

Popis služby IBM Cloud Service**IBM Digital Data Exchange**

Níže je uveden Popis služeb pro Vaši Objednávku:

1. Cloud Service

Nabídka Cloud Service, včetně základní nabídky a dostupných volitelných komponent, je popsána níže a odpovídá výběru v Dokumentu objednávky. Dokument objednávky bude zahrnovat Cenovou nabídku předloženou IBM, a Dokument o oprávnění (Proof of Entitlement) uvádějící datum zahájení poskytování služeb a smluvní období pro služby Cloud Service a datum zahájení fakturace.

1.1 IBM Digital Data Exchange

IBM Digital Data Exchange je řešení, které Vám poskytuje jediné rozhraní pro konfiguraci a implementaci tagů webových a mobilních stránek.

IBM Digital Data Exchange Vám umožňuje spravovat tagy IBM a tagy Obchodního partnera IBM určené k implementaci na Vaše webové nebo mobilní stránky. Uživatelské rozhraní IBM Digital Data Exchange poskytuje přímou kontrolu nad procesem označování prostřednictvím tagů, což uživatelům umožňuje definovat tagy stránek a skupiny stránek na základě souboru pravidel určujících provedení tagu. Jakmile si zakoupíte IBM Digital Data Exchange, můžete spravovat aktuální i předchozí implementaci tagů IBM, tagů Obchodních partnerů IBM a přizpůsobeného JavaScriptu nebo vlastního kódu v rámci více prostředí.

2. Popis zabezpečení**2.1 Zásady zabezpečení**

IBM dodržuje zásady v oblasti zabezpečení a ochrany soukromí, které jsou zveřejněny a s nimiž jsou seznámeni zaměstnanci IBM. IBM vyžaduje, aby osoby na celém světě, které poskytují podporu datovým střediskům IBM, byly proškoleny v oblasti ochrany soukromí a zabezpečení. IBM disponuje vlastním bezpečnostním týmem, který se specializuje na zabezpečení informací. Zásady a standardy IBM v oblasti zabezpečení jsou každoročně přezkoumávány a přehodnocovány. Bezpečnostní incidenty IBM jsou zpracovávány v souladu s komplexním postupem reagování na incidenty.

2.2 Řízení přístupu

IBM udržuje logickou separaci dat zákazníka. Data zákazníka jsou uložena v rámci vlastního schématu specifického pro zákazníka a měla by být přístupná prostřednictvím služby Cloud Service nebo exportu dat specifických pro zákazníka. Přístup ke službě Cloud Service a k datům zákazníka je řízen a spravován určeným administrátorem zákazníka. IBM využívá při přístupu k systémům zákazníka technologii multifaktorového ověřování a šifrování VPN tunelu. Přístup je omezen na osoby, které jej potřebují, aby mohly udržovat a administrovat službu Cloud Service a související hardwarovou a softwarovou infrastrukturu v datových střediscích třetích stran. IBM využívá WIFI (a/k/a 802.11) provoz na síti, který je šifrovaný pomocí WPA2 s šifrovacím algoritmem AES a zajišťuje při přístupu k systémům obsahujícím data zákazníka nevysílající SSID a vzájemné ověření mezi serverem a koncovými zařízeními.

2.3 Integrita a dostupnost služeb

Úpravy prostředků operačního systému (OSR - operating system resource) a úpravy aplikačního softwaru se řídí procesem řízení změn IBM. V rámci síťové infrastruktury a na pracovních stanicích osob pracujících v datových střediscích IBM nebo s daty zákazníka v datových střediscích IBM je používán hardware, software, protokoly přístupů, přístup pouze pro čtení a ovládací prvky šifrování za účelem snížení pravděpodobnosti šíření a spuštění počítačových virů a jiných forem známého škodlivého kódu. IBM používá šifrování "over-the-network" přes standardní připojení SSL (https) a infrastruktura IBM využívá technologických řešení pro zajištění komplexního zabezpečení, včetně brány firewall, ochrany před neoprávněným vniknutím a technologií pro ochranu před škodlivým softwarem. Oprávnění administrátoři pravidelně skenují možné ohrožení zabezpečení protokolů TCP/IP (Transmission Control Protocols/Internet Protocols) s cílem detekovat a vyřešit potenciální bezpečnostní rizika, jimž může být systém vystaven. Data z datového skladu IBM jsou zkopírována do sekundární paměti v datovém středisku IBM a terciální archiv (páska) je zašifrován a duplikován pro úložiště v offsite zařízení třetí strany pro účely zotavení z havárie.

