**UMOWA**

**POWIERZENIA DALSZEGO PRZETWARZANIA DANYCH 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 Link4 Towarzystwem Ubezpieczeń 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 (dalej „Umowa 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**

Następujące pojęcia należy rozumieć tak, jak zostały one poniżej zdefiniowane, o ile nic innego nie wynika z treści Umowy:

1) **Dane Osobowe**: oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, których dotyczy powierzenie przetwarzania na mocy niniejszego Umowy; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Dane Osobowe określa załącznik nr 1 do Umowy przez wskazanie kategorii osób, których dane dotyczą, rodzaju danych oraz czynności przetwarzania dokonywanych na tych danych. Dane Osobowe obejmują:

a) zwykłe dane osobowe;

b) szczególne kategorie danych osobowych, o których mowa w art. 9 Rozporządzenia;

c) dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o których mowa w art. 10 Rozporządzenia;

2) **Rozporządzenie**: oznacza Rozporządzenie 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;

3) **Administrator**: oznacza osobę fizyczną lub prawną, samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania Danych Osobowych;

4) **Podmiot Przetwarzający**: osobę fizyczną lub prawną, która przetwarza Dane Osobowe w imieniu Administratora;

5) **Dalszy Podmiot Przetwarzający**: oznacza inny Podmiot Przetwarzający, z którego usług korzysta Subprocesor do wykonania w imieniu Administratora konkretnych czynności przetwarzania Danych Osobowych i który będzie miał dostęp do Danych Osobowych;

6) **Organ Nadzoru**: organ nadzorujący właściwy dla ochrony danych osobowych;

7) **Umowa**: niniejsza umowa;

8) **Umowa o współpracy:** umowa o współpracy w zakresie pośrednictwa ubezpieczeniowego zawarta pomiędzy Stronami.

**§ 2**

**OŚWIADCZENIA STRON**

Strony oświadczają, co następuje:

1) Procesor oświadcza, iż na podstawie zawartej z Towarzystwem Ubezpieczeń i Reasekuracji Warta S. A. z siedzibą w Warszawie (00-805) przy ul. Chmielnej 85/87, wpisanym do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XII Wydział Gospodarczy pod numerem KRS 0000016432, NIP 5210420047, o kapitale zakładowym 187.938.580,00 zł, który został opłacony w całości, umowy powierzenia przetwarzania danych osobowych, przetwarza dane osobowe, których Towarzystwo Ubezpieczeń i Reasekuracji Warta S.A. jest Administratorem.

2) Strony oświadczają, że niniejsza Umowa została zawarta w celu wykonania obowiązków, o których mowa w art. 28 Rozporządzenia w związku z zawarciem Umowy o współpracy.

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

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

**§ 3**

**POSTANOWIENIA OGÓLNE**

1) Procesor powierza Subprocesorowi przetwarzanie Danych Osobowych Administratora, Subprocesor zobowiązuje się do ich przetwarzania zgodnego z prawem i postanowieniami Umowy i Umowy o współpracy. Subprocesor zobowiązuje się, że nie będzie przetwarzał Danych Osobowych w jakikolwiek sposób i w zakresie wykraczającym poza zakres niezbędny dla realizacji Umowy o współpracy.

2) Subprocesor będzie przetwarzać Dane Osobowe w celu wykonania zobowiązań wynikających z Umowy o współpracy.

3) Subprocesor będzie przetwarzać Dane Osobowe wyłącznie przez okres obowiązywania Umowy o współpracy.

4) Subprocesor jest obowiązany przetwarzać Dane Osobowe wyłącznie na udokumentowane polecenie Administratora lub Administratora za pośrednictwem Procesora - co dotyczy również przekazywania Danych Osobowych do państwa trzeciego - chyba że obowiązek taki nakładają na niego przepisy prawa. Za udokumentowane polecenie przyjmuje się polecenie wynikające z Umowy o współpracy. Subprocesor obowiązany jest przed rozpoczęciem przetwarzania poinformować Administratora za pośrednictwem Procesora o ciążącym na nim obowiązku prawnym przetwarzania Danych Osobowych, wynikającym z przepisu prawa, chyba że przepis prawa zabrania udzielenia takiej informacji.

4) Jeżeli Subprocesor, będzie przetwarzał Dane Osobowe w zakresie wykraczającym poza polecenie Administratora robi to na własny rachunek i z innego powierzenia, co powoduje, że musi spełnić obowiązki Administratora.

5) Subprocesor może przetwarzać Dane Osobowe wyłącznie na terenie Rzeczypospolitej Polskiej (RP). Jeżeli Subprocesor będzie chciał przetwarzać Dane Osobowe poza terenem Rzeczypospolitej Polskiej to zobowiązany jest poinformować Administratora za pośrednictwem Procesora i uzyskać jego zgodę. Informacja przesłana do Administratora powinna zawierać wskazanie adresu, gdzie będą przetwarzane Dane Osobowe i powodu ich przetwarzania poza RP.

6) Subprocesor oświadcza, że dokonał oceny ryzyka możliwości wystąpienia naruszeń ochrony danych osobowych i na podstawie analizy tych czynników wdrożył odpowiednie do ustalonego ryzyka środki organizacyjne w związku z przetwarzaniem danych osobowych. Wykaz podstawowych środków ochrony fizycznej oraz środków organizacyjnych znajduje się w załączniku nr 3 do niniejszej Umowy. Wykaz ten nie stanowi pełnego katalogu środków ochrony fizycznej i ochrony organizacyjnej, które Subprocesor może wdrożyć.

**§ 4**

**TAJEMNICA UBEZPIECZENIOWA**

1) Subprocesor przyjmuje do wiadomości, że powierzone mu Dane Osobowe są objęte tajemnicą ubezpieczeniową, o której mowa w ustawie o działalności ubezpieczeniowej i reasekuracyjnej.

2) Subprocesor jest obowiązany do zachowania tajemnicy ubezpieczeniowej, w tym do zachowania w poufności przekazanych mu Danych Osobowych i innych informacji, przy czym obowiązek ten istnieje również po okresie obowiązywania Umowy o współpracy.

3) Subprocesor przyjmuje do wiadomości, że zasady współpracy określone w Umowie oraz informacje techniczne, technologiczne, organizacyjne jakie otrzymał od Administratora i Procesora stanowią tajemnicą przedsiębiorstwa i nie mogą być ujawniane do wiadomości publicznej w trakcie trwania Umowy o współpracy oraz po jej zakończeniu.

