BEZPEČNOST POČÍTAČOVÉ SÍTĚ A OCHRANA OSOBNÍCH ÚDAJŮ SPOLEČNOSTI HELIsmile s.r.o.

Společnost HELIsmile s.r.o. (dále jen Společnost) zavádí tato pravidla a postupy, jejichž dodržováním zajišťuje bezpečnost počítačové sítě Společnosti a ochranu dat a osobních údajů v této síti, stejně jako ochranu počítačových sítí a osobních dat uživatelů produktů a služeb Společnosti (dále jen Zákazníků), se kterými Pracovníci Společnosti spolupracují při poskytování podpory při používání těchto produktů (informační systémy „HELIOS" a program easyR).

Tímto 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").

1. POUŽITÉ ZKRATKY A POJMY

Společnost – Společnost HELIsmile s.r.o., Šlechtitelů 813/21, Holice, 779 00 Olomouc, Česká republika, IČ: 07222670

Zákazník – uživatel produktů a služeb Společnosti.

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

DB – Databáze Společnosti nebo Zákazníka

Pracovník Společnosti – Zaměstnanec/pracovník společnosti HELIsmile s.r.o. nebo osoba řádně pověřená ze strany Společnosti (konzultant, provozní programátor, technik apod.)

Helpdesk – systém zajišťující evidenci požadavků Pracovníků Společnosti 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 Společnosti

2. VZDÁLENÝ PŘÍSTUP K ZÁKAZNÍKŮM A PRÁCE S DB ZÁKAZNÍKŮ

2.1 Vzdálený přístup

Vzdálený přístup do počítačové sítě Zákazníka je nezbytným předpokladem včasného řešení požadavků Zákazníků týkajících se problémů a chyb (vad) v produktech HELIOS i easyR. 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.

- Pro vzdálený přístup je možné využít pouze jeden z dále definovaných způsobů přístupu – jiný způsob připojení je možný pouze ze závažných důvodů Zákazníka akceptovaných Společností.

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

2.1.1 Přístup pomocí TeamViewer – upřednostňovaný způsob přístupu

Pro vzdálený přístup Společnosti do počítačové sítě Zákazníka je přednostně používán software TeamViewer.

TeamViewer je integrován do systémů HELIOS a na jehož využívání má Společnost zakoupenou licenci. Připojení je plně řízeno Zákazníkem a Zákazník v reálném čase vidí, jakou činnost Pracovník Společnosti na jeho počítači vykonává.

Možný je i bezobslužný přístup (Zákazník povolí přístup do svojí sítě a předá přístupové informace, což je důležité při požadavku Zákazníka na zásah mimo pracovní dobu Zákazníka, a tedy bez jeho součinnosti v době přístupu).

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.
- 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 (Společnost 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.
- Společnost je zodpovědná za zabezpečení přístupů do sítě Zákazníka pouze těm Pracovníkům Společnosti, 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 Společnosti měnit konfiguraci klienta stejně jako síťové infrastruktury, která by měla dopad na vzdálený přístup.
- Společnost nezodpovídá za škody způsobené v případě výpadku služeb ISP Zákazníka.

2.1.2 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.

- Terminálový přístup

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

- Skype

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

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

2.1.3 Práce s DB Zákazníků – v počítačových sítích Společnosti a Zákazníků

Přístup k DB Zákazníka je nezbytným předpokladem řešení specifických problémů hlášených Zákazníky, které vyžadují otestování ze strany Společnosti přímo v počítačové síti Zákazníka nebo v prostředí počítačové sítě Společnosti, kde je možné využití vývojových nástrojů, které není možné u Zákazníka instalovat z technických nebo licenčních důvodů.

2.1.4 Předávání dat mezi Zákazníky a Společností

DB Zákazníka je možné předávat následujícími způsoby:

