Plan Bezpieczeństwa Informacji
Załącznik Regulacyjny UE

Niniejszy Załącznik opisuje zobowiązania Infor w odniesieniu do szczególnych wymogów wynikających z obowiązujących dyrektyw, rozporządzeń oraz krajowych przepisów wykonawczych UE dotyczących cyberbezpieczeństwa i zarządzania danymi (dalej: „***obowiązujące przepisy dotyczące cyberbezpieczeństwa i zarządzania danymi***") i zostaje włączony, w zakresie mającym zastosowanie do Klienta (zgodnie z zasadami zastosowania określonymi poniżej), do umów zawartych przez Klienta z Infor (dalej łącznie: „***Umowy***"). W przypadku sprzeczności lub niespójności pomiędzy postanowieniami niniejszego Załącznika a innymi postanowieniami Umów w zakresie spraw dotyczących cyberbezpieczeństwa, niniejszy Załącznik ma charakter rozstrzygający.

I. OGÓLNE

1. DEFINICJE

1.1 Pojęcia zapisane wielką literą, użyte w niniejszym Załączniku, lecz w nim niezdefiniowane, mają znaczenie nadane im w Planie Bezpieczeństwa Informacji, dostępnym pod adresem www.infor.com/security-plan (dalej: „Plan Bezpieczeństwa Informacji"). Pojęcia „Proces ICT", „Produkt ICT", „Usługa ICT" (ICT = technologie informacyjno-komunikacyjne), „Incydenty", „Sieci i Systemy Informatyczne", „Ryzyko", „Znaczące Cyberzagrożenie", „Przeniesienie", „Opłaty za Przeniesienie", „Interoperacyjność", „Dane Eksportowalne", „Aktywa Cyfrowe" mają znaczenie nadane im w obowiązujących przepisach dotyczących cyberbezpieczeństwa i zarządzania danymi.

2. ZGODNOŚĆ Z PRZEPISAMI I WSPÓŁPRACA

2.1 Infor będzie przestrzegać obowiązujących przepisów dotyczących cyberbezpieczeństwa i zarządzania danymi mających zastosowanie do jego działalności oraz, na uzasadnione żądanie, będzie współpracować z każdym właściwym organem rządowym i/lub Klientem w zakresie przestrzegania przez Infor zobowiązań wynikających z Umowy w świetle obowiązujących przepisów dotyczących cyberbezpieczeństwa i zarządzania danymi. Zarówno Infor, jak i Klient będą informować drugą Stronę oraz ostrzegać ją o wszelkich istotnych zmianach lub zdarzeniach, trudnościach, ryzykach lub informacjach, które mogłyby wywrzeć niekorzystny wpływ na Usługi ICT lub wykonywanie Umowy (chyba że przekazanie takich informacji jest zabronione na mocy Obowiązującego Prawa).

3. DATA WEJŚCIA W ŻYCIE

3.1 Postanowienia niniejszego Załącznika wchodzą w życie w dniu, w którym obowiązujące przepisy dotyczące cyberbezpieczeństwa i zarządzania danymi staną się skuteczne i wykonalne.

4. AKTUALIZACJE

4.1 Klient przyjmuje do wiadomości, że techniczne i organizacyjne środki bezpieczeństwa opisane w niniejszym Załączniku podlegają zaktualizowanym wymogom wynikającym z obowiązujących przepisów dotyczących cyberbezpieczeństwa i zarządzania danymi oraz postępowi technicznemu i rozwojowi, a Infor może od czasu do czasu aktualizować lub modyfikować te środki, pod warunkiem, że takie aktualizacje i modyfikacje nie spowodują pogorszenia ogólnego poziomu bezpieczeństwa Usług świadczonych na rzecz Klienta.

5. PRAWO WŁAŚCIWE

5.1 Niniejszy Załącznik podlega prawu właściwemu określonemu w Umowie i będzie interpretowany zgodnie z tym prawem, chyba że obowiązujące przepisy dotyczące cyberbezpieczeństwa i zarządzania danymi wymagają zastosowania odrębnego prawa właściwego. W takim przypadku, na potrzeby niniejszego Załącznika, takie wymagane prawo właściwe ma pierwszeństwo przed prawem właściwym określonym w Umowie.

6. ODPOWIEDZIALNOŚĆ

6.1 Infor i Klient uzgadniają, że całkowita odpowiedzialność każdej ze Stron oraz jej Podmiotów Powiązanych (zgodnie z definicją zawartą w Umowie), wynikająca z niniejszego Załącznika lub z nim związana, niezależnie od tego, czy wynika z naruszenia Umowy, czynu niedozwolonego czy z innego tytułu, podlega. w relacjach pomiędzy Stronami (w tym ich Podmiotami Powiązanymi). odpowiednim postanowieniom Umowy dotyczącym ograniczenia odpowiedzialności. Ponadto Infor nie ponosi odpowiedzialności za jakiekolwiek naruszenie przez

Klienta obowiązujących przepisów dotyczących cyberbezpieczeństwa i zarządzania danymi ani za niezastosowanie się przez Klienta do wymogów właściwego organu.

