Název dokumentu:	**SMĚRNICE Bezpečnost počítačové sítě a ochrana osobních údajů**
Garant dokumentu:	Jaroslav Otcovský – vedoucí technického oddělení
Seznam příloh:	Příloha č. 1 – G2S GDPR info sheet
Změny v dokumentu:	Verze 3.0

OBSAH:

1 ÚČEL

Tato směrnice popisuje pravidla a postupy, jejichž dodržování zajišťuje bezpečnost počítačové sítě společnosti Asseco Solutions, a.s. (dále jen „ASOL“) a ochranu dat a osobních údajů v této síti, stejně jako ochranu počítačových sítí a osobních dat zákazníků, se kterými pracovníci ASOL mohu pracovat při zajišťování podpory zákazníků, kteří používají její produkty (informační systémy „HELIOS“).

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 ASOL (dále jen „Pracovník ASOL“), která jsou nezbytná pro zajištění potřebných znalostí Pracovníků ASOL, aktualizaci takových znalostí, jejich ověřování a evidenci.

2 PLATNOST

Tato směrnice je součástí směrnicové základny systému managementu kvality ASOL a je závazná pro všechny Pracovníky ASOL.

3 POUŽITÉ ZKRATKY A POJMY

3.1 Zkratky

ASOL – Společnost Asseco Solutions a.s., IČ: 64949541

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

DB – Databáze ASOL nebo zákazníka

VIS – Vnitřní informační systém ASOL

TO – Technické oddělení ASOL

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

3.2 Pojmy

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

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

IMS – Incident Management systém – systém evidence a řešení bezpečnostních problémů v počítačové síti ASOL

Servisní zásah – činnost pracovníka ASOL, která je zaměřena na řešení požadavků zákazníků týkajících se problémů a chyb (vad) v produktech ASOL. Servisní zásah může být realizován například prostřednictvím:

- Vzdáleného přístupu do počítačové sítě zákazníka
- Prací s DB nebo jinými datovými soubory zákazníka v počítačové síti zákazníka nebo v počítačové síti ASOL

Je v zájmu zákazníka jakožto správce osobních údajů mít ještě před realizací vzdáleného přístupu uzavřenou s ASOL smlouvu o zpracování osobních údajů. ASOL v tomto směru poskytuje zákazníkům podporu formou distribuce vzorového dokumentu „Smlouva o zpracování osobních údajů a Smlouva o podmínkách Sdílení dat“, viz https://www.helios.eu/gdpr.

Záznam informací o provedeném servisním zásahu – každý pracovník ASOL je povinný provést záznam o provedeném servisním zásahu. Tento záznam musí být uložen ve VIS, v pořadači, který tým pracovníka ASOL pro záznam prací pro zákazníky používá – např. Poskytnuté služby, Kauzy hotline, Kontaktní jednání apod. Záznam musí vždy obsahovat informace, kdo, kdy, a jakou práci pro zákazníka provedl. V případě, že během jednoho dne pracovník ASOL provedl pro zákazníka více zásahů, je možné provést pouze jeden záznam, který bude obsahovat souhrnné informace o všech pracovníkem ASOL v daný den provedených zásazích. Pro záznam informací je možné použít následující postupy/nástroje:

- Záznam ve VIS, provedený pracovníkem ASOL
- Log vzdáleného přístupu (VPN klienta, Teamviewer, Terminálového přístupu apod.)
- TeamViewer „Session recording“ – záznam celé relace vzdáleného přístupu a všech aktivit prováděných během vzdáleného přístupu

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 (vad) v produktech ASOL. 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 je nutné dodržovat následující pravidla postupy.

- Pro vzdálený přístup je možné využít pouze dále definované způsoby přístupu – jiný způsob připojení je možný pouze ze závažných důvodů zákazníka akceptovaných ASOL
- Pracovník ASOL používá, pokud to konfigurace na straně zákazníka umožňuje, pro zásah vždy svoje unikátní přístupové informace (např. jméno a heslo)
- Pracovník ASOL 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 ASOL do počítačové sítě zákazníka je přednostně používán software TeamViewer.

TeamViewer je integrován do systémů HELIOS a na jehož využívání má ASOL zakoupené licence. Připojení je plně řízeno zákazníkem a zákazník v reálném čase vidí, jakou činnost Pracovník ASOL na jeho PC vykonává. Zároveň TeamViewer obsahuje vlastní logování připojení.

Vzhledem k možnost záznamu veškerých aktivit Pracovníka ASOL 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 ASOL upřednostňován a nabízen zákazníkovi jako doporučení ASOL.

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 ASOL 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 (ASOL 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.
- ASOL je zodpovědná za zabezpečení přístupů do sítě zákazníka pouze těm Pracovníkům ASOL, 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 ASOL měnit konfiguraci klienta stejně jako síťové infrastruktury, která by měla dopad na vzdálený přístup.
- ASOL 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 ASOL 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. Z důvodu nízké úrovně zabezpečení není tento způsob doporučen.