- Zabezpečený FTP server Společnosti
  Zákazník obdrží své unikátní přístupové údaje na zabezpečený FTP server Společnosti, na který nahraje data. Následně jsou data přemístěna na zabezpečenou počítačovou síť Společnosti, která je přístupná relevantním Pracovníkům Společnosti řešící problém Zákazníka.
  Po nahrání databáze Zákazníkem na zabezpečený FTP server je tato databáze Pracovníkem ASOL (technikem) přemístěna na zabezpečený server Společnosti, který je již přístupný dalším relevantním Pracovníkům Společnosti (konzultantům či vývojářům), řešícím problémy Zákazníka.
- Přenosné úložiště (NTB, flashdisk, externí HDD, CD, DVD)
- Vzdálené připojení (VPN, RDP, TeamViewer apod.)
- Datové úložiště Zákazníka (jiné FTP, Sharepoint, OneDrive, webové služby pro přenos dat, e-mail)
  Výjimečné řešení, použitelné výhradně ze závažných důvodů Zákazníka akceptovaných Společností. 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 Společnost nemá plnou kontrolu nad případným smazáním databáze z úložiště, či naopak nechtěným dlouhodobým uchováním databáze v rukou třetí strany. V tomto případě doporučuje Společnost data před odesláním uložit do archivu s heslem. Heslo pro rozbalení archivu zašle Zákazník Společnosti pomocí e-mailu či sms zprávy.

3. OCHRANA KONCOVÝCH ZAŘÍZENÍ V POČÍTAČOVÉ SÍTI SPOLEČNOSTI

Počítače, notebooky i mobilní zařízení (tablety a mobilní telefony), které se připojují do počítačové sítě Společnosti používají následující ochranu:

- spuštěný antivirový program se skenováním hrozeb v reálném čase s pravidelně aktualizovanou virovou databází
- šifrování dat obsahující osobní údaje na harddiscích počítačů programem BitLocker

Pro týmovou spolupráci je využíváno cloudové úložiště OneDrive. Každý zaměstnanec Společnosti má sdílenou společnou složku Společnosti v rámci svého účtu na OneDrive. Je povinností každého zaměstnance používat pro přístup do služby OneDrive silné heslo. V případě synchronizace obsahu sdílené společné složky Společnosti na harddisk počítače Zaměstnance Společnosti je třeba i tuto složku šifrovat programem BitLocker.

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

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

Bezpečnost je založena na definici poskytovatele datového centra.

Společností jsou poskytovány dvě platformy řešení:

- ERPORT – poskytovatelem je Asseco Solutions, a.s. 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

5. ŠKOLENÍ PRACOVNÍKŮ SPOLEČNOSTI – SYSTÉMY, DATA A OSOBNÍ ÚDAJE A JEJICH OCHRANA

Každý Pracovník Společnosti je pravidelně 1x ročně povinen absolvovat školení v problematice bezpečnosti a ochrany dat a osobních údajů. Školení může probíhat interní nebo externí formou. Účast na školení bude potvrzena certifikátem o absolvování, který každý Pracovník Společnosti podepíše.

Každý nový Pracovník Společnosti je proškolen ihned po nástupu do zaměstnání.

6. ŘÍZENÍ RIZIK

V případě, že jakýkoliv Pracovník Společnosti má podezření na možné zneužití osobních údajů, nahlásí tuto skutečnost bez zbytečného odkladu jednateli Společnosti. O této skutečnosti bude vyhotoven zápis podepsaný zaměstnancem, který skutečnost nahlásil a jednatelem Společnosti. Jednatel Společnosti tuto skutečnost ověří a v případě skutečného incidentu okamžitě podnikne kroky k nápravě. Nejpozději do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl zaměstnance, který podezření nahlásil, informuje Úřad pro ochranu osobních údajů.

7. OCHRANA OSOBNÍCH ÚDAJŮ (GDPR)

S poskytováním služeb může být spojeno zpracování osobních údajů, jak je definováno v ZOOÚ a Obecném nařízení.

Účelem zpracování osobních údajů je řádné poskytování služeb.

Osobní údaje zpracovává Společnost v rozsahu, který je nezbytný pro poskytnutí služby, kterou si se Společností Zákazník sjednává. Osobní údaje rozdělujeme je do dvou skupin – osobní údaje, které může Společnost zpracovávat bez souhlasu Zákazníka, a osobní údaje, které bez souhlasu Zákazníka zpracovávat Společnost nemůže.

Zpracování osobních údajů, ke kterému je nutný souhlas Zákazníka:

- marketingové činnosti,
- nefinanční služby našich partnerů,

Zpracování osobních údajů, ke kterému není nutný souhlas Zákazníka:

- plnění povinností Společnosti, které vyplývají z uzavřených smluv,
- splnění povinností Společnosti, které nám ukládá zákon a jiné právní předpisy,
- zajištění ochrany práv Společnosti a práv chráněných zájmů (např. při uplatnění nároků u soudů, pojišťoven), rozsah poskytnutých osobních údajů je omezen na osobní údaje, které jsou nezbytné pro úspěšné uplatnění nároku,
- splnění úkolu prováděného ve veřejném zájmu.