**§ 5**

**ŚRODKI TECHNICZNE I ORGANIZACYJNE**

1) Subprocesor oświadcza, że zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wszystkie wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.

2) Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, Subprocesor wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający wiążącemu się z przetwarzaniem ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w szczególności ryzyku naruszenia ochrony Danych Osobowych, o którym mowa w art. 4 pkt 12 oraz art. 32 Rozporządzenia.

3) Subprocesor oświadcza, że jest gotowy do stosowania środków technicznych i organizacyjnych, które uniemożliwiają: nieuprawnione ujawnienie lub nieuprawniony dostęp do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, przypadkowe lub niezgodne z prawem zniszczenie, utratę, modyfikację, zabranie ich przez osobę nieuprawnioną lub inne przetwarzanie z naruszeniem Rozporządzenia oraz że zobowiązuje się je stosować do Danych Osobowych od momentu ich otrzymania do zakończenia ich przetwarzania, chyba że w trakcie realizacji Umowy otrzyma inne wytyczne od Administratora lub Administratora za pośrednictwem Procesora.

4) Subprocesor oświadcza, że będzie przetwarzał Dane Osobowe w systemach informatycznych udostępnionych przez Administratora lub Procesora lub we własnych systemach informatycznych, do których posiada prawo własności, oraz że wszystkie systemy, w których przetwarzane są Dane Osobowe są zgodne z Rozporządzeniem, w szczególności w zakresie bezpieczeństwa przetwarzania. Jeżeli Subprocesor przetwarza Dane Osobowe w systemach innych niż określone w zdaniu pierwszym zobowiązany jest do poinformowania Administratora za pośrednictwem Procesora.

5) Subprocesor jest zobowiązany w szczególności do zastosowania takich środków technicznych, które chronią Dane Osobowe przed dostępem nieuprawnionych użytkowników do systemów informatycznych stosowanych przez Subprocesora lub odczytaniem przez osoby nieuprawnione Danych Osobowych w trakcie teletransmisji (m.in. konieczność aktualizowania używanego przez Subprocesora systemu operacyjnego, konieczność stosowania zaktualizowanych programów antywirusowych) oraz przed utratą Danych Osobowych wskutek zaburzeń w działaniu systemów informatycznych będących rezultatem przeniknięcia do nich wirusów lub niewłaściwej pracy systemu wskutek przerw w dostawie energii i pozostałych czynników elektromagnetycznych. Administrator lub Administrator za pośrednictwem Procesora jest upoważniony do wskazywania szczegółowych wymogów dotyczących obowiązkowych zabezpieczeń, a Subprocesor jest zobowiązany do każdorazowego zastosowania ich w swojej działalności.

6) Subprocesor jest zobowiązany do stosowania zasad bezpieczeństwa informatycznego - bezpieczeństwo komputera i miejsca przetwarzania danych, incydenty bezpieczeństwa, które zawarte są w załączniku nr 3 do niniejszej Umowy.

7) Strony zgodnie oświadczają, że w celu realizacji Umowy o współpracy Subprocesor będzie realizował dostęp zdalny do sieci

teleinformatycznej Procesora i Administratora. Subprocesor jest obowiązany korzystać z narzędzi do zdalnego dostępu do sieci teleinformatycznej Procesora i Administratora zapewniających bezpieczeństwo przetwarzania Danych Osobowych. Procesor i Administrator mają prawo nie udzielić zdalnego dostępu do sieci teleinformatycznej, jeżeli uzna proponowane przez Subprocesora narzędzie do zdalnego dostępu za niedające gwarancji bezpieczeństwa. Odmowa udzielenia zdalnego dostępu z ww. przyczyny nie stanowi niewykonania, nienależytego wykonania lub opóźnienia wykonania niniejszej Umowy.

8) Administrator lub Administrator za pośrednictwem Procesora jest uprawniony do wydawania wytycznych w zakresie środków bezpieczeństwa Danych Osobowych w każdym momencie, a Subprocesor jest obowiązany je uwzględnić.

9) Korespondencja wymieniana między stronami zawierająca Dane Osobowe będzie przesyłana w formie zaszyfrowanej, wyłącznie przy użyciu rozwiązań informatycznych uprzednio zatwierdzonych lub udostępnionych Subprocesorowi przez Administratora lub Administratora za pośrednictwem Procesora.

**§ 6**

**PERSONEL PODMIOTU PRZETWARZAJĄCEGO**

1) Subprocesor jest obowiązany dopuszczać do dostępu do Danych Osobowych jedynie osoby działające z jego upoważnienia oraz których dostęp do Danych Osobowych jest niezbędny do wykonywania czynności wynikających z Umowy o współpracy.

2) Subprocesor jest obowiązany zapewnić, by osoby działające z jego upoważnienia mające dostęp do Danych Osobowych miały odpowiednie kwalifikacje oraz by dawały rękojmię przetwarzania Danych Osobowych zgodnie z zasadą integralności i poufności, o której mowa w art. 5 ust. 1 lit. f Rozporządzenia.

3) Subprocesor jest obowiązany zapewnić, by osoby działające z jego upoważnienia mające dostęp do Danych Osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.

4) Subprocesor jest obowiązany prowadzić wykaz osób działających z upoważnienia Subprocesora mających dostęp do Danych Osobowych oraz przedstawić go Procesorowi i Administratorowi wraz z odpowiednim dokumentem stwierdzającym zobowiązanie do zachowania tajemnicy, na każde żądanie w wersji aktualnej lub pełnej zgodnie ze wskazaniem Procesora i Administratora.

**§ 7**

**DALSZY PODMIOT PRZETWARZAJĄCY**

1) Subprocesor może korzystać przy wykonaniu postanowień Umowy o współpracy z usług Dalszego Podmiotu Przetwarzającego wyłącznie po uzyskaniu uprzedniej pisemnej zgody Administratora za pośrednictwem Procesora na dalsze powierzenie przetwarzania Danych Osobowych wskazanemu Dalszemu Podmiotowi Przetwarzającemu. Zwracając się do Administratora o udzielenie zgody na korzystanie z usług Dalszego Podmiotu Przetwarzającego, Subprocesor uzupełnia szablon zgłoszenia INFORMACJA O DALSZYM PODMIOCIE PRZETWARZAJĄCYM stanowiący załącznik nr 2 do Umowy. Zgłoszenie powinno zostać przesłane na adres pocztowy lub adres e-mail Procesora.

