Plán informační bezpečnosti
Příloha k právním předpisům EU

Tato Příloha popisuje závazky společnosti Infor týkající se konkrétních požadavků vyplývajících z platných směrnic, nařízení a vnitrostátních prováděcích právních předpisů EU v oblasti kybernetické bezpečnosti a správy dat („***Platné právní předpisy v oblasti kybernetické bezpečnosti a správy dat***“) a je, pokud se to na Zákazníka vztahuje (s výhradou definice použitelnosti uvedené níže), začleněna do smluv uzavřených mezi Zákazníkem a společností Infor (dále souhrnně jen „***Smlouvy***“). V případě jakéhokoli rozporu nebo nesouladu mezi podmínkami této Přílohy a jakýmikoli jinými podmínkami Smluv v souvislosti s otázkami kybernetické bezpečnosti má přednost tato Příloha.

I. OBECNÉ

1. DEFINICE

1.1 Pojmy psané velkými písmeny, které jsou v této Příloze použity, ale nejsou zde definovány, mají význam stanovený v Plánu informační bezpečnosti, který je k dispozici na adrese www.infor.com/security-plan (dále jen „ISP“). Pojmy „IKT Proces“, „IKT Produkt“, „IKT Služba“, „Incidenty“, „Síťové a informační systémy“, „Riziko“, „Významná kybernetická hrozba“, „Změna“, „Poplatky za změnu poskytovatele“, „Interoperabilita“, „Exportovatelná data“ a „Digitální aktiva“ mají význam, který jim byl přiřazen v platných právních předpisech v oblasti kybernetické bezpečnosti a správy dat.

2. DODRŽOVÁNÍ PŘEDPISŮ A SPOLUPRÁCE

2.1 Společnost Infor bude dodržovat Platné právní předpisy v oblasti kybernetické bezpečnosti a správy dat, které se vztahují na její podnikání, a na základě odůvodněné žádosti bude spolupracovat s jakýmkoli příslušným orgánem veřejné správy a/nebo Zákazníkem, pokud jde o plnění jejích povinností vyplývajících z této Smlouvy s ohledem na Platné právní předpisy v oblasti kybernetické bezpečnosti a správy dat. Společnost Infor i Zákazník jsou povinny informovat a upozornit druhou stranu na jakoukoli významnou změnu nebo událost, potíže, Riziko či informaci, která by mohla mít nepříznivý vliv na IKT Službu nebo plnění této Smlouvy (ledaže by sdílení takových informací bylo zakázáno podle platných právních předpisů).

3. DATUM ÚČINNOSTI

3.1 Ustanovení této Přílohy nabývají účinnosti dnem, kdy vstoupí v platnost a stane se vymahatelným Platný právní předpis v oblasti kybernetické bezpečnosti a správy dat.

4. AKTUALIZACE

4.1 Zákazník bere na vědomí, že technická a organizační bezpečnostní opatření popsaná v této Příloze podléhají aktualizovaným požadavkům vyplývajícím z Platných právních předpisů v oblasti kybernetické bezpečnosti a správy dat, jakož i technickému pokroku a vývoji, a že společnost Infor může tato opatření čas od času aktualizovat nebo upravovat, za předpokladu, že takové aktualizace a úpravy nepovedou ke snížení celkové bezpečnosti služeb poskytovaných Zákazníkovi.

5. ROZHODNÉ PRÁVO

6. Tato Příloha se řídí a uplatňuje v souladu s volbou rozhodného práva stanovenou ve Smlouvě, ledaže by Platné právní předpisy v oblasti kybernetické bezpečnosti a správy dat vyžadovaly jinou volbu rozhodného práva; v takovém případě má pro účely této Přílohy přednost volba rozhodného práva požadovaná těmito předpisy před volbou rozhodného práva uvedenou ve Smlouvě.

7. ODPOVĚDNOST

7.1 Společnost Infor a Zákazník se dohodly, že celková odpovědnost každé ze stran a jejích přidružených společností (jak jsou definovány ve Smlouvách) vyplývající z této Přílohy nebo s ní související, ať již na základě porušení smlouvy, deliktu či z jiného důvodu, podléhá ve vztahu mezi stranami (včetně Přidružených společností) příslušným ustanovením o omezení odpovědnosti obsaženým ve Smlouvách. Společnost Infor dále nenese odpovědnost za jakékoli porušení Platných právních předpisů v oblasti kybernetické bezpečnosti a správy dat ze strany Zákazníka ani za nesplnění požadavků příslušného orgánu ze strany Zákazníka.