II. DYREKTYWA NIS 2

1. ZAKRES I DEFINICJE

1.1 Postanowienia określone w Sekcji II niniejszego Załącznika mają zastosowanie wyłącznie do Klientów z UE, którzy spełniają kryteria i progi dla podmiotów „ważnych" lub „kluczowych", podlegających regulacjom na mocy Dyrektywy NIS 2. Dla uniknięcia wątpliwości Sekcję I uważa się za włączoną do niniejszej Sekcji II.

1.2 „**Dyrektywa NIS 2**" oznacza Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE, zmieniającą Rozporządzenie (UE) nr 910/2014 i Dyrektywę (UE) 2018/1972 oraz uchylającą Dyrektywę (UE) 2016/1148, wraz z odpowiednimi przepisami wykonawczymi.

2. ZASADY ADMINISTRACJI

2.1 Infor posiada w ramach swojej struktury bezpieczeństwa organy zarządzające, które zatwierdzają środki zarządzania ryzykiem cyberbezpieczeństwa Infor, sprawują nad nimi nadzór oraz odpowiadają za ich wdrożenie, w tym za Plan Bezpieczeństwa Informacji.

3. PLAN BEZPIECZEŃSTWA INFORMACJI

3.1 Infor wdrożył i będzie utrzymywać Plan Bezpieczeństwa Informacji w taki sposób, aby: (A) został zaprojektowany w celu: (1) zapewnienia bezpieczeństwa i poufności Sieci i Systemów Informatycznych Infor; (2) ochrony przed wszelkimi przewidywanymi zagrożeniami lub ryzykami dla bezpieczeństwa albo integralności Sieci i Systemów Informatycznych Infor; oraz (3) ochrony przed nieuprawnionym dostępem do Sieci i Systemów Informatycznych lub nieuprawnionym korzystaniem z nich; oraz (B) określał politykę Infor dotyczącą reagowania na każdy Incydent.

3.2 Plan Bezpieczeństwa Informacji jest dostępny pod adresem: www.infor.com/security-plan.

4. ŚRODKI ZARZĄDZANIA RYZYKIEM W ZAKRESIE CYBERBEZPIECZEŃSTWA

4.1 Infor wdrożył i będzie utrzymywać środki zarządzania ryzykiem w zakresie cyberbezpieczeństwa, które:

(A) są proporcjonalne do ryzyk stwarzanych dla Sieci i Systemów Informatycznych Infor, z uwzględnieniem aktualnego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia;

(B) opierają się na podejściu obejmującym wszystkie rodzaje zagrożeń, mającym na celu ochronę Sieci i Systemów Informatycznych Infor oraz fizycznego środowiska tych systemów przed Incydentami; oraz

(C) obejmują co najmniej: (a) polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych;
(b) środki służące identyfikacji ryzyk Incydentów, w tym procedury obsługi incydentów; (c) ciągłość działania, taką jak zarządzanie kopiami zapasowymi, odtwarzanie po awarii oraz zarządzanie kryzysowe; (d) bezpieczeństwo łańcucha dostaw, w tym aspekty bezpieczeństwa dotyczące relacji pomiędzy Infor a jej bezpośrednimi dostawcami lub usługodawcami; (e) bezpieczeństwo w zakresie nabywania, rozwoju i utrzymania Sieci i Systemów Informatycznych, w tym zarządzanie podatnościami oraz ich ujawnianie; (f) polityki i procedury służące ocenie skuteczności środków zarządzania w zakresie cyberbezpieczeństwa stosowanych przez Infor; (g) podstawowe praktyki cyberhigieny, takie jak zasady zerowego zaufania, aktualizacje oprogramowania, konfiguracja urządzeń, segmentacja sieci, zarządzanie tożsamością i dostępem, świadomość użytkowników, regularne szkolenia personelu w zakresie cyberbezpieczeństwa oraz podnoszenie świadomości dotyczącej cyberzagrożeń, phishingu lub technik socjotechnicznych; (h) polityki i procedury dotyczące stosowania kryptografii i szyfrowania; (i) bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu oraz zarządzanie aktywami; oraz (j) stosowanie rozwiązań uwierzytelniania wieloskładnikowego lub ciągłego uwierzytelniania, zabezpieczonej komunikacji głosowej, wideo i tekstowej oraz zabezpieczonych systemów komunikacji awaryjnej w ramach Infor.

