Název dokumentu:	**SMĚRNICE Bezpečnost počítačové sítě a ochrana osobních údajů**
Garant dokumentu:	Jaroslav Otcovský
Seznam příloh:	Příloha č. 1 – G2S GDPR info sheet
Změny v dokumentu:	Verze 2.0

OBSAH:

1 ÚČEL

Tato směrnice popisuje pravidla a postupy, jejichž dodržování zajišťuje bezpečnost počítačové sítě společnosti NZ SERVIS, spol. s r.o. (dále jen „NZS“) a ochranu dat a osobních údajů v této síti, stejně jako ochranu počítačových sítí a osobních dat zákazníků, se kterými pracovníci NZS mohou pracovat při zajišťování podpory zákazníků, kteří používají její produkty.

Zajišťuje splnění povinností vyplývajících zejména ze zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění a Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů; známé pod označením „GDPR“).

Směrnice zároveň popisuje i rozsah školení pracovníků NZS (dále jen „Pracovník NZS“), která jsou nezbytná pro zajištění potřebných znalostí Pracovníků NZS, aktualizaci takových znalostí, jejich ověřování a evidenci.

2 PLATNOST

Tato směrnice je součástí směrnicové základny NZS a je závazná pro všechny Pracovníky NZS.

3 POUŽITÉ ZKRATKY A POJMY

3.1 Zkratky

NZS – Společnost NZ SERVIS, spol. s r.o., IČ: 25637151

VPN – Virtual private network – zabezpečení přístupu a komunikace mezi počítačovými sítěmi

DB – Databáze NZS nebo zákazníka

VIS – Vnitřní informační systém NZS

TO – Technické oddělení NZS

Pracovník NZS – Zaměstnanec/pracovník NZS nebo osoba řádně pověřená ze strany NZS (konzultant, programátor, technik apod.)

3.2 Pojmy

Helpdesk – systém zajišťující evidenci požadavků Pracovníků NZS na podporu počítačové sítě

CLOUD – provozování IS bez nutnosti zajištění a provozu vlastního HW a SW (např. pomocí služby ERPORT nebo Microsoft Azure)…

4 VZDÁLENÝ PŘÍSTUP K ZÁKAZNÍKŮM A PRÁCE S DB ZÁKAZNÍKŮ

4.1 Vzdálený přístup

Vzdálený přístup do počítačové sítě zákazníka je nezbytným předpokladem včasného řešení požadavků zákazníků týkajících se problémů a chyb v produktech NZS. Rychlost odezvy na takové požadavky zákazníků je smluvně definována a stanovené lhůty často znemožňují řešení požadavků osobní návštěvou u zákazníka.

Z důvodu zajištění bezpečnosti počítačových sítí, dat i osobních údajů je nutné definovat možné způsoby připojení a není možné akceptovat všechny možnosti přístupu používané zákazníky – je nutné dodržovat následující pravidla postupy.

Je v zájmu zákazníka jakožto správce osobních údajů mít ještě před realizací vzdáleného přístupu uzavřenu s NZS smlouvu o zpracování osobních údajů. NZS v tomto směru poskytuje zákazníkům podporu formou distribuce vzorového dokumentu „Smlouva o zpracování osobních údajů a Smlouva o podmínkách Sdílení dat“, viz gdpr_smlouva_o_zpracovani_osobnich_udaj_s179 (odkaz přístupný Pracovníkům NZS)

Pro vzdálený přístup je možné využít pouze jeden z dále definovaných způsobů přístupu – jiný způsob připojení je možný pouze ze závažných důvodů zákazníka akceptovaných NZS

- Každý Pracovník NZS musí mít unikátní přístupové údaje, které není povoleno sdílet s kolegy
- Pracovník NZS smí provádět na serverech zákazníka pouze činnosti přímo související s účelem zřízení vzdáleného přístupu

4.1.1 Přístup pomocí TeamViewer – upřednostňovaný způsob přístupu!

Pro vzdálený přístup NZS do počítačové sítě zákazníka je přednostně používán software TeamViewer.