II. SMĚRNICE NIS 2

1. PŮSOBNOST A DEFINICE

1.1 Podmínky uvedené v oddíle II této Přílohy se vztahují výhradně na zákazníky z EU, kteří splňují kritéria a prahové hodnoty pro „důležité“ nebo „základní“ subjekty, na něž se vztahuje směrnice NIS 2. Pro vyloučení pochybností se oddíl I považuje za součást tohoto oddílu II.

1.2 „**Směrnice NIS 2**“ znamená směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148, jakož i veškeré odpovídající prováděcí předpisy.

2. SPRÁVA A ŘÍZENÍ

2.1 Společnost Infor má v rámci svého bezpečnostního útvaru řídící orgány, které schvalují a dohlížejí na provádění opatření společnosti Infor v oblasti řízení kybernetických rizik a nesou za ně odpovědnost, včetně Plánu informační bezpečnosti (ISP).

3. PROGRAM INFORMAČNÍ BEZPEČNOSTI

3.1 Společnost Infor zavedla a bude udržovat ISP tak, aby: (A) byla navržena tak, aby: (1) zajišťovala bezpečnost a důvěrnost Síťových a informačních systémů společnosti Infor; (2) chránil před jakýmikoli předpokládanými hrozbami nebo riziky pro bezpečnost nebo integritu Síťových a informačních systémů společnosti Infor; a (3) chránil před neoprávněným přístupem k Síti a informačním systémům nebo jejich neoprávněným používáním; a (B) stanovil zásady společnosti Infor pro reakci na jakýkoli Incident.

3.2 ISP je k dispozici na adrese: www.infor.com/security-plan.

4. OPATŘENÍ K ŘÍZENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH RIZIK

4.1 Společnost Infor zavedla a bude udržovat opatření k řízení kybernetických bezpečnostních rizik, která:

(A) jsou přiměřené Rizikům, jimž jsou Síťové a informační systémy společnosti Infor vystaveny, s přihlédnutím k nejmodernějším technologiím a případně k příslušným evropským a mezinárodním normám, jakož i k nákladům na jejich zavedení;

(B) vycházejí z přístupu zohledňujícího všechna možná rizika, jehož cílem je chránit Síťové a informační systémy společnosti Infor a fyzické prostředí těchto systémů před Incidenty; a

(C) zahrnují alespoň následující: (a) zásady týkající se analýzy Rizik a bezpečnosti informačních systémů; (b) opatření k identifikaci jakýchkoli Rizik Incidentů, včetně postupů pro řešení Incidentů; (c) zajištění kontinuity provozu, jako je správa záloh a obnova po havárii, a krizové řízení; (d) bezpečnost dodavatelského řetězce, včetně bezpečnostních aspektů týkajících se vztahů mezi společností Infor a jejími přímými dodavateli nebo poskytovateli služeb; (e) bezpečnost při pořizování, vývoji a údržbě Síťových a informačních systémů, včetně řešení zranitelností a jejich zveřejňování; (f) zásady a postupy pro posuzování účinnosti Opatření k řízení kybernetických bezpečnostních rizik společnosti Infor; (g) základní postupy kybernetické hygieny, jako jsou zásady nulové důvěry, aktualizace softwaru, konfigurace zařízení, segmentace sítě, správa identit a přístupů nebo informovanost uživatelů, pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti a zvyšování povědomí o kybernetických hrozbách, phishingu nebo technikách sociálního inženýrství; (h) zásady a postupy týkající se používání kryptografie a šifrování; (i) bezpečnost lidských zdrojů, zásady řízení přístupu a správa aktiv; a (j) používání řešení pro vícefaktorovou autentizaci nebo nepřetržitou autentizaci, zabezpečenou hlasovou, video a textovou komunikaci a zabezpečené systémy nouzové komunikace v rámci společnosti Infor.

5. DODAVATELSKÝ ŘETĚZEC

5.1 Společnost Infor prohlašuje a zaručuje, že opatření k zajištění bezpečnosti dodavatelského řetězce, která zavedla, zohledňují následující kritéria: (a) zranitelnosti specifické pro každého přímého dodavatele a poskytovatele služeb společnosti Infor; (b) celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti dodavatelů a poskytovatelů služeb společnosti Infor, včetně jejich postupů pro bezpečný vývoj; a případně (c) výsledky

jakýchkoli koordinovaných posouzení bezpečnostních rizik konkrétních kritických dodavatelských řetězců IKT Služeb, IKT Produktů nebo IKT Procesů provedených členskými státy EU a jakýmkoli příslušným orgánem.