2) Zwracając się o udzielenie zgody na korzystanie z usług Dalszego Podmiotu Przetwarzającego, Subprocesor informuje szczegółowo o:

a) tożsamości Dalszego Podmiotu Przetwarzającego,

b) okolicznościach świadczących o tym, że Dalszy Podmiot Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, zamierzonym zakresie powierzenia przetwarzania z oznaczeniem konkretnych czynności przetwarzania, rodzajów danych oraz kategorii osób, których dane dotyczą,

c) środkach technicznych i organizacyjnych stosowanych przez Dalszy Podmiot Przetwarzający, których celem jest zabezpieczenie Danych Osobowych przed nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, przypadkowe lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, zabraniem ich przez osobę nieuprawnioną lub innym przetwarzaniem z naruszeniem Rozporządzenia,

d) wyniku oceny skutków czynności przetwarzania Danych Osobowych planowanych do realizacji przez Dalszy Podmiot Przetwarzający,

e) systemach informatycznych, w których Dalszy Podmiot Przetwarzający będzie przetwarzał Dane Osobowe.

3) Pomiędzy Subprocesorem a Dalszym Podmiotem Przetwarzającym powinna zostać zawarta umowa, która nakłada na Dalszy Podmiot Przetwarzający, te same obowiązki ochrony Danych Osobowych jak te nałożone na Subprocesora. Ponadto umowa zawarta pomiędzy Subprocesorem a Dalszym Podmiotem Przetwarzającym powinna nakładać na Dalszy Podmiot Przetwarzający obowiązek:

a) niezwłocznego informowania Administratora za pośrednictwem Procesora o żądaniach na podstawie art. 15-22 Rozporządzenia, z którymi osoby, których Dane Osobowe dotyczą, zwróciły się bezpośrednio do Dalszego Podmiotu Przetwarzającego,

b) niezwłocznego, nie dłuższego niż 12 godzin od stwierdzenia naruszenia, zgłoszenia Administratorowi za pośrednictwem Procesora stwierdzonych naruszeń ochrony Danych Osobowych, o których mowa w art. 4 pkt 12 Rozporządzenia,

c) udostępnienia Procesorowi i Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków wynikających z umowy zawartej z Dalszym Podmiotem Przetwarzającym oraz umożliwienia Procesorowi i Administratorowi albo audytorowi upoważnionemu przez Procesora lub Administratora na przeprowadzenie audytów, w tym inspekcji.

4) Subprocesor zobowiązuje się przedłożyć Procesorowi i Administratorowi kopię umowy zawartej z Dalszym Podmiotem Przetwarzającym na każde żądanie Procesora lub Administratora w ciągu 3 dni roboczych od otrzymania żądania przez Subprocesora. Obowiązkowi temu czyni zadość przedłożenie kopii, z której usunięto postanowienia zawierające tajemnicę przedsiębiorstwa Subprocesora lub Dalszego Podmiotu Przetwarzającego, o ile postanowienia te nie odnoszą się do powierzenia przetwarzania Danych Osobowych.

5) Jeżeli Dalszy Podmiot Przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Procesora i Administratora za wypełnienie tych obowiązków spoczywa na Subprocesorze.

**§ 8**

**DALSZE OBOWIĄZKI SUBPROCESORA**

1) Subprocesor jest zobowiązany:

a) zbierać jedynie te Dane Osobowe, które wynikają z procedur i formularzy przekazywanych przez Administratora lub Administratora za pośrednictwem Procesora,

b) przekazywać do Administratora za pośrednictwem Procesora wszystkie Dane Osobowe, jakie w związku z realizacją Umowy o współpracy zebrał od klientów lub potencjalnych klientów. Przetwarzanie danych przez Subprocesora bez wiedzy i nadzoru Administratora lub Procesora tj. np. brak wprowadzania wszystkich danych osobowych do systemów informatycznych Administratora lub Procesora będzie traktowane jako niezgodne z wytycznymi Administratora i będzie stanowiło przesłankę do rozwiązania Umowy o współpracy w trybie natychmiastowym,

c) wpisywać w Dokumentację Ubezpieczeniową przekazywaną do Administratora oraz w jej systemy informatyczne prawidłowe i rzeczywiste Dane Osobowe klientów i potencjalnych klientów. Subprocesorowi nie wolno podawać w Dokumentacji Ubezpieczeniowej oraz wpisywać do systemów informatycznych Administratora i Procesora swoich Danych Osobowych lub Danych Osobowych osób trzecich, w tym danych kontaktowych, niezgodnych z informacjami otrzymanymi od osób, których dane dotyczą,

d) należycie, zgodnie z zaleceniami Administratora i Procesora weryfikować tożsamość osoby, od której Dane Osobowe zbiera oraz inne informacje podawane przez tę osobę,

e) zgodnie z otrzymanymi od Administratora lub Administratorem za pośrednictwem Procesora wytycznymi przekazywać klientom klauzule i zbierać od klientów zgody wymagane przez Administratora przy zawarciu umowy ubezpieczenia jak i w procesie obsługi umów ubezpieczenia.

2) Postępowanie Subprocesora wbrew postanowieniom niniejszej Umowy powoduje przejście odpowiedzialności na tego Subprocesora za przetwarzanie danych osobowych jak na administratora tych danych.

