**Zpracování osobních údajů týkajících se zakázek, které byly financovány z projektů podpořených z OP LZZ**

# 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 OP LZZ:

Ministerstvo práce a sociálních věcí

Sekce evropských fondů

**Oddělení klientské podpory a publicity projektů**

Na Poříčním právu 1/376

128 01 Praha 2

Datová schránka: sc9aavg

#  Účel zpracování

Ministerstvo práce a sociálních věcí jakožto Řídicí orgán OP LZZ má povinnost na základě čl. 90 nařízení Rady (ES) č. 1083/2006 ze dne 11. července 2006, o obecných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu a Fondu soudržnosti a o zrušení nařízení (ES) č. 1260/1999, zajistit auditní stopu o provádění OP LZZ.

Agenda osob, které byly zapojeny do realizace výběrových / zadávacích řízení v rámci projektů podpořených z OP LZZ, uveřejňovaných na portálu [www.esfcr.cz](http://www.esfcr.cz/), představuje jednu z oblastí, na kterou se povinnost zachovat záznamy o provádění vztahuje.

# Popis kategorií subjektů údajů a kategorií osobních údajů

Subjekty údajů jsou osoby, které zadavatel zakázky financované z projektu podpořeného z OP LZZ uvedl v dokumentaci k dané zakázce. K těmto osobám jsou zpracovávány maximálně tyto kategorie údajů: jméno a příjmení, telefon a e-mail.

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

Účelem sběru a zpracování osobních týkajících se zakázek je prokázání řádného zadávání zakázek v rámci projektů podpořených z OP LZZ a dodržení pravidel veřejné soutěže. Z tohoto důvodu jsou osobní údaje zveřejněny na portálu OP LZZ ([www.esfcr.cz](http://www.esfcr.cz)). Údaje mohou být v  případě kontroly či auditu dále zpřístupněny orgánům, které jsou oprávněny ke kontrole či auditu OP LZZ, 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 90 nařízení Rady (ES) č. 1083/2006 ze dne 11. července 2006, o obecných ustanoveních o Evropském fondu pro regionální rozvoj, Evropském sociálním fondu a Fondu soudržnosti a o zrušení nařízení (ES) č. 1260/1999, zavazuje Řídicí orgán OP LZZ k zajištění dostupnosti dokladů po dobu vymezenou od tzv. uzavření operačního programu. Nicméně lhůta navázaná na tzv. uzavření operačního programu může být přerušena v případě jakéhokoli právního řízení či na základě žádosti Evropské komise.

# 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).