Příloha Podmínek zpracování osobních údajů

Tato Příloha Podmínek zpracování osobních údajů (dále jen „**Příloha Podmínek**“) upravuje zpracování osobních údajů pro uvedenou Službu.

* 1. Zpracování

IBM bude jako zpracovatel zpracovávat (zejména nahlížet) Osobní údaje Subjektů údajů Zákazníka v rámci Služby dle popisu uvedeném ve Smlouvě a dle této Přílohy Podmínek.

* + 1. Délka doby zpracování

IBM bude za účelem poskytování Služby jednorázových zásahů technické podpory ve smyslu Smlouvy (dále jen „účel“) zpracovávat Osobní údaje Subjektů údajů Zákazníka v rozsahu, který je blíže specifikován v čl. 2.2.1 této Přílohy Podmínek vždy po dobu nezbytnou pro provedení jednorázového zásahu po dobu platnosti Smlouvy.

* + 1. Aktivity zpracování

Aktivity zpracování ve vztahu k Osobním údajům Subjektů údajů Zákazníka zahrnují:

1. Nahlížení.
	1. Osobní údaje Zákazníka
		1. Kategorie Subjektů údajů Zákazníka

Zpracovatel bude zpracovávat Osobní údaje následujících Subjektů údajů Zákazníka:

1. Zaměstnanců Zákazníka;
2. Žadatelů využívající službu poskytovanou Zákazníkem.

Zákazník bude IBM informovat o veškerých potřebných změnách výše uvedeného seznamu písemnou formou do datové schránky IBM (*číslo datové schránky:* ***e69bcfy***). Pokud jsou vyžadovány změny sjednaného zpracování dle seznamu Kategorií Subjektů údajů Zákazníka, Zákazník je povinen poskytnout IBM Doplňující pokyny v souladu s Podmínkami.

* + 1. Typy Osobních údajů a Zvláštní kategorie Osobních údajů
			1. Typy Osobních údajů

Následující seznam uvádí, které Typy Osobních údajů Subjektu údajů Zákazníka mohou být zpracovávány pro daný účel:

1. Schopnosti a kompetence fyzické osoby
	1. Vzdělání a odborné certifikace
	2. Informace o profesi a pracovním poměru
	3. Zaměstnavatel
2. Charakteristiky fyzické osoby
	1. Biometrické údaje (otisky prstů, biometrická fotografie)
	2. Adresní údaje
	3. Národnost a občanství
	4. Důvod zamítnutí žádosti (např. údaje související s trestnými činy a přestupky)
3. Identita fyzické osoby
	1. Státní identifikace
	2. Identifikační číslo (zejména rodné číslo, číslo dokladu, zaměstnanecké číslo)
	3. Přihlašovací údaje pro přístup ke konzulárním systémům
	4. Data o připojení a síťové konektivitě
	5. Jméno osoby
	6. Datum narození
	7. Technologické identifikátory (zejména číslo žádosti, IP adresa)

IBM může zpracovávat výše uvedené Osobní údaje všech Subjektů údajů v souladu se Smlouvou a dle GDPR.

* + - 1. Zvláštní kategorie osobních údajů

Následující seznam stanovuje, které Zvláštní kategorie Osobních údajů Subjektu údajů Zákazníka mohou být za sjednaným účelem zpracovávány.

1. Biometrické údaje
2. Osobní údaje související s trestnými činy a přestupky
	* + 1. Obecné

Seznamy uvedené v částech 2.2.1 a 2.2.2 výše poskytují informace o tom, jaké Typy Osobních údajů Zákazníka, a které Zvláštní kategorie Osobních údajů Zákazníka mohou být zpracovávány v této Službě.

S ohledem na povahu Služby se IBM zavazuje, že bude zpracovávat Osobní údaje Subjektů údajů Zákazníka dle pokynů Zákazníka a v souladu s GDPR. V případě, jakékoliv změny týkající se Typu Osobních údajů, které IBM zpracovává, Zákazník bude IBM informovat o veškerých potřebných změnách výše uvedených seznamů písemnou formou do datové schránky IBM (**e69bcfy**). IBM zpracuje veškeré Typy osobních údajů Zákazníka a Zvláštní kategorie Osobních údajů Zákazníka uvedené výše v souladu se Smlouvou. Pokud změny seznamů Typů Osobních údajů Zákazníka nebo Zvláštních kategorií Osobních údajů Zákazníka vyžadují změny sjednaného Zpracování, Zákazník je povinen poskytnout IBM Doplňující pokyny v souladu s Podmínkami.