3) Subprocesor obowiązany jest, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomagać Procesorowi i Administratorowi wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia. W szczególności Subprocesor obowiązany jest w odniesieniu do przetwarzanych Danych Osobowych:

a) współpracować z Administratorem i Procesorem w prowadzeniu oceny skutków operacji przetwarzania dla ochrony danych, o której mowa w art. 35 ust. 7 Rozporządzenia i udzielać im niezbędnych informacji w tym zakresie;

b) odpowiedzieć, w sposób uprzednio uzgodniony z Procesorem lub Administratorem, na żądanie osoby, która zwróciła się z żądaniem na podstawie art. 15-22 Rozporządzenia bezpośrednio do Subprocesora, oraz podjąć działania w celu zadośćuczynienia żądaniu poprzez niezwłoczne:

· poinformowania Administratora za pośrednictwem Procesora o fakcie zgłoszenia przez osobę, której dane dotyczą, żądania prawa dostępu, o którym mowa w art. 15 Rozporządzenia, oraz do przygotowania raportu dla Administratora i Procesora umożliwiającego przedstawienia osobie, której dane dotyczą, informacji, o których mowa w tym przepisie,

· odnotowania żądania osoby i aktualizacji jej danych w razie zgłoszenia, żądania sprostowania danych, o którym mowa w art. 16 Rozporządzenia,

· przekazanie do Administratora za pośrednictwem Procesora żądania osoby usunięcia tych danych (bycia zapomnianym), o którym mowa w art. 17 Rozporządzenia,

· przekazania do Administratora za pośrednictwem Procesora żądania osoby ograniczenia przetwarzania danych, o którym mowa w art. 18 Rozporządzenia,

· przekazania do Administratora za pośrednictwem Procesora żądania osoby przenoszenia danych, o którym mowa w art. 20 Rozporządzenia,

· przekazania do Administratora za pośrednictwem Procesora sprzeciwu osoby, której dane dotyczą, o którym mowa w art. 21 Rozporządzenia,

· przekazania do Administratora za pośrednictwem Procesora zgłoszenia przez osobę, której dane dotyczą, żądania uzyskania interwencji ludzkiej ze strony Administratora lub wyrażenia własnego stanowiska i zakwestionowania decyzji Administratora, o których mowa w art. 22 Rozporządzenia,

c) podać osobie, której dane dotyczą, podczas pozyskiwania jej Danych Osobowych wszystkie informacje, o których mowa art. 13 Rozporządzenia. Treść i forma klauzuli informacyjnej przedstawianej przez Subprocesora w imieniu Administratora zostanie przekazana Subprocesorowi;

4) Subprocesor jest obowiązany, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomagać Procesorowi i Administratorowi stosując odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której Dane Osobowe dotyczą, inne niż te, o których mowa w ustępie poprzedzającym, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia.

5) Subprocesor zobowiązuje się do niezwłocznego poinformowania Administratora za pośrednictwem Procesora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych Danych Osobowych przez Subprocesora, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym Przetwarzania powierzonych Danych Osobowych, skierowanych do Subprocesora, a także o wszelkich kontrolach i inspekcjach dotyczących Przetwarzania powierzonych Danych Osobowych przez Subprocesora, w szczególności prowadzonych przez Organ Nadzoru.

**§ 9**

**NARUSZENIE OCHRONY DANYCH OSOBOWYCH**

1) Subprocesor jest obowiązany pomagać Administratorowi wywiązać się z obowiązku zgłoszenia organowi nadzorczemu naruszenia ochrony Danych Osobowych oraz z obowiązku zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony Danych Osobowych, zgodnie z art. 33 i 34 Rozporządzenia.

2) W przypadku stwierdzenia naruszenia ochrony Danych Osobowych lub naruszenia postanowień niniejszego paragrafu, Subprocesor obowiązany jest niezwłocznie, lecz nie później niż w ciągu 12 godzin od stwierdzenia naruszenia zgłosić stwierdzone naruszenia. Zgłoszenie powinno zostać dokonane mailowo, na adres: iodo@asist.pl

3) Zgłoszenie, o którym mowa w ust. 2 powinno:

a) opisywać znane Subprocesorowi okoliczności zdarzenia stanowiącego naruszenie oraz jego ustalone lub podejrzewane przyczyny,

b) opisywać charakter naruszenia ochrony Danych Osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów Danych Osobowych, których dotyczy naruszenie,

c) opisywać możliwe konsekwencje naruszenia ochrony Danych Osobowych,

d) zawierać wstępną analizę ryzyka naruszenia praw i wolności osób, których dane dotyczą i informacje niezbędne do zawiadomienia tych osób, o których mowa w art. 34 ust. 3 Rozporządzenia,

e) opisywać środki proponowane przez Subprocesora w celu zaradzenia naruszeniu ochrony Danych Osobowych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.

4) W przypadku stwierdzenia naruszenia ochrony Danych Osobowych, o których mowa w art. 4 pkt 12 Rozporządzenia Subprocesor:

a) zobowiązany jest zastosować się do wszystkich instrukcji przekazanych mu przez Administratora lub Administratora za pośrednictwem Procesora, w tym, na żądanie Procesora i Administratora, zastosować środki techniczne i organizacyjne w celu zaradzenia naruszeniu ochrony Danych Osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków,

b) w przypadku, gdyby zastosowanie określonych środków miało lub mogło wpłynąć na integralność lub dostępność Danych Osobowych, niezwłocznie zwraca się do Administratora za pośrednictwem Procesora o zgodę na zastosowanie tych środków.

5) Subprocesor obowiązany jest ponadto współpracować z Procesorem i Administratorem w celu wykrycia naruszenia, wyjaśnienia jego charakteru oraz zaradzenia naruszeniu, w tym zminimalizowania jego negatywnych konsekwencji.

6) Subprocesor obowiązany jest zachować wszelkie informacje o naruszeniach ochrony Danych Osobowych w tajemnicy i ujawniać je wyłącznie Procesorowi i Administratorowi lub podmiotom uprawnionym do otrzymania tych informacji na podstawie przepisów prawa.

**§ 10**

**INFORMOWANIE ADMINISTRATORA**

1) Subprocesor obowiązany jest niezwłocznie poinformować Administratora za pośrednictwem Procesora, jeżeli zdaniem Subprocesora wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów Unii Europejskiej lub państwa członkowskiego o ochronie danych.

2) Subprocesor odpowiada wobec Procesora i Administratora jak za działania i zaniechania własne, za działania i zaniechania osób wykonujących w imieniu Subprocesora przetwarzania Danych Osobowych, z pomocą których wykonuje niniejszą Umowę.

**§11**

**WYKAZANIE SPEŁNIENIA OBOWIĄZKÓW**

1) Subprocesor obowiązany jest udostępnić Procesorowi i Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków nałożonych na niego na mocy Rozporządzenia lub niniejszego postanowienia oraz umożliwić Procesorowi i Administratorowi lub audytorowi upoważnionemu przez Procesora lub Administratora przeprowadzenie audytów, w tym inspekcji. W szczególności Subprocesor obowiązany jest zapewnić Procesorowi i Administratorowi lub audytorowi/podmiotowi trzeciemu upoważnionemu przez Procesora lub Administratora:

a) wstęp na grunt oraz do budynków, lokali lub innych pomieszczeń,

b) wgląd do dokumentów i informacji mających związek z przetwarzaniem Danych Osobowych,

c) oględziny urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania Danych Osobowych,

d) uzyskanie ustnych lub pisemnych wyjaśnień.

