Załącznik nr 1 do Umowy współpracy

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu …… roku, w Warszawie (dalej „**Umowa**"), pomiędzy:

UNILINK Życie Sp. z o.o. z siedzibą w Warszawie, al. Krakowska 2, 02-284 Warszawa, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000334376, NIP 5342429016, Regon 141982123, zwanej w dalszej części umowy **„Powierzającym"**, reprezentowaną przez:

1) Igor Rusinowski,
2) Piotr Głowski,

oraz

Panią/Panem ……., zam. ……,
(imię i nazwisko) *(adres)*
prowadzącą/ym działalność gospodarczą pod nazwą: ……., adres: ……, wpisaną/y do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, posiadający nr PESEL ……., NIP ……., REGON ……., działającą/ym w imieniu własnym/przez pełnomocnika ……
(imię i nazwisko pełnomocnika, adres, nr PESEL)

umocowanego na podstawie pełnomocnictwa z dnia ……

(do uzupełnienia w przypadku Partnera – osoby fizycznej prowadzącej jednoosobową działalność gospodarczą)

……
z siedzibą w ……. wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd …… pod nr KRS ……., NIP ……., REGON ……., o kapitale zakładowym w wysokości …… wpłaconym w ……. reprezentowaną przez:
……
(do uzupełnienia w przypadku Partnera – osoby prawnej)

zwaną dalej **„Procesorem"**.

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

§ 1
PRZEDMIOT UMOWY

1. Powierzający i Procesor zawierają umowę powierzenia przetwarzania danych osobowych, zwaną dalej "**Umową**", na mocy której Powierzający powierza Procesorowi przetwarzanie danych osobowych, rozumianych jako informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), w zakresie wskazanym w Załączniku nr 1.
2. Powierzenie danych osobowych Procesorowi następuje w celu wykonania umowy współpracy zawartej pomiędzy Stronami w dniu …… roku (dalej jako „**Umowa główna**").
3. Zakres powierzenia, wskazany w Załączniku nr 1, może zostać w każdym momencie rozszerzony albo ograniczony przez Powierzającego. Ograniczenie albo rozszerzenie może być dokonane poprzez przesłanie przez Powierzającego do Procesora nowej wersji Załącznika nr 1 w formie elektronicznej (na adres e-mail wskazany w Załączniku nr 1). W przypadku braku reakcji Procesora w ciągu 5 Dni Roboczych (na potrzeby Umowy „**Dni Robocze**" należy rozumieć dni od poniedziałku do piątku, poza dniami ustawowymi wolnymi od pracy) od daty wysłania wiadomości przez Powierzającego przyjmuje się, że Procesor zaakceptował zmianę zakresu powierzenia.
4. Procesor może przetwarzać powierzone mu dane osobowe wyłącznie w zakresie i celu określonym w niniejszej Umowie oraz w celu i zakresie niezbędnym do świadczenia usług określonych w Umowie głównej.