* 1. Technická a organizační opatření a Přidělení odpovědnosti

Technická a organizační opatření (TOMs) včetně oblastí odpovědnosti jednotlivých stran vztahující se ke Službě jsou následující a jsou definována s ohledem na skutečnost, že IBM zpracovává Osobní údaje Subjektů údajů Zákazníka vždy na prostředcích Zákazníka:

|  |  |  |
| --- | --- | --- |
| **Krátký popis** | **Popis kontrolních opatření** | **Odpovědná strana** |
| Opakované použití záložních médií | Vymazávejte a odstraňujte všechny OÚ z úložných zařízení zálohy ve správě IBM tak, aby nebylo možné získat přístup k OÚ, ani je znovu vytvořit poté, co bude zařízení vyřazeno, nebo opakovaně použito. | Zákazník |
| Šifrování systémů | Šifrujte OÚ uložené na systémech zákazníka spravovaných IBM. | Zákazník |
| Ochrana šifrovacích klíčů | Ukládejte šifrovací klíče používané k ochraně OÚ v systémech zákazníka spravovaných IBM způsobem stanoveným pro zabránění neoprávněnému přístupu. | Zákazník |
| Šifrujte zálohy | Šifrujte OÚ na přenosných záložních úložných médiích používaných pro zálohování dat ze systémů zákazníka spravovaných IBM. | Zákazník |
| Ochrana záloh | Skladujte záložní média obsahující OÚ v uzamčených kontejnerech, pokud se tato média právě nepoužívají. | Zákazník |
| Omezení USB jednotky | Zaveďte technická kontrolní opatření, která jsou navržena k tomu, aby pomohla předejít neoprávněnému přenosu OÚ z pracovních stanic zákazníka spravovaných IBM na USB jednotky nebo jiná externí média, nebo ho zjistila a centrálně oznámila. | Zákazník |
| Uzamykání obrazovky | Konfigurujte uzamčení obrazovky pro omezení přístupu k pracovním stanicím zákazníka, spravovaným IBM, bez přítomnosti uživatele, které zpracovávají OÚ. | Zákazník |
| Zabezpečení datových center zákazníka | Umístěte systémy zákazníka spravované IBM, které ukládají OÚ, v zařízeních s omezením přístupu, která umožňují přístup pouze oprávněnému personálu. | Zákazník |
| Prevence ztráty síťových dat | Implementujte síťové senzory, které pomáhají zjišťovat a blokovat pokusy o exfiltraci OÚ ze sítí spravovaných IBM. | Zákazník |
| Omezení přístupu k údajům | Implementace kontrol pro zabránění tomu, aby správci získali kopie OÚ zpracovávaných v zákaznických systémech spravovaných IBM.  | Zákazník |
| Zálohování dat | Denně zálohujte systémy zákazníka spravované IBM, které obsahují OÚ, do šifrovaného úložiště. Minimálně jeden cíl zálohování nesmí být soustavně adresovatelný prostřednictvím volání operačního systému. | Zákazník |
| Testování záloh | Pravidelně ověřujte integritu procesu zálohování prováděním testování obnovení dat. | Zákazník |
| Ukládání záloh na odděleném umístění | Záložní média PI skladujte na vzdáleném umístění, odděleně od produktivních systémů. | Zákazník |
| Zotavení z havárie | Zaveďte opatření (funkce) pro zotavení z havárie, jejichž úkolem bude obnovit fungování systému OÚ ve sjednané časové lhůtě, která musí vycházet z vyhodnocení dopadu. Server a systémy obnovy by měly mít zavedená bezpečnostní opatření minimálně tak přísná, jako jsou ta, která platí pro primární server. Doporučujeme provádět a dokumentovat kontrolu plánování DR. | Zákazník |
| Reakce na incidenty | Udržujte možnosti vyšetřování incidentu a reakce na něj prostřednictvím informačních technologií dostatečné pro splnění platných právních předpisů, včetně vztahu k oznamování narušení bezpečnosti údajů. | Zákazník |
| Přehled systémů | Veďte přesné přehledy systémů zákazníka připojených do sítě spravovaných IBM a označte systémy, které zpracovávají OÚ. | Zákazník |
| Přehled softwaru | Veďte přesné přehledy softwaru na systémech zákazníka spravovaných IBM, včetně verzí a výchozích operačních systémů, u systémů, které zpracovávají OÚ. | Zákazník |
| Šifrujte aplikace | Konfigurujte aplikace umístěné v systémech zákazníka spravovaných IBM tak, aby šifrovaly OÚ při přenosu přes jakoukoliv síť. | Zákazník |
