Plan Bezpieczeństwa Informacji

Zakres: Niniejszy Plan Bezpieczeństwa Informacji (dalej: „Plan Bezpieczeństwa Informacji") stanowi część Umów zawartych przez Klienta z Infor (dalej łącznie: „***Umowy***"). W przypadku sprzeczności lub niespójności pomiędzy warunkami niniejszego Planu Bezpieczeństwa Informacji a innymi postanowieniami Umów, niniejszy Plan Bezpieczeństwa Informacji ma charakter rozstrzygający. Niniejszy Plan Bezpieczeństwa Informacji określa stosowane obecnie przez Infor środki bezpieczeństwa mające na celu zabezpieczenie, w odniesieniu do wszystkich Klientów co do zasady:

i. sprzętu, urządzeń oraz konfiguracji oprogramowania systemowego, przy wykorzystaniu których Infor świadczy:

   a. Usługi w Chmurze (dla jasności, Usługi w Chmurze obejmują Wsparcie),
   b. Usługi Profesjonalne, oraz
   c. Wsparcie dotyczące Oprogramowania Instalowanego Lokalnie,

   (wszelki taki sprzęt, urządzenia oraz konfiguracja oprogramowania systemowego są łącznie zdefiniowane w niniejszym Planie Bezpieczeństwa Informacji jako „Systemy", a Usługi w Chmurze, Usługi Profesjonalne oraz Wsparcie dotyczące Oprogramowania Instalowanego Lokalnie są łącznie zdefiniowane w niniejszym Planie Bezpieczeństwa Informacji jako „Usługi"); jak również

ii. Danych Klienta przekazanych Infor:

   a. jako Dane Klienta, lub
   b. przekazanych Infor w celu świadczenia Usług Profesjonalnych i/lub Wsparcia z poziomu środowiska Infor,

(wszelkie takie dane są łącznie zdefiniowane w niniejszym Planie Bezpieczeństwa Informacji jako „Dane").

Definicje: Pojęcia zapisane wielką literą, użyte w niniejszym Planie Bezpieczeństwa Informacji, a niezdefiniowane w jego treści, mają znaczenie nadane im w Umowie Oprogramowania zawartej pomiędzy Infor a danym Klientem (dalej: „Umowa").

Wyłączenia: Niniejszy Plan Bezpieczeństwa Informacji nie ma zastosowania: (i) do uzgodnień dotyczących Usług Profesjonalnych Infor, w ramach których Oprogramowanie Instalowane Lokalnie Klienta jest hostowane przez Infor na podstawie odrębnie wynegocjowanej umowy dotyczącej Usług Profesjonalnych, lub
(ii) w przypadku, gdy Infor świadczy usługi w siedzibie Klienta i/lub uzyskuje dostęp do systemów Klienta. W takich przypadkach Infor będzie przestrzegać administracyjnych, technicznych i fizycznych wymogów Klienta, uzgodnionych przez Strony w odpowiednim zleceniu, a w związku z takim dostępem do systemów Klienta Klient będzie odpowiedzialny za nadawanie personelowi Infor uprawnień użytkownika i haseł umożliwiających dostęp do jego systemów, jak również za cofanie takich uprawnień oraz zakończenie takiego dostępu, zgodnie z własną oceną Klienta.

Aktualizacje: Zagrożenia bezpieczeństwa oraz środki służące ochronie przed takimi zagrożeniami stale ewoluują, a Infor może w każdym czasie zmienić niniejszy Plan Bezpieczeństwa Informacji bez

uprzedniego powiadomienia Klienta, pod warunkiem że Infor utrzyma porównywalny lub wyższy, całościowy poziom bezpieczeństwa w odniesieniu do Systemów i Danych.