§ 2

OŚWIADCZENIA I OBOWIĄZKI PROCESORA

1. Procesor niniejszym oświadcza, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie niniejszej Umowy, w zgodzie z obowiązującymi przepisami prawa. W szczególności Procesor oświadcza, że znane mu są zasady przetwarzania i zabezpieczenia danych osobowych wynikające z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej jako: „RODO").
2. Procesor jest zobowiązany:
   1) przetwarzać powierzone dane osobowe wyłącznie w okresie niezbędnym do wykonania Umowy głównej, z zastrzeżeniem § 2 ust. 2 pkt 16 Umowy;
   2) przetwarzać powierzone dane osobowe wyłącznie na postawie Umowy oraz na udokumentowane polecenie Powierzającego (tj. przekazane w formie instrukcji, o których mowa w § 2 ust. 2 pkt 2 lub w innym pisemnym lub elektronicznym dokumencie dostarczonym Procesorowi przez Powierzającego, w tym w Umowie głównej), chyba że obowiązek taki nakłada na niego obowiązujące prawo krajowe lub unijne. W sytuacji, gdy obowiązek przetwarzania danych osobowych przez Procesora wynika z przepisów prawa, informuje on Powierzającego drogą elektroniczną - przed rozpoczęciem przetwarzania - o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
   3) przetwarzać powierzone dane osobowe zgodnie z RODO, polskimi przepisami przyjętymi w celu umożliwienia stosowania RODO, innymi obowiązującymi przepisami prawa, niniejszą Umową oraz ewentualnie instrukcjami Powierzającego. Instrukcje (polecenia) mogą być przekazywane przez Powierzającego drogą elektroniczną (przesyłane na adres e-mail Procesora wskazany w Załączniku nr 1); z zastrzeżeniem § 3 ust. 5 Procesor powinien w miarę możliwości wdrożyć instrukcje niezwłocznie, jednak nie później niż w terminie 5 Dni Roboczych od ich otrzymania; jeżeli w ocenie Procesora termin 5-dniowy jest zbyt krótki na realizację instrukcji lub ich wykonanie wiąże się z nieuzasadnionymi lub znaczącymi kosztami dla Procesora, powinien poinformować o tym fakcie Powierzającego drogą elektroniczną (przesyłając informację na adres e-mail Procesora wskazany w Załączniku nr 1) wskazując uzasadnienie dla takiej oceny; w takim przypadku Strony wspólnie ustalą późniejszy termin wdrożenia lub zmianę treści instrukcji Powierzającego albo sposób pokrycia kosztów jej realizacji;
   4) przetwarzać powierzone mu dane osobowe z zachowaniem najwyższych zasad bezpieczeństwa i ochrony danych osobowych wymaganych przez obowiązujące przepisy prawa;
   5) udzielać dostępu do powierzonych danych osobowych wyłącznie osobom, które ze względu na zakres wykonywanych zadań otrzymały od Procesora pisemne upoważnienie do ich przetwarzania oraz wyłącznie w celu wykonywania obowiązków wynikających z Umowy;
   6) zapewnić, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy; Procesor niniejszym potwierdza, że został pouczony, że powierzone mu dane osobowe mogą stanowić także tajemnicę ubezpieczeniową w rozumieniu ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (tj. z dnia 26 maja 2017 r., Dz.U. 2017, poz. 1170 ze zm.) i ich procesowanie wymaga zachowania najwyższej staranności, w tym w zakresie zasad bezpieczeństwa wynikających z obowiązujących przepisów prawa i Umowy głównej;
   7) wdrożyć, zgodnie z wytycznymi wskazanymi w § 3 Umowy, odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane osobowe będą przetwarzane na podstawie Umowy oraz zapewnić realizację zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych (określonych w art. 25 RODO);
   8) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Powierzającemu (poprzez stosowanie odpowiednich środków technicznych i organizacyjnych) w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO. Współpraca Procesora z Powierzającym, w zakresie wskazanym w zdaniu poprzednim, powinna odbywać się w formie i terminie umożliwiającym realizację tych obowiązków przez Powierzającego; w związku z realizacją tego obowiązku Procesor jest w szczególności zobowiązany do udzielania informacji oraz udostępniania powierzonych danych osobowych (lub ich kopii) na żądanie Powierzającego w terminie 3 Dni Roboczych w formie określonej przez Powierzającego w żądaniu; Procesor powinien również niezwłocznie, jednak nie później niż w terminie 1 Dnia Roboczego, poinformować Powierzającego o wniosku dotyczącym realizacji praw osoby, której dane dotyczą, złożonym u Procesora; Procesor nie będzie jednak odpowiadał na taki wniosek bez uprzedniej zgody lub wyraźnego polecenia Powierzającego;
   9) o ile w ramach realizacji Umowy głównej Procesor dokonuje w imieniu Powierzającego czynności polegających na zbieraniu i utrwalaniu danych osobowych, Procesor zobowiązuje się przedstawić podmiotom danych informacje, wynikające z treści art. 13 i 14 RODO najpóźniej w momencie zbierania tych danych. Treść obowiązku informacyjnego oraz sposób jego prezentacji i udokumentowania zostanie Procesorowi dostarczona przez Powierzającego zgodnie z procedurą określoną w ust. 2 powyżej;

