INTEGROVANÝ REGIONÁLNÍ
OPERAČNÍ PROGRAM

Seminář pro žadatele ke 120. výzvě IROP – Kybernetická bezpečnost II. - SC 1.1 (PR)

MS Teams, 16. 4. 2026

Spolufinancováno Evropskou unií

Ministerstvo pro místní rozvoj

Program

8:45 – 9:00	Prezence účastníků
9:00 – 9:10	Zahájení, aktuální informace o IROP 2021 - 2027 a jeho SC 1.1 (zástupce ŘO IROP)
9:10 – 9:40	Představení parametrů výzvy, podporovaných aktivit, přímé a nepřímé náklady, povinné přílohy, indikátory, dotazy (zástupce ŘO IROP)
9:40 – 9:55	Povinná příloha Souhlasné stanovisko OHA, proces podávání žádosti prostřednictvím ISDŘ (zástupce Digitální a informační agentury)
9:55 – 10:55	Systém hodnocení projektů a další administrace projektů, dotazy (zástupce Centra pro regionální rozvoj)
10:55	Závěr

Zahájení, aktuální informace o IROP 2021 - 2027 a jeho SC 1.1

PhDr. Aleš Pekárek, ŘO IROP

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

Aktuality z IROP 2021-2027

data k 15. 4. 2026

- Vyhlášeno 118 výzev
- Z toho 53 výzev uzavřeno
- Vyhlášeno 101,4 % alokace IROP (116,0 mld. Kč z EFRR)
- Vydáno 5 610 právních aktů v objemu 80,4 mld. Kč (70,2 % alokace)
- Dokončeno 3 103 projektů

Role MMR a Centra

- **Ministerstvo pro místní rozvoj ČR = Řídicí orgán IROP**
- řízení programu
- příprava výzev a pravidel pro žadatele a příjemce
- poskytovatel dotace
- **Centrum pro regionální rozvoj ČR = Zprostředkující subjekt IROP**
- Konzultační servis, konzultace
- příjem a hodnocení žádostí o podporu
- administrace změn, kontroly projektů, kontroly žádostí o platbu

Otevřené výzvy ve SC 1.1 IROP

Využívání přínosů digitalizace pro občany, podniky, výzkumné organizace a veřejné orgány

- 10. výzva IROP - eGovernment a kybernetická bezpečnost - SC 1.1 (VRR)

Příjem žádostí: 17. 10. 2022 - 28. 5. 2026 | 82,2 %| https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/10vyzvairop

- 29. výzva IROP - eGovernment a Kybernetická bezpečnost - SC 1.1 (ITI)

Příjem žádostí: 10. 11. 2022 - 31. 12. 2027 | 53,8 % | https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/29vyzvairop

- 78. výzva IROP - eHealth -SC 1.1 (MRR)

Příjem žádostí: 28. 11. 2023 - 2. 6. 2026 | 84,4 % | https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/78vyzvairop

- 79. výzva IROP - eHealth - SC 1.1 (PR)

Příjem žádostí: 28. 11. 2023 - 2. 6. 2026 | 73,5 % | https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/79vyzvairop

- 80. výzva IROP - eHealth SC 1.1 (ČR)

Příjem žádostí: 28. 11. 2023 - 2. 6. 2026 | 51,5 % | https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/80vyzvairop

Nové výzvy v IROP 2021-2027

- 119. výzva IROP - Infrastruktura pro cyklistickou dopravu II. - SC 6.1 (MRR)

310,3 mil Kč z EFRR, vyhlášení 17. 3. 2026 | https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/119vyzvairop

- **120. výzva IROP - Kybernetická bezpečnost II. - SC 1.1 (PR)**

1,798 mld. Kč z EFRR, vyhlášení 30. 3. 2026 | https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/120vyzvairop

- 121. výzva IROP - Bezemisní vozidla pro veřejnou dopravu - SC 6.1 (MRR)

393,7 mil. Kč z EFRR, vyhlášení 31. 3. 2026 | https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/121vyzvairop

- 122. výzva IROP - Bezemisní vozidla pro veřejnou dopravu - SC 6.1 (PR)

413,9 mil. Kč z EFRR, vyhlášení 31. 3. 2026 | https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/122vyzvairop

Představení
120. výzvy – Kybernetická bezpečnost II. - SC 1.1 (PR)

Ing. Jan Mazanik, ŘO IROP

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

Odkazy na výzvu

Text výzvy, obecná a specifická pravidla včetně příloh, postup pro podání žádosti v MS2021+:

https://irop.gov.cz/cs/vyzvy-2021-2027

https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/120vyzvairop

Kontrolní listy k hodnocení:

https://crr.gov.cz/irop/projekt-a-kontrola/kontrolni-listy/

Parametry výzvy

územní zaměření výzvy

obec/obce na území Středočeského kraje, Jihočeského kraje, Plzeňského kraje, Kraje Vysočina, Jihomoravského kraje → **přechodové regiony**

V případě žadatelů Krajského ředitelství policie Středočeského kraje a Středočeského kraje a jím zřizovaných nebo zakládaných organizací je přípustné místo realizace hl. m. Praha.