2) Procesor i Administrator obowiązany jest zawiadomić Subprocesora o zamiarze przeprowadzenia audytu co najmniej na 3 dni robocze przed rozpoczęciem audytu ze wskazaniem zakresu i terminu audytu oraz osób upoważnionych do jego przeprowadzenia.

3) Prowadzenie audytu nie może powodować nadmiernych obciążeń dla Subprocesora. W szczególności audyt nie może być prowadzony poza zwykłymi godzinami pracy Subprocesora w danym budynku, lokalu lub innym pomieszczeniu, chyba że przeprowadzenie audytu jest uzasadnione nagłą potrzebą.

2

**§12**

**ZAKOŃCZENIE PRZETWARZANIA DANYCH**

1) Subprocesor jest obowiązany w ostatnim dniu obowiązywania Umowy o współpracy i niniejszej Umowy usunąć zgodnie z decyzją Administratora, zniszczyć lub zwrócić Administratorowi za pośrednictwem Procesora Dane Osobowe oraz usunąć lub zniszczyć wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie Danych Osobowych.

2) Jeżeli, zgodnie z decyzją Administratora, Subprocesor jest obowiązany usunąć, zniszczyć Dane Osobowe, po dokonaniu tej czynności, przesyła Administratorowi za pośrednictwem Procesora oświadczenie o usunięciu, zniszczeniu Danych Osobowych pozyskanych w trakcie realizacji Umowy o współpracy. Oświadczenie powinno zawierać co najmniej nazwę i adres Subprocesora dokumenty, dokumenty jakie zostały usunięte lub zniszczone, daty i miejsca usunięcia, zniszczenia dokumentów, metodę usunięcia, zniszczenia oraz zakres dokumentacji objętej usunięciem, zniszczeniem.

3) Jeżeli Subprocesor zwraca Administratorowi za pośrednictwem Procesora Dane Osobowe, zwrot powinien nastąpić przez bezpieczny transfer plików w formacie żądanym przez Administratora lub na nośniku fizycznym dostarczonym przez Administratora.

**§ 13**

**POSTANOWIENIA KOŃCOWE**

1) 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**

**DANE OSOBOWE**

| **Kategorie osób, których dane dotyczą** | **Rodzaj danych osobowych** | **Czynności przetwarzania** | **Forma przetwarzania** |
|---|---|---|---|
| potencjalni klienci | · zwykłe dane osobowe – dane osobowe znajdujące się w dokumentacji ubezpieczeniowej oraz innych dokumentach, których wzory są zatwierdzone przez TUiR "WARTA" S.A. do celów zawarcia umowy ubezpieczenia, umożliwiającym nawiązanie kontaktu, ocenę wymagań i potrzeb ubezpieczeniowych klienta i przedstawienie oferty ubezpieczeniowej,<br>· szczególne kategorie danych -dane dotyczące zdrowia (tj. dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia),<br>· dane osobowe ujawnione w orzeczeniach dotyczących naruszeń prawa, w szczególności w wyrokach skazujących. | zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie ujawnianie poprzez przesłanie, usuwanie lub niszczenie | Subprocesor zobowiązuje się przetwarzać dane osobowe: zarówno w formie papierowej, jak i elektronicznej |
| klienci – ubezpieczający, osoby ubezpieczone, poszkodowane oraz osoby uprawnione wskazane w dokumentacji ubezpieczeniowej i w aktach szkody | · zwykłe dane osobowe - dane osobowe znajdujące się w dokumentacji ubezpieczeniowej oraz innych dokumentach, których wzory są zatwierdzone przez TUiR "WARTA" S.A. do celów zawarcia umowy ubezpieczenia a także dane osobowe znajdujące się w aktach szkody.<br>· szczególne kategorie danych - dane dotyczące zdrowia (tj. dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia).<br>· dane osobowe ujawnione w orzeczeniach dotyczących naruszeń prawa, w szczególności w wyrokach skazujących. | zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, usuwanie lub niszczenie | Subprocesor zobowiązuje się przetwarzać dane osobowe: zarówno w formie papierowej, jak i elektronicznej |

**ZAŁĄCZNIK NR 2**

**SZABLON - WZÓR**

**DOKUMENTU: INFORMACJA O DALSZYM PODMIOCIE PRZETWARZAJĄCYM**

**ZGŁOSZENIE**

Wnioskuję o wyrażenie przez TUIR "WARTA" S.A. zgody na korzystanie przez

.....(nazwa i numer NIP)

z usług Dalszego Podmiotu Przetwarzającego:

| | | |
|---|---|---|
| Nazwa i adres Dalszego Podmiotu Przetwarzającego | | |
| Jakie czynności na powierzonych danych wykonywał będzie Dalszy Podmiot Przetwarzający (cel przekazania) | | |
| Czy została zawarta pomiędzy Subprocesorem a Dalszym Podmiotem Przetwarzającym pisemna umowa, która nakłada na Dalszy Podmiot Przetwarzający, te same obowiązki ochrony danych osobowych jak te nałożone przez Procesora? | TAK | NIE |
| Czy umowa, o której mowa powyżej, nakłada na Dalszy Podmiot Przetwarzający obowiązek niezwłocznego informowania TUiR „WARTA" S.A. za pośrednictwem Procesora o żądaniach na podstawie art. 15-22 Rozporządzenia, z którymi osoby, których Dane Osobowe dotyczą, zwróciły się bezpośrednio do Dalszego Podmiotu Przetwarzającego? | TAK | NIE |
| Czy umowa, o której mowa powyżej**,** nakłada na Dalszy Podmiot Przetwarzający obowiązek niezwłocznego, nie dłuższego niż 12 godziny od stwierdzenia naruszenia, zgłoszenia TUiR „WARTA" S.A. za pośrednictwem Procesora stwierdzonych naruszeń ochrony Danych Osobowych, o których mowa w art. 4 pkt 12 Rozporządzenia? | TAK | NIE |
| Czy umowa, o której mowa powyżej**,** nakłada na Dalszy Podmiot Przetwarzający obowiązek udostępnienia TUiR „WARTA" S.A. i Procesorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków wynikających z umowy zawartej z Subprocesorem oraz umożliwienia TUiR „WARTA" S.A. i Procesorowi albo audytorowi upoważnionemu przez TUiR „WARTA" S.A. lub Procesora przeprowadzenie audytów, w tym inspekcji? | TAK | NIE |
| Czy Dalszy Podmiot Przetwarzający zapewnia gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, których celem jest zabezpieczenie Danych Osobowych przed nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do Danych Osobowych? | TAK | NIE |
| Czy Dalszy Podmiot Przetwarzający stosuje zatwierdzony przez Organ Nadzoru kodeks postępowania, zgodnie z art. 40 Rozporządzenia? | TAK | NIE |
| Czy Dalszy Podmiot Przetwarzający stosuje zatwierdzony mechanizm certyfikacji w rozumieniu art. 42 Rozporządzenia w zamierzonym zakresie powierzenia przetwarzania z oznaczeniem konkretnych czynności przetwarzania, rodzajów danych oraz kategorii osób, których dane dotyczą? | TAK | NIE |
| Adres, pod którym Dalszy Podmiot Przetwarzający będzie przetwarzał Dane Osobowe. | | |