10) uwzględniając charakter przetwarzania i dostępne Procesorowi informacje, pomagać Powierzającemu wywiązać się z obowiązków określonych w RODO (w tym w art. 32–36 RODO), tj. w szczególności w zakresie:
    a) zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez wdrożenie stosownych środków technicznych oraz organizacyjnych (standard środków, które zobowiązany jest wdrożyć Procesor został określony w Załączniku nr 2);
    b) dokonywania zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osób, których dane dotyczą o takim naruszeniu (obowiązki Procesora w odniesieniu do zgłaszania naruszeń zostały określone w § 7 Umowy);
    c) dokonywania przez Powierzającego oceny skutków dla ochrony danych oraz przeprowadzania konsultacji Powierzającego z organem nadzorczym, w tym, w szczególności, jest zobowiązany dostarczać Powierzającemu informacji niezbędnych do opisu planowanych operacji przetwarzania oraz celu przetwarzania, a także jest zobowiązany do uczestniczenia w dokonywaniu oceny, czy te operacje są niezbędne oraz proporcjonalne do celu przetwarzania oraz oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą;
11) prowadzić, w formie pisemnej (w tym elektronicznej), rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Powierzającego, zawierający informacje o:
    a) nazwie oraz danych kontaktowych Procesora oraz innych podmiotów przetwarzających (w przypadku podpowierzenia danych osobowych, o którym mowa w § 4 Umowy) oraz administratora danych osobowych (którym co do zasady będzie ubezpieczyciel), a także inspektora ochrony danych, gdy ma to zastosowanie;
    b) kategoriach przetwarzań dokonywanych w imieniu Powierzającego;
    c) gdy ma to zastosowanie - przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwie tego państwa trzeciego lub organizacji międzynarodowej;
    d) ogólnym opisie technicznych i organizacyjnych środków bezpieczeństwa, służących do zabezpieczenia powierzonych danych osobowych.
12) udostępniać Powierzającemu, na każde jego żądanie, nie później niż w terminie 3 Dni Roboczych, wszelkie informacje niezbędne do wykazania spełnienia przez Powierzającego obowiązków wynikających z właściwych przepisów prawa, w szczególności z RODO, w tym przekazywać informacje o stosowanych zabezpieczeniach, zidentyfikowanych zagrożeniach i incydentach w obszarze ochrony danych osobowych;
13) umożliwić Powierzającemu lub audytorowi upoważnionemu przez Powierzającego przeprowadzanie audytów na zasadach określonych w § 6 Umowy;
14) niezwłocznie informować Powierzającego, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów krajowych lub unijnych o ochronie danych; informacja w tym przedmiocie przekazana powinna zostać Powierzającemu w formie elektronicznej (na adres e-mail wskazany w Załączniku nr 1) oraz powinna zawierać stosowne uzasadnienie i wskazanie przepisu prawa, który zdaniem Procesora został naruszony;
15) niezwłocznie, jednak nie później niż w ciągu 2 Dni Roboczych, informować (o ile nie doprowadzi to do naruszenia przepisów obowiązującego prawa) Powierzającego o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych przez Procesora, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych, skierowanej do Procesora, o wszelkich kontrolach i inspekcjach dotyczących przetwarzania danych osobowych przez Procesora, w szczególności prowadzonych przez organ nadzoru, a także o wszelkich skargach osób, których dane dotyczą związanych z przetwarzaniem ich danych osobowych;
16) przechowywać dane osobowe tylko tak długo, jak jest to niezbędne dla realizacji przez Procesora Umowy głównej w stosunku do danego podmiotu danych, a po tym okresie usunąć te dane ze wszelkich nośników. Obowiązek usunięcia nie dotyczy sytuacji, gdy Procesor posiada samodzielną podstawę do przetwarzania danych, w takim przypadku jednak zobowiązany jest wprowadzić mechanizmy uniemożliwiające przetwarzanie danych osobowych w imieniu Powierzającego.

§ 3
ŚRODKI ORGANIZACYJNE I TECHNICZNE

1. Procesor wdraża i stosuje adekwatne środki techniczne i organizacyjne, w celu zapewnienia stopnia bezpieczeństwa odpowiedniego do ryzyka naruszenia praw lub wolności osób fizycznych, których dane osobowe są przetwarzane na podstawie Umowy. Procesor powinien w szczególności wdrożyć – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – odpowiednie środki zaprojektowane w celu skutecznej realizacji zasad ochrony danych określonych w RODO oraz w celu ochrony praw osób, których dane dotyczą (zasada ochrony danych osobowych w fazie projektowania określona w art. 25 ust. 1 RODO), a także aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania określonego w Załączniku nr 1 (zasada

domyślnej ochrony danych określona w art. 25 ust. 2 RODO). Standard środków, które zobowiązany jest wdrożyć Procesor został określony w Załączniku nr 2.