5.2 Společnost Infor provádí u svých externích poskytovatelů služeb hloubkovou prověrku s cílem posoudit jejich opatření k řízení kybernetických bezpečnostních rizik a uzavírá s těmito externími poskytovateli služeb smlouvy, které obsahují požadavky na kybernetickou bezpečnost a správu dat v podstatě shodné s požadavky uvedenými v této Příloze.

5.3 Společnost Infor předloží přiměřené důkazy o těchto bezpečnostních opatřeních v dodavatelském řetězci v přiměřené lhůtě po obdržení žádosti Zákazníka.

6. REAKCE NA INCIDENTY

6.1 Společnost Infor bude sledovat své Síťové a informační systémy z hlediska neoprávněného přístupu a zavede zásady pro reakci na Incidenty, které stanoví opatření, jež je třeba přijmout, jakmile společnost Infor zjistí nebo se dozví o jakémkoli Incidentu.

6.2 Pokud se společnost Infor dozví o významném incidentu, který má dopad na Zákazníka, je povinna:

(A) Informuje Zákazníka následovně:

(1) Neprodleně a bez zbytečného odkladu (a v každém případě do 24 hodin od zjištění takového Významného incidentu) (a) informuje Zákazníka o výskytu takové Významné incidentu; a (b) poskytněte Zákazníkovi podrobné informace o Významné incidentu, včetně těchto informací: (i) zda existuje podezření, že Významný incident byl způsoben protiprávním nebo zlovolným jednáním nebo zda by mohl mít přeshraniční dopad; (ii) veškeré informace k určení případného přeshraničního dopadu Významného incidentu; a (iii) počáteční posouzení Významného incidentu, včetně jeho závažnosti a dopadu, jakož i, jsou-li k dispozici, indikátory narušení;

(2) Neprodleně a bez zbytečného odkladu poskytne Zákazníkovi následující doplňující informace o Významném incidentu: (a) podrobný popis Významného incidentu, včetně jeho závažnosti a dopadu; (b) typ hrozby nebo základní příčinu, která pravděpodobně vyvolala Významný incident; (c) přijatá a probíhající opatření ke zmírnění dopadů; a (d) v příslušných případech přeshraniční dopad Významného incidentu.

(B) Prošetřit a provést přiměřenou analýzu příčiny (příčin) takového významného incidentu;

(C) Pravidelně informovat Zákazníka o průběhu jakéhokoli probíhajícího šetření;

(D) Vypracovat a zavést vhodný plán ke zmírnění a odstranění příčiny takového Významného incidentu v rozsahu, v jakém je tato příčina v moci společnosti Infor; a

(E) Spolupracovat s Zákazníkem při jeho přiměřeném vyšetřování a při jeho snahách o splnění jakýchkoli oznamovacích povinností vztahujících se k takovému Významnému incidentu, včetně pomoci při vypracování jakékoli zprávy o Významném incidentu pro příslušné orgány.

6.3 Pokud se společnost Infor dozví o Významné kybernetické hrozbě, která má dopad na Zákazníka (včetně zveřejněných zranitelností aplikací Infor, které splňují definici Významné kybernetické hrozby), je povinna:

(A) Neprodleně a bez zbytečného odkladu informovat Zákazníka o takové Významné kybernetické hrozbě;

(B) Poskytnout Zákazníkovi podrobné informace o dopadu významné kybernetické hrozby na Zákazníka, jak je společnosti Infor znám;

(C) Prošetřit a provést přiměřenou analýzu příčin takové Významné kybernetické hrozby;

(D) Vypracovat a implementovat vhodný plán k nápravě příčiny takové Významné kybernetické hrozby v rozsahu, v jakém se taková Významná kybernetická hrozba projeví a její příčina je v rámci kontroly společnosti Infor; a

(E) Vyhovět přiměřeným požadavkům Zákazníka na poskytnutí informací o Významné kybernetické hrozbě, které Zákazník použije ve svých povinných oznámeních třetím stranám souvisejících s Významnou

kybernetickou hrozbou, pokud jsou takové oznámení vyžadovány podle Platných právních předpisů v oblasti kybernetické bezpečnosti a správy dat.