.....

Miejscowość i data

.....

Podpis Subprocesora/osoby uprawnionej do składania oświadczeń woli w imieniu Subprocesora

*Dokument podpisany elektronicznie przez użytkownika ID [9477], Anna Słowińska, ip 95.160.84.73, dnia 2020-08-04 08:30:01*

**ZAŁĄCZNIK NR 3**

**„ŚRODKI OCHRONY FIZYCZNEJ ORAZ ŚRODKI ORGANIZACYJNE”**

I. OBOWIĄZKOWE ŚRODKI OCHRONY FIZYCZNEJ ORAZ ŚRODKI ORGANIZACYJNE

Zgłoszenie danych na policję w przypadku incydentu naruszenia Danych Osobowych

W przypadku, gdy dojdzie do naruszenia ochrony Danych Osobowych w postaci zagubienia bądź kradzieży dokumentacji bądź nośnika, na którym znajdują się Dane Osobowe, Subprocesor powinien podjąć następujące działania:

1) incydent należy niezwłocznie zgłosić na policję wraz z informacją, jakie dokumenty zostały zgubione/skradzione;

2) do protokołu policyjnego należy dołączyć listę osób, których dane osobowe zostały utracone (ujawnione) oraz podać listę dokumentów, których dotyczy naruszenie. Np. gdy jest to dokumentacja ubezpieczeniowa (polisy, wnioski ubezpieczeniowe), informacja do protokołu powinna zawierać: numer umowy ubezpieczenia (numer wniosku ubezpieczeniowego) oraz dane osobowe, które widniały na polisach, tj. imię, nazwisko, adres, numer pesel. Informacja ta może być załącznikiem do protokołu lub stanowić jego treść;

3) należy natychmiast formalnie zgłosić incydent do Administratora za pośrednictwem Procesora dołączając skan zawiadomienia złożonego na policji wraz z dodatkową informacją, o której mowa w pkt. 2;

Zgodnie z art. 33 Rozporządzenia w przypadku stwierdzenia naruszenia ochrony Danych Osobowych, Administrator ma 72 godziny na zgłoszenie sprawy do Organu Nadzoru. W związku z tym należy podjąć przedmiotowe czynności w trybie natychmiastowym.

**Zasad bezpieczeństwa informatycznego – bezpieczeństwo komputera i miejsca przetwarzania danych, incydenty bezpieczeństwa**

1. Bezpieczne zachowania podczas obsługi klienta TUiR „WARTA” S.A.:

1) zaleca się usuwanie z widocznych miejsc wszystkich niewykorzystanych nośników zawierających informacje chronione;

2) dostęp wzrokowy osób nieupoważnionych do informacji chronionej wykorzystywanej przy obsłudze klienta powinien zostać ograniczony;

3) na stanowisku pracy należy przechowywać wyłącznie dokumenty niezbędne, związane z obsługą danego klienta;

4) należy zwracać uwagę na osoby podejrzane (charakteryzujące się dziwnym zachowywaniem) przebywające w pomieszczeniu, gdzie występuje przetwarzanie danych chronionych.

2. Rozmowy z klientami TUiR „WARTA” S.A.:

1) nie należy przeprowadzać rozmów w miejscach publicznych;

2) zaleca się zwracanie uwagi na otaczających ludzi w trakcie rozmowy.

3. Bezpieczna praca w systemie informatycznym:

1) logowanie do systemu musi się odbywać przy użyciu unikalnego dla danego użytkownika loginu i hasła (wymagania dotyczące hasła – poniżej);

2) należy blokować komputer przy każdym odejściu od komputera (klawisze Win + L);

3) na zakończenie pracy należy zamknąć używane aplikacje i wylogować się z komputera;

4) zaleca się używanie ekranów polaryzacyjnych.

4. Hasła do komputera:

1) hasło musi być znane tylko jego użytkownikowi – nie wolno go udostępniać innym;

2) hasła należy chronić przed nieautoryzowanym dostępem;

3) hasła do systemów służących obsłudze klientów muszą być inne niż te stosowane do prywatnych kont np. do systemu bankowego, portalów społecznościowych, poczty prywatnej;

4) hasła powinny być przechowywane w bezpiecznym miejscu;

5) nie można przechowywać haseł pod klawiaturą lub przyklejać na monitorze;

6) hasło powinno być trudne do odgadnięcia;

7) hasło powinno składać się z 8 znaków, być kombinacją małych i wielkich liter, cyfr lub znaków specjalnych;

8) hasło powinno być zmieniane co 30 dni i się nie powtarzać.

5. Zabezpieczenie komputera:

1) zaleca się pracę na komputerze na uprawnieniach zwykłego użytkownika, uprawnienia administracyjne powinny być używane celowo przez uprawnionych, zaawansowanych w kwestiach IT użytkowników;

2) należy aktualizować system operacyjny (pobierać wszystkie zalecane poprawki bezpieczeństwa producenta);

3) należy pracować wyłącznie na legalnych wersjach systemów, oprogramowania;

4) na komputerze powinien być zainstalowany system antywirusowy, posiadający zaktualizowane definicje wirusów;

5) należy włączyć zapory sieciowe systemu operacyjnego lub innej aplikacji spełniającej tę samą funkcję.