5. ŁAŃCUCH DOSTAW

5.1 Infor oświadcza i zapewnia, że środki bezpieczeństwa łańcucha dostaw wdrożone przez Infor uwzględniają następujące kryteria: (a) podatności właściwe dla każdego bezpośredniego dostawcy i usługodawcy Infor; (b) ogólną jakość produktów oraz praktyk cyberbezpieczeństwa dostawców i usługodawców Infor, w tym ich bezpieczne procedury rozwoju; oraz, w stosownych przypadkach, (c) wyniki wszelkich skoordynowanych ocen ryzyka bezpieczeństwa dotyczących określonych krytycznych łańcuchów dostaw Usług ICT, Produktów ICT lub Procesów ICT, przeprowadzanych przez państwa członkowskie UE oraz właściwe organy.

5.2 Infor przeprowadza badania due diligence swoich zewnętrznych usługodawców w celu oceny stosowanych przez nich środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa oraz zawiera z takimi zewnętrznymi usługodawcami umowy zawierające wymogi dotyczące cyberbezpieczeństwa i zarządzania danymi zasadniczo podobne do określonych w niniejszym Załączniku.

5.3 Infor przedstawi zasadne dowody stosowania takich środków bezpieczeństwa łańcucha dostaw w rozsądnym terminie po otrzymaniu żądania Klienta.

6. REAGOWANIE NA INCYDENTY

6.1 Infor będzie monitorować swoje Sieci i Systemy Informatyczne pod kątem nieuprawnionego dostępu oraz wdroży politykę reagowania na Incydenty określającą działania podejmowane w przypadku wykrycia lub powzięcia wiadomości o jakimkolwiek Incydencie.

6.2 Jeżeli Infor powezmie wiadomość o Znaczącym Incydencie mającym wpływ na Klienta, Infor:

(A) powiadomi Klienta w następujący sposób:

(1) niezwłocznie i bez zbędnej zwłoki (w każdym przypadku w terminie 24 godzin od powzięcia wiadomości o takim Znaczącym Incydencie): (a) powiadomi Klienta o wystąpieniu takiego Znaczącego Incydentu; oraz (b) przekaże Klientowi szczegółowe informacje dotyczące Znaczącego Incydentu, w tym: (i) czy istnieje podejrzenie, że Znaczący Incydent został spowodowany działaniami bezprawnymi lub złośliwymi albo czy może wywołać skutki transgraniczne; (ii) wszelkie informacje pozwalające ustalić ewentualny transgraniczny wpływ Znaczącego Incydentu; oraz (iii) wstępną ocenę Znaczącego Incydentu, w tym jego wagę i wpływ, a także, jeżeli są dostępne, wskaźniki naruszenia bezpieczeństwa;

(2) niezwłocznie i bez zbędnej zwłoki przekaże Klientowi następujące uzupełniające informacje dotyczące Znaczącego Incydentu: (a) szczegółowy opis Znaczącego Incydentu, w tym jego wagę i wpływ; (b) rodzaj zagrożenia lub przyczynę źródłową, która mogła spowodować Znaczący Incydent; (c) zastosowane i bieżące środki ograniczające skutki; oraz (d) w stosownych przypadkach transgraniczny wpływ Znaczącego Incydentu;

(B) przeprowadzi dochodzenie oraz dokona zasadnej analizy przyczyny lub przyczyn takiego Znaczącego Incydentu;

(C) będzie przekazywać Klientowi okresowe aktualizacje dotyczące trwającego dochodzenia;

(D) opracuje i wdroży odpowiedni plan ograniczenia skutków oraz usunięcia przyczyny takiego Znaczącego Incydentu w zakresie, w jakim przyczyna ta pozostaje pod kontrolą Infor; oraz

(E) będzie współpracować przy zasadnym dochodzeniu prowadzonym przez Klienta oraz działaniach Klienta mających na celu spełnienie obowiązków informacyjnych mających zastosowanie do takiego Znaczącego Incydentu, w tym poprzez pomoc w sporządzeniu raportu dotyczącego Znaczącego Incydentu dla właściwych organów.

6.3 Jeżeli Infor powezmie wiadomość o Znaczącym Cyberzagrożeniu mającym wpływ na Klienta (w tym o opublikowanych podatnościach aplikacji Infor spełniających definicję Znaczącego Cyberzagrożenia), Infor:

(A) niezwłocznie i bez zbędnej zwłoki powiadomi Klienta o takim Znaczącym Cyberzagrożeniu;

(B) przekaże Klientowi szczegółowe informacje dotyczące wpływu takiego Znaczącego Cyberzagrożenia na Klienta, w zakresie znanym Infor;

(C) przeprowadzi dochodzenie oraz dokona zasadnej analizy przyczyny lub przyczyn takiego Znaczącego Cyberzagrożenia;

(D) opracuje i wdroży odpowiedni plan usunięcia przyczyny takiego Znaczącego Cyberzagrożenia w zakresie, w jakim takie Znaczące Cyberzagrożenie się zmaterializuje, a przyczyna pozostaje pod kontrolą Infor; oraz

(E) zastosuje się do zasadnych żądań Klienta dotyczących przekazania informacji o Znaczącym Cyberzagrożeniu, aby Klient mógł wykorzystać je do wymaganych powiadomień kierowanych do osób trzecich w związku z takim Znaczącym Cyberzagrożeniem, jeżeli takie powiadomienia są wymagane na mocy obowiązujących przepisów dotyczących cyberbezpieczeństwa i zarządzania danymi.

