Závazné stanovisko Řídicího orgánu IROP č. 41

Datum platnosti: 6. 1. 2026

Datum účinnosti: 6. 1. 2026

Číslo jednací: MMR-691/2026-26

Schválil: Ing. Rostislav Mazal

Podpis: Digitálně podepsal:
Ing. Rostislav Mazal
06.01.2026 11:19

Část I.
Důvody pro vydání a předmět závazného stanoviska

Článek 1
Důvody pro vydání závazného stanoviska

Řídicí orgán IROP („ŘO IROP“) vydává toto závazné stanovisko v návaznosti na účinnost zákona č. 264/2025 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále také „nový zákon“). Stanovisko se týká dopadu tohoto zákona na vyhlášené výzvy specifického cíle 1.1 v IROP 2021 - 2027, ve kterých je podporována aktivita „Kybernetická bezpečnost“:

- 3. výzva IROP – Kybernetická bezpečnost – SC 1.1 (MRR);
- 4. výzva IROP – Kybernetická bezpečnost – SC 1.1 (PR);
- 5. výzva IROP – Kybernetická bezpečnost – SC 1.1 (ČR);
- 10. výzva IROP – eGovernment a kybernetická bezpečnost – SC 1.1 (VRR);
- 29. výzva IROP – eGovernment a kybernetická bezpečnost – SC 1.1 (ITI);
- 89. výzva IROP – Kybernetická bezpečnost – NÚKIB – SC 1.1 (ČR).

Podporovaná aktivita specifického cíle 1.1 „Kybernetická bezpečnost“ vychází ze znění Programového dokumentu (dále jen „PD“) Integrovaného regionálního operačního programu pro programové období 2021-2027. Pro cíl politiky 1, specifický cíl 1.1 a podporovanou aktivitu je v PD explicitně odkazováno na zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále také „starý zákon“), a na Směrnici Evropského parlamentu a Rady (EU) 2016/1148 („Směrnice NIS“). Realizace projektů se řídí technickými bezpečnostními opatřeními podle § 5 odst. 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a mezinárodními standardy a normami v oblasti bezpečnosti informací.

Hodnotící kritéria a systém hodnocení žádostí o podporu v IROP 2021–2027 pro SC 1.1 zohledňují uvedené požadavky a odkazují na prováděcí legislativu, konkrétně na vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech,

reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. Specifická pravidla pro žadatele a příjemce (dále jen „SPPŽP“) výše uvedených výzev tak vycházejí z legislativy zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Zákon č. 264/2025 Sb. zcela nahrazuje zákon č. 181/2014 Sb., a implementuje požadavky Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 („Směrnice NIS 2“) do českého právního řádu. Nejde tedy o novelu, ale o rekodifikaci celé oblasti kybernetické bezpečnosti. Nový zákon vychází z principů původní úpravy, avšak rozšiřuje okruh regulovaných subjektů, zpřísňuje povinnosti a zavádí nové mechanismy (např. prověřování dodavatelských řetězců, osobní odpovědnost vedení apod.). Výzvy SC 1.1 byly připraveny před účinností zákona č. 264/2025 Sb., proto se technické požadavky odvíjejí od předchozí právní úpravy. Nejde o náhradu zákonných povinností, ale o podmínky programu.

S ohledem na programový cyklus jsou ve výzvách SC 1.1 evidovány projekty ve všech fázích, od přípravy žádosti o podporu, přes hodnocení a výběr projektů, realizaci až po fázi udržitelnosti.

Obecně je žadatel podle platné metodiky povinen postupovat v souladu s Pravidly pro žadatele a příjemce od jejich účinnosti. Do vydání Právního aktu (dále jen „PA“) / Rozhodnutí o poskytnutí dotace (dále jen „Rozhodnutí“) se žadatel řídí verzí Pravidel účinnou ke dni podání žádosti o podporu, po vydání PA / Rozhodnutí se řídí vždy aktuální verzí. Aktuálně platná Pravidla odkazují na legislativu starého zákona o kybernetické bezpečnosti (zákon č. 181/2014 Sb.), včetně prováděcích předpisů, a stanovují požadavky na realizaci technických bezpečnostních opatření v souladu s touto právní úpravou.

V návaznosti na účinnost nového zákona bude sjednocen výklad a aplikace pravidel tak, aby bylo jednoznačně stanoveno, podle které právní úpravy se mají žadatelé a příjemci řídit. Cílem je eliminovat nejasnosti a zajistit jednotný postup pro všechny projekty, bez ohledu na fázi jejich realizace.