6. Zabezpieczenie telefonu/tabletu:

1) w przypadku przetwarzania danych chronionych (w szczególności osobowych) na telefonach/tabletach, dostęp do urządzenia powinien być zabezpieczony hasłem;

2) na urządzeniu powinno być zainstalowane oprogramowanie antywirusowe.

7. Dokumenty papierowe i elektroniczne zawierające dane chronione (w szczególności dane osobowe):

1) należy bezwzględnie ograniczyć do minimum tworzenie kopii danych chronionych udostępnionych przez TUiR „WARTA” S.A.;

2) zakazane jest gromadzenie dokumentów zawierających nadmiarowe dane w szczególności takie, dla których nie ma już podstawy ich przetwarzania;

3) dokumenty należy trwale usuwać zgodnie z postanowieniami Umowy o współpracy i instrukcji TUiR „WARTA” S.A. dotyczących okresu retencji;

4) zakazane jest przechowywania dokumentów w prywatnej poczcie email i w „chmurze danych”;

5) dane należy przechowywać bezpiecznie tj.:

a) w formie papierowej w biurkach/szafach zamykanych na klucz;

b) w formie elektronicznej w bezpiecznych aplikacjach (rekomendowanych/udostępnionych przez TUiR „WARTA” S.A.), w przypadku, gdy przechowywanie danych poza aplikacją jest niezbędne z uwagi na realizację procesu biznesowego – dane muszą być zabezpieczone przed nieuprawnionym dostępem np. hasłem lub zaszyfrowane;

6) przenoszenie danych w formie elektronicznej np. na pendrive musi odbywać się na nośnikach lub w formie zaszyfrowanej;

7) kopie danych należy zabezpieczać tak jak oryginalne dane.

8. Drukowanie dokumentów:

1) drukowanie i kopiowanie dokumentów należy ograniczyć do niezbędnego minimum;

2) zakazane jest pozostawianie wydruków na drukarce, należy jak najszybciej odbierać dokumenty z urządzenia.

9. Niszczenie dokumentów:

1) dokumenty zawierające informacje chronione muszą być niszczone zgodnie z postanowieniami Umowy agencyjnej i instrukcji TUiR „WARTA” S.A. dotyczących okresu retencji;

2) zakazane jest wyrzucanie poufnych dokumentów do kosza na śmieci bez uprzedniego ich zniszczenia zgodnie z pkt 3;

3) niszczenie dokumentów zawierających informacje chronione musi odbywać się w sposób trwale uniemożliwiający ich odczytanie (np. poprzez stosowanie niszczarki do dokumentów).

10. Usuwanie danych z elektronicznych nośników danych:

1) w przypadku ustania zasadności dalszego przetwarzania, dane należy usuwać lub nadpisywać informacjami nieistotnymi, w sposób uniemożliwiający ich ponowne odczytanie bez zastosowania specjalistycznego oprogramowania;

2) należy zwrócić szczególną uwagę na cykliczne opróżnianie Kosza na swoim komputerze, samo wybranie opcji „Usuń” na pliku nie usuwa go trwale z pamięci urządzenia;

3) usuwanie danych może odbywać się za pomocą dedykowanego oprogramowania, urządzenia, metody lub usługi zewnętrznej.

11. Niszczenie elektronicznych nośników danych:

1) w przypadku konieczności likwidacji elektronicznego nośnika danych, zaleca się korzystanie z usług podmiotów zewnętrznych, które zapewniają techniczne możliwości prawidłowego i bezpiecznego niszczenia nośników informacji.

12. Wysyłanie maili:

1) wysyłanie danych osobowych mailowo musi być ograniczone do niezbędnego minimum i mieć swoje uzasadnienie w procesie biznesowym;

2) pliki zawierające dane osobowe muszą być wcześniej zaszyfrowane np. poprzez archiwum 7-ZIP zabezpieczone hasłem:

a) hasło należy przekazać odbiorcy innym kanałem komunikacji np. smsem;

b) hasło powinno być odpowiedniej złożoności, zawierać co najmniej 8 znaków, składających się z wielkich i małych liter, cyfr lub znaków specjalnych;

c) zaleca się, aby hasło było okresowo zmieniane.

13. Ochrona przez złośliwym oprogramowaniem:

1) należy zachować szczególną ostrożność podczas korzystania z poczty elektronicznej, a w szczególności:

a) należy uważnie weryfikować treść każdego otrzymanego maila, gdyż potencjalnie może zawierać złośliwe oprogramowanie lub być próbą wyłudzenia danych. Podejrzenia powinny wzbudzić m.in.: - brak polskich znaków w mailu, - błędy logiczne i stylistyczne w treści, - załączniki z rozszerzeniami .exe, .scr, .pif, .vbs. lub archiwa zaszyfrowane hasłem (jeśli nie oczekiwano takiego załącznika);

b) nie należy otwierać załączników w wiadomościach zakwalifikowanych jako spam;

c) nie należy otwierać załączników/linków z maili pochodzących z nieznanego źródła; d) należy czytać uważnie komunikaty przy uruchamianiu plików w formacie word czy excel (.doc, .docx, .xls, .xlsx) i nie zezwalać na uruchamianie makr w przypadku maili z niezaufanych źródeł; e) nie należy odpowiadać na wiadomości, które wzbudziły jakiekolwiek podejrzenia;

2) do komputera, na którym są przetwarzane dane nie można podłączać nośników zewnętrznych pochodzących z nieznanego źródła;

3) nie należy podłączać się z komputerem/tabletem, na którym są przetwarzane dane chronione do sieci WIFI publicznych oraz niechronionych hasłem dostępowym;

4) należy dbać o bezpieczeństwo sieci informatycznej, w której są przetwarzane dane chronione poprzez zabezpieczenie routera (urządzenia stojącego na brzegu sieci i Internetu), w szczególności poprzez:

a) zmianę hasła domyślnego na takim urządzeniu;

b) stosowanie filtracji ruchu sieciowego pochodzącego z sieci Internet;

c) aktualizację systemu operacyjnego takiego urządzania.

14. Przenoszenie sprzętu:

1) nie należy pozostawiać sprzętu przenośnego bez opieki w środkach lokomocji, np. w samochodzie, nawet przy chwilowym opuszczaniu pojazdu;

2) zaleca się zakupienie i użytkowanie specjalnej linki do komputera (zabezpieczającej laptop przed kradzieżą).