2. Oceniając, czy stopień bezpieczeństwa, o którym mowa w ust. 1, jest odpowiedni, Procesor jest zobowiązany uwzględnić ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Wdrażając środki organizacyjne i techniczne, o których mowa w ust. 1 i 2, Procesor:
   1) w miarę możliwości przestrzega wytycznych Powierzającego w zakresie sposobu zabezpieczenia procesów przetwarzania danych osobowych zgodnie z przepisami obowiązującego prawa, o których mowa w § 2 ust. 1 pkt 1 oraz 2;
   2) powinien uwzględnić stan wiedzy technicznej oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, których dane osobowe będzie przetwarzał na podstawie niniejszej Umowy.
4. W przypadku stwierdzenia, że stosowane środki mogą być nieadekwatne do rozpoznanych zagrożeń, Procesor informuje o tym Powierzającego i w porozumieniu z Powierzającym dostosowuje odpowiednio zabezpieczenia przetwarzania danych osobowych.
5. Powierzający ma prawo wydawać Procesorowi wiążące instrukcje dotyczące wdrożenia dodatkowych środków zabezpieczających. Procesor powinien wdrożyć takie środki w terminie uzgodnionym z Powierzającym.
6. Na każde żądanie Powierzającego, Procesor jest zobowiązany do udostępniania dokumentacji (procedur) dotyczącej przetwarzania danych osobowych nie później niż w terminie 3 Dni Roboczych od dnia złożenia takiego żądania.

§ 4
PODPOWIERZENIE

1. Powierzający nie wyraża zgody na dalsze powierzenie przez Procesora przetwarzania danych osobowych innym podmiotom przetwarzającym, za wyjątkiem sytuacji, w której Procesor wystąpi o indywidualne wyrażenie takiej zgody w formie pisemnej i taka zgoda w formie pisemnej pod rygorem nieważności zostanie Procesorowi przez Powierzającego udzielona. Brak odpowiedzi na złożony wniosek nie oznacza zgody na dalsze powierzenie przetwarzania danych osobowych.
2. W przypadku otrzymania przez Procesora indywidualnej zgody Powierzającego na podpowierzenie przetwarzania danych osobowych:
   1) Procesor zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz przepisów obowiązującego prawa z zakresu ochrony danych osobowych, a także chroniło prawa osób, których dane dotyczą.
   2) Procesor zapewni w umowie z dalszym podmiotem przetwarzającym, że na podmiot ten zostaną nałożone obowiązki odpowiadające obowiązkom Procesora określonym w Umowie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.
   3) Procesor zapewni również w umowie z dalszym podmiotem przetwarzającym możliwość realizacji przez Powierzającego bezpośredniej kontroli względem dalszego podmiotu przetwarzającego (w tym możliwość przeprowadzania audytów, o których mowa w § 6 Umowy). Procesor jest zobowiązany poinformować dalszy podmiot przetwarzający, że informacje, w tym dane osobowe, na temat tego podmiotu przetwarzającego mogą być udostępnione Powierzającemu w celu wykonania przez niego uprawnień, o których mowa w zdaniu poprzedzającym.
   4) Procesor jest w pełni odpowiedzialny przed Powierzającym za spełnienie obowiązków wynikających z umowy powierzenia zawartej pomiędzy Procesorem a dalszym podmiotem przetwarzającym. Jeżeli dalszy podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Powierzającego za wypełnienie obowiązków tego dalszego podmiotu przetwarzającego spoczywa na Procesorze.

§ 5
TRANSFER DANYCH OSOBOWYCH

Procesor nie może przekazywać (transferować) danych osobowych do państwa trzeciego, które znajduje się poza Europejskim Obszarem Gospodarczym („EOG").

