych (kontrola dostępu),

3. zapewnienie, aby osoby uprawnione do korzystania z systemu Przetwarzania Danych osobowych miały dostęp jedynie do danych objętych takim uprawnieniem oraz aby Dane osobowe nie mogły być odczytywane, kopiowane, zmieniane ani usuwane bez uprawnienia w trakcie ich Przetwarzania i po ich zapisie (kontrola dostępu) w systemach utrzymywanych przez Subprocesora,

4. zapewnienie, aby Dane osobowe nie mogły być odczytywane, kopiowane, zmieniane ani usuwane bez uprawnienia podczas ich elektronicznego przesyłu lub transportu, a także w trakcie zapisu na nośnikach danych, oraz aby możliwe było określenie, którym organom Dane osobowe mają zostać przesłane za pośrednictwem urządzeń do transmisji danych (kontrola ujawniania danych),

5. zapewnienie - po fakcie - możliwości sprawdzenia, czy Dane osobowe zostały wprowadzone, zmienione lub usunięte z systemów

Przetwarzania danych utrzymywanych przez Subprocesora, a jeżeli tak, to przez kogo (kontrola wprowadzania danych),

6. zapewnienie, aby Przetwarzanie Danych osobowych w imieniu innych podmiotów przebiegało ściśle według instrukcji Administratora (kontrola zadań),

7. zapewnienie ochrony Danych osobowych przed przypadkowym zniszczeniem lub utratą (kontrola dostępności),

8. zapewnienie, aby Dane osobowe zbierane w różnych celach były przetwarzane oddzielnie.

3) Subprocesor gwarantuje przestrzeganie powyższych technicznych i organizacyjnych środków bezpieczeństwa niezależnie od miejsca, w którym faktycznie odbywa się Przetwarzanie Danych osobowych. Miejsca takie mogą obejmować biura domowe lub mobilne pracowników Subprocesora, za wyraźną zgodą Administratora.

4) Minimalny zakres środków bezpieczeństwa do stosowania których zobowiązuje się Subprocesor został określony w Załączniku nr 2.

§ 17

POSTANOWIENIA KOŃCOWE

1) Niniejsza Umowa podlega prawu polskiemu. W sprawach, które nie zostały uregulowane Umową, znajdują zastosowanie odpowiednie przepisy Kodeksu cywilnego, Rozporządzenia 2016/679 (RODO) oraz innych obowiązujących przepisów z zakresu ochrony Danych osobowych.

2) Zmiany Umowy są możliwe wyłącznie w formie dokumentowej (art. 77^2 Kodeksu cywilnego) lub pisemnej pod rygorem nieważności z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian.

3) Subprocesor nie może przenieść praw lub obowiązków wynikających z niniejszej Umowy bez pisemnej zgody Procesora.

4) O ile Umowa nie stanowi inaczej, wszelkie spory w związku z niniejszą Umową zostaną poddane pod rozstrzygnięcie sądu powszechnego miejscowo właściwego ze względu na siedzibę Procesora.

5) Umowa zastępuje wszelkie wcześniejsze stosunki obligacyjne między stronami w zakresie ochrony Danych osobowych.

6) O każdej zmianie danych, Strony powiadomią się na piśmie lub w formie dokumentowej.

ZAŁĄCZNIK NR 1

OPIS DANYCH I CZYNNOŚCI PRZETWARZANIA DANYCH

1) Opis celów i sposobów przetwarzania Danych osobowych: Dane osobowe będą Przetwarzane w celu wykonywania Umowy o współpracy, tj. w celu świadczenia na rzecz Procesora czynności pośrednictwa ubezpieczeniowego. Dane osobowe będą Przetwarzane w sposób ciągły.

2) Czynności Przetwarzania: Zbieranie, Porządkowanie, Przechowywanie, Przeglądanie, Utrwalanie, Wyodrębnianie, Porównywanie, Pobieranie, Modyfikowanie, adaptowanie lub zmiana, Dopasowywanie lub łączenie.

3) Kategorie Osób, Których Dane Dotyczą: Ubezpieczający, Ubezpieczony, Uprawniony, Wnioskodawca, Poszkodowany, Przedstawiciel Ubezpieczającego, Przedstawiciel Ubezpieczonego, Przedstawiciel Uprawnionego, Przedstawiciel Wnioskodawcy, Przedstawiciel Poszkodowanego, Uczestnik zdarzenia ubezpieczeniowego, Dziecko Ubezpieczonego.

4) Kategorie Danych osobowych - dot. Ubezpieczającego: Imię (imiona), Nazwisko, Nazwisko rodowe, Płeć, Data urodzenia, PESEL, Seria i numer dokumentu tożsamości, Adres zamieszkania (ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, kraj), REGON, NIP, Firma pod jaką jest prowadzona działalność gospodarcza, Nazwa pracodawcy i lokalizacja miejsca pracy, Obywatelstwo, Nr polisy, Nr wniosku, Suma ubezpieczenia, Dane dotyczące rachunku bankowego, Adres e-mail, Nr telefonu.

5) Kategorie Danych osobowych - dot. Ubezpieczonego: Imię (imiona), Nazwisko, Nazwisko rodowe, Płeć, Data urodzenia, PESEL, REGON, Seria i numer dokumentu tożsamości, Imię (imiona) i nazwisko dziecka, Imię (imiona) i nazwisko małżonka, Adres zamieszkania (ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, kraj), Status podatkowy (rezydent/nierezydent), Dane dotyczące przedmiotu ubezpieczenia, Firma pod jaką jest prowadzona działalność gospodarcza, Nazwa pracodawcy, lokalizacja miejsca pracy, stanowisko, Obywatelstwo, Nr polisy, Nr wniosku, Suma ubezpieczenia, Dane dotyczące rachunku bankowego, Adres e-mail, Nr telefonu, Dane dotyczące stanu zdrowia.