V aplikaci TeamViewer je připojení plně řízeno zákazníkem a zákazník v reálném čase vidí, jakou činnost Pracovník NZS na jeho PC vykonává. Zároveň TeamViewer obsahuje vlastní logování připojení – záznamy o tom, kdo a kdy.

Vzhledem k možnosti záznamu veškerých aktivit Pracovníka NZS v počítačové síti zákazníka a možnosti využití nejen v součinnosti se zákazníkem (přístup musí být zákazníkem povolen a může být i kdykoliv ukončen), ale i bezobslužný přístup (zákazník povolí přístup do svojí sítě a předá přístupové informace - důležité při požadavku zákazníka na zásah mimo pracovní dobu zákazníka, a tedy bez jeho součinnosti v době přístupu) je tento způsob NZS upřednostňován a nabízen zákazníkovi jako doporučení NZS.

Tento způsob přístupu může být použit i při požadavku zákazníka na jiný způsob přístupu (např. pomocí VPN, Terminálový přístup apod).

Bezpečnost použití TeamViewer je následující:

- Šifrování – TeamViewer pracuje s šifrováním 2048 RSA založeným na výměně veřejných a soukromých klíčů a šifrováním relací AES (256 bitů). Tato technika je založena na stejných standardech jako https/SSL a splňuje aktuální bezpečnostní normy. Výměna klíčů také zabezpečuje plnou ochranu údajů mezi klienty. To znamená, že ani směrovací servery NZS nemohou datový proud přečíst.

- Zabezpečení přístupu – Kromě automaticky vytvářené dynamické identifikace Partner ID vytváří TeamViewer heslo relace, které je při každém spuštění programu jiné, aby tak poskytoval další zabezpečení proti neoprávněnému přístupu do systému. Další funkce související se zabezpečením (např. přenos souborů) vyžadují další, manuální potvrzení od vzdáleného partnera. Není možné ovládat počítač zákazníka „neviditelně“. Z důvodu ochrany údajů uložených na vzdáleném počítači musí být uživatel vzdáleného počítače informován o pokusu o přístup.

Zodpovědnosti při konfiguraci připojení:

- Ve fázi zřizování přístupu se zavazují obě strany (NZS i zákazník) spolupracovat a bez zbytečných průtahů implementovat potřebné softwarové vybavení jak na straně serveru, tak i na straně klienta, a přizpůsobit síťovou infrastrukturu tak, aby bylo možné navázat síťové spojení mezi klientem a serverem.
- NZS je zodpovědná za zabezpečení přístupů do sítě zákazníka pouze těm Pracovníkům NZS, kteří jsou pověřeni pracovat na úkolech souvisejících s poskytováním služeb sjednaným se zákazníkem.
- Zákazník je zodpovědný za nepřetržitý běh softwarového a jiného vybavení potřebného na síťové spojení a nesmí bez předešlého informování NZS měnit konfiguraci klienta stejně jako síťové infrastruktury, která by měla dopad na vzdálený přístup.
- NZS nezodpovídá za škody způsobené v případě výpadku služeb ISP zákazníka.

4.1.2 Ostatní způsoby vzdáleného přístupu

V případě požadavku zákazníka na jiný způsob vzdáleného přístupu mimo TeamViewer (technické důvody, striktně definované postupy na straně zákazníka apod.) je možné využít i jiné způsoby vzdáleného přístupu – např.

- VPN přístup

Z důvodu bezpečnosti se na PC/NTB Pracovníka NZS pro připojení k síti zákazníka pomocí VPN používá např. SW OpenVPN klient (též Sophos SSL VPN klient) apod.

- Terminálový přístup

Pro připojení ke vzdálené ploše Windows pomocí veřejné IP zákazníka lze využít výhradně Remote Desktop klienta integrovaného v operačním systému Windows.

- Skype pro firmy

V tomto případě je možné použít „sdílení plochy počítače“.

Při používání takových jiných způsobů vzdáleného přístupu za bezpečnost odpovídá Pracovník NZS, který takový jiný způsob přístupu používá. Je zajištěna potřebná konfigurace takového přístupu na server NZS, na který Pracovník NZS následně může přistupovat opět pomocí TeamViewer a získat tak opět možnost záznamu veškerých svých aktivit v počítačové síti zákazníka.