| Ochrana před neoprávněným vniknutím do sítě | Zaveďte senzory systémů ochrany před neoprávněným vniknutím na sítích, které obsahují systémy zákazníka spravované IBM, které zpracovávají OÚ. | Zákazník |
| Segmentace sítě | Segmentujte sítě zákazníka, jako jsou systémy zákazníka spravované IBM, které zpracovávají osobní údaje, aby byly v samostatných logických sítích nebo sítích VLAN s kontrolami firewallu, které umožní obousměrný provoz pouze se schválenými zdroji. | Zákazník |
| Host firewally | Aplikujte Host firewally nebo nástroj filtrování portů na systémech zákazníka spravovaných IBM, které zpracovávají OÚ, s výchozím pravidlem odmítnutí, které ruší veškerý provoz, kromě těch služeb a portů, které jsou výslovně povoleny. | Zákazník |
| Integrita síťových zařízení | Znovu ověřujte pravidla brány firewall minimálně jednou ročně u zařízení, která chrání systémy zákazníka spravované IBM, které zpracovávají OÚ. Veškeré změny těchto konfigurací dokumentujte a schvalujte dle standardního procesu řízení změn. | Zákazník |
| Časové lhůty pro opravy | Použijte opravy zabezpečení na zákaznické systémy spravované IBM, které zpracovávají OÚ během pravidelně plánovaného změnového okna. Změnové okno musí být zajištěno dle následujícího rozvrhu: Systémy s přístupem k Internetu: minimálně jednou za 14 dní Systémy bez přístupu k Internetu: minimálně jednou za 30 dní | Zákazník |
| Podpora softwaru | Zajistěte, aby veškeré používané verze softwaru (operační systémy, aplikace, prohlížeče, e-mailoví klienti, middleware atd.) na systémech zákazníka spravovaných IBM, které zpracovávají OÚ, byly aktuálně podporovány příslušnými dodavateli. | Zákazník |
| Testování softwaru | Testujte nový software (včetně oprav, servisních balíčků a dalších aktualizací) v neproduktivním prostředí před jejich přesunutím do produktivních prostředí systémů zákazníka spravovaných IBM, které zpracovávají OÚ. | Zákazník |
| Provádějte opravy aplikací spravovaných IBM | Aplikujte opravy na middleware spravovaný IBM a na aplikace v systémech zákazníka spravovaných IBM, které zpracovávají OÚ. | Zákazník |
| Provádějte opravy aplikací spravovaných zákazníkem | Aplikujte opravy na middleware spravovaný zákazníkem a na aplikace v systémech zákazníka spravovaných IBM, které zpracovávají OÚ. | Zákazník |
| Opravy síťových zařízení | Aplikujte opravy zabezpečení síťových zařízení zákazníka spravovaných IBM, která hostují nebo chrání systémy zákazníka, které zpracovávají OÚ. | Zákazník |
| Opravy zařízení pro ukládání | Aplikujte upgrady firmwaru úložných zřízení zákazníka spravovaných IBM, která zpracovávají OÚ. | Zákazník |
| Monitorování privilegovaného přístupu | Monitorujte systémy zákazníka spravované IBM, které zpracovávají OÚ, z hlediska vytváření neoprávněných správcovských ID uživatele nebo neoprávněného udílení oprávnění stávajícím ID uživatele. | Zákazník |
| Monitorování integrity souboru | Zaveďte monitorování integrity souborů ke zjištění neoprávněných změn systémových a konfiguračních souborů na systémech zákazníka spravovaných IBM, které zpracovávají OÚ. | Zákazník |
| Požadavky na protokolování | Protokoly systému a událostí ze systémů zákazníka spravovaných IBM, které zpracovávají OÚ, je třeba zkopírovat do systému mimo kontrolu správce systému nebo obsluhy, jejichž činnosti jsou do protokolu zahrnuty.  | Zákazník |
| Požadavky na monitorování | Je třeba používat nástroje monitorování protokolů k analýze protokolů ze systémů zákazníka spravovaných IBM, které zpracovávají OÚ, z hlediska podezřelého chování a zasílání výstrah.  | Zákazník |
| Uchovávání protokolů  | Protokoly ze systémů zákazníka spravovaných IBM, které zpracovávají OÚ, je třeba uchovávat po dobu vyžadovanou platnými právními předpisy. | Zákazník |
| Správa konfigurace systému | Nasaďte nástroje řízení konfigurace systému, které v pravidelných plánovaných intervalech automaticky vynutí a znovu nasadí nastavení konfigurace systémů zákazníka spravovaných IBM, které zpracovávají OÚ. | Zákazník |