2.4 Protokolování aktivity

IBM uchovává protokoly aktivity pro systémy, aplikace, datová úložiště, middleware a zařízení síťové infrastruktury, které umožňují protokolovat aktivitu a jsou pro tento účel nakonfigurovány. IBM udržuje protokoly pro zaznamenávání i) úspěšných a neúspěšných pokusů o přihlášení, ii) úspěšných a neúspěšných pokusů o získání přístupu k infrastruktuře z externí lokality, iii) pokusů o přístup k OSR za účelem aktualizace a iv) aktivit prováděných s administrativním oprávněním pro systém nebo zabezpečení.

2.5 Fyzické zabezpečení

IBM omezuje přístup pouze na oprávněné zaměstnance datového střediska IBM v datových střediscích IBM nebo v datových střediscích, jež IBM poskytuje třetí strana. Prostředí služby IBM Cloud Service zahrnuje multifaktorové ověřování fyzického přístupu, včetně jedinečného kódu a biometrického skenování, a rovněž bezpečnostní službu 24 hodin denně, 7 dní v týdnu, ostrahu a kamerový dozor. IBM zakazuje neoprávněné prohlížení, kopírování, změny nebo odstranění jakýchkoli médií obsahujících data zákazníka. Vyjímatelná média, na nichž jsou uložena data zákazníka (včetně USB disků, disků CD a DVD), jsou šifrována pomocí přinejmenším 256bitového AES (nebo ekvivalentu). Laptopy a pracovní stanice, které vydá IBM, vyžadují implementaci šifrování celého disku (PGP), kde mohou být vyžadována přístupová práva k citlivým informacím nebo datům zákazníka. IBM zlikviduje vyjímatelná média a jakákoli mobilní zařízení (jako jsou disky, USB jednotky, DVD, zálohovací pásy, tiskárny a laptopy) obsahující data zákazníka nebo převede data zákazníka uložená na takových fyzických médiích před opětovným použitím média do nesrozumitelné podoby, aby data zákazníka nebylo možno žádnými technickými prostředky rekonstruovat. IBM skartuje papírový odpad a likviduje jej v souladu se zásadami zabezpečení a ochrany důvěrných informací, aby byla zajištěna následná nečitelnost takového papírového odpadu.

2.6 Dodržování požadavků

IBM certifikuje své postupy v oblasti ochrany soukromí vždy jednou ročně z hlediska souladu se zásadami U.S. Department of Commerce's Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement. Vždy jednou ročně je v našich produktivních datových střediscích prováděn odvětvový audit dle SSAE 16 (dříve SAS 70) nebo ekvivalentní audit. IBM přezkoumává činnosti související se zabezpečením a ochranou soukromí z hlediska dodržování obchodních požadavků IBM. IBM pravidelně provádí hodnocení a prověřování, jejichž cílem je ověřit dodržování zásad zabezpečení informací. Zavedené bezpečnostní zásady umožňují audity zabezpečení, periodické aplikování bezpečnostních záplat a rovněž správu a řízení hesel. Zaměstnanci IBM a zaměstnanci dodavatelů každoročně absolvují školení pracovních sil zaměřené na vzdělávání a získání povědomí v oblasti zabezpečení. Pracovníkům jsou každý rok znovu připomínány jejich pracovní cíle a povinnosti ohledně dodržování etického obchodního chování, ochrany důvěrných informací a závazků IBM v oblasti zabezpečení.

3. Cíle týkající se úrovně služeb (Service Level Objectives, SLO)

Snahou IBM je zpřístupnit IBM SaaS Zákazníkovi s mírou dostupnosti 99 %. SLO nepředstavují smluvní závazek, je to spíše množina cílů, jichž IBM tým podpory usiluje dosáhnout nebo které se snaží překročit prostřednictvím svých procesů, technologie a lidí.