7. AUDYT

7.1 Infor będzie posiadać i utrzymywać co najmniej jeden z następujących certyfikatów lub poświadczeń dotyczących Usług w Chmurze (w zależności od przypadku), a na pisemne żądanie Klienta przekaże Klientowi dowód posiadania takich certyfikatów lub poświadczeń:

(1) SSAE SOC 2 Type 2 (znany również jako AICPA TSC 2014 Type 2)
(2) ISO 27001:2022
(3) FedRAMP

Infor zapewni, że jego zewnętrzni usługodawcy będą posiadać lub utrzymywać co najmniej jeden z powyższych certyfikatów lub poświadczeń odnoszących się do usług świadczonych przez takiego usługodawcę na rzecz Infor i/lub klientów Infor albo przedstawią zadowalające alternatywne dowody stosowania środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa odpowiednich do zakresu świadczonych usług.

7.2 Oprócz raportów audytowych opisanych w Sekcji 7.1 powyżej, na żądanie Klienta i z zastrzeżeniem zobowiązań do zachowania poufności wynikających z Umowy, nie częściej niż raz w roku, chyba że Klient działa na podstawie żądania właściwego organu rządowego (w takim przypadku roczne ograniczenie nie ma zastosowania), Infor niezwłocznie udzieli pisemnej odpowiedzi na wszelkie zasadne pytania lub kwestionariusze Klienta (i/lub jego przedstawicieli) dotyczące treści programu bezpieczeństwa Infor oraz przedstawi zasadne dowody zgodności z wymogami niniejszego Załącznika, w tym ogólnie dostępne kopie danych, dokumentów i informacji związanych z Usługami, niezbędne do wsparcia Klienta w wykonaniu wiążącego żądania lub nakazu otrzymanego od właściwego organu rządowego. Infor przekaże odpowiednie informacje bez zbędnej zwłoki (w każdym przypadku w terminie wskazanym w wiążącym żądaniu lub nakazie otrzymanym przez Klienta od właściwego organu rządowego).

7.3 Klient może, raz w roku, przeprowadzić audyt zgodności Infor z obowiązkami wynikającymi z niniejszego Załącznika, w tym audyt praktyk bezpieczeństwa IT Infor oraz odpowiednich środowisk kontrolnych, zgodnie z procedurą określoną w niniejszej Sekcji 7, wyłącznie, jeżeli:

(A) Infor nie przedstawił wystarczających potwierdzeń zgodności ze środkami zarządzania ryzykiem w zakresie cyberbezpieczeństwa opisanymi w niniejszym Załączniku w raportach i dokumentacji wskazanych w Sekcji 7.2 powyżej ani, w stosownych przypadkach, w innych raportach audytowych lub informacjach ogólnie udostępnianych klientom Infor;

(B) wystąpił Znaczący Incydent;

(C) Infor powiadomił Klienta, że podlega żądaniu dostępu organu publicznego dotyczącemu Danych Klienta;

(D) audyt został formalnie zażądany przez właściwy organ rządowy sprawujący jurysdykcję nad Klientem; lub

(E) bezwzględnie obowiązujące przepisy dotyczące cyberbezpieczeństwa i zarządzania danymi przyznają Klientowi bezpośrednie prawo audytu.

7.4 Przed rozpoczęciem audytu Klient i Infor wspólnie uzgodnią jego zakres, termin, czas trwania oraz wymogi dotyczące kontroli i materiałów dowodowych. Klient może skorzystać z usług niezależnej akredytowanej firmy audytorskiej będącej osobą trzecią w celu przeprowadzenia audytu w jego imieniu, pod warunkiem, że taki audytor zostanie wspólnie zaakceptowany przez Klienta i Infor (z zastrzeżeniem, że nie mogą to być podmioty

będące konkurentami Infor ani podmioty niewystarczająco wykwalifikowane lub niezależne). Klient zgadza się, że audyt będzie przeprowadzany bez nieuzasadnionego zakłócania działalności Infor (lub jego podwykonawców), w zwykłych godzinach pracy, z odpowiednim wyprzedzeniem oraz z zastrzeżeniem obowiązujących u Infor (lub jego podwykonawców) polityk bezpieczeństwa i procedur poufności. W przypadku gdy audyty na miejscu dotyczące fizycznych centrów danych, systemów lub obiektów nie są dozwolone, Infor będzie współpracować z Klientem (oraz, w stosownych przypadkach, swoimi podwykonawcami) w celu wypracowania wspólnie akceptowalnego rozwiązania wystarczającego do przekazania informacji niezbędnych Klientowi do spełnienia wymogów audytowych wynikających z obowiązujących przepisów dotyczących cyberbezpieczeństwa i zarządzania danymi. Ani Klient, ani audytor nie będą mieli dostępu do danych innych klientów Infor ani do systemów lub obiektów Infor niezwiązanych z Usługami świadczonymi na rzecz Klienta. Klient przekaże Infor wyniki każdego audytu. Strony wspólnie uzgodnią wszelkie odpowiednie raporty lub działania naprawcze. Infor dołoży handlowo uzasadnionych starań w celu wdrożenia uzgodnionych działań naprawczych.