- Skype pro firmy

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

Při používání takových jiných způsobů vzdáleného přístupu za bezpečnost odpovídá Pracovník ASOL, který takový jiný způsob přístupu používá.

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

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

- Při předávání a práci s DB je nutné dodržovat definované postupy a úložiště/servery
- Pracovník ASOL používá, pokud to konfigurace na straně zákazníka umožňuje, pro zásah vždy svoje unikátní přístupové informace (např. jméno a heslo)
- Pracovník ASOL 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 ASOL

DB zákazníka je možné předávat následujícími způsoby:

- Zabezpečený FTP server ASOL

Pracovník ASOL, který potřebuje doručit zákazníkovu databázi prostřednictvím zabezpečeného FTP serveru, zaregistruje na Helpdesk servisní požadavek, ve kterém požádá TO o vytvoření přístupu pro daného zákazníka na zabezpečený FTP server. Požadavek lze zadat pouze přímo na https://helpdesk pomocí služby „Přenos zákaznické DB“, kde pracovník vyplní formulář, který musí obsahovat tyto informace:

1) Název organizace, která databázi poskytuje
Název je potřebný pro správné pojmenování přihlašovacího účtu na FTP

2) Kontaktní email, na který bude zaslán postup na připojení k FTP
Na tuto adresu budou zaslány instrukce pro zákazníka, včetně návodu, jak se k FTP připojit

3) Kontaktní telefon, na který budou zaslány přihlašovací údaje na FTP

Z důvodu bezpečnosti není žádoucí posílat přihlašovací údaje emailem spolu s adresou FTP serveru, proto budou zákazníkovi, který bude nahrání databáze provádět, zaslány přihlašovací údaje v SMS

4) Verze MS SQL Serveru, na kterém má být databáze obnovena

Aby technické oddělení mohlo databázi obnovit, je nutné mu poskytnout informaci, jaká verze MS SQL Serveru má být pro obnovení použita.
Na databázovém serveru se nacházejí následující instance MS SQL Serveru:

SQLSRV2012	*GREEN2014*
SQLSRV2014	*GREEN2016*
SQLSRV2016	*GREEN2017*
SQLSRV2017	*GREEN2019*
SQLSRV2019	

5) Seznam uživatelů ASOL, kteří mohou do databáze přistupovat

Technické oddělení standardně nastavuje oprávnění „public“ na instanci a „db_owner“ na databázi. Má-li být nastaveno jinak, též je potřeba úroveň oprávnění do požadavku specifikovat.

6) Souhlas zákazníka s uložením databáze

Bez souhlasu zákazníka s uložením databáze do prostředí Asseco Solutions, nelze databázi v našem prostředí využívat. Proto je nutné založit ve VISu na dané organizaci nové kontaktní jednání s názvem "DB souhlas", kde musí být zákazníkův souhlas přiložen i s termínem, do kdy může být databáze v naší síti uložena. Do požadavku v Helpdesku je následně potřeba přiložit odkaz na tento záznam. Souhlas může být v libovolném formátu, např. souhlasný email od zákazníka, naskenovaný dokument apod.

7) Přibližná doba uložení databáze

Doba uložení DB musí být definována v bodu 6), tedy jednoznačně odsouhlasena zákazníkem. Po uplynutí této lhůty bude DB v případě její neprodloužení automaticky smazána.

Následně zákazník obdrží své unikátní přístupové údaje, jejichž délka platnosti je definována rovněž v požadavku na Helpdesku. Po uplynutí této doby je účet zákazníka smazán.

Na tento FTP server má v ASOL přístup pouze Technické oddělení a veškeré přístupy jsou zaznamenávány – evidence, který technik konkrétní databázi ze serveru stáhl.

Po nahrání databáze zákazníkem na zabezpečený FTP server je tato databáze Pracovníkem ASOL (technikem) přemístěna na zabezpečený databázový server, který je již přístupný dalším relevantním Pracovníkům ASOL (konzultantům či vývojářům), řešícím problémy zákazníka.

V případě požadavku Pracovníka ASOL na umístění databáze na jiném místě v počítačové síti ASOL než na k tomu účelu připraveném zabezpečeném SQL Serveru, za bezpečnost dat (omezení přístupu k DB, smazání DB ihned po vyřešení problému, zákaz předání DB jinam, záznam práce s DB) odpovídá Pracovník ASOL, který DB na jiné místo ukládá. Nezbytnou podmínkou umístění DB na takovém jiném místě je požadavek Pracovníka ASOL zaslaný do Helpdesku, který obsahuje údaje o zákazníkovi, důvodu jiného umístění DB a doby trvání umístění DB.

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

V případě, že Pracovník ASOL obdrží od zákazníka databázi na přenosném úložišti, je tento Pracovník ASOL 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 ASOL neb dokonce mimo tuto síť.

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

Je popsáno v bodu 4.1.

Pracovník ASOL je 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 ASOL nebo dokonce mimo tuto síť.