4. Oprávnění a informace o fakturaci

4.1 Metriky poplatků

Cloud Service je dostupná na základě jedné z níže uvedených metrik poplatků, jak je uvedeno v Dokumentu objednávky.

- a. Milión volání serveru (Million Server Calls, MSC) je měrnou jednotkou, na jejímž základě lze získat Cloud Service. Volání serveru jsou data předaná službě Cloud Service a zpracovaná službou Cloud Service jako výsledek indikované události, kterou inicioval sledovaný návštěvník pro jedno ID subjektu. Volání serveru, které je zpracováváno různými ID subjektů, bude započítáno jako jedinečné Volání serveru pro každé jedinečné ID subjektu. ID subjektu vymezuje a/nebo řídí v rámci služby Cloud Service přístupová práva k datům, jež mohou zahrnovat zpracovaná data z jednoho nebo více Vašich webových serverů. Každé oprávnění MSC představuje jeden Milión volání serveru. Je nutno získat dostatečný počet oprávnění MSC, který bude pokrývat celkový počet Volání serveru zpracovaných během období měření uvedeného v Dokumentu objednávky.

4.2 Poplatky a fakturace

Výše platby za Cloud Service je specifikována v Dokumentu objednávky.

5. Smluvní období a možnost prodloužení

5.1 Smluvní období

Smluvní období pro poskytování Cloud Service začíná datem, kdy Vám IBM oznámí, že Vám byl poskytnut přístup ke službě Cloud Service, jak je uvedeno v Dokumentu objednávky. V Dokumentu o oprávnění (Proof of Entitlement), který je součástí Dokumentu objednávky, bude stvrzeno přesné datum začátku a konce smluvního období. V průběhu smluvního období jste oprávněni zvýšit Vaši úroveň užívání Cloud Service. Chcete-li tak učinit, obraťte se na IBM nebo na Obchodního partnera IBM. Zvýšená úroveň užívání bude potvrzena IBM v Dokumentu objednávky.

5.2 Volby prodloužení smluvního období pro služby Cloud Service

Ve Vašem Dokumentu objednávky je pro smluvní období určena jedna z následujících voleb, která uvádí, zda na konci smluvního období bude služba Cloud Service prodloužena:

5.2.1 Automatické prodloužení

Jestliže je ve Vašem Dokumentu objednávky uvedeno automatické prodloužení, jste oprávněni ukončit končící smluvní období pro poskytování služby Cloud Service prostřednictvím písemné žádosti zaslané přinejmenším devadesát (90) dní před datem uplynutí smluvního období, které je uvedeno v Dokumentu objednávky. Neobdrží-li IBM nebo Váš Obchodní partner IBM takové oznámení o ukončení do data ukončení smluvního období, bude končící smluvní období automaticky prodlouženo o jeden rok nebo o období rovnající se původnímu smluvnímu období uvedenému v Dokumentu o oprávnění (Proof of Entitlement).

5.2.2 Pokračující fakturace

Je-li v Dokumentu objednávky uvedena pokračující fakturace, budete mít i nadále přístup ke Cloud Service a užívání Cloud Service Vám bude fakturováno na bázi pokračující fakturace. Chcete-li ukončit užívání Cloud Service a zastavit proces pokračující fakturace, musíte zaslat IBM nebo svému Obchodnímu partnerovi IBM devadesát (90) dní předem písemnou žádost o zrušení Cloud Service. Poté, co bude zrušen Váš přístup, budou Vám vyfakturovány jakékoli nesplacené poplatky za přístup až do měsíce, v němž zrušení nabylo účinnosti.

5.2.3 Požadavek prodloužení

Je-li v Dokumentu objednávky pro prodloužení uvedena volba "ukončení", znamená to, že k datu ukončení smluvního období bude poskytování Cloud Service ukončeno a Váš přístup ke Cloud Service bude odstraněn. Chcete-li pokračovat v užívání Cloud Service i po datu ukončení, musíte svému obchodnímu zástupci IBM nebo Obchodnímu partnerovi IBM zaslat objednávku za účelem zakoupení nového registračního období.