§ 6
AUDYT

1. Powierzający jest w każdym momencie upoważniony do przeprowadzenia audytu zgodności przetwarzania danych osobowych przez Procesora z Umową oraz obowiązującymi przepisami prawa, w szczególności Powierzający może przeprowadzić weryfikację zgodności i adekwatności środków technicznych i organizacyjnych zabezpieczających przetwarzanie danych osobowych wdrożonych przez Procesora.
2. Powierzający poinformuje Procesora co najmniej 3 Dni Robocze przed planowaną datą audytu o zamiarze jego przeprowadzenia. Jeżeli z ważnych powodów, w ocenie Procesora, audyt nie może zostać przeprowadzony we wskazanym terminie Procesor powinien poinformować o tym fakcie Powierzającego drogą elektroniczną (przesyłając informację na adres e-mail Procesora wskazany w Załączniku nr 1) wskazując uzasadnienie dla takiej oceny. W takim przypadku Strony wspólnie ustalą późniejszy termin audytu.
3. Audyt, o których mowa w § 6 ust. 1, mogą być wykonywane przez Powierzającego (osoby przez niego wyznaczone) lub podmioty zewnętrzne, którym Powierzający zleci wykonanie audytu, w miejscu przetwarzania danych osobowych objętych powierzeniem w Dni Robocze w godzinach od 8 do 16.
4. Procesor ma obowiązek współpracować z Powierzającym i upoważnionymi przez niego audytorami, w szczególności zapewniać im dostęp do pomieszczeń i dokumentów obejmujących dane osobowe oraz informacje o sposobie przetwarzania danych osobowych, infrastruktury teleinformatycznej oraz systemów IT, a także do osób mających wiedzę na temat procesów przetwarzania danych osobowych realizowanych przez Procesora.
5. Po przeprowadzonym audycie przedstawiciel Powierzającego sporządza protokół pokontrolny, który podpisują przedstawiciele obu Stron. Procesor zobowiązuje się w terminie uzgodnionym z Powierzającym, dostosować do zaleceń pokontrolnych zawartych w protokole, mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
6. Powierzającym ma także prawo żądać od Procesora składania pisemnych, w tym w formie elektronicznej, wyjaśnień dotyczących realizacji Umowy. Procesor zobowiązuje się odpowiedzieć niezwłocznie, jednak nie później niż w terminie 3 Dni Roboczych, na każde pytanie Powierzającego dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.
7. Procesor jest zobowiązany zapewnić w umowie z dalszym podmiotem przetwarzającym możliwość przeprowadzania przez Powierzającego (lub podmiot zewnętrzny, któremu Powierzający zleci wykonanie audytu) audytu zgodności przetwarzania danych osobowych przez dalszy podmiot przetwarzający z Umową na zasadach określonych w § 6 ust. 1 – 5.
8. Koszty związane z przeprowadzeniem audytu ponosi podmiot, który zlecił przeprowadzenie audytu, bez prawa do żądania zwrotu takich kosztów ani zapłaty dodatkowego wynagrodzenia.

§ 7
ZGŁASZANIE NARUSZEŃ

1. Procesor jest zobowiązany do wdrożenia i stosowania rozwiązań organizacyjnych i technicznych służących wykrywaniu naruszeń ochrony danych osobowych oraz wdrażaniu właściwych środków naprawczych. Procesor jest zobowiązany do udostępniania informacji dotyczących stosowanych rozwiązań, o których mowa w zdaniu poprzedzającym, na każde żądanie Powierzającego, nie później niż w terminie 3 Dni Roboczych od dnia złożenia takiego żądania.
2. Po stwierdzeniu naruszenia ochrony powierzonych mu przez Powierzającego danych osobowych Procesor, bez zbędnej zwłoki, jednak w miarę możliwości nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, zgłasza je Powierzającemu. Zgłoszenie powinno zawierać co najmniej informacje o:
   1) dacie, czasie trwania oraz lokalizacji naruszenia ochrony danych osobowych chyba że ustalenie tych informacji przez Procesora jest niemożliwe lub wymagałoby poniesienia niewspółmiernie wysokich kosztów lub nakładów pracy;
   2) charakterze i skali naruszenia, w tym w miarę możliwości o kategoriach i przybliżonej liczbie osób, których dane dotyczą, oraz kategoriach i przybliżonej liczbie wpisów danych osobowych, których dotyczy naruszenie, a w razie możliwości, także wskazania podmiotów danych, których dotyczyło naruszenie;
   3) systemie informatycznym, w którym wystąpiło naruszenie (jeżeli naruszenie nastąpiło w związku z przetwarzaniem danych w systemie informatycznym);
   4) możliwych konsekwencjach naruszenia, z uwzględnieniem konsekwencji dla osób, których dane dotyczą;
   5) środkach podjętych w celu zminimalizowania konsekwencji naruszenia oraz proponowanych działaniach zapobiegawczych i naprawczych;
   6) danych kontaktowych osoby mogącej udzielić dalszych informacji o naruszeniu.
3. Jeżeli Procesor nie jest w stanie w tym samym czasie przekazać Powierzającemu wszystkich informacji, o których mowa w ust. 2, powinien je udzielać sukcesywnie, bez zbędnej zwłoki.
4. Do czasu uzyskania instrukcji od Powierzającego, Procesor bez zbędnej zwłoki podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.