| Skenování ohrožení zabezpečení | Provádějte měsíční skenování ohrožení zabezpečení systémů zákazníka spravovaných IBM, které zpracovávají OÚ. Skenery je třeba pravidelně aktualizovat, aby zjistily nejnovější ohrožení zabezpečení. | Zákazník |
| Testujte připravenost organizace | Nejdůležitější testy podle tabulky "červeného týmu" provádějte minimálně jednou ročně s cílem testovat připravenost zákazníka k identifikaci a zmírnění kyber útoků. | Zákazník |
| Testování penetrace | Minimálně jednou ročně provádějte externí a interní testy penetrace na systémech zákazníka spravovaných IBM, které zpracovávají OÚ. Dovolujeme si upozornit, že tento požadavek není splněn použitím automatických testů zabezpečení, a je třeba provádět testy penetrace. | Zákazník |
| Školení pro povědomí o zabezpečení | Zaveďte povinné roční programy povědomí o zabezpečení pro zaměstnance a dodavatele zákazníka, kteří pracují se systémy zákazníka spravovanými IBM, které zpracovávají OÚ. | Zákazník |
| Opakované ověření ID uživatelů zákazníka | Jednou ročně opakovaně ověřujte obchodní potřebu ID uživatelů zákazníka a související oprávnění s přístupem k OÚ v systémech zákazníka spravovaných IBM. | Zákazník |
| Automatické odhlášení OS | Automaticky odhlašujte uživatele ze systémů zákazníka spravovaných IBM, které zpracovávají OÚ, po uplynutí stanovené doby nečinnosti. | Zákazník |
| Omezení přístupu  | Omezte přístup k OÚ v systémech souborů, sdílených místech sítě, aplikacích a databázích s využitím seznamů kontroly přístupu v systémech zákazníka spravovaných IBM pouze na osoby s platnou potřebou. | Zákazník |
| Osobní odpovědnost | Zaveďte odpovídající kontrolní opatření pro zajištění osobní odpovědnosti u systémů zákazníka spravovaných IBM, které zpracovávají OÚ. | Zákazník |
| Vícefaktorové ověření správy | Pokud je to technicky možné, vyžadujte vícefaktorové ověření pro přístup všech správců systému k systémům zákazníka spravovaným IBM, které zpracovávají OÚ. | Zákazník |
| Uzamčení účtu OS | Zaveďte kontroly pro zablokování útoků spojených s hádáním hesla hrubou silou u systémů zákazníka spravovaných IBM, které zpracovávají OÚ. Například účty uzamkněte po stanoveném počtu nezdařených pokusů o přihlášení. | Zákazník |
| Délka hesla OS | V případě, že vícefaktorové ověření není podporováno, je-li to technicky možné, vyžadujte dlouhá hesla (více než 14 znaků) u ID uživatelů s přístupem k systémům zákazníka spravovaným IBM, které zpracovávají OÚ. | Zákazník |
| Šifrování síťového přístupu | Šifrujte veškeré síťové přístupy k systémům zákazníka spravovaným IBM, které zpracovávají OÚ. (Např. nelze používat žádné čistě textové protokoly, jako jsou HTTP, FTP nebo Telnet. Protokoly, jako jsou RDP a VNC, je třeba konfigurovat pro používání šifrování.). | Zákazník |
| Šifrování souboru ID | Šifrujte nebo hašujte veškeré ověřovací soubory a zajistěte, aby byly tyto soubory přístupné pouze pro kmenové nebo správcovské účty pro systémy zákazníka spravované IBM, které zpracovávají OÚ. | Zákazník |
| Ukončení ID zákazníka | Odvolejte přístup pro ID uživatele Zákazníka s přístupem k OÚ na systémech zákazníka spravovaných IBM v co nejkratším možném čase po skončení platnosti požadavku na obchodní potřebu.  | Zákazník |
| Opakované ověření ID uživatelů IBM | Jednou ročně opakovaně ověřujte obchodní potřebu ID uživatelů IBM a související oprávnění s přístupem k OÚ na systémech zákazníka spravovaných IBM. | IBM |
| Automatické uzamčení aplikace | Zaveďte kontroly pro zablokování útoků spojených s hádáním hesla hrubou silou u aplikací, které běží na systémech zákazníka spravovaných IBM, které zpracovávají OÚ. Například účty uzamkněte po stanoveném počtu nezdařených pokusů o přihlášení. | Zákazník |
| Délka hesla k aplikaci | V případě, že vícefaktorové ověření není podporováno, je-li to technicky možné, vyžadujte dlouhá hesla (více než 14 znaků) u ID uživatelů s přístupem k aplikacím, které běží na systémech zákazníka spravovaných IBM, které zpracovávají OÚ. | Zákazník |

