**Zpracování osobních údajů registrovaných uživatelů portálu OPZ a účastníků akcí řídicího orgánu OPZ**

# 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 jakožto Řídicí orgán OPZ má povinnost na základě čl. 140 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, zajistit auditní stopu o provádění OPZ.

Jistá část provádění OPZ je zajišťována prostřednictvím portálu OPZ ([www.esfcr.cz](http://www.esfcr.cz)). Vymezené úkony prováděné na tomto portálu (přihlášení účastníků na akce pořádané Řídicím orgánem OPZ, editace údajů týkajících se akcí projektu podpořeného z OPZ, vkládání výběrových řízení na vymezené zakázky apod.) jsou vyhrazeny pouze registrovaným uživatelům tohoto portálu.

Dále je Řídicí orgán OPZ povinen uchovávat záznamy o účastnících akcí, které byly v rámci provádění OPZ realizovány z jeho úrovně (např. semináře či konference).

# Popis kategorií subjektů údajů a kategorií osobních údajů

Subjekty údajů jsou osoby, které se zaregistrovaly jako uživatelé portálu OPZ anebo se přihlásily, resp. se účastnily některé z akcí, které byly v rámci provádění OPZ realizovány z úrovně Řídicího orgánu OPZ.

K registrovaným uživatelům portálu OPZ jsou zpracovávány maximálně tyto kategorie údajů:

* Základní údaje osoby (jméno a příjmení a e-mail)
* Doplňující údaje, které osoba může, nicméně nemusí uvést (fotografie či obrázek, titul, telefon, přezdívka, webová stránka, identifikace profilu na sociálních sítích a klientech pro instant messaging)

K účastníkům akce Řídicího orgánu OPZ jsou zpracovávány maximálně tyto kategorie údajů:

* Základní údaje kontaktní osoby (jméno a příjmení, e-mail a organizace, kterou osoba na akci zastupuje)

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

Účelem sběru a zpracování osobních údajů je prokázání řádného provádění OPZ. Údaje mohou být v  případě kontroly či auditu 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 údajů bude zajištěn v souladu s platnou legislativou.

Článek 140 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, zavazuje Řídicí orgán OPZ k zajištění dostupnosti dokladů po dobu vymezenou na tzv. uzavírání účtů programu. Nicméně lhůta navázaná na tzv. uzavírání účtů programu může být přerušena v případě jakéhokoli právního řízení či na základě žádosti Evropské komise. Řídicí orgán OPZ plánuje zajistit výmaz údajů do deseti let od ukončení implementace OPZ.

# 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).