Pokud Zákazník osobní údaje nutné pro některý z výše uvedených důvodů odmítnete sdělit, není možné poskytnout příslušný produkt, službu či jiné plnění, pro které osobní údaje Společnost potřebuje.

Typ/kategorie osobních údajů:

Společnost je při plnění služeb oprávněna zpracovávat všechny osobní údaje potřebné pro splnění tohoto účelu, přičemž zejména se bude jednat o tyto osobní údaje:

- Jméno
- Příjmení
- Titul
- Kontaktní údaje (email, telefon, adresa trvalého pobytu, doručovací adresa)
- Lokalita místa výkonu práce
- Podpis (typicky u smluvních dokumentů, protokolů o provedené práci, akceptačních protokolech, prezenčních listinách při školeních apod.)
- Údaje o využívání služeb
- Údaje o bonitě a důvěryhodnosti
- Kromě výše uvedeného takové osobní údaje, k jejichž zpracování udělí příslušný subjekt údajů prokazatelně souhlas

Společnost prohlašuje, že nebudou zpracovávány žádné citlivé osobní údaje ve smyslu ustanovení § 4 písm. b) ZOOÚ, resp. osobní údaje zvláštních kategorií ve smyslu čl. 9 Obecného nařízení.

Společnost se zavazuje zpracovávat osobní údaje po dobu trvání poskytování služeb a dále po dobu, po kterou má oprávněný zájem na jejich uchování (v souladu s Obecným nařízením a/nebo ZOOÚ) nebo po kterou jejich uchování vyžaduje příslušná tuzemská legislativa nebo právo EU. Nejdéle však jeden rok ode dne daňového promlčení práv a povinností vztahujících se k účelu zpracování.

Po ukončení této doby má Společnost povinnost předané osobní údaje vrátit Zákazníkovi nebo je vymazat včetně existujících kopií.

Společnost bude zpracovávat osobní údaje v souladu se ZOOÚ, Obecným nařízením, a pokyny Zákazníka, které budou prokazatelně Zákazníkem uděleny. Udělování pokynů Zákazníka bude probíhat písemně nebo elektronicky.

Společnost se zavazuje dodržovat veškeré povinnosti vyplývající pro Zákazníka z Obecného nařízení. Zejména, nikoliv výlučně, se tedy Společnost zavazuje:

- poskytnout Zákazníkovi nezbytnou součinnost při plnění povinnosti reagovat na žádosti o výkon práv subjektů údajů (fyzických osob, k nímž se osobní údaje vztahují) ve smyslu čl. 28 odst. 3 písm. e) Obecného nařízení. Zákazník je povinen Společnost bez zbytečného odkladu informovat o nutnosti poskytnutí takové součinnosti.
- ve smyslu článku 32 Obecného nařízení přijmout taková technická a organizační opatření, aby nemohlo dojít k protiprávnímu nebo náhodnému zničení, ztrátě, pozměňování, k neoprávněnému zpřístupnění předávaných, uložených nebo jinak

zpracovávaných osobních údajů, nebo neoprávněnému přístupu k nim. Tato povinnost platí i po ukončení zpracování osobních údajů. Dodavatel při zpracování osobních údajů implementuje proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování osobních údajů. Mezi přijatá technická a organizační opatření, je-li to nezbytné s ohledem na riziko zpracování osobních údajů, patří zejména:

-

a) Pseudonymizace nebo šifrování osobních údajů;
b) Uzamykání prostor Společnosti, kde se osobní údaje zpracovávají;
c) Zaheslování počítačů nebo jiných zařízení, ve kterých se osobní údaje zpracovávají;
d) Zpracování osobních údajů pouze odpovědnými osobami;
e) Proškolení odpovědných osob, jak mají s osobními údaji nakládat.

- ve smyslu čl. 28 odst. 3 písm. h) Obecného nařízení poskytnout Zákazníkovi veškeré nezbytné informace potřebné k doložení toho, že byly splněny povinnosti stanovené v článku 28 Obecného nařízení, a umožnit audity, včetně inspekcí, prováděné Zákazníkem nebo jiným auditorem, kterého Zákazník pověřil, a k těmto auditům přispět. Na způsobu provedení auditu včetně termínu a účastníků se smluvní strany předem dohodnou, ledaže to budou okolnosti jednoznačně vylučovat.

