

Příloha dodatku o zpracování dat

Tato Příloha dodatku o zpracování dat (Příloha DPA) stanoví DPA pro uvedenou Službu.

1. Zpracování

SPCSS bude zpracovávat Osobní údaje Zákazníka pro Službu dle ustanovení této přílohy DPA.

1.1 Délka trvání zpracování

SPCSS uchová Osobní údaje Zákazníka po Dobu uchování v rámci zálohy systému.

1.2 Aktivity zpracování

Aktivity zpracování ve vztahu k Osobním údajům Zákazníka zahrnují:

- Spojování
- Kopírování
- Vymazávání
- Odkazy
- Analýza
- Čtení
- Přijímání
- Odesílání
- Sdílení
- Ukládání
- Zálohování
- Obnovování
- Aktualizace

2. Osobní údaje Zákazníka

2.1 Kategorie Dotčených osob (Datových subjektů)

- Osoby, jejichž osobní údaje zpracovává při plnění svých povinností stanovených právními předpisy, anebo při plnění svých úkolů prováděných ve veřejném zájmu.
- Zaměstnanci Zákazníka
- Účastníci výběrových řízení a účastníci veřejných dražeb
- Osoby oprávněné k výkonu věcných práv zatěžujících majetek ve vlastnictví ČR, s nímž je příslušný správce oprávněn hospodařit, anebo s nímž hospodaří Správce,
- Zaměstnanci organizačních složek státu v působnosti zákona 219/2000 Sb., o majetku ČR a jejím vystupování v právních vztazích
- Zaměstnanci obcí
- Státní instituce, organizace a Organizační složky státu, které jsou ve spojení se Zákazníkem
- Zaměstnanci dodavatelů Zákazníka

Výše uvedený seznam obsahuje informace o Kategoriech Subjektů údajů, jejichž Osobní údaje mohou být v rámci Služby obecně zpracovávány.

S ohledem na povahu služby Zákazník potvrzuje, že SPCSS není schopna ověřovat nebo uchovávat výše uvedený seznam Kategorii Datových subjektů. Z tohoto důvodu bude Zákazník SPCSS informovat o veškerých potřebných změnách výše uvedeného seznamu písemně. SPCSS bude zpracovávat výše uvedené Osobní údaje všech Subjektů údajů v souladu se Smlouvou. Pokud jsou vyžadovány změny sjednaného zpracování dle seznamu Kategorii Datových subjektů, Zákazník je povinen poskytnout SPCSS Doplňující pokyny v souladu s DPA.

2.2 Typy Osobních údajů a Zvláštní kategorie Osobních údajů

2.2.1 Typy Osobních údajů

Následující seznam uvádí, které Typy Osobních údajů Zákazníka mohou být obecně zpracovávány v rámci Služby:

- Schopnosti a kompetence fyzické osoby
 - Vzdělání
 - Informace o profesi a pracovním poměru
 - Obchodní vztahy
- Charakteristiky fyzické osoby
 - Ekonomické a finanční údaje
 - Národnost a občanství
- Identita fyzické osoby
 - Státní příslušnost
 - Identifikační číslo
 - Přihlašovací údaje
 - Data o připojení
 - Online identifikátor
 - Jméno a příjmení osoby
 - Technologické identifikátory
 - Telefonie
 - Adresa
 - Datum narození
 - Rodné číslo
 - Místo narození
 - Rodné příjmení
 - E-mail
 - Pohlaví
 - Datum úmrtí
- Umístění fyzické osoby
 - Fyzické místo fyzické osoby

2.2.2 Zvláštní kategorie osobních údajů

Následující seznam upravuje, které Speciální kategorie Osobních údajů Zákazníka mohou být obecně v rámci Služby zpracovávány.

- Není aplikovatelné pro tento projekt.

2.2.3 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 Zákazník potvrzuje, že SPCSS není schopna ověřit ani uchovávat výše uvedené Typy Osobních údajů Zákazníka a Speciálních kategorií Osobních údajů Zákazníka. Z tohoto důvodu bude Zákazník SPCSS informovat o veškerých potřebných změnách výše uvedených seznamů písemně. SPCSS zpracuje veškeré Typy osobních údajů Zákazníka a Speciální 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 SPCSS Doplňující pokyny v souladu s DPA.

