Bezpečnost

OFFICE 365

CloudForce s.r.o.
IČ: 03905209, DIČ: CZ03905209
Společnost je zapsána do OR vedeného Městským soudem v Praze, oddíl C, vložka 239706
Registrované sídlo a poštovní adresa: Nad Lesním divadlem 1214/4, Braník, 142 00 Praha 4
info@cloudforce.cz | www.cloudforce.cz

1 ONLINE BEZPEČNOST

- Microsoft sdílí informace o všech certifikacích, atestech a auditech s cílem zjednodušit vaše procesy v souladu se zákony a normami.
- Zákazník stále zůstává odpovědný za naplnění všech vlastních požadavků na soulad se zákony a normami.

1.1 OCHRANA NA VÍCE ÚROVNÍCH

Management bezpečnosti	•Management hrozeb & zranitelností. •Monitorování & reakce.
Data	•Řízení přístupu & monitorování. •Souborová/Datová integrita.
Uživatel	•Správa účtů. •Vzdělávání & budování povědomí, Screening.
Aplikace	•Bezpečný vývoj (SDL). •Řízení přístupu & monitorování, Anti-Malware.
Hostitel	•Řízení přístupu & monitorování. •Antimalware, Patch & Config Mgmt.
Interní síť	•Dual-factor Auth, Intrusion Detection. •Monitorování zranitelností.
Perimeter sítě	•Edge routery, IDS systémy. •Vulnerability scanning.
Budovy	•Fyzická kontrola, video ostraha. •Řízení přístupu.

2 GLOBAL FOUNDATION SERVICES - BEZPEČNOST

3 SOUKROMÍ

Strategie Microsoftu je zaměřena na vysokou úroveň ochrany osobních údajů tak, aby plně odpovídala globálním standardům pro nakládání a přenos dat.

DEFINICE SOUKROMÍ & PRŮHLEDNOST

- Microsoft Online Service Privacy Statement
- Microsoft Online Code of Conduct
- Microsoft Online Subscription Agreement
- Certifikace EU Safe Harbor – klasifikuje MS jako držitele enterprise dat & správce dat, nikoli jejich jako jejich vlastníka

Zajišťujeme, že jsou použity správné politiky a principy, které umožňují zákazníkům a koncovým uživatelům udržet kontrolu nad jejich osobními informacemi (PII).

Při použití Microsoft online služeb zákazník vyhoví těmto regulacím na ochranu soukromí:

- HIPAA, GLBA, FERPA, Mass 201, PIPEDA,
- EU Data Protection Directive a bezpečnostní požadavky v EU národních zákonech na ochranu soukromí;

4 SOULAD

POŽADAVKY NA AUDIT

Microsoft nabízí:

- Soulad a přijetí průmyslových standardů.
- Ucelenou množinu postupů a procesů pro ochranu vašich dat.
- Zaměřeno na milióny uživatelů na celém světě.
- Nezávislé atesty třetích stran v oblasti bezpečnosti, soukromí a řízení kontinuity.

Možnost přizpůsobení a bohatá funkcionalita umožňuje reagovat na individuální potřeby zákazníka

- Použijte vlastnosti služeb pro implementaci vlastních politik.
- Retenční politiky, archivace, litigation hold, apod.

Společnost Microsoft je v souladu s:

- ISO 27001
- ISO 27018
- SAS 70 Type II
- HIPAA/HITECH
- EU Safe Harbor
- Různé národní, federální a mezinárodní zákony na ochranu soukromých dat
    - (95/46/EC - aka EU Data Protection Directive; California SB1386; atd.)

- PCI Data Security Standard
- FISMA Certification & Accreditation

5 KONTINUITA SLUŽEB

Zajištění kontinuity služeb a závazek společnosti Microsoft ke kontinuitě služeb naleznete podrobně rozepsaný na této stránce v sekci SLA - Service Level Agreements for Microsoft Online Services.

Smlouvy o úrovni služeb (Service Level Agreements - SLA) popisují závazek společnosti Microsoft o provozuschopnosti a konektivitě služeb Microsoft Online Services. Aktuální a archivovaná vydání SLA jsou k dispozici ke stažení a pokrývají Office 365, Intune, Dynamics 365 a Azure.

https://www.microsoft.com/en-us/licensing/product-licensing/products

6 PODMÍNKY ONLINE SLUŽEB

Podmínky online služeb (OST – Online services terms)

Pokud odebíráte online služby prostřednictvím programu Microsoft Volume Licensing, podmínky pro používání této služby jsou definovány v dokumentu OST (Volume Licensing Online Services Terms) a dohodě o programu. OST je měsíčně aktualizován jako nástupce práv k užívání služeb Microsoft Online Services. Aktuální a archivovaná vydání OST jsou k dispozici ke stažení.

https://www.microsoft.com/en-us/licensing/product-licensing/products

OST obsahuje přílohu 4, kde jsou vypsány podmínky obecného nařízení o ochraně osobních údajů Evropské unie:

Příloha 4 – Podmínky obecného nařízení o ochraně osobních údajů Evropské unie

Společnost Microsoft se v těchto podmínkách obecného nařízení o ochraně osobních údajů zavazuje všem zákazníkům s platností od 25. května 2018. Tyto závazky jsou závazné pro společnost Microsoft vůči zákazníkovi bez ohledu na (1) verzi podmínek pro služby online, která je jinak platná pro každý daný odběr služeb online, a na (2) jakoukoli jinou smlouvu odkazující na tuto přílohu.