Společnost je vázána mlčenlivostí a dále pak se zavazuje zajistit, aby odpovědné osoby byly taktéž zavázány k mlčenlivosti.

Práva Zákazníka v souvislosti s ochranou osobních údajů

Osobní údaje Zákazníka zpracovává Společnost transparentně, korektně a v souladu s legislativními požadavky. Zákazník má však zároveň právo se kdykoli na Společnost obrátit, aby získal informace o procesu zpracování svých osobních údajů, či za účelem uplatnění níže uvedených práv, která souvisejí s osobními údaji.

Právo na přístup k osobním údajům: právo vyžádat si kopii osobních údajů, které o Zákazníkovi Společnost zpracovává.

Právo na opravu osobních údajů: pokud se Zákazník domnívá, že osobní údaje, které o něm Společnost vede, jsou nepřesné či neúplné, má právo požádat Společnost o jejich aktualizaci či doplnění.

Právo na výmaz osobních údajů (právo být zapomenut): Zákazník má právo požadovat výmaz svých osobních údajů, pokud nejsou potřebné pro účel, pro který byly zpracovávány, pokud odvolal souhlas s jejich zpracováním, byly zpracovány protiprávně, musí být vymazány ke splnění právní povinnosti, nebo byly shromážděny v souvislosti s nabídkou služeb informační společnosti.

Právo na omezení zpracování osobních údajů: Zákazník má právo požadovat omezení zpracování, pokud popírá přesnost osobních údajů, nebo je jejich zpracování protiprávní, ale odmítá výmaz takových osobních údaj, nebo pokud požádá Společnost, může jeho vybrané osobní údaje zpracovávat i po té, co nejsou potřebné k účelu, pro který byly Společnosti poskytnuty (např. v souvislosti s uplatněním nároku u soudu, k němuž námi zpracovávané osobní údaje potřebujete), nebo Zákazník vznesl námitku proti zpracování, přičemž není zřejmé, zda oprávněný zájem Společnosti převažuje nad oprávněnými zájmy Zákazníka.

Právo na přenositelnost osobních údajů: v případě automatizovaného zpracování osobních údajů, které je založeno na uzavřené smlouvě nebo souhlasu, který Společnosti Zákazník udělil, má právo na tzv. přenositelnost těchto údajů, které budou Zákazníkovi poskytnuty ve strukturovaném, běžně používaném a strojově čitelném formátu.

Právo vznést námitku proti zpracování osobních údajů: kdykoli může Zákazník vznést námitku proti zpracování osobních údajů, včetně profilování, které Společnost zpracovává z důvodu oprávněného zájmu. Stejně tak může Zákazník vznést námitku proti zpracování v situaci, že jeho

osobní údaje zpracovává Společnost pro účely přímého marketingu. V takovém případě osobní údaje Zákazníka již nadále nebude Společnost takto zpracovávat pro tento účel.

Právo odvolat souhlas se zpracováním osobních údajů: v případě, že Zákazník poskytli Společnosti souhlas se zpracováním osobním údajů pro účely, které vyžadují souhlas, má právo kdykoli tento souhlas odvolat. Zpracování osobních údajů, ke kterému došlo před odvoláním souhlasu, je zákonné.

Pro uplatnění svých práv může Zákazník využít elektronické komunikační kanály, které v komunikaci se Společností využívá. V případě pochyb je možné využít e-mailovou adresu info@helismile.cz.

Na žádosti, které se týkají uplatnění práv Zákazníků, bude Společnost reagovat bez zbytečného odkladu ve lhůtě do 30 dnů od obdržení žádosti. Lhůtu je však v případě potřeby možné prodloužit o další dva měsíce. O takovém prodloužení včetně důvodů, které k němu vedly, bude Společnost vždy Zákazníka informovat. Komunikace bude vedena způsobem, který Zákazník preferujete (e-mail, dopis).

Zákazník má právo podat stížnost u dozorového úřadu (Úřad pro ochranu osobních údajů), pokud se domnívá, že při zpracování jeho osobních údajů došlo k porušení pravidel ochrany osobních údajů.

Úřad pro ochranu osobních údajů:
Pplk. Sochora 27
170 00 Praha 7
telefon: +420 234 665 111

Tato pravidla nabývají platnosti a účinnosti od 19. 6. 2018.