5. Procesor jest zobowiązany do dokumentowania wszelkich naruszeń ochrony powierzonych mu danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych. Procesor jest zobowiązany na każde żądanie Powierzającego niezwłocznie udostępnić mu dokumentację, o której mowa w zdaniu poprzedzającym.
6. Procesor nie będzie bez wyraźnej instrukcji Powierzającego powiadamiał o naruszeniu:
   1) osób, których dane dotyczą ani
   2) organu nadzorczego.
7. Informacje, o których mowa w ust, 2 powinny być dostarczone Powierzającemu przy zastosowaniu ścieżek komunikacji określonych w Załączniku nr 1.

§ 8
CZAS TRWANIA UMOWY ORAZ ZASADY ODPOWIEDZIALNOŚCI

1. Niniejsza Umowa zostaje zawarta na czas określony i przestaje obowiązywać wraz z zakończeniem obowiązywania Umowy głównej.
2. Powierzający może rozwiązać Umowę z zachowaniem okresu wypowiedzenia odpowiadającemu okresowi przewidzianemu dla wypowiedzenia Umowy głównej.
3. Powierzający uprawniony jest do wypowiedzenia Umowy ze skutkiem natychmiastowym w przypadku zaistnienia ważnych powodów, w szczególności gdy::
   1) organ nadzoru nad przestrzeganiem zasad przetwarzania danych osobowych stwierdzi, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych;
   2) prawomocne orzeczenie sądu powszechnego wykaże, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych;
   3) Powierzający, w wyniku przeprowadzenia audytu, o którym mowa w § 6 Umowy stwierdzi, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych wynikających z Umowy lub obowiązujących przepisów prawa lub Procesor nie zastosuje się do zaleceń pokontrolnych, o których mowa w § 6 ust. 5.
4. Naruszenie przez Procesora postanowień niniejszej Umowy, RODO lub innych obowiązujących przepisów prawa z zakresu ochrony danych osobowych stanowi podstawę do wypowiedzenia Umowy głównej.
5. Po zakończeniu obowiązywania Umowy Procesor powinien, zgodnie z dyspozycją Powierzającego, zwrócić lub zniszczyć, w sposób i w terminie odrębnie wskazanym przez Powierzającego, wszelkie dane osobowe i ich kopie, chyba że właściwe przepisy prawa krajowego lub unijnego nakazują przechowywanie tych danych osobowych. Koszty zwrotu lub zniszczenia danych osobowych oraz ich kopii ponosi Procesor.
6. Procesor przesyła pisemne potwierdzenie zniszczenia danych osobowych w sposób i w terminie uzgodnionym z Powierzającym, jednak nie później niż w terminie 5 Dni Roboczych od terminu zniszczenia lub zwrotu, wskazanego w dyspozycji opisanej w § 8 ust. 5 Umowy.
7. W przypadku ograniczenia zakresu powierzenia przetwarzania przez Powierzającego, w trybie określonym w Umowie, postanowienia o rozwiązaniu Umowy stosuje się odpowiednio do danych, które wskutek ograniczenia zakresu nie mogą już być przetwarzane przez Procesora.
8. W przypadku dalszego powierzenia przetwarzania danych osobowych Procesor zobowiązuje się do zawarcia w umowach z dalszymi podmiotami przetwarzającymi postanowień, zgodnie z którymi umowy dalszego przetwarzania danych będą ulegały automatycznemu rozwiązaniu w razie zakończenia obowiązywania niniejszej Umowy.
9. Procesor odpowiada za szkody, jakie powstaną u Powierzającego, osób, których dane dotyczą lub innych osób trzecich w wyniku niezgodnego z Umową lub przepisami prawa przetwarzania przez Procesora danych osobowych objętych powierzeniem na podstawie Umowy, a w szczególności w związku z udostępnianiem danych osobowych osobom nieupoważnionym.
10. W przypadku naruszenia obowiązujących przepisów prawa lub niniejszej Umowy z przyczyn leżących po stronie Procesora, w następstwie czego Powierzający zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany administracyjną karą finansową, Procesor zobowiązuje się pokryć Powierzającemu poniesione z tego tytułu koszty.
11. W przypadku niewykonania lub nienależytego wykonania przez Procesora niniejszej Umowy, Procesor zobowiązuje się do zapłaty kary umownej w wysokości 10.000,- zł (słownie: dziesięć tysięcy złotych) za każdy przypadek naruszenia, na podstawie noty obciążeniowej, płatnej w terminie 10 Dni Roboczych od dnia jej wystawienia przez Powierzającego. Przez nienależyte wykonanie Umowy należy w szczególności rozumieć sytuację, gdy organ nadzoru nad przestrzeganiem zasad przetwarzania danych osobowych stwierdzi, że przetwarzanie danych osobowych w zakresie realizowanym przez Procesora nie jest zgodne z tymi zasadami. Powierzający zastrzega sobie prawo do dochodzenia odszkodowania na zasadach ogólnych ponad taką karę umowną.