Zákazník potvrzuje svou povinnost implementovat příslušná TOMs v rámci své vlastní oblasti odpovědnosti dle ustanovení výše nebo dle požadavků příslušných Právních předpisů o ochraně údajů.

IBM získala ve vztahu ke Službě následující standardní certifikace zabezpečení a osobní datové pečeti a značky:

* ISO 9001
* ISO 20000
* ISO 27001
	1. Vymazání a vrácení Osobních údajů Subjektů údajů Zákazníka

IBM v souladu s pokyny Zákazníka vymaže nebo vrátí Zákazníkovi veškeré Osobní údaje Subjektů údajů Zákazníka po ukončení zpracování za sjednaným účelem, a vymaže případné kopie, pokud příslušný právní předpis nepožaduje uložení daných osobních údajů.

* 1. Dílčí zpracovatelé

IBM je oprávněna využívat následující Dílčí zpracovatele ke zpracování Osobních údajů Subjektů údajů Zákazníka za sjednaným účelem

* + - * 1. Společnosti IBM se sídlem v Evropském hospodářském prostoru nebo zemích, které jsou Evropskou komisí považovány za země zajišťující přiměřenou ochranu

| Jméno Dílčího zpracovatele | Adresa Dílčího zpracovatele |
| --- | --- |
| Společnosti skupiny IBM, které na základě závazných vnitropodnikových pravidel (BCR) garantují dostatečnou úroveň ochrany osobních údajů pro celou skupinu. (Povolení UOOU ze dne 3. listopadu 2017, č.j. UOOU-106-74/17-2) | Konkrétní identifikace jednotlivých IBM společnosti je možno nalézt po zvolení příslušné země ze seznamu v tomto odkazu:<https://www.ibm.com/planetwide/> |

* + - * 1. Nezávislí Dílčí zpracovatelé se sídlem v Evropském hospodářském prostoru nebo zemích, které jsou Evropskou komisí považovány za země zajišťující přiměřenou ochranu

| Jméno Dílčího zpracovatele | Země, kde Dílčí zpracovatel sídlí |
| --- | --- |
|  |  |

* + - * 1. Importér dat IBM (společnosti IBM se sídlem mimo Evropský hospodářský prostor nebo země, u nichž má Evropská komise za to, že zajišťují přiměřenou ochranu)

| Jméno Importéra dat IBM | Adresa Importéra dat IBM |
| --- | --- |
|  |  |

* + - * 1. Nezávislý Importér dat (společnosti jiné než IBM se sídlem mimo Evropský hospodářský prostor nebo země, u nichž má Evropská komise za to, že zajišťují přiměřenou ochranu)

| Jméno Nezávislého importéra dat | Země, kde sídlí Nezávislý dovozce údajů |
| --- | --- |
|  |  |

IBM bude Zákazníka informovat o zamýšlených změnách Dílčích zpracovatelů písemnou formou. Za písemnou formu je považováno doručení do datové schránky Zákazníka (**e4xaaxh**)

* 1. Pověřenec pro ochranu osobních údajů Zákazníka

Bližší informace o Pověřenci pro ochranu údajů Zákazníka jsou dostupné na adrese: [*https://www.mzv.cz/jnp/cz/o\_ministerstvu/zpracovani\_a\_ochrana\_osobnich\_udaju/index.html*](https://www.mzv.cz/jnp/cz/o_ministerstvu/zpracovani_a_ochrana_osobnich_udaju/index.html)

* 1. Kontaktní osoba pro Ochranu osobních údajů IBM

Kontaktní osobu pro Ochranu osobních údajů IBM lze kontaktovat na adrese DPA.Help.project@uk.ibm.com.