4.2 Práce s DB zákazníků – v počítačových sítích NZS a zákazníků

Přístup k DB zákazníka je nezbytným předpokladem řešení specifických problémů hlášených zákazníky, které vyžadují otestování ze strany NZS přímo v počítačové síti zákazníka nebo v prostředí počítačové

sítě NZS, kde je možné využití vývojových nástrojů, které není možné u zákazníka instalovat z technických nebo licenčních důvodů. Vzhledem k ochraně dat a osobních údajů v DB je nutné dodržovat následující pravidla a postupy.

Je v zájmu zákazníka jakožto správce osobních údajů mít ještě před poskytnutím databáze uzavřenou s NZS smlouvu o zpracování osobních údajů. NZS v tomto směru poskytuje zákazníkům podporu formou distribuce vzorového dokumentu „Smlouva o zpracování osobních údajů a Smlouva o podmínkách Sdílení dat“, viz gdpr_smlouva_o_zpracovani_osobnich_udaj_s179 (odkaz přístupný Pracovníkům NZS).

- Při předávání a práci s DB je nutné dodržovat definované postupy a úložiště/servery
- Každý Pracovník NZS musí mít unikátní přístupové údaje, které není povoleno sdílet s kolegy
- Pracovník NZS smí na serverech zákazníka provádět pouze činnosti související s účelem poskytnutí DB

4.2.1 Přístup k DB v počítačové síti zákazníka

Přístup je možný pomocí vzdáleného přístupu – popis v bodu 4.1.

4.2.2 Databáze zákazníků v prostředí počítačové sítě NZS

DB zákazníka je možné předávat následujícími způsoby:

- Přenosné úložiště (NTB, flashdisk, externí HDD, CD, DVD)

V případě, že Pracovník NZS obdrží od zákazníka databázi na přenosném úložišti, je tento Pracovník povinen informovat prostřednictvím Helpdesku TO a neprodleně databázi nahrát na databázový server a veškeré úpravy a testování databáze provádět již na tomto serveru a neponechávat databázi na svém PC/NTB, ani jiných místech v počítačové síti NZS neb dokonce mimo tuto síť.

- Vzdálené připojení (VPN, RDP, TeamViewer apod.)

Je popsáno v bodu 4.1.

- Datové úložiště zákazníka (FTP, Sharepoint, OneDrive, webový odkaz apod.)

Výjimečné řešení, použitelné výhradně ze závažných důvodů zákazníka akceptovaných NZS. Zákazníka je v takovém případě nutné informovat o riziku, že se jeho databáze dostává do rukou třetí strany a jeho data jsou snáze zneužitelná, protože NZS nemá plnou kontrolu nad případným smazáním databáze z úložiště, či naopak nechtěným dlouhodobým uchováním databáze v rukou třetí strany. V tomto případě je nezbytné nabídnout zákazníkovi jinou, bezpečnější cestu, jak databázi do prostředí NZS doručit.

5 OCHRANA KONCOVÝCH ZAŘÍZENÍ V POČÍTAČOVÉ SÍTI NZS

Počítače, notebooky i mobilní zařízení (tablety a mobilní telefony), které se připojují do počítačové sítě NZS, používají dále definovanou ochranu. Instalaci a konfiguraci provádí TO.

- Stolní počítače
  - OfficeScan od Trend Micro – aktualizace v LAN NZS
  - pravidelně aktualizována virová databáze

  - skenování hrozeb v reálném čase
- Notebooky
  - Officescan
    - Schopnost aktualizovat virové databázi i mimo firemní síť
    - Skenování hrozeb v reálném čase
  - implementace šifrování HDD pro NB – Trend Micro – květen 2018 (povinné šifrování pro všechny notebooky, kterých uživatelé pracují s firemními daty a daty zákazníků na lokálním disku
- BYOD – bring your own device – použití vlastních zařízení Pracovníků NZS v počítačové síti NZS