§ 9
ADRESY STRON I DANE OSÓB

1. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana na adresy Stron wskazane w Załączniku nr 1.
2. Procesora w kontaktach z Powierzającym oraz Powierzającego w kontaktach z Procesorem w zakresie ustaleń Umowy reprezentować będą osoby wskazane w Załączniku nr 1.
3. Zmiana adresów i danych tych osób nie stanowi zmiany Umowy. O każdej zmianie danych, o których mowa w § 9 ust. 1 – 2, Strony powiadomią się na piśmie, za potwierdzeniem odbioru lub drogą elektroniczną.

§ 10
POSTANOWIENIA KOŃCOWE

4. Niniejsza Umowa podlega prawu polskiemu. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej Strony.
5. W sprawach, które nie zostały uregulowane Umową, znajdują zastosowanie odpowiednie przepisy powszechnie obowiązującego prawa polskiego, a w szczególności Kodeksu cywilnego, RODO oraz innych obowiązujących przepisów z zakresu ochrony danych osobowych.
6. Zmiany Umowy są możliwe wyłącznie w formie pisemnej pod rygorem nieważności, z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian.
7. Procesor nie może przenieść praw lub obowiązków wynikających z niniejszej Umowy bez pisemnej zgody Powierzającego.
8. O ile Umowa główna nie stanowi inaczej, wszelkie spory w związku z niniejszą Umową zostaną poddane pod rozstrzygnięcie sądu powszechnego miejscowo właściwego ze względu na siedzibę Powierzającego.
9. Właściwym do rozstrzygania sporów wynikających z Umowy jest prawo polskie.

_____ _____

Powierzający Procesor

_____

Powierzający

ZAŁĄCZNIK NR 1

ZAKRES POWIERZENIA DANYCH OSOBOWYCH ORAZ DANE KONTAKTOWE STRON

1) Cele przetwarzania: realizacja postanowień Umowy głównej / usługi pośrednictwa ubezpieczeniowego
2) Kategorie osób, których dane dotyczą: ubezpieczający, ubezpieczony, poszukujący ochrony ubezpieczeniowej
3) Rodzaje danych osobowych: dane zawarte we wniosku ubezpieczeniowym wynikającym z rodzaju umowy ubezpieczenia, a określonymi przez system informatyczny służący do zawierania umów ubezpieczenia
4) Obszar, na którym przetwarzane będą dane osobowe: Polska
5) Dane kontaktowe Stron:
    a. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana do Powierzającego na następujące dane kontaktowe:
        i. Unilink Życie Sp. z o.o., ul. K.I. Gałczyńskiego 2A, 05-090 Raszyn
        ii. telefon: +48 22 483 19 19
        iii. email: biuro@unilink.pl

    Strony ustalają, że preferowaną formą kontaktu w sprawach bieżącej obsługi jest forma kontaktu przy użyciu email.
    b. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana do Procesora na następujące dane kontaktowe:
        i. adres …….
        ii. tel. …….
        iii. email …….
6) Dane do zgłaszania naruszeń:
    a. Adres email: rodo@unilink.pl
    b. Telefon: +48 22 483 19 19

ZAŁĄCZNIK NR 2
STANDARD ŚRODKÓW BEZPIECZEŃSTWA DLA PODMIOTÓW WSPÓŁPRACUJĄCYCH
(ROZWIĄZANIA ORGANIZACYJNE I TECHNICZNE)

Część I – rozwiązania organizacyjne.	Zastosowano (TAK / NIE)	Uzasadnienie dla braku wdrożenia (obligatoryjne w przypadku wskazanie NIE)
1. Do przetwarzania danych osobowych dopuszczano są wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych (zgodne ze wzorem stosowanym w Grupie Unilink).		
2. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych (odrębna dla każdego procesu przetwarzania).		
3. Powołano Inspektora Ochrony Danych Osobowych.		
4. Wdrożono Politykę Bezpieczeństwa dot. ochrony danych osobowych.		
5. Wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.		
6. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych (obowiązek udokumentowania).		
7. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy (obowiązek udokumentowania).		
8. Wprowadzono politykę haseł (konieczność cyklicznej aktualizacji, wymogi dot. formatu i złożoności hasła).		
9. Wprowadzono politykę tzw. „czystego biurka” (zakaz przechowywania dokumentów zawierających dane osobowe w miejscach powszechnie dostępnych, w szczególności na meblach takich jak biurka, czy szafki).		
10. Wprowadzono obowiązek dokonywania i dokumentowania regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.		