7. AUDIT

7.1 Společnost Infor musí být držitelem a udržovat v platnosti alespoň jednu z následujících certifikací a osvědčení týkajících se jejích Cloudových služeb (podle okolností) a na písemnou žádost Zákazníka mu předloží doklad o těchto certifikacích a/nebo osvědčeních:

(1) SSAE SOC 2 Type 2 (známý také jako AICPA TSC 2014 typu 2)
(2) ISO 27001:2022
(3) FedRAMP

Společnost Infor zajistí, aby její externí poskytovatelé služeb disponovali nebo udržovali alespoň jednu z výše uvedených certifikací a osvědčení týkajících se služeb, které tito externí poskytovatelé služeb poskytují společnosti Infor a/nebo zákazníkům společnosti Infor, nebo aby předložili uspokojivý alternativní důkaz o svých opatřeních k řízení kybernetických bezpečnostních rizik v souvislosti s rozsahem poskytovaných služeb.

7.2 Kromě auditních zpráv popsaných v bodě 7.1 výše, na žádost Zákazníka a s výhradou povinností mlčenlivosti vyplývajících ze Smluv, a to nejvýše jednou ročně, ledaže by Zákazník jednal na základě žádosti příslušného orgánu veřejné moci (v takovém případě se roční omezení neuplatní), společnost Infor neprodleně písemně odpoví na jakékoli přiměřené dotazy nebo dotazníky od Zákazníka (a/nebo jeho zástupců) týkající se obsahu bezpečnostního programu společnosti Infor a poskytne přiměřené důkazy o jeho souladu s požadavky této Přílohy, včetně obecně dostupných kopií dat, dokumentů a informací souvisejících se službami, které jsou nezbytné k tomu, aby Zákazníkovi pomohly při plnění jakékoli závazné žádosti nebo příkazu obdrženého od jakéhokoli příslušného orgánu veřejné moci. Společnost Infor poskytne příslušné informace bez zbytečného odkladu (a v každém případě ve lhůtě stanovené v závazné žádosti nebo příkazu, který Zákazník obdržel od příslušného orgánu veřejné správy).

7.3 Zákazník může jednou ročně provést audit dodržování povinností společnosti Infor vyplývajících z této Přílohy, včetně auditu postupů společnosti Infor v oblasti IT bezpečnosti a příslušných kontrolních prostředí, v souladu s postupem popsaným v tomto oddíle 7, a to pouze za předpokladu, že:

(A) společnost Infor neposkytla dostatečné důkazy o dodržování opatření k řízení kybernetických bezpečnostních rizik popsaných v této Příloze prostřednictvím zpráv a dokumentace uvedených v bodě 7.2 výše nebo, je-li to relevantní, prostřednictvím jakýchkoli jiných auditních zpráv nebo jiných informací, které společnost Infor obecně zpřístupňuje svým Zákazníkům;

(B) došlo k Významnému incidentu;

(C) společnost Infor informovala Zákazníka, že je předmětem žádosti vládního orgánu o přístup k údajům Zákazníka;

(D) O audit formálně požádal příslušný orgán veřejné moci s jurisdikcí nad Zákazníkem; nebo

(E) Platné právní předpisy v oblasti kybernetické bezpečnosti a správy dat přiznávají Zákazníkovi přímé právo na audit.

7.4 Před zahájením auditu se Zákazník a společnost Infor vzájemně dohodnou na rozsahu, termínu, délce trvání, kontrolních postupech a požadavcích na předkládání důkazů. Zákazník může k provedení auditu ve svém zastoupení využít nezávislou akreditovanou externí auditorskou společnost, za předpokladu, že se na této externí auditorské společnosti Zákazník a společnost Infor vzájemně dohodnou (což nezahrnuje žádné externí auditory, kteří jsou buď konkurenty společnosti Infor, nebo nejsou dostatečně kvalifikovaní či nezávislí). Zákazník souhlasí s tím, že audit bude proveden bez nepřiměřeného narušení obchodních činností společnosti Infor (nebo jejích subdodavatelů), během běžných pracovních hodin s přiměřeným předběžným oznámením a v souladu s platnými bezpečnostními zásadami a postupy pro zachování důvěrnosti společnosti Infor (nebo jejích subdodavatelů). V případě, že nejsou povoleny audity fyzických datových center, systémů nebo zařízení na místě, bude společnost Infor spolupracovat se Zákazníkem (a případně s jeho subdodavateli) na dosažení vzájemně přijatelného řešení, které bude dostatečné k poskytnutí informací nezbytných pro to, aby Zákazník splnil požadavky na audit podle Platných právních předpisů v oblasti kybernetické bezpečnosti a správy dat. Zákazník ani auditor nebudou mít přístup k žádným údajům od jiných zákazníků společnosti Infor ani k systémům nebo zařízením společnosti Infor, které se netýkají služeb poskytovaných Zákazníkovi. Zákazník poskytne společnosti Infor výsledky jakéhokoli

auditu. Strany se vzájemně dohodnou na příslušných zprávách nebo nápravných opatřeních. Společnost Infor vynaloží obchodně přiměřené úsilí k provedení dohodnutých nápravných opatření.

