



ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ KONTAKTNÍCH OSOB PRO AKCE REALIZOVANÉ V RÁMCI PROJEKTŮ PODPOŘENÝCH Z OPZ+

1. 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

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

Ministerstvo práce a sociálních věcí

Sekce evropských fondů a mezinárodní spolupráce

Oddělení podpory implementace

Na Poříčním právu 1/376

128 01 Praha 2

Datová schránka: sc9aavg

2. Účel zpracování

Ministerstvo práce a sociálních věcí je jakožto Řídicí orgán OPZ+ odpovědné za zviditelnění podpory při všech činnostech souvisejících s projekty podporovanými z fondů EU, včetně realizace opatření potřebných k poskytování informací a sdělení veřejnosti o projektech podporovaných z OPZ+ a k jejich propagaci (viz čl. 46 nařízení Evropského parlamentu a Rady (EU) č. 1060/2021 ze dne 24. 6. 2021, o společných ustanoveních pro Evropský fond pro regionální rozvoj, Evropský sociální fond plus, Fond soudržnosti, Fond pro spravedlivou transformaci a Evropský námořní, rybářský a akvakulturní fond a o finančních pravidlech pro tyto fondy a pro Azylový, migrační a integrační fond, Fond pro vnitřní bezpečnost a Nástroj pro finanční podporu správy hranic a vízové politiky, dále jen „obecné nařízení“).

Zpracování osobních údajů kontaktních osob pro akce projektů podpořených z OPZ+, které jsou určeny veřejnosti (semináře, workshopy, konference, vzdělávací aktivity, rekvalifikace, poradenské služby apod.) probíhá právě za účelem zviditelnění podpory, čímž se rozumí také poskytování informací a sdělení veřejnosti o aktivitách, které jsou realizovány s podporou Evropského sociálního fondu plus a do kterých se může kdokoli z cílové skupiny účastníků dané akce zapojit. Identifikace kontaktní osoby pro příslušnou akci projektu je nezbytnou podmínkou pro zprostředkování kontaktu mezi realizátorem akce a potenciálními účastníky této akce z řad veřejnosti.

3. Popis kategorií subjektů údajů a kategorií osobních údajů

Subjekty údajů jsou osoby, které realizátoři akcí v rámci projektů podpořených z OPZ+ uvedli jako kontaktní osoby pro příslušnou akci.

K těmto osobám jsou zpracovávány maximálně tyto kategorie údajů:

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

4. Popis kategorií příjemců, kterým byly nebo budou osobní údaje zpřístupněny

Účelem sběru a zpracování osobních údajů kontaktních osob pro akce v rámci projektů podpořených z OPZ+ je poskytování informací a sdělení veřejnosti o realizovaných aktivitách a zejména zprostředkování kontaktu mezi realizátorem akce a potenciálními účastníky této akce z řad veřejnosti. Z tohoto důvodu jsou osobní údaje zveřejněny na portálu OPZ+ (www.esfcr.cz).

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

5. Plánovaná lhůta pro výmaz kategorií údajů

Výmaz všech kategorií údajů bude zajištěn v souladu s platnou legislativou.

Dle čl. 82 obecného nařízení platí minimální lhůta dostupnosti/archivace dokumentace po dobu 5 let počítáno od 31. prosince roku, ve kterém řídicí orgán provedl poslední platbu příjemcům.

Lhůta se přeruší buď v případě soudního řízení, nebo na základě řádně odůvodněné žádosti EK.

Řídicí orgán OPZ+ plánuje zajistit výmaz údajů do deseti let od ukončení implementace OPZ+.

6. 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. 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).