1. Ogólne standardy bezpieczeństwa

Infor stosuje administracyjne, techniczne i fizyczne zabezpieczenia mające na celu ochronę Systemów i Danych przed zniszczeniem, utratą, nieuprawnionym dostępem lub zmianą, które są: (i) nie mniej rygorystyczne niż zabezpieczenia stosowane przez Infor w odniesieniu do własnych informacji o podobnym charakterze; (ii) nie mniej rygorystyczne niż powszechnie przyjęte standardy branżowe; oraz (iii) wymagane przez Obowiązujące Przepisy Prawa. Infor nie ponosi odpowiedzialności za systemy operacyjne osób trzecich oraz produkty i usługi współdziałające z Systemami, które Klient (a) opracowuje lub zleca ich opracowanie na własny użytek, lub (b) licencjonuje na warunkach właściwych dla takich osób trzecich.

1.1. Specjaliści ds. bezpieczeństwa

Infor wyznaczył co najmniej jednego specjalistę ds. bezpieczeństwa odpowiedzialnego za koordynowanie i monitorowanie środków bezpieczeństwa określonych w niniejszym Planie Bezpieczeństwa Informacji.

1.2. Kontrola dostępu

Infor wdraża mechanizmy kontroli dostępu do Danych, obejmujące między innymi następujące środki:

i. Infor przypisuje unikalny identyfikator każdej osobie posiadającej komputerowy dostęp do Danych.

ii. Infor wskazuje personel uprawniony do nadawania, zmiany lub cofania dostępu do Danych oraz ogranicza dostęp do Danych zgodnie z zasadą minimalnych uprawnień. Dostęp do Danych jest przyznawany wyłącznie personelowi, który musi go posiadać w celu świadczenia Usług, a Infor prowadzi i aktualizuje rejestr takiego personelu. Dostęp do Danych jest rejestrowany i monitorowany.

iii. Infor zobowiązuje personel Infor posiadający dostęp do Danych do wyłączania sesji administracyjnych w przypadku pozostawienia komputerów bez nadzoru.

iv. Infor dezaktywuje konta pracowników Infor w aplikacjach lub repozytoriach danych zawierających Dane w przypadku rozwiązania stosunku pracy, przeniesienia pracownika lub ustania potrzeby dostępu do takich Danych. Infor regularnie dokonuje przeglądu listy osób i usług posiadających dostęp do Danych oraz usuwa konta, które nie wymagają już takiego dostępu. Infor przeprowadza taki przegląd co najmniej dwa razy w roku.

v. Infor nie stosuje domyślnych haseł producenta ani innych domyślnych parametrów bezpieczeństwa w żadnych Systemach. Infor wymaga stosowania wymuszanych systemowo „silnych haseł" zgodnie z powszechnie przyjętymi najlepszymi praktykami branżowymi we wszystkich Systemach Infor. Infor wymaga zachowania poufności wszystkich haseł i danych uwierzytelniających oraz zakazuje ich współdzielenia pomiędzy personelem, a także dezaktywuje hasła, co do których wiadomo, że zostały naruszone lub ujawnione.

vi. Infor stosuje mechanizm „blokady konta" poprzez dezaktywację kont z dostępem do Danych po przekroczeniu określonej liczby kolejnych nieprawidłowych prób podania hasła.

vii. Zdalny dostęp do Systemów zawierających Dane wymaga uwierzytelniania dwuskładnikowego (tj. zastosowania co najmniej dwóch odrębnych czynników identyfikujących użytkownika).

1.3. Wykrywanie i zapobieganie włamaniom

Infor wykorzystuje system wykrywania włamań/system zapobiegania włamaniom (IDS/IPS) do monitorowania swoich Systemów oraz procedur pod kątem naruszeń bezpieczeństwa, naruszeń zasad oraz podejrzanej aktywności. Obejmuje to podejrzaną aktywność zewnętrzną (w tym między innymi nieuprawnione próby sondowania, skanowania lub włamania) oraz podejrzaną aktywność wewnętrzną (w tym między innymi nieuprawniony dostęp administratora systemu, nieuprawnione zmiany w Systemach, niewłaściwe wykorzystanie Systemów lub ich kradzież, bądź niewłaściwe obchodzenie się z Danymi). Infor regularnie dokonuje przeglądu dzienników dostępu pod kątem oznak złośliwego działania lub nieuprawnionego dostępu.

