**Zpracování osobních údajů osob uvedených v licenčních / podlicenčních smlouvách v rámci Databáze produktů**

# Identifikace správce osobních údajů

Správce osobních údajů

Ministerstvo práce a sociálních věcí

Na Poříčním právu 1/376

128 01 Praha 2

Datová schránka: sc9aavg

Pověřenec Ministerstva práce a sociálních věcí pro ochranu osobních údajů: viz [www.mpsv.cz](http://www.mpsv.cz)

Kontakt na útvar Řídicího orgánu OPZ odpovědný za údaje na portálu OPZ:

Ministerstvo práce a sociálních věcí

Sekce evropských fondů

**Oddělení monitorování a reportingu**

Na Poříčním právu 1/376

128 01 Praha 2

Datová schránka: sc9aavg

# Účel zpracování

Ministerstvo práce a sociálních věcí je jakožto Řídicí orgán OPZ odpovědné za zajištění opatření potřebných k poskytování informací a sdělení veřejnosti o projektech podporovaných OPZ a k jejich propagaci (viz příloha XII nařízení Evropského parlamentu a Rady (EU) č. 1303/2013 ze dne 17. 12. 2013, o společných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu, Fondu soudržnosti, Evropském zemědělském fondu pro rozvoj venkova a Evropském námořním a rybářském fondu, o obecných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu, Fondu soudržnosti a Evropském námořním a rybářském fondu a o zrušení nařízení Rady (ES) č. 1083/2006). Čl. 115 odst. 1 písm. d) výše uvedeného nařízení dále kromě jiného zavazuje Řídicí orgán OPZ seznámit občany EU s výsledky a dopady projektů podpořených z OPZ.

Za účelem seznámení veřejnosti s produkty projektů podpořených z OPZ a zejména za účelem dalšího využití těchto produktů uzavírá Řídicí orgán OPZ s realizátory projektů podpořených z OPZ licenční či podlicenční smlouvy. Díky těmto smlouvám Řídicímu orgánu OPZ vzniká oprávnění k šíření daného produktu. Ve smlouvách jsou obsaženy osobní údaje osob oprávněných jednat za subjekt, který Řídicímu orgánu OPZ poskytuje licenci, resp. podlicenci k šíření daného produktu vzniklého díky realizaci projektu podpořeného z OPZ.

# Popis kategorií subjektů údajů a kategorií osobních údajů

Subjekty údajů jsou osoby, které jsou jakožto osoby oprávněné jednat za subjekt, který Řídicímu orgánu OPZ poskytuje licenci, resp. podlicenci k šíření produktu vzniklého díky realizaci projektu podpořeného z OPZ, uvedeny v příslušné licenční či podlicenční smlouvě.

K těmto osobám jsou zpracovávány maximálně tyto kategorie údajů:

* Základní údaje kontaktní osoby (jméno a příjmení a e-mail)

# Popis kategorií příjemců, kterým byly nebo budou osobní údaje zpřístupněny

Účelem sběru a zpracování osobních údajů osob jednajících za realizátory projektů podpořených z OPZ ve věci licenční či podlicenční smlouvy, na základě které Řídicímu orgánu OPZ vzniká oprávnění k šíření produktu daného projektu, je prokázání řádného provádění OPZ. Údaje mohou být v  případě kontroly či auditu dále zpřístupněny orgánům, které jsou oprávněny ke kontrole či auditu OPZ, kterými jsou zejména orgány finanční správy, Ministerstvo financí, Nejvyšší kontrolní úřad, Evropská komise a Evropský účetní dvůr.

Osobní údaje nejsou předávány do zemí mimo Evropskou unii, ani mezinárodním organizacím.

# Plánovaná lhůta pro výmaz kategorií údajů

Výmaz všech kategorií osobních údajů bude zajištěn po uplynutí doby, na kterou byla smlouva uzavřena, přičemž smlouvy jsou uzavírány na dobu do 31. 12. 2036.

# Obecný popis technických a organizačních opatření

Všichni zaměstnanci Ministerstva práce a sociálních věcí jsou povinni dodržovat vnitřní předpisy upravující ochranu osobních údajů a také obecnější politiky, jako je bezpečnostní politika ICT, zákon č. 234/2014 Sb., o státní službě, resp. zákon č. 262/2006 Sb., zákoník práce, služební předpisy týkající se etických principů, interní Směrnici k zabezpečení ochrany osobních údajů aj.

* Je zajištěno seznámení oprávněných osob s jejich konkrétními povinnostmi při zpracování osobních údajů vzhledem k působnosti daného útvaru a  vykonávané činnosti.
* K osobním údajům v elektronické podobě mají přístup pouze oprávněné osoby s přidělenými přístupovými právy a přihlašovacími údaji, IT systémy jsou chráněny proti neoprávněnému přístupu.
* Zpracovávající osoby jsou povinny zachovávat mlčenlivost o zpracovávaných osobních údajích a o přijatých opatřeních k jejich ochraně, o nichž se v souvislosti se svým zaměstnáním nebo plněním smlouvy dozvěděly, a to i po skončení svého pracovního či služebního poměru u MPSV nebo platnosti smlouvy. Tito pracovníci nejsou oprávněni pořizovat kopie záznamů obsahujících osobní údaje či osobních údajů samých pro jinou než pracovní potřebu, obdobně nejsou oprávněni toto umožnit jiným osobám. Jsou povinni s případnými kopiemi nakládat stejně jako s originálem.
* Ministerstvo práce a sociálních věcí má nastaveny zásady hlášení nedostatků.

Obecně lze konstatovat, že Ministerstvo práce a sociálních věcí splňuje požadavky na ochranu osobních údajů ve všech těchto agendách:

* Politika bezpečnosti informací (určeny požadavky týkající se vytvoření a udržování aktuální sady bezpečnostní dokumentace, ve které jsou stanoveny bezpečnostní požadavky na jednotlivé oblasti informační bezpečnosti, kde se vyskytují a kde se zpracovávají osobní údaje fyzických osob);
* Organizace bezpečnosti informací (existuje dokumentace týkající se stanovení odpovědností v oblasti řízení bezpečnosti IT a její aktualizace);
* Řízení aktiv (stanoveny požadavky přípustného nakládání s osobními údaji);
* Řízení přístupu (stanoveny požadavky na správu a řízení přístupu uživatelů k osobním údajům);
* Bezpečnost provozu (stanoveny požadavky na bezpečnost provozních postupů a  stanovení odpovědností);
* Bezpečnost komunikací (stanoveny požadavky na správu bezpečnosti sítě, se zaměřením na bezpečnost síťových služeb a bezpečnostní opatření v sítích);
* Akvizice, vývoj a údržba systému (stanoveny bezpečnostní požadavky na úpravu a vývoj nových informačních systémů (update) s ohledem na bezpečnost zpracování osobních údajů);
* Vztahy s dodavateli (stanoveny požadavky na bezpečnost osobních údajů ve vztazích s externími dodavateli);
* Řízení incidentů bezpečnosti informací (stanoveny požadavky na řízení bezpečnostních incidentů);
* Fyzická bezpečnost (zajištěna fyzická bezpečnost zařízení, kde jsou zpracovávány osobní údaje).