7.5 Zákazník nese veškeré náklady a poplatky spojené s auditem, včetně všech přiměřených nákladů a poplatků, které společnosti Infor v souvislosti s auditem vzniknou, a veškerých nákladů a poplatků, které společnosti Infor vzniknou v souvislosti s případným zapojením subdodavatele do auditu, ledaže by takový audit odhalil podstatné porušení této Přílohy ze strany společnosti Infor; v takovém případě ponese společnost Infor vlastní náklady na tu část auditu, která se týká daného porušení.

III. DORA

1. PŮSOBNOST A DEFINICIE

1.1 Podmínky uvedené v oddíle III této Přílohy se vztahují výhradně na zákazníky z EU, kteří splňují kritéria a prahové hodnoty pro finanční subjekty podléhající regulaci podle nařízení DORA. Pro vyloučení pochybností se oddíl I považuje za součást tohoto oddílu III; konkrétní odstavce oddílu II se rovněž použijí, pokud je na ně v tomto oddílu III výslovně odkazováno.

1.2 "**DORA**" znamená nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru.

2. SLUŽBY

2.1 IKT Služby poskytované společností Infor Zákazníkovi jsou popsány ve Smlouvách.

3. MÍSTO

3.1 Pro vyloučení pochybností se uvádí, že produkční data Zákazníka jsou uložena ve zvoleném místě nasazení a společnost Infor nepřesune žádná produkční data Zákazníka mimo toto místo bez předchozího písemného souhlasu a pokynu Zákazníka. Na pokyn Zákazníka může být k omezenému množství osobních údajů přistupováno vzdáleně z místa mimo vybrané místo nasazení za účelem poskytování podpory a služeb Zákazníkovi. Společnost Infor předem informuje Zákazníka, pokud plánuje změnu míst (tj. regionů nebo zemí), kde budou služby poskytovány a kde budou data Zákazníka ukládána a zpracovávána, jak je stanoveno ve Smlouvě.

4. BEZPEČNOSTNÍ PROGRAM A SMLOUVY O ÚROVNI SLUŽEB (SLA)

4.1 Platí opatření k řízení kybernetických bezpečnostních rizik popsaná výše v oddílech II.3 a II.4. Platí rovněž závazky společnosti Infor týkající se reakce na incidenty uvedené v oddílu II.6. Pro vyloučení pochybností se má za to, že případ insolvence společnosti Infor představuje dodatečnou povinnost k vrácení dat Zákazníka v rámci ISP.

4.2 Závazky společnosti Infor týkající se dostupnosti služeb jsou popsány ve Smlouvě o úrovni služeb na adrese https://www.infor.com/service-level-description („SLA"). Závazky týkající se podpory konkrétních produktů jsou popsány v Objednávkovém formuláři, je-li to relevantní.

5. ŠKOLENÍ A OSVĚTOVÉ PROGRAMY V OBLASTI BEZPEČNOSTI INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

5.1 Pokud bude společnost Infor v rámci Služeb přistupovat k lokálním síťovým a informačním systémům Zákazníka, může Zákazník po včasném oznámení požádat společnost Infor, aby se zúčastnila jakéhokoli vhodného programu zvyšování povědomí o bezpečnosti ICT a/nebo školení v oblasti digitální provozní odolnosti, které Zákazník poskytuje nebo organizuje v souvislosti se svou podnikatelskou činností („Školení"). V této souvislosti se strany dohodly, že:

(A) Četnost, načasování a délka trvání takového školení budou předem dohodnuty stranami;

(B) Společnost Infor si vyhrazuje právo požadovat od Zákazníka úhradu svých přiměřených a řádně vynaložených výdajů; a

(C) Účast společnosti Infor na takovém školení nebude vyžadovat, aby společnost Infor činila cokoli, co by mohlo narušit, zabránit nebo bránit společnosti Infor v poskytování IKT Služeb nebo v plnění jejích povinností vyplývajících z této Smlouvy.