3. Technická a organizační opatření

Zpracovatel tímto prohlašuje, že ochrana osobních údajů podléhá interním bezpečnostním předpisům Zpracovatele v rámci jeho systému řízení bezpečnosti informací, který je v souladu s bezpečnostními požadavky ISO 27001.

Zpracovatel se zavazuje, že zpracování údajů bude zabezpečeno zejména následujícím způsobem:

- a) k osobním údajům budou mít přístup pouze oprávněné osoby Zpracovatele, které budou mít Zpracovatelem stanoveny podmínky a rozsah zpracování údajů a každá taková osoba bude přistupovat k osobním údajům pod svým jednoznačným identifikátorem;
- b) oprávněné osoby Zpracovatele, které zpracovávají osobní údaje podle této Smlouvy, jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opářeních, jejichž zveřejnění by ohrozilo jejich zabezpečení. Zpracovatel zajistí jejich prokazatelné zavázání k této povinnosti. Zpracovatel zajistí, že tato povinnost pro Zpracovatele a jejich oprávněné osoby bude trvat 5 let po skončení pracovního nebo jiného vztahu ke Zpracovateli. V případě porušení této povinnosti se Zpracovatel zavazuje nahradit veškerou způsobenou škodu.

Technická a organizační opatření (TOMs) včetně oblastí odpovědnosti jednotlivých stran vztahující se ke Službě jsou následující:

Technická a organizační opatření (TOMs) vztahující se ke Službě v zodpovědnosti SPCSS jsou následující:

- Evidovat záznamy o schválení SPCSS dokumentů o bezpečnosti a soukromí dat (dále jen „DS & P“) a zpřístupňovat je pro kontrolní a auditní účely.
- Vytvořit a zkontrolovat SPCSS dokumenty DS & P a pravidelně je revidovat.
- Uložit a archivovat dokumentaci související s Projektem v zabezpečeném úložišti.
- Spravovat dokumenty podle zásad společnosti SPCSS.
- Zajistit interně dostupnost vhodných dovedností v oblasti DS & P.
- Definovat role a odpovědnosti v oblasti zabezpečení a ochrany osobních údajů na podnikové úrovni SPCSS.
- Interně provádět pravidelné DS & P školení.
- Interně provádět pravidelné DS & P školení subdodavatelů.
- Provádět pravidelné DS & P školení na SPCSS organizační úrovni.
- Interně provádět pravidelné školení o správném zacházení s důvěrnými údaji.
- Definovat pravidla pro zacházení s hesly v pokynech společnosti SPCSS a provádět každoroční interní školení s cílem zvýšit informovanost zaměstnanců.
- Interně zavést fyzickou bezpečnost na pracovišti.
- Kontrolovat přístup na pracoviště SPCSS.
- Správa přístupů k log souborům na serverech ve správě SPCSS.
- Kritéria pro hesla, aby podle dohody na projektové úrovni splňovala požadavky zákazníka a / nebo standardy SPCSS.
- Kontrolovat přístup k interním systémům SPCSS v souladu se zásadami SPCSS.
- Realizovat obnovení po havárii a možnosti zálohování k obnovení osobních dat klienta.
- Chránit a kontrolovat přístup do zabezpečených prostor SPCSS
- Zaznamenávání činností systému, uživatelů a administrátorů.
- Aktualizace bezpečnostní dokumentace.
- Zvládání bezpečnostních událostí a incidentů (formu zavedeného HelpDesku. Jednotlivé události a incidenty jsou do helpdesku zanášeny a je sledován a logován průběh jejich řešení).
- Řízení kontinuity činností.