6) Kategorie Danych osobowych - dot. Uprawnionego: Imię (imiona), Nazwisko, Nazwisko rodowe, Płeć, Data urodzenia, PESEL, Seria i numer dokumentu tożsamości, Nazwa i adres urzędu skarbowego, Dane dotyczące rachunku bankowego, Adres do wypłaty gotówkowej, Adres zamieszkania (ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, kraj), Adres e-mail, Nr telefonu.

7) Kategorie Danych osobowych - dot. Przedstawicieli: Ubezpieczającego, Ubezpieczonego, Uprawnionego, Poszkodowanego: Imię (imiona), Nazwisko, Płeć, Seria i numer dokumentu stwierdzającego tożsamość (dowód osobisty/paszport), Inne dane wskazane w treści pełnomocnictwa, Adres e-mail, Nr telefonu, Adres, PESEL.

8) Kategorie Danych osobowych - dot. Wnioskodawcy: Imię (imiona), Nazwisko, Nazwisko rodowe, Płeć, Data urodzenia, PESEL, Seria i numer dokumentu tożsamości, Adres zamieszkania (ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, kraj), REGON, NIP, Firma pod jaką jest prowadzona działalność gospodarcza, Nazwa pracodawcy i lokalizacja miejsca pracy, Obywatelstwo, Nr wniosku, Suma ubezpieczenia, Dane dotyczące rachunku bankowego, Adres e-mail, Nr telefonu.

9) Kategorie Danych osobowych - dot. Poszkodowanego: Imię (imiona), Nazwisko, Nazwisko rodowe, Data urodzenia, Płeć, PESEL, Seria i numer dokumentu tożsamości, Adres zamieszkania (ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, kraj), E-mail, Nr telefonu.

10) Kategorie Danych osobowych - dot. Uczestników zdarzenia ubezpieczeniowego: Imię (imiona), Nazwisko, Płeć, Seria i numer dokumentu tożsamości, Adres zamieszkania (ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, kraj), Adres e-mail, Nr telefonu.

ZAŁĄCZNIK NR 2

MINIMALNE TECHNICZNE I ORGANIZACYJNE ŚRODKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

CZEŚĆ I

Środki organizacyjne

1) Subprocesor musi posiadać formalnie udokumentowaną politykę bezpieczeństwa informacji.

2) W strukturze organizacyjnej Subprocesora:

1) musi zostać wyznaczona osoba odpowiedzialna za bezpieczeństwo informacji,

2) muszą obowiązywać formalnie zatwierdzone wymogi przestrzegania zasad i procedur bezpieczeństwa informacji dla podwykonawców, pracowników stałych oraz kontraktowych mających wgląd do danych osobowych,

3) musi obowiązywać formalnie zatwierdzona procedura ochrony antywirusowej dotycząca komputerów osobistych, laptopów, serwerów plików i poczty oraz innych urządzeń, które przechowują, przetwarzają i transmitują dane, których administratorem jest Allianz. Dodatkowo użytkownicy powinni mieć ograniczone możliwości interwencji w zakresie modyfikacji programu antywirusowego,

4) muszą obowiązywać formalnie udokumentowane plany ciągłości działania i usuwania skutków awarii dla usług / systemów / aplikacji Przetwarzających dane, których administratorem jest Allianz, Plany opierają się na analizie wpływu na biznes, która identyfikuje ryzyko przerwania działalności związane z dostarczanymi produktami / usługami / aplikacjami. Analiza wpływu na biznes jest zatwierdzana przez kierownictwo i weryfikowana, co najmniej raz w roku,

5) musi obowiązywać formalnie udokumentowany plan/procedura zarządzania incydentami bezpieczeństwa, w ramach, którego personel (stały, kontraktowy i tymczasowy) musi zgłaszać wszelkie faktyczne lub podejrzewane incydenty dotyczące danych, których administratorem jest Allianz; Taki plan/procedura jasno określa:

a) role i obowiązki,

b) definicja zdarzenia,

c) proces oceny ryzyka i działania ograniczające,

d) proces powiadomienia klienta,

e) drogi eskalacji (listę hierarchiczną osób biorących udział w obsłudze incydentu).

6) musi funkcjonować cykliczny przegląd uprawnień do systemów oraz pomieszczeń,

7) musi obowiązywać formalnie udokumentowana polityka dotycząca haseł do stacji roboczych Subprocesora przewidująca co najmniej następujące zasady:

a) hasła do kont administracyjnych zmienione z domyślnych

b) hasła posiadają minimum 6 znaków, posiadają małą oraz wielką literę, cyfrę i znak specjalny

c) hasła nie mogą zawierać identyfikatorów użytkowników

d) wylogowanie po bezczynności wynoszącej maksymalnie 60 minut

e) hasła zmieniane co 30 dni

3. Bieżące działania w zakresie monitorowania zgodności, przeprowadzane w odniesieniu do danych, których administratorem jest Allianz z niedociągnięciami kontrolnymi, są śledzone i zarządzane za pomocą formalnego procesu naprawczego.

4. Zgodność z odpowiednimi normami prawnymi / regulacyjnymi jest regularnie monitorowana.

CZĘŚĆ II

Środki techniczne

1) Aktualizacje zabezpieczeń (poprawki) są stosowane do systemów/urządzeń przechowujących lub przetwarzających dane, których administratorem jest Allianz.

2) Informacje zawierające Dane osobowe, których administratorem jest Allianz przesyłane przez sieć są szyfrowane.

3) Istnieje formalnie stosowana polityka czystego biurka, a dokumenty w formie papierowej są przechowywane z należytą starannością o bezpieczeństwo.