6. UKONČENÍ

6.1 Kromě práv na výpověď stanovených ve Smlouvě a jinde v těchto smluvních podmínkách může Zákazník v souladu s čl. 28 odst. 7 nařízení DORA a s výhradou postupu pro výpověď uvedeného ve Smlouvě vypovědět Smlouvu zcela nebo zčásti výhradně v následujících případech: (i) pokud společnost Infor nenapravila významné porušení Platných právních předpisů v oblasti kybernetické bezpečnosti a správy dat nebo této Přílohy, (ii) pokud Zákazník zjistí okolnosti, které by mohly ovlivnit poskytování IKT Služeb společností Infor, včetně podstatných změn, které mají dopad na Smlouvy nebo situaci společnosti Infor, (iii) pokud budou zjištěny prokázané slabiny týkající se celkového řízení IKT rizik společnosti Infor, a to zejména ve způsobu, jakým společnost Infor zajišťuje dostupnost, autentičnost, integritu a důvěrnost dat, ať už se jedná o osobní údaje, jinak citlivá data nebo neosobní údaje, nebo (iv) pokud příslušný orgán veřejné moci již nemůže účinně dohlížet na Zákazníka v důsledku podmínek nebo okolností souvisejících se společností Infor nebo Smlouvami.

7. JEDNÁNÍ S PŘÍSLUŠNÝMI ORGÁNY VEŘEJNÉ MOCI

7.1 Společnost Infor bude plně spolupracovat s příslušnými orgány veřejné moci a orgány pro řešení sporů Zákazníka, včetně osob jimi jmenovaných.

IV. DATA ACT

1. PŮSOBNOST A DEFINICE

1.1 Podmínky uvedené v oddíle IV této Přílohy se vztahují výhradně na Zákazníky z EU a to v rozsahu, v jakém společnost Infor splňuje kritéria a prahové hodnoty pro poskytovatele služeb zpracování údajů podle Data Actu. Pro vyloučení pochybností se má za to, že oddíl I je součástí tohoto oddílu IV; konkrétní odstavce oddílu II se rovněž použijí, pokud je na ně v tomto oddílu IV výslovně odkazováno.

1.2 "**Data Act**" znamená nařízení Evropského parlamentu a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828.

2. PŘÍSTUP ZÁKAZNÍKŮ K ÚDAJŮM

2.1 ISP popsaný v bodě II.3 výše stanoví podmínky, za nichž má zákazník po celou dobu trvání smlouvy přístup k Zákaznickým datům, jakož i podmínky pro vrácení a zničení Zákaznických dat v případě ukončení nebo vypršení platnosti Cloudových služeb.

3. PROCES ZMĚNY

3.1 Jak je popsáno v této Příloze, může Zákazník přejít na službu zpracování dat nabízenou jiným poskytovatelem služeb zpracování dat nebo přenést Zákaznická data do lokální IKT infrastruktury, a to v souladu se specifickým postupem společnosti Infor („Postup při změně poskytovatele"), za předpokladu, že Zákazník:

(A) Doručí společnosti Infor písemnou výpověď s minimálně dvouměsíční (2) výpovědní lhůtou v souladu s postupy pro výpověď stanovenými ve Smlouvě;

(B) Uzavře se společností Infor vzájemně přijatelnou smlouvu o přechodových službách obsahující níže popsané informace; a

(C) Uhradí všechny příslušné poplatky (definované níže).

3.2 Smlouva o přechodných službách stanoví:

(A) Zda Zákazník požaduje (i) export svých Zákaznických dat a jejich přesun k určenému alternativnímu poskytovateli, (ii) export svých Zákaznických dat a jejich přesun z cloudu do lokálního prostředí, nebo (iii) vymazání svých Zákaznických dat;

(B) Kategorie Zákaznických dat, která lze během Procesu změny přenést, a kategorie dat, která jsou z Změny vyňata z důvodu rizika porušení obchodního tajemství, je-li to relevantní.

