Magistrát města Zlína
náměstí Míru 12 • 760 01 Zlín

MMZLSS549138 2

[redacted]

NAŠE ČJ.: MMZL 026084/2026
VYŘIZUJE: Bc. Ivana Kopečná
TEL.: 577 630 193
FAX: 577 432 911
E-MAIL: IvanaKopecna@zlin.eu

DATUM: 02.02.2026

Sdělení k žádosti o poskytnutí informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Magistrát města Zlína, Odbor kanceláře tajemníka, Oddělení vnitřních služeb (dále jen „povinný subjekt“) obdržel dne 19.01.2026 žádost o poskytnutí informací (dále jen „žádost“) podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon o svobodném přístupu k informacím“), kterou podal prostřednictvím veřejné datové sítě do datové schránky statutárního města Zlína (dále jen „datová schránka“) [redacted] (dále jen „žadatel“).

Na základě výše uvedené žádosti sdělujeme následující:

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

Statutární město Zlín jako obec s rozšířenou působností je povinným subjektem veřejné správy, na který se vztahuje právní úprava kybernetické bezpečnosti vycházející ze směrnice Evropské unie 2022/2555 (NIS2), implementovaná do českého právního řádu zákonem č. 264/2025 Sb., o kybernetické bezpečnosti.
Na základě vyhlášky č. 408/2025 Sb., o regulovaných službách, je statutární město Zlín zařazeno mezi poskytovatele regulované služby v režimu nižších povinností. Rozsah bezpečnostních povinností v tomto režimu je stanoven zejména vyhláškou č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

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

Rozsah povinností statutárního města Zlín v oblasti kybernetické a informační bezpečnosti je určen právní úpravou uvedenou v bodě 1 této odpovědi, zejména zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, a jeho prováděcími předpisy.
Statutární město Zlín je v souvislosti s implementací směrnice Evropské unie 2022/2555 (NIS2) nově regulovaným subjektem, přičemž konkrétní rozsah povinností odpovídá režimu nižších povinností stanovenému platnou legislativou.

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)?*

V souvislosti s implementací právní úpravy kybernetické bezpečnosti probíhá u statutárního města Zlín implementace organizačních i technických opatření, a to v rozsahu odpovídajícím stanovenému režimu regulace. Součástí tohoto procesu je rovněž průběžná úprava a aktualizace vnitřních předpisů a souvisejících interních procesů v oblasti informační a kybernetické bezpečnosti.

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

Personální zajištění oblasti kybernetické bezpečnosti je řešeno zejména určením povinných rolí v souladu s platnou právní úpravou. Jsou stanoveny osoby pověřené kybernetickou bezpečností. K navýšení počtu zaměstnanců v této oblasti nedošlo.

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

V oblasti kybernetické bezpečnosti jsou u statutárního města Zlín již realizovány vybrané vzdělávací a osvětové aktivity v rámci rozvoje bezpečnostního povědomí, a to zejména v podobě poučení vrcholného vedení a průběžného vzdělávání zaměstnanců se zaměřením na bezpečné chování uživatelů.

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)?*

Konkrétní finanční náklady spojené s implementací požadavků vyplývajících ze směrnice NIS2 nelze v současné době vyčíslit. Důvodem je skutečnost, že zajišťování kybernetické bezpečnosti představuje kontinuální proces průběžného zlepšování, který je realizován v rámci PDCA cyklu, tj. neustálého hodnocení, plánování, realizace a vyhodnocování přijatých opatření. Finanční náklady tak vznikají a budou vznikat postupně v souvislosti se zaváděním a rozvojem organizačních i technických opatření.

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)?*

V souvislosti s implementací právní úpravy kybernetické bezpečnosti jsou u statutárního města Zlín postupně realizována technická opatření, přičemž další opatření jsou a budou průběžně rozvíjena v návaznosti na požadavky platné legislativy a stanovený režim regulace.

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?*

V souvislosti s implementací právní úpravy kybernetické bezpečnosti dochází u statutárního města Zlín k vytváření bezpečnostních politik, aktualizaci interních předpisů a vedení související

bezpečnostní evidence a dokumentace, a to v rozsahu stanoveném platnou legislativou, zejména prováděcí vyhláškou č. 410/2025 Sb. k zákonu o kybernetické bezpečnosti.

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

Platná právní úprava v režimu nižších povinností neukládá povinnost provádět formální analýzu rizik ani analýzu dopadů v rozsahu vyžadovaném pro subjekty v režimu vyšších povinností.

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?*

Statutární město Zlín plánuje v souvislosti s implementací právní úpravy kybernetické bezpečnosti realizaci penetračních testů jako nástroje pro ověřování úrovně kybernetické bezpečnosti. Současně není vyloučeno využití externího auditu či jiných forem nezávislého odborného posouzení úrovně kybernetické bezpečnosti.

Mgr. Pavlína Hrnčiříková
vedoucí Oddělení vnitřních služeb
Odbor kanceláře tajemníka

(podepsáno elektronicky)