Pro účely těchto podmínek obecného nařízení o ochraně osobních údajů se zákazník a společnost Microsoft dohodli, že zákazník je správcem osobních údajů zákazníka, které jsou osobními údaji, a Microsoft je zpracovatelem těchto údajů. Výjimku představují případy, kdy zákazník působí jako zpracovatel osobních údajů. V takovém případě je Microsoft dalším zpracovatelem. Tyto podmínky obecného nařízení o ochraně osobních údajů platí pro zpracování osobních údajů společností Microsoft jménem zákazníka v rámci působnosti obecného nařízení o ochraně osobních údajů. Tyto podmínky obecného nařízení o ochraně osobních údajů neomezují ani nesnižují žádné závazky ochrany osobních údajů, které má společnost Microsoft vůči zákazníkovi dle Podmínek pro služby online nebo dle jiných dohod mezi společností Microsoft a zákazníkem. Tyto podmínky obecného nařízení o ochraně osobních údajů se neuplatní, pokud je společnost Microsoft správcem osobních údajů.

Příslušné povinnosti dle obecného nařízení o ochraně osobních údajů: Články 28, 32 a 33

1. Společnost Microsoft nezapojí dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení od zákazníka. V případě obecného písemného povolení bude společnost Microsoft informovat zákazníka o jakýchkoli zamýšlených změnách týkajících se přijetí nebo výměny dalších zpracovatelů, a poskytne tak zákazníkovi možnost vyslovit vůči těmto změnám námitky. (Článek 28(2))

2. Zpracování společností Microsoft se řídí těmito podmínkami obecného nařízení o ochraně osobních údajů podle práva Evropské unie (dále jako „EU") nebo práva některého z jejích členských států a jsou pro společnost Microsoft vůči zákazníkovi závazné. Předmět a trvání zpracování, jeho povaha a účel, typ osobních údajů, kategorie subjektů údajů a povinnosti a práva zákazníka jsou stanoveny v licenční smlouvě zákazníka, včetně těchto podmínek obecného nařízení o ochraně osobních údajů. Společnost Microsoft konkrétně:

(a) zpracovává osobní údaje pouze na základě doložených pokynů od zákazníka, včetně v otázkách předání osobních údajů do třetích zemí nebo mezinárodních organizací, pokud mu toto zpracování již neukládají právo EU nebo členského státu, které se na společnost Microsoft vztahuje; v takovém případě bude společnost Microsoft informovat zákazníka o tomto právním požadavku před zpracováním, ledaže tyto právní předpisy toto informování zakazují z důležitých důvodů veřejného zájmu;

(b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

(c) přijme veškerá opatření požadovaná podle článku 32 obecného nařízení o ochraně osobních údajů;

(d) dodržuje podmínky dle odstavce 1 a 3 této Přílohy č. 4 pro zapojení dalšího zpracovatele;

(e) zohledňuje povahu zpracování, je zákazníkovi nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, při plnění povinnosti zákazníka reagovat na žádosti o výkon práv subjektů údajů stanovených v kapitole III obecného nařízení o ochraně osobních údajů;

(f) je zákazníkovi nápomocen při zajištění souladu s povinnostmi stanovenými články 32 až 36 obecného nařízení o ochraně osobních údajů s ohledem na povahu zpracování a informace, které jsou společnosti Microsoft k dispozici;

(g) na žádost zákazníka vymaže nebo vrátí zákazníkovi veškeré osobní údaje po ukončení poskytování služeb souvisejících se zpracováním a vymaže existující kopie, pokud právo EU nebo členského státu nepožaduje uložení daných osobních údajů;

(h) poskytne zákazníkovi veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v článku 28 obecného nařízení o ochraně osobních údajů a umožní audity, včetně inspekcí, prováděné zákazníkem nebo jím pověřeným auditorem, a k těmto auditům přispěje.

Společnost Microsoft neprodleně informuje zákazníka v případě, že podle jejího názoru určitý pokyn porušuje nařízení o ochraně osobních údajů nebo jiné předpisy EU nebo členského státu týkající se ochrany údajů. (Článek 28(3))

3. Pokud společnost Microsoft pověří dalšího zpracovatele, aby jménem zákazníka provedl určité činnosti zpracování, budou tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva EU nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny v těchto podmínkách obecného nařízení o ochraně osobních údajů, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky nařízení o ochraně osobních údajů. Neplní-li uvedený další

zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá zákazníkovi za plnění povinností dotčeného dalšího zpracovatele i nadále plně společnost Microsoft. (Článek 28(4))

4. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou zákazník a společnost Microsoft vhodná technická a organizační opatření pro zajištění úrovně zabezpečení odpovídající daným rizikům, případně včetně:

(a) pseudonymizace a šifrování osobních údajů;

(b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

(c) schopnosti obnovit dostupnost osobních údajů a včasný přístup k nim v případě fyzických nebo technických incidentů;

(d) procesu pravidelného testování, posuzování a hodnocení efektivity zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. (Článek 32(1))

5. Při posuzování vhodné úrovně zabezpečení se zohlední zejména rizika, která přestavuje zpracování, zejména pak náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim. (Článek 32(2))

6. Zákazník a společnost Microsoft přijmou opatření pro zajištění toho, aby jakákoli fyzická osoba, která jedná z pověření zákazníka nebo společnosti Microsoft a která má přístup k osobním údajům, bude zpracovávat tyto údaje pouze na základě pokynu od zákazníka, pokud jí jejich zpracování již neukládá právo EU nebo členského státu EU. (Článek 32(4))

7. Poté, co se společnost Microsoft dozví o narušení bezpečnosti osobních údajů, neprodleně o tom uvědomí zákazníka. (Článek 33(2)). Takováto oznámení budou obsahovat informace, které musí zpracovatel poskytovat správci dle článku 33(3) v té míře, v níž jsou takovéto informace dostupné společnosti Microsoft.