6. Technická podpora

Technická podpora pro nabídku IBM SaaS a pro Aktivační software (je-li to relevantní) je poskytována během Období registrace. Taková technická podpora je součástí IBM SaaS a není dostupná jako samostatná nabídka.

Informace o technické podpoře jsou k dispozici na adrese: http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

7. Aktivační software

- a. Tato nabídka Cloud Service může zahrnovat aktivační software. Aktivační software smíte používat pouze ve spojení s Vaším užíváním Cloud Service, a to po celou dobu poskytování služby Cloud Service. V rozsahu, v němž aktivační software obsahuje vzorový kód, máte dodatečné právo vytvářet odvozená díla ze vzorového kódu a používat je v souladu uděleným oprávněním. Aktivační software je poskytován v souladu se smlouvou SLA (existuje-li nějaká) jako komponenta služby Cloud Service, jinak je dodáván "JAK JE".

8. Další informace

8.1 Podrobné informace o oprávnění

Do poplatku za registraci IBM Digital Data Exchange jsou zahrnuty následující položky:

- a. Bude Vám poskytnuta jedna instance IBM Digital Data Exchange.
- b. Standardní zpřístupnění až pěti (5) hodin služeb v oblasti vzdálené implementace pro Vaše počáteční užívání IBM Digital Data Exchange. Platnost vzdálených služeb končí 90 dní od data, kdy Vás IBM informovala o tom, že Vám byl udělen přístup ke službě Cloud Service, bez ohledu na to, zda byly vyčerpány všechny hodiny.

8.2 Informace o ochraně soukromí a zásadách ochrany soukromí

Souhlasíte, že (i) uvedete jasný a zřetelný odkaz na Vaši webovou verzi podmínek užívání a zásad ochrany soukromí, které budou zahrnovat odkaz na Vaše postupy i postupy IBM (<http://www.ibm.com/software/marketing-solutions/privacy/index.html>) týkající se shromažďování a užívání osobních údajů; (ii) uvedete upozornění, že IBM umístí Vaším jménem soubory cookies a obrázky typu gif/web beacon do počítače návštěvníka, s vysvětlením účelu a využití takové technologie; a (iii) v rozsahu vyžadovaném právními předpisy získáte souhlas od návštěvníků webových stránek dříve, než IBM Vaším jménem nebo Vy sami vložíte obrázky typu gif/web beacon do zařízení návštěvníka.

Berete na vědomí a souhlasíte s tím, že IBM smí v rámci své běžné obchodní činnosti a podpory služeb Cloud Service ve vztahu k užívání služeb Cloud Service prostřednictvím sledovacích a jiných technologií od Vás (Vašich zaměstnanců a smluvních partnerů) shromažďovat osobní údaje. IBM tak činí za účelem získání statistik užívání a informací o efektivitě našich služeb Cloud Service, které IBM umožní zlepšit zkušenosti uživatelů a/nebo přizpůsobit interakce na míru. Potvrzujete, že získáte nebo jste získali souhlas, který IBM zmocňuje ke zpracování shromážděných osobních údajů v souladu s příslušnými právními předpisy, a to pro výše uvedené účely v rámci IBM, jiných společností náležejících IBM a jejich subdodavatelů, kdekoli IBM a její subdodavatelé provádějí obchodní činnost. IBM vyhoví požadavkům Vašich zaměstnanců a smluvních partnerů, pokud jde o přístup, aktualizaci, opravu nebo vymazání jejich shromážděných osobních údajů.

8.3 Lokality, v nichž jsou využívány výhody

V případech, kdy je to relevantní, budou daně založeny na lokalitě(ách), kterou(é) jste uvedli jako místo, kde využíváte výhod služeb Cloud Service. IBM uplatní daně na základě obchodní adresy, která byla při objednání služby Cloud Service uvedena jako primární lokalita pro využívání výhod, ledaže byste IBM poskytli doplňující informace. Nesete odpovědnost za aktualizaci takových informací a za informování IBM o jakýchkoli změnách.