7.5 Klient ma obowiązek pokryć wszelkie koszty i opłaty związane z audytem, w tym wszelkie zasadne koszty i opłaty poniesione przez Infor w związku z audytem oraz wszelkie koszty i opłaty poniesione przez Infor na rzecz podwykonawcy, jeżeli audyt obejmuje podwykonawcę, chyba że audyt wykaże istotne naruszenie niniejszego Załącznika przez Infor, w którym to przypadku Infor pokryje własne koszty tej części audytu, która dotyczyła naruszenia.

III. DORA

1. ZAKRES I DEFINICJE

1.1 Postanowienia określone w Sekcji III niniejszego Załącznika mają zastosowanie wyłącznie do Klientów z UE, którzy spełniają kryteria i progi dla podmiotów finansowych regulowanych przez DORA. Dla uniknięcia wątpliwości Sekcję I uważa się za włączoną do niniejszej Sekcji III; określone postanowienia Sekcji II mają również zastosowanie, jeżeli zostały wyraźnie wskazane w niniejszej Sekcji III.

1.2 „**DORA**" oznacza Akt o Operacyjnej Odporności Cyfrowej (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r.).

2. USŁUGI

2.1 Usługa ICT świadczona przez Infor na rzecz Klienta została opisana w Umowach.

3. LOKALIZACJA

3.1 Dla uniknięcia wątpliwości dane produkcyjne Klienta są przechowywane w wybranej lokalizacji wdrożeniowej, a Infor nie przeniesie żadnych danych produkcyjnych Klienta poza tę lokalizację bez uprzedniej pisemnej zgody i polecenia Klienta. Na polecenie Klienta ograniczone ilości danych osobowych mogą być zdalnie udostępniane spoza wybranej lokalizacji wdrożeniowej w celu świadczenia wsparcia i usług na rzecz Klienta. Infor powiadomi Klienta z wyprzedzeniem, jeżeli przewiduje zmianę lokalizacji (tj. regionów lub państw), w których Usługi będą świadczone oraz w których Dane Klienta będą przechowywane i przetwarzane, zgodnie z Umową.

4. PROGRAM BEZPIECZEŃSTWA I UMOWY O GWARANTOWANYM POZIOMIE ŚWIADCZENIA USŁUG

4.1 Środki zarządzania ryzykiem w zakresie cyberbezpieczeństwie opisane powyżej w Sekcji II.3 oraz Sekcji II.4 mają zastosowanie. Zobowiązania Infor dotyczące reagowania na incydenty określone w Sekcji II.6 również mają zastosowanie. Dla uniknięcia wątpliwości niewypłacalność Infor uważa się za dodatkową podstawę obowiązku zwrotu Danych Klienta zgodnie z Planem Bezpieczeństwa Informacji.

4.2 Zobowiązania Infor dotyczące dostępności usług wynikające z Umowy o Gwarantowanym Poziomie Świadczenia Usług zostały opisane pod adresem https://www.infor.com/service-level-description (dalej: „Umowa o Gwarantowanym Poziomie Świadczenia Usług"). Zobowiązania dotyczące wsparcia właściwe dla danego produktu zostały opisane w Formularzu Zamówienia, jeżeli ma to zastosowanie.

5. PROGRAMY SZKOLENIOWE I PODNOSZENIE ŚWIADOMOŚCI W ZAKRESIE BEZPIECZEŃSTWA ICT

5.1 Jeżeli w ramach Usług Infor uzyska dostęp do lokalnych sieci i systemów informatycznych Klienta, Klient może zażądać od Infor, z zachowaniem rozsądnego wyprzedzenia, udziału w odpowiednim programie podnoszenia

świadomości w zakresie bezpieczeństwa ICT i/lub szkoleniu z zakresu cyfrowej odporności operacyjnej organizowanym lub prowadzonym przez Klienta w związku z jego działalnością (dalej: „Szkolenie"). W tym zakresie Strony uzgadniają, że:

(A) częstotliwość, terminy oraz czas trwania takiego Szkolenia zostaną uprzednio uzgodnione przez Strony;

(B) Infor zastrzega sobie prawo do odzyskania od Klienta zasadnie i prawidłowo poniesionych kosztów; oraz

(C) udział Infor w takim Szkoleniu nie będzie wymagał od Infor podejmowania działań, które mogłyby zakłócać, uniemożliwiać lub utrudniać świadczenie przez Infor Usług ICT lub wykonywanie innych zobowiązań wynikających z Umowy.