  - Použití bude umožněno do konce roku 2018
  - Do konce roku 2018 bude i na tato zařízení instalován OfficeScan Trend Micro a v případe, že Pracovník NZS ukládá firemní data, nebo data zákazníků, bude HDD kryptován pomocí TrendMicro
- Vzdálené připojení Pracovníků NZS do počítačové sítě NZS
  - Výhradně prostřednictvím Kerio VPN
  - Pracovník NZS se připojí k interní síti doménovým loginem

6 PŘEDÁVÁNÍ DAT MEZI NZS A ZÁKAZNÍKY

6.1 Další možnosti předávání dat

Další možnosti předávání dat a DB jsou popsány v bodu 4.2.2. Pokud zákazník použije pro předání jiný způsob, je nutné zákazníka a TO NZS neprodleně informovat o porušení bezpečnostních zásad, data neprodleně umístit na bezpečné úložiště a z jiného umístění data neprodleně smazat.

NZS a TO zodpovídá pouze za bezpečnost dat umístěných nebo předávaných pomocí definovaných a zabezpečených úložišť.

7 „CLOUD“ – PROVOZ IS FORMOU SLUŽBY BEZ VLASTNÍHO HW A SW

NZS nabízí svým zákazníkům možnost poskytnutí informačního systému včetně potřebného HW a SW formou služby. V takové případě NZS, jako dodavatel, instaluje informační systém do datového centra poskytovatele. Do tohoto prostředí mají přístup výhradně uživatelé definovaní zákazníkem jako jeho pracovníci a definovaní Pracovníci NZS nebo subdodavatele, kteří provádějí správu.

Bezpečnost je založena na definici poskytovatele datového centra.

Společností NZS jsou poskytovány dvě platformy řešení:

- ERPORT – poskytovatelem je ASOL a její smluvní partner, společnost G2 server CZ s.r.o., IČ 26846993 – viz Příloha 1 „G2S GDPR infosheet“
- Prostředí Microsoft Azure – řešení firmy Microsoft – podrobně viz stránky Micosoft - https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx

8 ŠKOLENÍ PRACOVNÍKŮ NZS – SYSTÉMY, DATA A OSOBNÍ ÚDAJE A JEJICH OCHRANA

V rámci vzdělávání Pracovníků NZS v problematice bezpečnosti a ochrany dat a osobních údajů je vytvořen systém dále popsaný vzdělávání během nástupu nových Pracovníků NZS i pro všechny stávající Pracovníky NZS.

Systém školení Pracovníků NZS v oblasti bezpečnosti používání IT a ochrany osobních údajů je založen na následujících školeních a nástrojích:

8.1 Školení nových Pracovníků

Cílem je předání potřebných informací v rámci osobních schůzek i s využitím webového školení s možností sledování účasti, otestování znalostí a elektronickým vydáním certifikátu o absolvování, který Pracovník NZS vytiskne, podepíše a předá do HR oddělení Asseco Solutions, a.s.

- Školení nových pracovníků– Téma obecná znalost GDPR a ochrany osobních údajů – zajišťuje HR Asseco Solutions, a.s. s použitím platformy „Instructor“ od firmy PREVENT s.r.o., IČ 25100998
- Školení nových pracovníků v rámci adaptačních schůzek nových pracovníků s vedoucím TO – osobní setkání s prezentací a prostorem pro otázky a odpovědi

8.2 Pravidelné školení stávajících Pracovníků NZS

Cílem je pravidelná aktualizace informací včetně praktických příkladů scénářů bezpečnostních rizik a jejich řešení využitím webového školení s možností sledování účasti, otestování znalostí a elektronickým vydáním certifikátu o absolvování, který Pracovník NZS vytiskne, podepíše a předá do HR oddělení Asseco Solutions, a.s.

Bezpečnost IT a ochrana osobních údajů – 1 x ročně, s použitím platformy externího dodavatele v rámci Projektu „Security“ v rámci Asseco Solutions, a.s. v celé Evropě – s možností sledování účasti, otestování znalostí a elektronickým vydáním certifikátu o absolvování, který Pracovník NZS vytiskne, podepíše a předá do HR oddělení Asseco Solutions, a.s.