1.4. Zapora sieciowa

Infor wdrożył i utrzymuje technologie zapory sieciowej mające na celu ochronę Danych dostępnych z Internetu.

1.5. Aktualizacje

Infor na bieżąco aktualizuje Systemy poprzez wdrażanie ulepszeń, aktualizacji, poprawek błędów oraz nowych wersji.

1.6. Szyfrowanie danych

i. Podczas transmisji przez sieci publiczne Dane są szyfrowane co najmniej przy użyciu TLS 1.2 lub jego logicznego następcy.

ii. Podczas przechowywania Danych w Systemach Dane są szyfrowane co najmniej przy użyciu AES 256-bit lub jego logicznego następcy (z wyjątkiem incydentów Wsparcia dotyczących odsprzedawanych przez Infor rozwiązań IBM z Serii i lub Platformy Z).

1.7. Zarządzanie tożsamością

Infor wykorzystuje model współdzielonego bezpieczeństwa w celu podziału odpowiedzialności za zarządzanie tożsamością. Infor posiada możliwość federacji aplikacji w ramach Systemów z dostawcą zarządzania tożsamością Klienta do celów uwierzytelniania.

1.8. Złośliwe oprogramowanie

Infor utrzymuje oprogramowanie przeciw oprogramowaniu złośliwemu/oprogramowanie antywirusowe zgodne z powszechnie przyjętymi standardami branżowymi oraz, w możliwym zakresie, wykorzystuje funkcje ochrony działające niemal w czasie rzeczywistym, aby świadczyć Usługi w Chmurze lub dostarczać Oprogramowanie Instalowane Lokalnie, które nie zawierają „bomb czasowych", „robaków", „wirusów", „koni trojańskich", „kodów ochronnych", „kluczy niszczących dane" ani innych mechanizmów programistycznych mających na celu: (i) w odniesieniu do Usług w Chmurze – modyfikowanie, usuwanie, uszkadzanie, dezaktywowanie lub wyłączanie Danych Klienta albo uniemożliwianie lub ograniczanie Klientowi dostępu do Danych Klienta; lub (ii) w odniesieniu do Oprogramowania Instalowanego Lokalnie – modyfikowanie, usuwanie, uszkadzanie, dezaktywowanie lub wyłączanie Danych Klienta znajdujących się w Oprogramowaniu Instalowanym Lokalnie.

1.9. Bezpieczeństwo fizyczne

Obiekty, w których znajdują się Systemy:

i. są zaprojektowane konstrukcyjnie w sposób umożliwiający wytrzymanie niekorzystnych warunków pogodowych oraz innych racjonalnie przewidywalnych zjawisk naturalnych;

ii. posiadają odpowiednie fizyczne zabezpieczenia środowiskowe pomagające chronić Systemy przed uszkodzeniami związanymi z dymem, ciepłem, wodą, ogniem, wilgotnością lub wahaniami zasilania elektrycznego;

iii. są wyposażone w lokalne awaryjne systemy zasilania; oraz

iv. posiadają odpowiednie mechanizmy kontrolne mające zapewnić, że fizyczny dostęp do obiektu mają wyłącznie osoby upoważnione.