15. Przekazywanie sprzętu do naprawy/serwisowania:

1) w przypadku konieczności przekazania sprzętu komputerowego zaleca się, aby zabezpieczyć dostępne na nim dane (zwłaszcza dane osobowe):

a) poprzez zaszyfrowanie przy pomocy dostępnych narzędzi np. spakowanie aplikacją 7-Zip z ustawioną opcją ochrony hasłem;

b) najbezpieczniejszą, rekomendowaną metodą jest wymontowanie dysku, na którym są przechowywane dane (samodzielnie lub przy pomocy serwisu);

2) wymaga się korzystania z usług podmiotów, z którymi użytkownik sprzętu komputerowego ma podpisaną umowę zgodnie z postanowieniami o dalszym podmiocie przetwarzającym.

16. Zgłaszanie nieprawidłowości, incydentów:

1) wszelkie incydenty bezpieczeństwa należy zgłaszać do Administratora za pośrednictwem Procesora, dotyczy to w szczególności:

a) odnotowania podejrzanej sytuacji;

b) zagubienia nośnika zawierającego dane;

c) kradzieży komputera – w przypadku kradzieży komputera istnieje obowiązek zgłoszenia tego faktu na Policję;

2) w przypadku naruszenia ochrony danych osobowych należy postępować zgodnie z postanowieniami Umowy agencyjnej i instrukcją dotyczącymi naruszenia ochrony danych.

17. Szkolenia i podnoszenie wiedzy z zakresu bezpieczeństwa informatycznego:

1) należy postępować zgodnie z postanowieniami Umowy agencyjnej dotyczącymi środków organizacyjnych oraz kwalifikacji i rękojmi osób, którym udostępniono dane osobowe.

## II. ZALECANE ŚRODKI OCHRONY FIZYCZNEJ ORAZ ŚRODKI ORGANIZACYJNE

### Środki ochrony fizycznej

Środki ochrony fizycznej dotyczą przede wszystkim wszelkiego zabezpieczenia danych osobowych przed dostępem do nich osób nieupoważnionych. Najpierw należy ocenić, czy w agencji istnieje dane ryzyko, a następnie zastosować adekwatne środki bezpieczeństwa:

1) dane osobowe należy przechowywać w pomieszczeniu zabezpieczonym drzwiami zamykanymi na klucz; wejście do pomieszczenia powinno być zabezpieczone mechanizmem antywłamaniowym lub być kontrolowane przez system monitoringu z zastosowaniem kamer, bądź nadzorowane przez służbę ochrony;

2) jeśli dane osobowe przechowywane są na parterze budynku, należy zabezpieczyć okna mechanizmem antywłamaniowym lub pomieszczenie powinno być kontrolowane przez system monitoringu z zastosowaniem kamer lub nadzorowane przez system kamer;

3) dokumenty w formie papierowej, które zawierają dane osobowe, wewnątrz pomieszczenia powinny być przechowywane w szafie zamykanej na klucz;

4) dokumenty w formie papierowej zawierające dane osobowe, po ustaniu swojej przydatności powinny być niszczone w sposób mechaniczny i nieodwracalny, np. za pomocą niszczarek do dokumentów;

5) drukarki i inne urządzenia z dostępem do danych powinny znajdować się wewnątrz pomieszczenia, w którym przebywa korzystający z przedmiotowego urządzenia pracownik;

6) jeśli drukarki i inne urządzenia z dostępem do danych osobowych znajdują się poza pomieszczeniem, w którym pracownik/współpracownik przebywa, wówczas pracownik/współpracownik zobowiązany jest do korzystania z zasad bezpiecznego wydruku (jeżeli drukarka stoi w miejscu publicznym, wydruk powinien być zawieszony do czasu podejścia do niej osoby upoważnionej i zalogowania się w celu wydruku).

### Środki organizacyjne

Poza środkami ochrony fizycznej, należy również wdrożyć u Subprocesora środki organizacyjne, które dotyczą organizacji pracy pracowników/współpracowników obsługujących dane osobowe:

1) pracownicy/współpracownicy, którzy wykonując swoje zadania przetwarzają dane osobowe, muszą być uprzednio zaznajomieni z przepisami dotyczącymi ochrony danych osobowych. Subprocesor jest zobowiązany przeszkolić pracowników/współpracowników i posiadać stosowne dokumenty potwierdzające ten fakt;

2) pracownicy/współpracownicy, którzy zostali zatrudnione przez Subprocesora przy przetwarzaniu danych osobowych, muszą zostać przeszkolone w zakresie zabezpieczeń systemu informatycznego. Subprocesor musi posiadać stosowne dokumenty potwierdzające ten fakt;

3) pracownicy/współpracownicy, którzy zostali zatrudnieni przez Subprocesora przy przetwarzaniu danych osobowych są zobowiązane do zachowania poufności. Pracownicy/współpracownicy zobowiązani są do zachowania danych i sposobu ich przetwarzania w tajemnicy. Subprocesor musi posiadać stosowne dokumenty potwierdzające powyższe;

4) pracownicy/współpracownicy, którzy zostali zatrudnieni przez Subprocesora przy przetwarzaniu danych osobowych powinny posiadać imienne upoważnienie do przetwarzania danych. Subprocesor jest zobowiązany posiadać stosowne dokumenty potwierdzające powyższe;

5) monitory komputerów, na których przetwarzane są dane osobowe powinny zostać ustawione w taki sposób, żeby uniemożliwiały wgląd w wyświetlane dane osobom nieupoważnionym;

6) dokumentacja papierowa, w której zawarte są dane osobowe, powinna być umiejscowiona w sposób uniemożliwiający wgląd w

znajdujące się tam dane osobom nieupoważnionym;

7) w pomieszczeniu, w którym przetwarzane są dane osobowe obowiązuje zasada „czystego biurka”. Oznacza to, że w przypadku dłuższej nieobecności przy stanowisku pracy lub po jej zakończeniu Subprocesor i jego pracownicy/współpracownicy zobowiązani są do umieszczenia wszelkich dokumentów i nośników zawierających dane osobowe w bezpiecznym miejscu, np. w zamykanej na klucz szafie;

8) przebywanie osób trzecich w pomieszczeniu, gdzie przetwarzane są dane osobowe jest dozwolone jedynie w obecności upoważnionego pracownika/współpracownika.