6. ROZWIĄZANIE UMOWY

6.1 Oprócz praw do rozwiązania Umowy określonych w Umowie oraz w innych postanowieniach niniejszych warunków, zgodnie z art. 28 ust. 7 DORA oraz z zastrzeżeniem procedury rozwiązania Umowy określonej w Umowie, Klient może rozwiązać Umowę w całości lub w części wyłącznie w następujących przypadkach: (i) jeżeli Infor nie usunął istotnego naruszenia obowiązujących przepisów dotyczących cyberbezpieczeństwa i zarządzania danymi lub niniejszego Załącznika; (ii) jeżeli Klient stwierdzi okoliczności, które można uznać za mogące wpłynąć na wykonywanie przez Infor Usług ICT, w tym istotne zmiany wpływające na Umowę lub sytuację Infor; (iii) jeżeli zostaną stwierdzone udokumentowane słabości dotyczące ogólnego zarządzania ryzykiem ICT przez Infor, a w szczególności sposobu, w jaki Infor zapewnia dostępność, autentyczność, integralność oraz poufność danych, niezależnie od tego, czy są to dane osobowe, inne dane wrażliwe czy dane nieosobowe; lub (iv) jeżeli właściwy organ rządowy nie będzie już mógł skutecznie nadzorować Klienta z uwagi na warunki lub okoliczności związane z Infor lub Umową.

7. WSPÓŁPRACA Z WŁAŚCIWYMI ORGANAMI RZĄDOWYMI

7.1 Infor będzie w pełni współpracować z właściwymi organami rządowymi oraz organami ds. restrukturyzacji i uporządkowanej likwidacji właściwymi dla Klienta, w tym z osobami przez nie wyznaczonymi.

IV. AKT W SPRAWIE DANYCH

1. ZAKRES I DEFINICJE

1.1 Postanowienia określone w Sekcji IV niniejszego Załącznika mają zastosowanie wyłącznie do Klientów z UE oraz wyłącznie w zakresie, w jakim Infor spełnia kryteria i progi dla dostawcy usług przetwarzania danych na podstawie Aktu w sprawie danych. Dla uniknięcia wątpliwości Sekcję I uważa się za włączoną do niniejszej Sekcji IV; określone postanowienia Sekcji II mają również zastosowanie, jeżeli zostały wyraźnie wskazane w niniejszej Sekcji IV.

1.2 „**Akt w sprawie danych**" oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz zmieniające Rozporządzenie (UE) 2017/2394 i Dyrektywę (UE) 2020/1828.

2. DOSTĘP KLIENTA DO DANYCH

2.1 Plan Bezpieczeństwa Informacji opisany powyżej w Sekcji II.3 określa warunki dostępu Klienta do Danych Klienta przez cały Okres Obowiązywania Umowy oraz zasady zwrotu i zniszczenia Danych Klienta po rozwiązaniu lub wygaśnięciu Usług w Chmurze.

3. PROCES PRZENIESIENIA

3.1 Zgodnie z postanowieniami niniejszego Załącznika Klient może dokonać przeniesienia do usługi przetwarzania danych oferowanej przez innego dostawcę usług przetwarzania danych albo przenieść Dane Klienta do lokalnej infrastruktury ICT, z zastrzeżeniem szczególnego procesu Infor (dalej: „**Proces Przeniesienia**"), pod warunkiem, że Klient:

(A) przekaże Infor pisemne wypowiedzenie z co najmniej dwumiesięcznym wyprzedzeniem zgodnie z procedurą wypowiedzenia określoną w Umowie;

(B) zawrze z Infor uzgodnioną przez Strony umowę o usługi przejściowe zawierającą informacje opisane poniżej; oraz

(C) uiści wszystkie mające zastosowanie opłaty (zdefiniowane poniżej).

3.2 Umowa o usługi przejściowe określi:

(A) czy Klient żąda: (i) eksportu swoich Danych Klienta i przeniesienia ich do wskazanego alternatywnego dostawcy, (ii) eksportu swoich Danych Klienta i przeniesienia ich z chmury do środowiska lokalnego, czy też (iii) usunięcia swoich Danych Klienta;

(B) kategorie Danych Klienta, które mogą zostać przeniesione w ramach Procesu Przeniesienia, oraz kategorie danych wyłączonych z Przeniesienia z uwagi na ryzyko naruszenia tajemnicy przedsiębiorstwa, jeżeli ma to zastosowanie;

(C) mające zastosowanie terminy zakończenia Przeniesienia, w tym terminy pobrania danych po zakończeniu okresu przejściowego uzgodnionego przez Strony;

(D) wszelkie ograniczenia techniczne lub wykonalności dotyczące Przeniesienia, w tym informacje dotyczące Interoperacyjności, jeżeli mają zastosowanie, udostępnione przez Infor;