2. Audyt

2.1. Prawa do audytu

W ramach programu nadzoru nad dostawcami Klient oraz (jeżeli ma to zastosowanie) właściwy organ regulacyjny mogą raz w roku zwrócić się, w formie audytu korespondencyjnego (tj. kwestionariusza opartego na normie ISO 27001), o dokumentację proceduralną dotyczącą programu bezpieczeństwa informacji, procesów i mechanizmów kontrolnych Infor. Infor uzgadnia, że w zakresie, w jakim taka dokumentacja proceduralna jest łatwo dostępna, przekaże dokumentację, o którą Klient zasadnie wystąpi, o ile dokumentacja taka: (a) nie zagraża poufności, integralności lub dostępności danych albo usług innych klientów Infor; lub (b) nie narusza poufność, integralność lub dostępność danych albo usług osób trzecich świadczących Usługi na rzecz Klienta w imieniu Infor. Dokumentacja proceduralna przekazywana przez Infor nie obejmuje materiałów dowodowych (na przykład między innymi potwierdzeń szkoleń, potwierdzeń testów, wyników ocen ryzyka). Infor udzieli odpowiedzi na kwestionariusz w terminie 30 dni. Jeżeli dotrzymanie tego terminu nie będzie możliwe, Infor podejmie współpracę z Klientem w celu uzgodnienia wzajemnie akceptowalnego, rozsądnego terminu zakończenia procesu. Wszelka taka dokumentacja stanowi Informacje Poufne Infor. Infor nie będzie uwzględniać ustaleń Klienta wynikających z takiego audytu korespondencyjnego.

2.2. Audyt strony trzeciej

Raz w każdym 12-miesięcznym okresie trwania Okresu Subskrypcji Infor, na własny koszt i własny rachunek, zaangażuje należycie wykwalifikowanego, niezależnego audytora w celu przeprowadzenia przeglądu projektu oraz skuteczności operacyjnej zdefiniowanych celów kontrolnych i działań kontrolnych Infor w związku z Usługami w Chmurze (z wyłączeniem Wsparcia). Infor zapewni sporządzenie przez takiego audytora raportu SOC I Type 2 dla wszystkich Usług w Chmurze oraz, wyłącznie dla wielodostępnych Usług w Chmurze, raportu SOC II Type 2 (dalej łącznie: „Raport z Audytu"). Raport z Audytu stanowi Informacje Poufne Infor, lecz jest dostępny dla Klienta za pośrednictwem Portalu Wsparcia Infor. Klient może udostępnić kopię takiego Raportu z Audytu swoim audytorom i organom regulacyjnym, pod warunkiem poinformowania tych audytorów i organów regulacyjnych, że Raport z Audytu stanowi Informacje Poufne Infor i musi być odpowiednio chroniony.

Ponadto Infor corocznie, na własny koszt i własny rachunek, zaangażuje należycie wykwalifikowanego, niezależnego audytora w celu przeprowadzenia przeglądu bezpieczeństwa informacji w związku z określonymi wielodostępnymi Usługami w Chmurze wskazanymi na trust.infor.com, jak również Wsparciem zarówno dla Oprogramowania Instalowanego Lokalnie, jak i Usług w Chmurze, w każdym

przypadku zgodnie z normą ISO 27001 Międzynarodowej Organizacji Normalizacyjnej. Infor zapewni sporządzenie przez takiego audytora raportu zgodnie z tą normą. Raport z audytu nie będzie dostępny dla Klienta, Klient może jednak w każdym czasie uzyskać kopię wydanego certyfikatu za pośrednictwem strony bezpieczeństwa chmury Infor (trust.infor.com). Certyfikat będzie wskazywać oprogramowanie objęte raportem. W ramach tej certyfikacji ISO 27001 Infor utrzymuje podręcznik Systemu Zarządzania Bezpieczeństwem Informacji dotyczący oprogramowania objętego certyfikacją oraz powiązanego Wsparcia, co pomaga zapewnić ochronę, poufność, integralność i dostępność zasobów Infor wykorzystywanych do świadczenia takich Usług.

Dodatkowe certyfikacje stron trzecich są dostępne na stronie trust.infor.com.

3. Zarządzanie zmianą w odniesieniu do Usług w Chmurze

Infor stosuje proces kontroli zmian regulujący identyfikowanie i wdrażanie zmian w zasobach wykorzystywanych do świadczenia Usług w Chmurze przez Infor, w celu zapobiegania niepożądanym zmianom w kodzie źródłowym Aplikacji, interfejsach, systemach operacyjnych lub zmianom zaplecza dotyczącym danych w istniejących polach i tabelach. Wszystkie zgłaszane zmiany dotyczące zasobów wykorzystywanych do świadczenia Usług w Chmurze przez Infor muszą podlegać procesowi kontroli zmian wdrożeniowych. Infor dokumentuje i przechowuje szczegółową dokumentację potwierdzającą zgodność z tym procesem, taką jak system zgłoszeniowy oraz zapisy procedur testowych dotyczących każdej zmiany, w tym między innymi datę i godzinę każdej takiej zmiany oraz opis jej charakteru.