Parametry výzvy

časové nastavení výzvy

Datum vyhlášení výzvy:	30. 3. 2026, 14:00
Datum zpřístupnění MS2021+ Datum zahájení příjmu žádostí:	**30. 4. 2026**, 14:00
Ukončení příjmu žádostí:	17. 12. 2026, 14:00
Nejzazší datum ukončení realizace projektu:	30. 9. 2029
Způsobilost výdajů:	Od 1. 1. 2021 do data ukončení realizace projektu

Parametry výzvy

oprávnění žadatelé

Ne všichni **typově** oprávnění žadatelé jsou skutečně oprávněnými žadateli. Rozhodující je vymezení ve výzvě a režim regulované služby podle zákona o kybernetické bezpečnosti.

Parametry výzvy

oprávnění žadatelé

A. Poskytovatelé regulované služby v režimu vyšších povinností:

- krajská ředitelství Policie České republiky;
- hasičské záchranné sbory krajů, případně MV-generální ředitelství Hasičského záchranného sboru České republiky jako subjekt řídící hasičské záchranné sbory krajů;
- Fakultní nemocnice Brno;
- Fakultní nemocnice Plzeň;
- Fakultní nemocnice u sv. Anny v Brně;
- Centrum kardiovaskulární a transplantační chirurgie Brno;
- Masarykův onkologický ústav;
- kraje;
- obchodní společnosti zakládané kraji nebo obcemi s rozšířenou působností, a to akciové společnosti a společnosti s ručením omezeným, které jsou ve 100 % vlastnictví kraje nebo obce s rozšířenou působností;
- příspěvkové organizace zřízené kraji nebo obcemi s rozšířenou působností;

Parametry výzvy
oprávnění žadatelé

B. Poskytovatelé regulované služby v režimu nižších povinností:

- obce s rozšířenou působností

Parametry výzvy

alokace, limity na projekt

Alokace výzvy: Evropský fond pro regionální rozvoj 1 798 341 944 Kč | Státní rozpočet 0 Kč

Limity na projekt:

- Minimální výše celkových způsobilých výdajů na jeden projekt: 1 mil. Kč
- Maximální výše celkových způsobilých výdajů na jeden projekt poskytovatele regulované služby v režimu nižších povinností (ve výzvě se týká pouze ORP): 15 mil. Kč
- Projekt poskytovatele regulované služby v režimu vyšších povinností: 20 mil. Kč
- V případě, že je oprávněný žadatel poskytovatelem regulované služby v režimu vyšších povinností podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti a zároveň subjektem kritické infrastruktury podle zákona č. 266/2025 Sb., o kritické infrastruktuře činí maximální výše celkových způsobilých výdajů pro jeden projekt: 40 mil. Kč
- V případě, že je oprávněný žadatel poskytovatelem regulované služby v režimu vyšších povinností a projektem dojde k zabezpečení informačního nebo komunikačního systému kritické informační infrastruktury podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, který byl kritickou informační infrastrukturou ke dní skončení platnosti zákona č. 181/2014 Sb., o kybernetické bezpečnosti činí maximální výše celkových způsobilých výdajů na jeden projekt: 40 mil. Kč

Parametry výzvy

alokace, limity na projekt

Ve výzvě je možné podpořit maximálně jednu žádost o podporu předloženou jedním žadatelem (IČO).

- druhá a každá další žádost podaná stejným žadatelem bude vyřazena
- pokud první žádost neuspěje v hodnocení, může žadatel podat žádost znovu

Výjimka pro MV-GŘ HZS ČR. MV může předložit více projektů, pokud každý projekt je podán za jiný HZS kraje (odlišné IČO) a je splněno, že jedno IČO HZS kraje je v rámci výzvy podpořeno pouze jedním projektem.

U předkládaných projektů **není přípustné** cílené rozdělování výdajů na jedno bezpečnostní opatření nebo jeden technický nástroj do více projektů s cílem **obejít limity výzvy, zvýšit míru podpory nebo jinak uměle navyšovat způsobilé výdaje**. Pokud je technické nebo bezpečnostní opatření realizováno jako jeden funkční celek (například jednotný nástroj, licence, instalace, funkcionalita), musí být uvedeno v jediném projektu.