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

Výjimečné řešení, použitelné výhradně ze závažných důvodů zákazníka akceptovaných ASOL. 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 ASOL 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 ASOL doručit (ideálně zabezpečený FTP server ASOL).

5 OCHRANA KONCOVÝCH ZAŘÍZENÍ V POČÍTAČOVÉ SÍTI ASOL

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

- Stolní počítače
  - OfficeScan od Trend Micro – aktualizace v LAN ASOL
  - 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 ASOL v počítačové síti ASOL je zakázáno
  - vlastních zařízení je v síti ASOL zakázáno
- Trend Micro Mobile Security – zabezpečení mobilních zařízení používaných pracovníky ASOL
- Vzdálené připojení Pracovníků ASOL do počítačové sítě ASOL
  - Každý Pracovník ASOL žádá o povolení prostřednictvím Helpdesk
  - Výhradně prostřednictvím Sophos VPN

- Pracovník ASOL se připojí k interní síti doménovým loginem a certifikátem X.509 vygenerovaným Sophos VPN při instalaci VPN klienta

6 PŘEDÁVÁNÍ DAT MEZI ASOL A ZÁKAZNÍKY

6.1 FTP Server

Pro předávání DB a obecně dat (včetně osobních údajů) se zákazníky firmy ASOL TO poskytuje zabezpečený FTP server-protokol FTPS / SFTP.

- každý Pracovník ASOL, který potřebuje přistupovat na server (primárně pouze administrátoři v rámci TO) používá vlastní účet
- zákazník vždy obdrží unikátní jednorázový přístup
- adresářová struktura rozdělena podle zákazníků, vždy s příslušnými právy
- změny provedené na serveru jsou zaznamenávány (logovány)
- **V případě nutnosti – požadavku vedoucího týmu, na možnost přístupu jiných Pracovníků ASOL (než pracovníků TO) na FTP server je nezbytnou podmínkou požadavek vedoucího týmu zaslaný do Helpdesku, který obsahuje údaje o zákazníkovi a Pracovníkovi ASOL, který přístup bude používat. Za bezpečnost dat (omezení přístupu k DB, smazání DB ihned po vyřešení problému, zákaz předání DB jinam, záznam práce s DB) v takovém případě odpovídá Pracovník ASOL, který přístup používá.**

6.2 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 ASOL neprodleně informovat o porušení bezpečnostních zásad, data neprodleně umístit na bezpečné úložiště a z jiného umístění data neprodleně smazat.

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

Výjimkou je možnost **předávání dat prostřednictvím elektronické pošty, které je například v produktu HELIOS Red integrováno.**

Prostřednictvím elektronické pošty je možné data předávat, je však nezbytné data od zákazníka zasílat pouze na definované mailové adresy (potřebné poštovní schránky na základě požadavku jednotlivých týmů zaslaných do Helpdesku zajistí a zabezpečí TO). Přístup do takových poštovních schránek pro jednotlivé Pracovníky ASOL nebo skupiny Pracovníků ASOL zajistí TO opět na základě požadavku zaslaného do Helpdesku. Za bezpečnost dat (omezení přístupu dalších Pracovníků ASOL, zákaz předání dat jiným Pracovníkům ASOL nebo mimo firmu, smazání dat ihned po skončení důvodu jejich použití) zodpovídá Pracovník ASOL, který s daty pracuje.

Zároveň doporučujeme data předávaná pomocí elektronické pošty předávat zašifrovaná.

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

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

Bezpečnost je založena na definici poskytovatele datového centra.

Společností ASOL 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 ASOL – SYSTÉMY, DATA A OSOBNÍ ÚDAJE A JEJICH OCHRANA

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

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

8.1 Školení nových Pracovníků ASOL

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 ASOL vytiskne, podepíše a předá do HR oddělení ASOL.

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

8.2 Pravidelné školení stávajících Pracovníků ASOL

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 ASOL vytiskne, podepíše a předá do HR oddělení ASOL.

Bezpečnost IT a ochrana osobních údajů – 1 x ročně, s použitím platformy externího dodavatele v rámci Projektu „Security“ v rámci ASOL v celé Evropě – s možností sledování účasti a otestování. Přístup do portálu školení: https://pollyform.asol.local/polly/

9 ŘÍZENÍ RIZIK

Rizika jsou řízena ve VIS v souladu se Směrnicí pro řízení kvality. ASOL provozuje IMS – Helpdesk pro evidenci bezpečnostních incidentů zjištěných uživateli a správci počítačové sítě (Pracovníky ASOL), jejich ověření TO ASOL a další zpracování, včetně případného řešení.

10 OCHRANA OSOBNÍCH ÚDAJŮ (GDPR)

V případě práce s osobními údaji je zapotřebí postupovat v souladu s GDPR a z toho vycházející **řízené dokumentace ASOL**, zejména s operativním pokynem pro Zpracování osobních údajů kontaktních osob (uvedené odkazy vedou do VIS a jsou tedy dostupné pouze pro Pracovníky ASOL).

11 PŘÍLOHY

11.1 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.