4. Rozdzielenie Danych; Zakaz wykorzystywania

4.1. Rozdzielenie

Dane są utrzymywane w logicznym odseparowaniu od danych Infor oraz danych innych klientów Infor przy zastosowaniu odpowiednich środków technicznych.

4.2. Zakaz wykorzystywania; Zagregowane Statystyki

Dane stanowią Informacje Poufne Klienta, a Klientowi przysługują wszelkie prawa własności do jego Danych. Infor nie będzie komercyjnie wykorzystywać Danych i nie będzie uzyskiwać dostępu do Danych inaczej niż w zakresie niezbędnym do świadczenia Usług oraz wykonywania swoich zobowiązań zgodnie z Umową.

Infor gromadzi dane statystyczne oraz informacje o wydajności, generowane za pośrednictwem systemów telemetrycznych i rejestrowania zdarzeń, dotyczące korzystania przez Klienta z Usług oraz ich działania (dalej: „Zagregowane Statystyki"). Zagregowane Statystyki stanowią wyłączną własność Infor i nie są uznawane za Dane.

5. Zarządzanie Aktywami

Infor stosuje formalny proces zarządzania aktywami obejmujący utrzymywanie:

i. ewidencji aktywów wykorzystywanych do świadczenia Usług (dalej: „Aktywa"), mającej na celu identyfikację oraz jednoznaczne określenie własności i kontroli nad Aktywami;

ii. procedur mających na celu zarządzanie zwrotem, zniszczeniem lub usunięciem Danych z odpowiednich Aktywów; oraz

iii. procedur mających na celu ochronę Aktywów przed zagrożeniami i podatnościami, zarówno wewnętrznymi, jak i zewnętrznymi, umyślnymi lub przypadkowymi.

6. Skanowanie pod kątem Podatności na zagrożenia i testy penetracyjne

Infor utrzymuje proces zarządzania podatnościami w celu wykrywania ryzyk wynikających z wykorzystania opublikowanych lub zidentyfikowanych wad albo słabości, które mogą zostać wykorzystane (przypadkowo lub umyślnie) i skutkować szkodą lub nieuprawnionym dostępem do Systemów (dalej: „Podatności"). Infor będzie podejmować działania wobec Podatności w terminach zgodnych z powszechnie przyjętymi standardami branżowymi. Infor usunie lub ograniczy skutki Podatności w sposób współmierny do ryzyka, jakie takie Podatności stwarzają, zgodnie z wewnętrznymi zasadami Infor zgodnymi z powszechnie przyjętymi standardami branżowymi.

Co roku Infor angażuje, na własny koszt, niezależny podmiot trzeci do przeprowadzania testów penetracyjnych wielodostępnych Usług w Chmurze, w tym ręcznych testów wykonywanych przez ludzi, w celu oceny mechanizmów bezpieczeństwa Systemów zgodnie z powszechnie przyjętymi standardowymi metodykami branżowymi.

W odniesieniu do wielodostępnego Oprogramowania Subskrypcyjnego oceny testów bezpieczeństwa, w tym skanowanie kodu źródłowego oraz skanowanie Podatności, są przeprowadzane przed wydaniem kodu oraz przez cały cykl życia produktu Usług w Chmurze (tj. w środowiskach deweloperskich i produkcyjnych) w celu identyfikacji potencjalnych Podatności wymagających usunięcia lub ograniczenia skutków. Co roku przeprowadzane są testy penetracyjne wielodostępnych Usług w Chmurze w celu identyfikacji Podatności wymagających usunięcia lub ograniczenia skutków.