Článek 2
Předmět závazného stanoviska

Závazným stanoviskem se aktualizuje kapitola Udržitelnost všech SPPŽP IROP 2021–2027 u vyhlášených výzev č. 3, 4, 5, 10, 29 a 89.

Při přípravě žádosti o podporu a v průběhu realizace projektu mají všichni žadatelé a příjemci povinnost i nadále postupovat v souladu s platnými Specifickými pravidly IROP, která v současnosti odkazují na zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a na vyhlášku č. 82/2018 Sb.

S ohledem na účinnost nového zákona č. 264/2025 Sb. (transpozice směrnice NIS2) od 1. listopadu 2025 nicméně ŘO IROP doporučuje, aby žadatelé již při návrhu řešení zohlednili požadavky nové legislativy, zejména v oblasti řízení rizik a hlášení incidentů, aby se předešlo dodatečným nákladným úpravám v období udržitelnosti.

Při posuzování plnění povinností příjemců dotace v období udržitelnosti v oblasti organizačních opatření se bude vycházet z aktuálně platné právní úpravy, tedy od účinnosti nového zákona o kybernetické bezpečnosti, který transponuje směrnici NIS2 do českého právního řádu. Příjemce ve zprávě o udržitelnosti (dále také “ZoU“) identifikuje právní úpravu, podle které postupuje, buď starého zákona, nebo již nového zákona

S ohledem na to, že ve výzvách IROP dosud nebylo sledováno, zda je příjemce regulovaným subjektem, budou příjemci ve zprávě o udržitelnosti uvádět požadavek a způsob plnění organizačních opatření podle nového zákona o kybernetické bezpečnosti v souladu s režimem povinností, ke kterému jsou registrováni (režim vyšších povinností nebo režim nižších povinností). V případě podpořené organizace, na kterou se nevztahuje žádný z režimů povinností podle nového zákona, bude příjemce uvádět požadavky plnění organizačních opatření podle režimu nižších povinností.

Pokud je příjemce registrovaným subjektem, ale nachází se v přechodné lhůtě jednoho roku a dosud nezavedl bezpečnostní opatření, tuto skutečnost uvede a bude se řídit původní právní úpravou, tedy mít zavedena organizační opatření definovaná podle starého zákona o kybernetické bezpečnosti.

Část II.
Aktualizované či nově doplňované kapitoly SPPŽP

Článek 3
Aktualizace kapitoly Udržitelnost

- **Text Upozornění pro aktivitu Kybernetická bezpečnost**:

Technická opatření bez implementace organizačních opatření jsou často neúčinná a neumožňují maximální využití vynaložených investic. Příjemce podpory je povinen po celou dobu udržitelnosti mít zavedena organizační opatření ~~definovaná § 5 odst. 2 zákona o kybernetické bezpečnosti.~~ **odpovídající právní úpravě, která je pro něj závazná.**

Od účinnosti nového zákona o kybernetické bezpečnosti (264/2025 Sb.) a po uplynutí přechodné lhůty je příjemce povinen plnit organizační opatření podle režimu povinností, ke kterému je registrován (vyšší režim, nižší režim). V případě, že se na příjemce zákon nevztahuje, plní minimální standard odpovídající režimu nižších povinností.

Pokud je příjemce registrovaným subjektem, ale nachází se v přechodné lhůtě a dosud nezavedl opatření dle nového zákona, uvede tuto skutečnost ve zprávě o udržitelnosti a doloží plnění organizačních opatření podle původní právní úpravy.

Příjemce ve ZoU uvádí rozsah a popis zavedených organizačních opatření včetně jejich podložení dokumenty dokladujícími jejich plnění a zajištění personálních kapacit, jako např. přehled směrnic pro používání a správu výpočetní techniky v organizaci včetně smluv o zajištění organizačních opatřeních, případně doložení pracovní náplně odpovědné osoby.

Část III.
Závěrečná ustanovení

Toto závazné stanovisko platí od data jeho účinnosti pro výzvy č. 3, 4, 5, 10, 29 a 89 a vztahuje se na všechny žádosti o podporu včetně již podaných.

ŘO IROP promítne změny uvedené v části II., článku 3 tohoto závazného stanoviska do SPPŽP při jejich nejbližší revizi.

Přílohy: nejsou