9 OCHRANA OSOBNÍCH ÚDAJŮ (GDPR)

V případě práce s osobními údaji je zapotřebí postupovat v souladu se zákonem č. 101/2000 Sb. o ochraně osobních údajů a nařízením evropského parlamentu a rady (EU) 2016/679 a z toho vycházející dokumentace, zejména s operativním pokynem pro Zpracování osobních údajů kontaktních osob NZS).

10 PŘÍLOHY

10.1 Příloha č. 1 – G2S GDPR info sheet

GDPR infosheet

GDPR, neboli Nařízení Evropského parlamentu a Rady (EU) doplňuje již stávající právní předpisy závazné pro poskytovatele cloudových služeb, obsažené zejména v:

- zákoně č. 101/2000 Sb., o ochraně osobních údajů,
- zákoně č. 181/2014 Sb., o kybernetické bezpečnosti
- zákoně č. 480/2004 Sb., o některých službách informační společnosti,

po transpozici Směrnice Evropského parlamentu a Rady EU č. 2016/1148, EU NIS. Účinnost GDPR je stanovena na 25.5.2018, nicméně vzhledem ke stávajícím přísným požadavkům výše uvedených právních předpisů je G2 server CZ s.r.o. po technické a procesní stránce předem připraven.

Zásadním krokem k prokazatelnosti nastavených procesních a technických opatření byla certifikace našich systémů managementu kvality dle ISO 9001:2016 a managementu bezpečnosti informací dle ISO/IEC 27001:2014 společností TÜV SÜD Czech s.r.o., jako světově uznávanou certifikační autoritou.

G2 server CZ s.r.o. vystupuje při poskytování Cloudu ve vztahu k zákazníkovi jak z pozice Správce osobních údajů, tak z pozice Zpracovatele, kdy:

- z pozice Správce osobních údajů G2 server CZ s.r.o. určuje, jaké údaje o zákazníkovi k poskytování služby potřebuje a jakým způsobem je bude pro zajištění této služby zpracovávat,
- a kdy z pozice Zpracovatele osobních údajů G2 server CZ s.r.o. na základě smluvního vztahu přebírá některé povinnosti zákazníka, který vůči třetím subjektům vystupuje jako Správce osobních údajů, a který tyto údaje zpracovává v infrastruktuře G2 server CZ s.r.o.

G2 server CZ s.r.o. tak ve smyslu čl. 32 odst. 1 GDPR poskytuje zákazníkovi jako Zpracovatel náležitá technická a organizační opatření, aby jako smluvní dodavatel zajistil úroveň zabezpečení odpovídající současnému stavu techniky, ke kterému je zákazník jako Správce povinen.

Veškerá data zpracovaná pro zákazníky jsou v rámci služeb Public Cloudu šifrována již od zákazníka, a jsou na úrovni storage ukládána do datových bloků, tudíž nemohou být ze strany G2 server CZ s.r.o. nikterak zneužita. G2 server CZ s.r.o. zároveň umožňuje zákazníkovi rozhodnout a mít přehled o tom, kde jsou jeho data uchována, dále díky virtualizaci a high-endovým zálohovacím technologiím garantuje neustálou přístupnost, obnovitelnost, přenositelnost a výmaz uložených dat.

G2 server CZ s.r.o. dle požadavků GDPR vytvořil pozici Pověřence pro ochranu osobních údajů, který má na starosti jak zpracování osobních údajů z pozice Správce, tak proces zpracování osobních údajů z pozice Zpracovatele. G2 server CZ s.r.o. zároveň do účinnosti GDPR zajistí kompletní smluvní potvrzení GDPR compliance všech partnerů a dodavatelů.

Zákazník je tak díky službám G2 server CZ s.r.o. jako Správce osobních údajů schopen dostát Zásadě integrity a důvěrnosti zpracování osobních údajů, obsažené v čl. 5 odst. 1 písm. f) GDPR, dále rozvedené v již zmíněném čl. 32 GDPR a recitálech č. 28, 29, 75, 78 a 83.

V případě dalších dotazů nás neváhejte kontaktovat.

S úctou

G2 server CZ s.r.o.