7. Reagowanie na Incydenty Bezpieczeństwa Informacji

Jeżeli Infor poweźmie wiadomość, że Dane były lub można zasadnie oczekiwać, że były przedmiotem wykorzystania lub ujawnienia nieautoryzowanego na podstawie Umowy (dalej: „Incydent Bezpieczeństwa Informacji"), Infor: (i) niezwłocznie i bez zbędnej zwłoki (w każdym przypadku nie później niż w terminie 48 godzin od powzięcia wiadomości o takim Incydencie Bezpieczeństwa Informacji) powiadomi Klienta, którego dotyczy dany Incydent Bezpieczeństwa Informacji, o jego wystąpieniu; (ii) przeprowadzi dochodzenie oraz dokona zasadnej analizy przyczyny lub przyczyn takiego Incydentu Bezpieczeństwa Informacji; (iii) będzie przekazywać Klientowi okresowe aktualizacje dotyczące trwającego dochodzenia; (iv) opracuje i wdroży odpowiedni plan usunięcia przyczyny takiego Incydentu Bezpieczeństwa Informacji w zakresie, w jakim przyczyna ta pozostaje pod kontrolą Infor; oraz (v) będzie współpracować przy zasadnym dochodzeniu prowadzonym przez Klienta lub działaniach Klienta mających na celu spełnienie obowiązków notyfikacyjnych lub innych wymogów regulacyjnych mających zastosowanie do takiego Incydentu Bezpieczeństwa Informacji. Na żądanie Klienta oraz na koszt Klienta, w przypadku Incydentu Bezpieczeństwa Informacji, Infor przekaże Klientowi (w zakresie dozwolonym przez prawo i z zastrzeżeniem odpowiednich zabezpieczeń poufności) kopie zapisów aktywności odpowiednich Systemów (wyłącznie w zakresie dotyczącym Incydentu Bezpieczeństwa Informacji odnoszącego się do Klienta) do wykorzystania w postępowaniu sądowym, regulacyjnym lub dochodzeniu prowadzonym przez organ administracji dotyczącym Klienta.

8. Rejestrowanie i monitorowanie

Infor monitoruje zasoby wykorzystywane do świadczenia Usług przy użyciu zestawu narzędzi skonfigurowanych specjalnie do zarządzania dziennikami oraz alertami. Zapisy dzienników są zabezpieczane fizycznie i logicznie w celu zapobiegania manipulacjom. Informacje wrażliwe oraz hasła nie są rejestrowane w żadnych okolicznościach. Oprócz rejestrowania informacji związanych z

Usługami narzędzia monitorujące umożliwiają administratorom śledzenie aktywności użytkowników przy wchodzeniu do Systemu i wychodzeniu z niego.

9. Bezpieczeństwo i szkolenia zasobów ludzkich

Personel Infor świadczący Usługi podlega zobowiązaniom w zakresie poufności, posiada wiedzę dotyczącą zagrożeń i zagadnień związanych z bezpieczeństwem informacji, odbywa ogólne szkolenia z zakresu bezpieczeństwa co najmniej raz w roku oraz jest przygotowany do wspierania organizacyjnych polityk bezpieczeństwa informacji zarówno ogólnie, jak i w ramach swoich konkretnych obowiązków służbowych.

10. Kontrola urządzeń końcowych (laptopów, stanowisk pracy, urządzeń mobilnych Infor)

Infor wdraża środki bezpieczeństwa zgodne z powszechnie przyjętymi praktykami branżowymi w celu ochrony urządzeń końcowych, obejmujące automatyczne zarządzanie poprawkami aplikacji i systemów operacyjnych oraz ochronę antywirusową.