Technická a organizační opatření (TOMs) vztahující se ke Službě v zodpovědnosti zákazníka jsou následující:

- Organizační bezpečnost, jsou ustanoveny bezpečnostní role. Dodavatel si je vědom ustanovené role manažera kybernetické bezpečnosti na straně Správce. Bezpečnostní role jsou popsány v bezpečnostní politice Správce.
- Spravovat uživatelské přístupy k technickým prostředím Projektu.
- Spravovat bezpečný přístup k síti a prostřednictvím sítě.

Zákazník potvrzuje svou povinnost implementovat příslušná TOMs ve své oblasti odpovědnosti dle požadavků příslušných Právních předpisů o ochraně údajů.

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

- ISO 9001
- ISO 20000
- ISO 27001

4. Vymazání a vrácení Osobních údajů Zákazníka

Zákazník bude moci vymazávat anebo kopírovat Osobní údaje Zákazníka až do vypršení nebo ukončení Služby. SPCSS vymaže veškeré Osobní údaje Zákazníka po skončení Služby.

5. Dílčí zpracovatelé

SPCSS je oprávněna využívat následující Dílčí zpracovatele ke zpracování Osobních údajů Zákazníka:

- a. 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 ze skupiny IBM, které na základě závazných vnitropodnikových pravidel (tzv. „BCR“) schválených od dozorového orgánu pro ochranu osobních údajů ve Velké Británii - Information Commissioner's Office („ICO“) dne 22. února 2017 a které garantují dostatečnou úroveň ochrany osobních údajů pro celou skupinu. Potvrzení o schválených závazných vnitropodnikových pravidlech je veřejně dostupné a lze nalézt v dokumentu na níže uvedených webových stránkách ICO pod položkou č. 30: https://ico.org.uk/media/for-organisations/binding-corporate-rules/1042460/binding-corporate-rules-ico-authorisation.pdf . Na základě schválených BCR dozorovým orgánem ICO bylo dne 3. listopadu 2017 českým Úřadem pro ochranu osobních údajů vydáno rozhodnutí č.j. UOOU-10674/17/2, povolující předání osobních údajů pro společnost IBM Česká republika, spol. s r.o.	https://www.ibm.com/cz-cs/

- b. 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
██████████	Česká republika
████████████████████	Česká republika
████████████████████	Česká republika

- c. 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
Společnosti ze skupiny IBM, které na základě závazných vnitropodnikových pravidel (tzv. „BCR“) schválených od dozorového orgánu pro ochranu osobních údajů ve Velké Británii - Information Commissioner's Office („ICO“) dne 22. února 2017 a které garantují dostatečnou úroveň ochrany osobních údajů pro celou skupinu. Potvrzení o schválených závazných vnitropodnikových pravidlech je veřejně dostupné a lze nalézt v dokumentu na níže uvedených webových stránkách ICO pod položkou č. 30: https://ico.org.uk/media/for-organisations/binding-corporate-rules/1042460/binding-corporate-rules-ico-authorisation.pdf . Na základě schválených BCR dozorovým orgánem ICO bylo dne 3. listopadu 2017 českým Úřadem pro ochranu osobních údajů vydáno rozhodnutí č.j. UOOU-10674/17/2, povolující předání osobních údajů pro společnost IBM Česká republika, spol. s r.o.	https://www.ibm.com/cz-cs/

- d. 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

- e. Příležitostní zpracovatelé poskytující standardní softwarovou podporu

Jméno Nezávislého importéra dat	Země, kde sídlí Nezávislý dovozce údajů
██████████	Česká republika
██████████	Česká republika
██████████	Česká republika

SPCSS bude Zákazníka informovat o zamýšlených změnách Dílčích zpracovatelů následovně:

- písemně (email je také považován za písemné informování).

6. Mezinárodní přenos dat

Žádný.

7. Inspektor ochrany údajů a další správci

Zákazník je povinen SPCSS písemně poskytnout úplné, správné a aktuální informace o Pracovníkovi pro ochranu údajů a ostatních Správcích (včetně jejich Pracovníků pro ochranu údajů).

8. Kontaktní osoba pro Ochranu osobních údajů SPCSS

Kontaktní osobu pro Ochranu osobních údajů IBM lze kontaktovat na adrese ██████████