(E) mające zastosowanie opłaty za Przeniesienie, które obejmują:

(1) pełną pozostałą do zapłaty na rzecz Infor kwotę za cały bieżący uzgodniony okres subskrypcji określony we właściwym Formularzu Zamówienia (kwota ta jest odrębna od „Opłaty za Przeniesienie" i nie stanowi takiej opłaty); oraz

(2) Opłaty za Przeniesienie, w zakresie dozwolonym przez obowiązujące prawo; oraz

(F) wszelką dodatkową dokumentację wymaganą do podpisania przez Klienta, taką jak nowa umowa licencyjna dotycząca Oprogramowania Instalowanego Lokalnie zastępująca umowę dotyczącą Usług w Chmurze, jeżeli Klient realizuje Przeniesienie opisane w Sekcji IV.3.2(A)(ii) powyżej.

3.3 W trakcie Procesu Przeniesienia Infor:

(A) utrzyma taki sam poziom bezpieczeństwa, jak opisany we właściwym Planie Bezpieczeństwa Informacji;

(B) będzie działać z należytą starannością w celu zachowania ciągłości działania i dalszego świadczenia Usług w Chmurze zgodnie z Umową zawartą z Klientem; oraz

(C) zapewni Klientowi zasadną pomoc (oraz innym osobom trzecim upoważnionym przez Klienta, które są związane pisemnym lub zawodowym obowiązkiem zachowania poufności), w tym poprzez zasadne wsparcie strategii wyjścia Klienta, zapewnienie przejrzystości oraz udostępnianie na żądanie ogólnie dostępnych informacji istotnych dla Procesu Przeniesienia, w tym informacji dotyczących Interoperacyjności eksportowanych Danych Klienta. Niezależnie od powyższego Infor nie będzie zobowiązany do udostępniania informacji ani świadczenia pomocy na rzecz Klienta (lub innych osób trzecich), jeżeli stwarzałoby to ryzyko dla praw własności intelektualnej i tajemnic przedsiębiorstwa Infor lub powodowałoby niekorzystną sytuację ekonomiczną dla Infor.

3.4 Klient ponosi odpowiedzialność za import oraz wdrożenie Danych Klienta we własnych systemach lub, w zależności od przypadku, w systemach Dostawcy Docelowego.

3.5 W zakresie dozwolonym przez Akt w sprawie danych Strony mogą wydłużyć terminy określone w umowie o usługi przejściowe.

3.6 Po zakończeniu Procesu Przeniesienia (lub po upływie dwumiesięcznego okresu wypowiedzenia, jeżeli Klient nie chce dokonać Przeniesienia, lecz zamiast tego żąda usunięcia Danych Klienta po zakończeniu świadczenia usługi), odpowiednie Formularze Zamówienia oraz wszystkie Umowy z Klientem uważa się za rozwiązane.

3.7 Infor oraz Klient (a także wskazany przez Klienta alternatywny dostawca, jeżeli ma to zastosowanie) będą działać w dobrej wierze w celu zapewnienia skuteczności Procesu Przeniesienia, umożliwienia terminowego transferu Danych Klienta oraz zachowania ciągłości usługi przetwarzania danych.

3.8 Infor nie jest zobowiązany do oferowania Procesu Przeniesienia w odniesieniu do:

(A) środowisk nieprodukcyjnych wykorzystywanych do celów testowych i ewaluacyjnych oraz przez ograniczony okres;

(B) Usług obejmujących wyjątkowo złożone lub kosztowne Przeniesienie, albo takich, w przypadku których Przeniesienie jest niemożliwe bez istotnej ingerencji w Dane Klienta lub architekturę Usługi; oraz/lub

(C) Usług, w których większość głównych funkcji została wykonana na zamówienie w celu zaspokojenia szczególnych potrzeb indywidualnego klienta lub w których wszystkie komponenty zostały opracowane na potrzeby indywidualnego klienta, a takie usługi przetwarzania danych nie są oferowane na szeroką skalę komercyjną za pośrednictwem katalogu usług dostawcy usług przetwarzania danych.

3.9 Infor nie jest zobowiązany do opracowywania nowych technologii lub usług ani do ujawniania lub przenoszenia aktywów cyfrowych chronionych prawami własności intelektualnej lub stanowiących tajemnicę przedsiębiorstwa na rzecz klienta lub innego dostawcy usług przetwarzania danych, ani do naruszania bezpieczeństwa i integralności usług klienta lub Infor.

4. ODPOWIEDZIALNOŚĆ I ZWOLNIENIE Z ODPOWIEDZIALNOŚCI

4.1 Kilka podmiotów prawnych może być uprawnionych do nabywania lub korzystania z Usług na podstawie Umowy (w tym między innymi Podmioty Powiązane Klienta oraz Upoważnieni Użytkownicy), a zatem podmioty inne niż Klient składający żądanie mogą zostać dotknięte żądaniem Przeniesienia zgodnie z niniejszą sekcją (dalej: „Podmioty Dotknięte"). Wyłączną odpowiedzialność za zapewnienie, że Klient posiada wszelkie prawa i zgody dotyczące żądań Przeniesienia oraz Danych Klienta przed skorzystaniem z uprawnień wynikających z niniejszego dokumentu, ponosi Klient.