11. Zwrot i zniszczenie Danych

11.1. Zwrot

Po rozwiązaniu lub wygaśnięciu Usług w Chmurze Infor niezwłocznie (w terminie 3-5 Dni Roboczych od otrzymania pisemnego wniosku Klienta złożonego poprzez standardowe zgłoszenie Wsparcia, przy czym wniosek taki musi zostać złożony w terminie 30 dni od rozwiązania (10 dni w przypadku środowiska dedykowanego)) udostępni Klientowi wszystkie Dane Klienta w postaci natywnego eksportu bazy danych przekazanego za pośrednictwem bezpiecznej usługi transferu plików Infor. Jeżeli Klient wymaga zwrotu Danych Klienta w alternatywnym formacie lub potrzebuje innych usług wsparcia związanego z zakończeniem współpracy, Infor i Klient wspólnie uzgodnią zakres takich usług oraz należne opłaty i koszty z tym związane. Przed rozwiązaniem Klient posiada dostęp do Danych Klienta za pośrednictwem interfejsów Aplikacji, a Infor, na żądanie Klienta zgłoszone za pośrednictwem Portalu Wsparcia, zwróci kopie kopii zapasowych danych maksymalnie dwa razy w każdym 12-miesięcznym okresie w postaci natywnego eksportu bazy danych przekazanego za pośrednictwem bezpiecznej usługi transferu plików Infor. Dodatkowe żądania będą podlegały opłatom.

Dla jasności, zwrot lub zniszczenie Danych Osobowych następuje zgodnie z postanowieniami Umowy Powierzenia Przetwarzania Danych.

Dane dotyczące systemów yield management (np. Infor Document Management, Infor EzRMS lub Infor Hospitality Price Optimizer) są usuwane po rozwiązaniu Umowy i nie są przekazywane Klientowi.

11.2. Zniszczenie

Z wyjątkiem usług wsparcia migracyjnego żądanych przez Klienta, Infor trwale zniszczy wszystkie instancje Danych Klienta (online lub dostępne za pośrednictwem sieci) w terminie 35 dni od rozwiązania lub wygaśnięcia Usług w Chmurze zgodnie z normą NIST 800-88.

Dane przekazane Infor na potrzeby świadczenia Wsparcia (tj. poprzez zgłoszenie Wsparcia zarejestrowane w Portalu Wsparcia) są niszczone po upływie pięciu lat od daty zamknięcia zgłoszenia. Imię i nazwisko oraz dane kontaktowe poszczególnych osób po stronie Klienta (np. adres e-mail użytkownika, imię i nazwisko oraz numer telefonu) wykorzystywane do obsługi cyklu życia zgłoszenia Wsparcia są dezaktywowane i anonimizowane po zakończeniu świadczenia Wsparcia.

12. Podwykonawcy

Podwykonawcy Infor dostarczający towary i usługi na rzecz Infor w związku z Usługami Infor świadczą takie towary i usługi na warunkach zasadniczo podobnych do określonych w niniejszym Planie Bezpieczeństwa Informacji. Przed zaangażowaniem takiego podwykonawcy będącego osobą trzecią do świadczenia którejkolwiek z Usług na podstawie niniejszego Planu Bezpieczeństwa Informacji Infor przeprowadzi wobec takiego podmiotu zasadną weryfikację w celu zapewnienia, że podmiot ten będzie w stanie przestrzegać zobowiązań w zakresie poufności i bezpieczeństwa wynikających z niniejszego Planu Bezpieczeństwa Informacji. Infor ponosi odpowiedzialność za wszystkie działania swoich podwykonawców związane ze wspieraniem Usług.

Zastrzeżenie: Następujące produkty mogą podlegać dodatkowym lub odmiennym warunkom bezpieczeństwa: Acumen Invest (Infor Trade Promotions Management) oraz Acumen Radar (Infor Strategic Pricing Management), Anael (SaaS) (Francja); Nexus AppXpress (SaaS), Nexus Live Visibility (SaaS), Nexus Factory Management (SaaS), Nexus Inventory Management (SaaS), Nexus Supply Chain Finance (SaaS), Nexus Supply Collaboration (SaaS), Nexus Transportation Management (SaaS), Nexus Supply Chain Visibility (SaaS), Nexus Procure to Pay (SaaS), Nexus Supply Chain Intelligence (SaaS); BPCS/LX, XA, System 21 (SaaS).

Wersja 1.26