Parametry výzvy

struktura financování

typ VR	EFRR	státní rozpočet	vlastní zdroje žadatele
OSS a PO OSS	**50 %**	**0**	**50 %**
kraje a jejich PO			
obce a jejich PO			
organizace zakládané kraji / obcemi			

Parametry výzvy

ukončení realizace projektu

Datem ukončení realizace projektu se rozumí termín, kdy dojde k naplnění účelu projektu. Tuto skutečnost je třeba doložit pořízenou fotodokumentací a dokumentem prokazujícím ono naplnění účelu projektu, např.:

- doklad o předání a převzetí díla;
- akceptační protokol;
- v případě, kdy nedochází k předání díla formou předávacího protokolu, je nutné uzavření činností projektu doložit jiným dokumentem (např. dokladem o zaplacení/úhradě);

Vždy musí být doložen dokument o úspěšném testování a ověření naplnění kybernetických požadavků - provedení **finálního nezávislého auditu** ověřujícího naplnění kybernetických požadavků, a to prostřednictvím **nezávislého auditora.**

Podporované aktivity

Kybernetická bezpečnost

Podpora zavádění bezpečnostních **technických opatření** podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, a souvisejících prováděcích předpisů (dále také „legislativa ZKB“), zaměřených na zajištění kybernetické bezpečnosti technických aktiv (souvisejících s informačním nebo komunikačním systémem) regulovaných služeb.

Podporované aktivity

Pro poskytovatele regulované služby v režimu **vyšších povinností** jsou podporovanými technickými opatřeními:

- bezpečnost komunikačních sítí;
- správa a ověřování identit;
- řízení přístupových práv a oprávnění;
- detekce kybernetických bezpečnostních událostí;
- zaznamenávání událostí;
- vyhodnocování kybernetických bezpečnostních událostí;
- aplikační bezpečnost;
- kryptografické algoritmy;
- zajišťování dostupnosti regulované služby.

Podporované aktivity

Pro poskytovatele regulované služby v režimu **nižších povinností** jsou podporovanými technickými opatřeními:

- řízení kontinuity činností;
- řízení přístupu;
- řízení identit a jejich oprávnění;
- detekce a zaznamenávání kybernetických bezpečnostních událostí;
- řešení kybernetických bezpečnostních incidentů;
- bezpečnost komunikačních sítí;
- aplikační bezpečnost;
- kryptografické algoritmy.

Podporované aktivity

nepodporovaná technická opatření

Do oblasti podporovaných opatření **nespadají** opatření ani činnosti související se zajištěním **fyzické bezpečnosti** a **zabezpečením průmyslových, řídicích či obdobných specifických technických aktiv.**

Související výdaje s těmito opatřeními nebo činnostmi nelze uplatnit jako přímé výdaje.

Žadatel ve studii proveditelnosti v kapitole 4.2 uvede přehled všech bezpečnostních opatření realizovaných projektem, a to s odkazem na plnění požadavků vyplývajících z vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby odpovídacího režimu povinností.

Podporované aktivity
sdílená technická bezpečnostní opatření

Pořizované bezpečnostní řešení může být sdíleně využíváno i pro IS/KS subjektů, které nejsou oprávněnými žadateli, pokud:

- primárním přínosem projektu je zvýšení kybernetické bezpečnosti žadatele,
- opatření jsou poskytována v identické podobě pro IS/KS žadatele,
- společné využití je technicky neoddělitelné.

Skutečnost sdílení musí být podrobně popsána ve studii proveditelnosti (kap. 4.2).

Ne všechny zabezpečované IS/KS mají stejný dopad na indikátory a způsobilé výdaje. **Do indikátoru se započítávají zabezpečované IS/KS subjektů spadajících mezi oprávněné žadatele výzvy.** Rozhodující je typ subjektu, ke kterému IS/KS náleží. Toto rozlišení musí být jednoznačně popsáno ve studii proveditelnosti a je klíčové pro výpočet indikátoru i případné krácení výdajů.

