Dobrý den,

dovoluji si na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, požádat Váš úřad o poskytnutí informací týkajících se dopadů implementace směrnice Evropské unie č.: EU 2022/2555 (NIS2) do českého právního řádu na fungování Vašeho úřadu.

Tuto žádost podávám z důvodu vypracování bakalářské práce na téma „Analýza a návrh vhodných bezpečnostních opatření v oblasti kybernetické bezpečnosti podle směrnice NIS2 na krajských úřadech“. Jsem ve služebním poměru příslušníka bezpečnostních sborů, Policie České republiky a studuji na Policejní akademii České republiky v Praze, studijní program Policejní činnosti. Informace poskytnuté Vaším úřadem mi poslouží jako odborný podklad, který je nezbytný pro vypracování mé bakalářské práce. Ačkoliv se v tématu práce zmiňují krajské úřady, obce s rozšířenou podléhají stejným požadavkům na kybernetickou bezpečnost.

Dovoluji si Vás proto požádat o zodpovězení následujících otázek:

1. Jakým způsobem se na Váš úřad konkrétně vztahuje implementace směrnice NIS 2 do českého právního řádu, spadáte do kategorie nižších, nebo vyšších povinností?

2. Jaké nové povinnosti v oblasti kybernetické a informační bezpečnosti pro Váš úřad z implementace směrnice NIS 2 vyplývají?

3. Jaké organizační změny musel nebo musí Váš úřad v souvislosti s implementací směrnice NIS 2 učinit (např. úprava vnitřních předpisů, změna v řízení IT/bezpečnosti)?

4. Jaké personální změny byly nebo budou realizovány (např. navýšení počtu zaměstnanců odpovědných za kybernetickou bezpečnost, posílení IT oddělení)?

5. Jaká školení či vzdělávací aktivity v oblasti kybernetické bezpečnosti byla zavedena pro zaměstnance Vašeho úřadu v souvislosti s požadavky vyplývajícími z NIS 2?

6. Jaké finanční náklady (orientačně či v odhadovaném rozpětí) si implementace požadavků směrnice NIS 2 vyžádala nebo vyžádá v rozpočtu Vašeho úřadu (např. vyčlenění na personální náklady, školení, infrastrukturu, služby externích dodavatelů)?

7. Jaká materiální a technická opatření byla či budou v souvislosti s NIS 2 realizována (např. obměna hardware, zavedení nových bezpečnostních technologií, systémů pro monitorování a detekci incidentů, zálohovací a obnovovací řešení)?

8. Zda byl v souvislosti s NIS 2 vytvořen nebo aktualizován soubor vnitřních bezpečnostních politik a metodik (např. bezpečnostní politika, politika řízení přístupů, řízení rizik, kontinuita provozu, incident response plány), a pokud ano, v jakém rozsahu?

9. Jakým způsobem Váš úřad zajišťuje analýzu a řízení rizik v oblasti kybernetické bezpečnosti po účinnosti nové právní úpravy vycházející z NIS 2?

10. Zda Váš úřad podstoupil (nebo plánuje podstoupit) v souvislosti s implementací NIS 2 nějaké externí audity, penetrační testy či jiné formy nezávislého ověřování úrovně kybernetické bezpečnosti?

Prosím o zaslání požadovaných informací do datové schránky ID: 9hhzwpr

Děkuji za Vaši vstřícnost a čas věnovaný vyřízení této žádosti.

S pozdravem,

Michal Drien

Lukavec 133

410 02 Lukavec

VÁŠ DOPIS ZN.	
ZE DNE	22.01.2026
ČÍSLO JEDNACÍ	SMOL/054474/2026/OCHR/KRB/Zou
VYŘIZUJE	Ing. Jiří Helfer
TELEFON	420 588 488 526
E-MAIL	jiri.helfer@olomouc.eu
DATUM	27.01.2026

Vážený pan
Michal Drien
Lukavec 133
410 02 Lukavec

Odpověď na žádost o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Vážený pane Driene,

na základě Vaší žádosti o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, Vám k jednotlivým otázkám sděluji následující.

1. ORP Olomouc jako poskytovatel regulovaných služeb podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti a příslušných prováděcích předpisů je zařazena do režimu s nižším rozsahem zákonných povinností.

2. Směrnice NIS2 zásadně rozšiřuje regulaci a zpřísňuje požadavky na řízení kybernetických rizik, odpovědnost vedení a povinné procesy. Nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti tyto změny přebírá a požadavky dopadají i na subjekty v nižším režimu povinností.

3. ORP Olomouc v rámci implementace zákona č. 264/2025 Sb., o kybernetické bezpečnosti a jeho prováděcích předpisů posiluje opatření v oblastech řízení aktiv a rizik, bezpečnosti chování lidských zdrojů, řízení kontinuity činností, řízení přístupů a identit, řízení zvládání bezpečnostních událostí a incidentů. Uvedené procesy vyžadují i úpravu vnitřních předpisů.

4. ORP Olomouc zřídila pozice metodika kybernetické bezpečnosti a koordinátora bezpečnosti informací.

5. ORP Olomouc zajišťuje vstupní i periodická školení pro své zaměstnance v souladu s politikou rozvoje bezpečnostního povědomí zaměstnanců v oblasti kybernetické bezpečnosti a bezpečnosti informací.

6. Rozpočet ORP Olomouc na rok 2026 byl stanoven v oblasti kybernetické bezpečnosti v řádu nižších jednotek mil. Kč.

7. ORP Olomouc průběžně modernizuje informační serverovou a síťovou infrastrukturu a současně posiluje dohledové platformy pro zajištění jejího bezpečného provozu.

8. ORP Olomouc má zavedený systém řízení bezpečnosti informací ISMS (Information Security Management Systém), který stanoví rozsah a popis životního cyklu systému řízení bezpečnosti informací v souladu s požadavky normy ČSN EN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky. Systém bude v

určené lhůtě aktualizován o požadavky stanovené v zákoně č. 264/2025 S., o kybernetické bezpečnosti a jeho prováděcích předpisech, které vycházejí ze směrnice NIS 2.

9. ORP Olomouc zajišťuje analýzu rizik a řízení rizik podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti a jeho prováděcích předpisů.

10. V rámci bezpečnostních opatření ORP ověřuje úroveň kybernetické bezpečnosti prostřednictvím nástrojů určených pro nezávislé posouzení její úrovně.

S pozdravem

Ing. Mgr. Jan Langr, MBA

vedoucí odboru ochrany