4.2 Klient będzie bronić Infor, zwolni Infor z odpowiedzialności oraz zabezpieczy Infor przed wszelkimi stratami, kosztami i wydatkami w zakresie wynikającym z jakiegokolwiek roszczenia, żądania, powództwa lub postępowania wniesionego przeciwko Infor przez Podmioty Dotknięte, zarzucającego, że żądanie Przeniesienia narusza prawa lub licencje takiego Podmiotu Dotkniętego, pod warunkiem że Infor: (A) niezwłocznie przekaże Klientowi pisemne zawiadomienie o takim roszczeniu skierowanym przeciwko Infor; (B) powierzy Klientowi wyłączną kontrolę nad obroną i ugodowym zakończeniem takiego roszczenia przeciwko Infor (z zastrzeżeniem, że Klient nie może zawrzeć ugody w imieniu Infor, chyba że bezwarunkowo zwolni Infor z wszelkiej odpowiedzialności oraz nie będzie to wymagało od Infor zapłaty jakiejkolwiek kwoty ani przyznania się do winy); oraz (C) udzieli Klientowi wszelkiej zasadnej pomocy, na koszt Klienta. Powyższe zobowiązania dotyczące obrony i zwolnienia z odpowiedzialności nie mają zastosowania, jeżeli takie roszczenie przeciwko Infor wynika z naruszenia Umowy przez Infor, w tym niniejszego Załącznika, i/lub odpowiednich Formularzy Zamówienia.

4.3 Infor nie ponosi odpowiedzialności za jakiekolwiek szkody, straty, koszty lub wydatki wynikające z żądania Przeniesienia lub z nim związane. Wyłączenie odpowiedzialności obejmuje między innymi wszelkie kwestie związane z integralnością lub utratą Danych Klienta, przestojami systemów, problemami kompatybilności oraz wszelkimi innymi zakłóceniami lub awariami, które mogą wystąpić w trakcie realizacji żądania Przeniesienia lub w jego wyniku. Klient ponosi pełną odpowiedzialność za skuteczne Przeniesienie Danych Klienta.

4.4 Dla jasności żadne postanowienie niniejszej Sekcji IV nie uchyla ani nie ogranicza obowiązku Klienta do zapłaty wszelkich należnych opłat wynikających z Umowy i/lub Formularza Zamówienia za cały bieżący uzgodniony okres subskrypcji określony we właściwych Formularzach Zamówienia. Jeżeli Klient zdecyduje się na Przeniesienie przed końcem bieżącego okresu subskrypcji wynikającego z właściwych Formularzy Zamówienia, Klient przyjmuje do wiadomości i zgadza się, że w żadnym przypadku takie Przeniesienie nie uprawnia Klienta do zwrotu jakichkolwiek opłat uprzednio uiszczonych na podstawie właściwej Umowy i/lub Formularza Zamówienia.

5. ŻĄDANIA DOSTĘPU ORGANÓW PUBLICZNYCH

5.1 W przypadku gdy Infor otrzyma wydane przez organ publiczny prawnie wiążące żądanie ujawnienia Danych Nieosobowych Klienta z UE hostowanych w UE albo żądanie bezpośredniego dostępu organu publicznego do takich Danych Nieosobowych, Infor, w zakresie dozwolonym przez prawo, podejmie próbę przekierowania takiego żądania do Klienta. Jeżeli przekierowanie żądania do Klienta nie będzie możliwe, Infor: (i) odrzuci żądanie, chyba że prawo wymaga jego wykonania; (ii) zakwestionuje takie żądanie, jeżeli pozostaje ono w sprzeczności z obowiązującym prawem, jest nadmiernie szerokie lub istnieje inna właściwa podstawa sprzeciwu; (iii) niezwłocznie powiadomi Klienta i przekaże kopię żądania, chyba że jest to prawnie zabronione; (iv) jeżeli będzie do tego zobowiązany, ujawni wyłącznie minimalny zakres Danych Nieosobowych Klienta z UE hostowanych w UE niezbędny do spełnienia żądania; oraz (v) jeżeli zezwalają na to przepisy państwa przeznaczenia, na pisemne żądanie Klienta (nie częściej niż raz w roku przez okres obowiązywania Umów) przekaże Klientowi możliwie najwięcej istotnych informacji dotyczących otrzymanych żądań ujawnienia. Dla uniknięcia wątpliwości żądania dostępu organów publicznych dotyczące Danych Osobowych podlegają odrębnie postanowieniom Umowy Powierzenia Przetwarzania Danych („DPA”) zawartej pomiędzy Stronami.