Způsobilé výdaje

Přímé výdaje

- musí být doloženy příslušnými doklady
- přímá vazba na podporované aktivity
- přímé výdaje **na hlavní část projektu** – bez limitů
- přímé výdaje **na doprovodnou část projektu** – max. 10 % CZV

Nepřímé náklady

- neprokazují se doklady, nelze zahrnout mezi přímé výdaje
- paušál = hodnota 7 % přímých výdajů

Přímé výdaje na hlavní část

- pořízení drobného hmotného majetku – HW;
- pořízení drobného nehmotného majetku – SW;
- pořízení dlouhodobého hmotného majetku – HW;
- pořízení dlouhodobého nehmotného majetku – SW;
- cloudová řešení (do doby ukončení realizace projektu);
- výdaje na koncová zařízení nezbytná pro realizaci technických opatření;
- DPH – podmínky týkající se způsobilosti DPH v projektu jsou uvedeny v kapitole 8 Obecných pravidel

Přímé výdaje na doprovodnou část

- pořízení nezbytné bezpečnostní politiky a dokumentace související s organizačními a technickými opatřeními podle legislativy ZKB (např. bezpečnostní politika, směrnice a interní a procesní postupy, plán reakce na incidenty, stanovení rozsahu), která bude udržována a aktualizována po dobu udržitelnosti projektu;
- výdaje na vyhotovení finálního nezávislého auditu ověřujícího naplnění kybernetických požadavků.

Nepřímé náklady

- **Dokumentace žádosti o podporu**
- **Projektová dokumentace a dokumentace pro realizaci projektu**
- **Administrativní kapacity a řízení projektu**
- **Poplatky**
- **Režijní, provozní a jiné náklady**
- **Publicita projektu**
- **Další náklady související s projektem:** výdaje na koncová zařízení, která nejsou nezbytná pro realizaci technických opatření; odborné konzultace a dozor při implementaci; ostatní náklady související s projektem a nespadající pod přímé výdaje nebo do nezpůsobilých výdajů.

.

Povinné přílohy k žádosti o podporu

1. **Plná moc**
2. **Zadávací a výběrová řízení**
3. **Doklady k právní subjektivitě žadatele**
4. **Studie proveditelnosti** - podle osnovy v příloze č. 2 SPPŽP

S ohledem, že oblast kybernetické bezpečnosti byla v uplynulých letech podporována z více veřejných dotačních programů, je žadatel povinen v povinné příloze Studie proveditelnosti zhodnotit **riziko dvojího financování** (kap. 3, část Popis vazeb na realizované či plánované projekty).

Povinné přílohy k žádosti o podporu

5. **Doklad o prokázání právních vztahů k nemovitému majetku, který je předmětem projektu**
6. **Znalecký posudek**
7. **Podklady pro stanovení kategorií intervencí a kontrolu limitů** - podle vzoru v příloze č. 4 SPPŽP
8. **Smlouva o zřízení bankovního účtu**

Povinné přílohy k žádosti o podporu

9. Rozhodnutí NÚKIB o registraci regulované služby

Žadatel, jako poskytovatel regulované služby, dokládá spolu s žádostí o dotaci rozhodnutí Národního úřadu pro kybernetickou bezpečnost o registraci regulované služby (dále také „rozhodnutí NÚKIB“).

Vydání rozhodnutí NÚKIB musí předcházet datu a času podání žádosti o podporu.

V případě, že žadatel hodlá v projektu zabezpečovat IS/KS pro jinou organizaci(e) (odlišnou od žadatele) doloží Rozhodnutí NÚKIB i pro tuto (tyto) organizaci(e).

MUSÍ BÝT DOLOŽENO VŽDY

10. Čestné prohlášení o zařazení do režimu povinností podle legislativy ZKB

Žadatel spolu s žádostí o dotaci dokládá čestné prohlášení o zařazení do režimu povinností podle legislativy ZKB. Čestné prohlášení obsahuje informaci, zda žadatel spadá do režimu vyšších povinností, režimu nižších povinností a zda je subjektem kritické infrastruktury podle zákona č. 266/2025 Sb., o kritické infrastruktuře. Vzor čestného prohlášení je uveden v příloze č. 5 SPPŽP.

V případě, že je žadatelem subjekt kritické infrastruktury podle zákona č. 266/2025 Sb., o kritické infrastruktuře, je součástí čestného prohlášení také prostá kopie dokumentu, na jehož základě byl tento subjekt určen jako subjekt kritické infrastruktury.

V případě, že žadatel hodlá v projektu zabezpečovat IS/KS pro jinou organizaci (odlišnou od žadatele) doloží Čestné prohlášení i pro tuto(tyto) organizaci(e).

MUSÍ BÝT DOLOŽENO VŽDY

Povinné přílohy k žádosti o podporu

11. Printscreen z Portálu NÚKIB prokazující příslušnost režimu povinností podle legislativy ZKB

Žadatel, spolu s žádostí o dotaci dokládá printscreen z Portálu NÚKIB prokazující příslušnost k režimu povinností podle legislativy ZKB.

Printscreen(y) musí zachycovat alespoň: název organizace, režim povinností (vyšší/nižší).