(C) Platné lhůty pro dokončení Změny, včetně lhůt pro získání dat po skončení přechodného období dohodnutého mezi stranami;

(D) Jakákoli technická nebo proveditelnostní omezení týkající se Změny, včetně podrobností o Interoperabilitě, pokud jsou dostupné, jak je poskytla společnost Infor;

(E) Platné poplatky za Změnu, které zahrnují:

(1) plnou částku zbývající k zaplacení společnosti Infor za celé aktuální období předplatného stanovené v příslušném Objednávkovém formuláři (tato částka je samostatná a nepovažuje se za „Poplatek za změnu poskytovatele“); a

(2) Poplatky za změnu poskytovatele, v rozsahu povoleném platnými právními předpisy; a

(F) Veškerou dodatečnou dokumentaci, kterou je třeba, aby Zákazník podepsal, jako je například nová licenční smlouva na lokální software, která nahradí Smlouva o poskytování cloudových služeb, pokud zákazník provádí změnu popsanou v bodě IV.3.2(A)(ii) výše.

3.3 Během procesu Změny je společnost Infor povinna:

(A) Zachovat stejnou úroveň zabezpečení, jaká je popsána v příslušném ISP;

(B) Jednat s náležitou péčí s cílem zajistit kontinuitu podnikání a pokračovat v poskytování Cloudových služeb v souladu se Smlouvou uzavřenou se Zákazníkem; a

(C) Poskytovat Zákazníkovi (a dalším třetím stranám pověřeným Zákazníkem, které jsou vázány písemnými nebo profesními povinnostmi mlčenlivosti) přiměřenou pomoc, včetně přiměřené podpory strategie odchodu Zákazníka, a to zajištěním transparentnosti a poskytováním obecně dostupných informací na vyžádání, které jsou relevantní pro proces Změny, včetně informací týkajících se Interoperability exportovaných Zákaznických dat. Bez ohledu na výše uvedené není společnost Infor povinna sdílet informace nebo poskytovat pomoc Zákazníkovi (nebo jiným třetím stranám), které představují riziko pro duševní vlastnictví společnosti Infor, obchodní tajemství nebo by společnosti Infor způsobily ekonomickou újmu.

3.4 Zákazník odpovídá za import a implementaci Zákaznických dat do svých vlastních systémů nebo do systémů Cílového poskytovatele služeb, podle toho, co je relevantní.

3.5 V souladu s Data Act mohou smluvní strany prodloužit lhůty stanovené ve smlouvě o přechodných službách.

3.6 Jakmile bude Proces změny dokončen (nebo po uplynutí dvouměsíční výpovědní lhůty, pokud si Zákazník nepřeje přejít k jinému poskytovateli, ale místo toho chce, aby byly jeho Zákaznická data po ukončení služby smazána), považují se příslušné Objednávkové formuláře a všechny Smlouvy se Zákazníkem za ukončené.

3.7 Společnost Infor a Zákazník (a případně jím určený náhradní poskytovatel) budou v dobré víře spolupracovat s cílem zajistit hladký průběh Procesu změny, umožnit včasný přenos Zákaznických dat a zachovat kontinuitu služby zpracování dat.

3.8 Společnost Infor není povinna nabídnout Proces změny u:

(A) Neprodukčních prostředí využívaných k testovacím a hodnotícím účelům a po omezenou dobu;

(B) Služeb, u nichž by změna byla velmi složitá nebo nákladná, nebo u nichž není možné provést změnu bez významného zásahu do Zákaznických dat nebo Architektury služby; a/nebo

(C) Služby, u nichž byla většina hlavních funkcí vytvořena na míru tak, aby vyhovovala specifickým potřebám jednotlivého zákazníka, nebo u nichž byly všechny komponenty vyvinuty pro účely

jednotlivého zákazníka, a kde tyto služby zpracování dat nejsou nabízeny v širokém komerčním měřítku prostřednictvím katalogu služeb poskytovatele služeb zpracování dat.

3.9 Společnost Infor není povinna vyvíjet nové technologie nebo služby, ani sdělovat či předávat digitální aktiva, která jsou chráněna právy duševního vlastnictví nebo která představují obchodní tajemství, zákazníkovi či jinému poskytovateli služeb zpracování dat, ani ohrozit bezpečnost a integritu služeb zákazníka či společnosti Infor.

3.10 **ODPOVĚDNOST A ODŠKODNĚNÍ**

3.11 K nákupu nebo využívání Služeb na základě těchto Smluv může být oprávněno několik právnických osob (mimo jiné včetně Přidružených společností Zákazníka a Autorizovaných uživatelů), a proto by se žádost o Změnu poskytovatele mohla v souladu s tímto oddílem dotknout i jiných subjektů než Zákazníka, který žádost podává („Dotčené strany“). Je výhradní odpovědností Zákazníka zajistit, aby měl všechna práva a oprávnění týkající se žádostí o Změnu poskytovatele a Zákaznických dat, než uplatní svá práva podle těchto Smluv.