Część II – Rozwiązania techniczne.	Zastosowano (TAK / NIE)	Uzasadnienie dla braku wdrożenia (obligatoryjne w przypadku wskazanie NIE)
1. Monitory komputerów, na których przetwarzane są dane osobowe w pomieszczeniach, do których mają dostęp osoby trzecie, ustawione są w sposób uniemożliwiający wgląd osobom postronnym. Obowiązek blokowania klawiatury przy odejściu od komputera. Zakaz korzystania z niezabezpieczonych sieci publicznych (w szczególności wi-fi).		
2. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco. Dostęp do tego pomieszczenia ograniczony jest do listy upoważnionych osób.		
3. Dane osobowe zapisywane na dyskach fizycznych (komputery stacjonarne, przenośne, serwery) są szyfrowane.		

4. Przy połączeniach do aplikacji webowych stosowany jest protokół HTTP OVER SSL (HTTPS).		
5. Szyfrowanie wiadomości mail zawierających dane osobowe (zarówno wewnętrznych i zewnętrznych).		
6. Zabezpieczenie urządzeń mobilnych (telefony, tablety), na których są incydentalnie przetwarzane dane osobowe – przynajmniej hasłem.		
7. Zabezpieczenie urządzeń mobilnych, na których są przetwarzane dane osobowe w szerokim zakresie (np. odbieranie mail) co najmniej dodatkowym hasłem do aplikacji (w której dane są przetwarzane). W przypadku przetwarzania danych osobowych w urządzeniu mobilnym na szeroką skalę, gdzie dane zapisywane są na tym urządzeniu, należy urządzenie szyfrować.		
8. Wprowadzono obowiązek usuwania danych osobowych na urządzeniach, na których nie można wprowadzić zabezpieczeń przed dostępem przez osoby nieupoważnione (np. aparat fotograficzny).		
9. Zastosowano techniki pseudonimizacji danych osobowych (np. tokenizacja lub szyfrowanie AES).		
10. Ograniczono uprawnienia do instalacji oprogramowania na komputerach służbowych dla użytkowników nieposiadających uprawnień administratora.		
11. Zapewniono możliwość ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów służących do przetwarzania danych osobowych oraz usług przetwarzania, w szczególności poprzez brak przechowywania danych w sposób niezabezpieczony; wyłączenie możliwości dostępu do zbiorów danych przez osoby nieupoważnione – zarówno poprzez zabezpieczenia fizyczne – drzwi antywłamaniowe, odpowiednie zamki, zamykane szafy, wyodrębnione pomieszczenia archiwum dla większych zbiorów danych; jak i informatyczne – konta użytkowników zabezpieczone hasłem; program internet security (antywirus+firewall); odpowiednie zabezpieczenie serwerów i dysków, na których przechowywane są dane. Wprowadzono procedury regularnego aktualizowania oprogramowania serwerowego pod kątem poprawek dot. Bezpieczeństwa.		
12. Zapewniono możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (umowy z dostawcą zewnętrznym lub przyjęte wewnętrznie standardy kopii zapasowych i możliwości ich przywrócenia przez IT).		
13. Wprowadzono okresy retencji i usuwania danych, wynikające z realizacji celu przetwarzania, okresu przedawnienia roszczeń lub ze szczególnych przepisów prawa oraz zapewniono monitorowania tych okresów.		
14. Do pracy z wykorzystaniem danych osobowych mogą być wykorzystywane tylko komputery służbowe z dedykowanym kontem dla użytkownika upoważnionego do przetwarzania danych, posiadające odpowiedni standard zabezpieczenia, zgodny z w/w wymogami oraz podlegające weryfikacji zarówno ze strony Grupy Unilink, jak i w razie audytu/kontroli ze strony ubezpieczyciela współpracującego.		