Printscreen může být doložen ve formě obrázku nebo PDF exportu, musí být však čitelný a obsahovat minimální rozsah uvedených údajů.

V případě, že žadatel hodlá v projektu zabezpečovat IS/KS pro jinou organizaci(e) (odlišnou od žadatele spadající mezi oprávněné žadatele) doloží Printscreen(y) i pro tuto(y) organizaci(e).

MUSÍ BÝT DOLOŽENO VŽDY

Povinné přílohy k žádosti o podporu

12. Souhlasné stanovisko odboru Hlavního architekta eGovernmentu

Datum vydání tohoto stanoviska OHA musí předcházet datu a času registrace žádosti o podporu.

Žádost o vydání souhlasného stanoviska OHA může být podána na OHA až po obdržení rozhodnutí NUKIB o registraci regulované služby (přičemž žádost je podávána společně s tímto rozhodnutím).

MUSÍ BÝT DOLOŽENO VŽDY

V této výzvě NENÍ akceptováno potvrzení o přijetí žádosti o vydání stanoviska.
Pro tuto výzvu není OHA vydáváno potvrzení o přijetí žádosti.

Povinné přílohy k žádosti o podporu

13. Čestné prohlášení žadatele k souhlasnému stanovisku odboru Hlavního architekta eGovernmentu

Vzor čestného prohlášení je uveden v příloze č. 6 SPPŽP.

MUSÍ BÝT DOLOŽENO VŽDY

14. Doklad o stanovení kritické informační infrastruktury

Dokládá se pouze v případě, kdy projektem dochází k realizaci opatření pro IS/KS určené jako KII podle starého zákona o kybernetické bezpečnosti a žadatel na základě tohoto určení uplatňuje zvýšený limit celkových způsobilých výdajů přesahující limit celkových způsobilých výdajů na projekt.

Žadatel ke každé KII doloží prostou kopii opatření/usnesení, kterým byla KII určena. Žadatel dále předloží ke každému KII čestné prohlášení o určení KII. Vzor čestného prohlášení není součástí Specifických pravidel.

Povinné přílohy k žádosti o podporu

15. **Výpis z Evidence skutečných majitelů**
16. **Pověřovací akt**
17. **Čestné prohlášení žadatele o podporu v režimu de minimis**
18. **Povinné přílohy prokazující vyhodnocení žadatele o podporu z pohledu podniku v obtížích**
19. **Stanovení hodnoty indikátoru 304 002**

Žadatel doloží vyplněnou tabulku vypracovanou podle vzoru v příloze č. 11 SPPŽP.

Indikátory

Informace k jednotlivým indikátorům jsou uvedeny v příloze č. 1 SPPŽP s názvem **Metodické listy indikátorů**, která obsahuje:

- podrobnou specifikaci jednotlivých indikátorů;
- způsob stanovení výchozích a cílových hodnot;
- konkrétní postup výpočtu;
- termíny vykazování dosažených hodnot;
- tolerance, ve kterých se indikátory považují za naplněné

Indikátory

304 002 - Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti

- Povinný k výběru a naplnění pro všechny žádosti o podporu
- Prvkem je technické bezpečnostní opatření podle zákona č. **264/2025 Sb.**, o kybernetické bezpečnosti, ve znění pozdějších předpisů, a souvisejících prováděcích předpisů (dále také „zákon o kybernetické bezpečnosti“).
- Každý prvek bude do hodnoty indikátoru započítán pro každý informační nebo komunikační systém (dále také IS/KS) zvlášť. Pokud bude technické opatření sdíleno více IS/KS, bude započítán tolikrát, kolika IS/KS bude sdílen.

Udržitelnost

Zachování účelu, cíle a výstupy projektu (kap. 4.4. OPPŽP)

- zajistit financování veškerých výdajů spojených s provozem a údržbou pořízených prvků kybernetické bezpečnosti;
- zajistit, aby pořízené prvky kybernetické bezpečnosti sloužily svému účelu, zejména se zohledněním maximálně přípustné doby odstávky systému či akceptovatelného výpadku;
- udržovat a aktualizovat projektem pořízenou bezpečnostní dokumentaci související s organizačními opatřeními podle legislativy ZKB (např. bezpečnostní politika, směrnice a interní a procesní postupy, plán reakce na incidenty, stanovení rozsahu);
- zachovat status poskytovatele regulované služby podle legislativy ZKB, a to minimálně v režimu nižších povinností, aby nedošlo k úplnému vypadnutí z působnosti zákona o kybernetické bezpečnosti.

DĚKUJEME ZA POZORNOST

ŘO IROP

Spolufinancováno
Evropskou unií

Ministerstvo
pro místní rozvoj