3.12 Zákazník bude bránit společnost Infor, odškodní ji a zbaví ji odpovědnosti za veškeré ztráty, náklady a výdaje v rozsahu, v jakém vyplývají z jakéhokoli nároku, požadavku, žaloby nebo řízení vzneseného či zahájeného proti společnosti Infor Dotčenými stranami, které tvrdí, že žádost o Změnu poskytovatele porušuje práva nebo licence takové Dotčené strany, za předpokladu, že společnost Infor (A) neprodleně písemně informuje Zákazníka o takovém nároku vzneseném proti společnosti Infor, (B) poskytne Zákazníkovi výhradní kontrolu nad obhajobou a urovnáním takového nároku vůči společnosti Infor (s výjimkou toho, že Zákazník nesmí žádný takový nárok vůči společnosti Infor urovnat, pokud bezpodmínečně nezbaví společnost Infor veškeré odpovědnosti a nevyžaduje, aby společnost Infor zaplatila peníze nebo přiznala vinu) a (C) poskytne Zákazníkovi veškerou přiměřenou pomoc na náklady Zákazníka. Výše uvedené povinnosti týkající se obhajoby a odškodnění se nevztahují na případy, kdy takový nárok vůči společnosti Infor vyplývá z porušení Smlouvy ze strany společnosti Infor, včetně této Přílohy a/nebo příslušných Objednávkových formulářů.

3.13 Společnost Infor nenese odpovědnost za žádné škody, ztráty, náklady ani výdaje vyplývající z Žádosti o změnu nebo s ní související. Toto vyloučení odpovědnosti zahrnuje mimo jiné jakékoli problémy týkající se integrity nebo ztráty Zákaznických dat, výpadky systému, problémy s kompatibilitou nebo jakékoli jiné poruchy či selhání, k nimž může dojít v průběhu Žádosti o Změnu nebo v jejím důsledku. Zákazník přebírá plnou odpovědnost za úspěšný převod Zákaznických dat.

3.14 Pro jasnost se žádná ustanovení této části IV nevztahují na zproštění ani omezení povinnosti Zákazníka uhradit veškeré poplatky splatné na základě těchto Smluv a/nebo jakéhokoli Objednávkového formuláře za celé aktuální Období předplatného stanovené v příslušném Objednávkovém formuláři (formulářích). Pokud se Zákazník rozhodne provést Změnu před koncem aktuálního Období předplatného příslušného Objednávkového formuláře (formulářů), bere na vědomí a souhlasí s tím, že za žádných okolností mu taková Změna nezakládá nárok na vrácení jakýchkoli poplatků dříve zaplacených podle příslušné Smlouvy a/nebo Objednávkového formuláře.

4. ŽÁDOSTI ORGÁNŮ VEŘEJNÉ MOCI O PŘÍSTUP K INFORMACÍM

4.1 V případě, že společnost Infor obdrží od orgánu veřejné moci jakoukoli právně závaznou žádost o poskytnutí neosobních údajů Zákazníka z EU, jehož služby jsou hostovány v EU, nebo jakoukoli žádost orgánu veřejné moci o přímý přístup k neosobním údajům Zákazníka z EU, jehož služby jsou hostovány v EU, pokusí se společnost Infor v rámci zákonných možností takovou žádost přesměrovat na Zákazníka. Pokud společnost Infor nemůže žádost přesměrovat na Zákazníka, pak (i) žádost zamítne, pokud to nevyžaduje zákon, (ii) napadne takové žádosti, pokud jsou v rozporu s platnými zákony, jsou příliš široké nebo se na ně vztahuje jiná příslušná námitka, (iii) neprodleně informuje Zákazníka a poskytne mu kopii žádosti, pokud to není zákonem zakázáno, (iv) pokud k tomu bude donucena, zveřejní pouze minimální množství neosobních údajů Zákazníka z EU hostovaného v EU, které je nezbytné k uspokojení žádosti, a (v) pokud to umožňují zákony země určení, na písemnou žádost Zákazníka (nejvýše jednou ročně po dobu trvání Smluv) poskytne Zákazníkovi co nejvíce relevantních informací o obdržených žádostech o zveřejnění. Pro vyloučení pochybností se žádosti vládních orgánů o přístup k osobním údajům řídí samostatně na základě Smlouvy o zpracování údajů („DPA“) uzavřené mezi stranami.