



## STATUTÁRNÍ MĚSTO DĚČÍN

MAGISTRÁT MĚSTA DĚČÍN

Tajemník magistrátu

Mírové nám. 1175/5, 405 38 Děčín

Datová schránka: x9hbpfn a nj6wxpq

Váš dopis zn.:

Ze dne:

Číslo jednací: MDC/177102/2025/30/JMa

Spisová zn.: MDC/29953/2025

Počet listů: 4

Počet příloh:

Vyřizuje: Ing. Josef Malovaník

Telefon: 412593314

E-mail: josef.malovanik@mmdecin.cz

Děčín: 05.11.2025

### Odpověď na žádost o poskytnutí informace podle zákona č. 106/1999 Sb.

Vážený pane,

v žádosti o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, doručené na podatelnu statutárního města Děčín (dále jen „povinný subjekt“) dne 25.10.2025 prostřednictvím datové schránky a zaevidované pod č. j. MDC/171787/2025, jste požádal o poskytnutí níže uvedených informací:

*„V souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, žádám město Děčín o poskytnutí následujících informací týkajících se projektu instalace 5G kamer s AI analýzou (viz příloha), financovaného z Národního plánu obnovy:*

#### A. Studie, posouzení a stanoviska

- 1. Bylo před zahájením projektu zpracováno Posouzení vlivu na ochranu osobních údajů (DPIA) dle čl. 35 GDPR? Pokud ano, žádám o kopii nebo shrnutí závěrů.*
- 2. Proběhla konzultace s Úřadem pro ochranu osobních údajů (ÚOOÚ)? Pokud ano, žádám o kopii komunikace či stanoviska.*
- 3. Byla provedena analýza kybernetických rizik nebo bezpečnostní audit podle doporučení NÚKIB? Uveďte rozsah, datum a výsledky.*
- 4. Kdo zpracoval technickou a bezpečnostní studii projektu a kdo ji schválil.*

#### B. Technické provedení systému

- 5. Jaké jsou značky a modely kamerových jednotek, jejich výrobce a země původu.*
- 6. Jaký software zajišťuje AI analýzu (název, verze, výrobce, licenční režim, on-premise / cloud).*
- 7. Kde jsou data fyzicky uložena a jaký je jejich zpracovatelský řetězec (město, městská policie, dodavatel).*

Držitel certifikátu ČSN EN ISO 9001:2015 – Quality Management System Certification

IČO: 00261238  
DIČ: CZ00261238

Česká spořitelna, a.s.  
č. ú. 19-921402389/0800

Tel.: 412 593 111  
Fax: 412 593 340

E-mail: posta@mmdecin.cz  
Internet: www.mmdecin.cz

otisk elektronického podpisu

8. Dochází k přenosu nebo zpracování dat mimo území ČR nebo EU (např. v cloudu AWS, Azure, Huawei Cloud apod.)?

9. Jaké mechanismy zajišťují šifrování, logování přístupů a mazání dat.

10. Jaká je doba uchovávání záznamů.

10b) Jsou tato HW zařízení v souladu s doporučením NÚKIB? Podléhají platným revizím, a jsou tyto revize pravidelně revidovány v souladu se zákonem?

C. Právní rámec a předávání dat

11. Kdo je správcem a kdo zpracovatelem osobních údajů.

12. Jaký je právní základ zpracování (čl. 6 GDPR).

13. Komu jsou data zpřístupňována nebo předávána (Policie ČR, Městská policie, dodavatelé apod.).

14. Existují-li smlouvy o předávání nebo zpracování dat, žádám o jejich kopie.

15. Kdo je odpovědný za bezpečnostní dohled a revize přístupových práv.

D. Etické a strategické aspekty

16. Kdo projekt inicioval a kdo jej odborně garantuje.

17. Jak město hodnotilo přiměřenost zásahu do soukromí vůči přínosu projektu.

18. Jaké alternativy nebo méně invazivní varianty byly zvažovány.

19. Zda je plánováno rozšíření systému a v jakém rozsahu.

E. Lhůta a způsob doručení

Žádám, aby byly informace poskytnuty elektronicky do mé datové schránky do 15 dnů ode dne doručení této žádosti, jak stanoví § 14 odst. 5 zákona č. 106/1999 Sb.

V případě, že město potřebuje lhůtu prodloužit, žádám o formální oznámení důvodu a konkrétního termínu, v souladu s § 14 odst. 7 tohoto zákona.“

K bodu 1 uvádí povinný subjekt, že posouzení vlivu na ochranu osobních údajů nebylo k datu podání žádosti zpracováno. Individuální komponenty projektu (kamery, routery, SW analytické nástroje) jsou standardizované a nasazované na úrovni dalších samospráv na území České republiky.

K bodu 2 uvádí povinný subjekt, že konzultace s Úřadem pro ochranu osobních údajů (dále jen „ÚOOÚ“) neproběhla.

K bodu 3 uvádí povinný subjekt, že dne 03.09.2025 publikoval Národní úřad pro kybernetickou bezpečnost (dále jen „NÚKIB“) Varování a strategické analýzy týkající se vysokého bezpečnostního rizika u technologií čínských výrobců zahrnující mj. komponenty kamerových systémů s uvedením hlavní hrozby v možném zneužití dat či vzdáleném neoprávněném přístupu do bezpečnostních systémů ze strany čínských státních orgánů. Rizikové technologie (ani další technologie jiných výrobců z rizikových zemí) však nejsou v rámci Městského kamerového dohlížecího systému (dále jen „MKDS“) instalovány či využívány.

Po zprovoznění MKDS budou kybernetická rizika vyhodnocována průběžně, i ad hoc, na úrovni provozu MKDS. Kamerový systém jako celek i nově instalované technologie naplňují požadavky EU Cyber Resilience Act (CRA).

K bodu 4 uvádí povinný subjekt, že technická specifikace zadávací dokumentace byla zpracovávána povinným subjektem ve spolupráci s externí odbornou poradenskou společností na základě priorit a požadavků Městské policie Děčín (dále jen „MP“) a Policie České republiky (dále jen „PČR“). Klíčové projektové podklady a výstupy (dotační záměr, zadávací dokumentace) byly schvalovány na úrovni zastupitelstva města.

K bodu 5 uvádí povinný subjekt, že se jedná o Hanwha Vision PNO-A9311RLP, XNP-9250 (ex Samsung Techwin), Jižní Korea.

K bodu 6 uvádí povinný subjekt, že pro sběr a hodnocení statistických dat o dopravě zajišťuje AI analýzu BriefCam Protect, člen dánské skupiny Milestone Systems, instalován a provozován bude na serveru MP Děčín (on-premise).

Pro potřeby bezpečnostního monitoringu PČR a zapojení vybraných kamer do Centrálního systému automatické kontroly vozidel (CAKV) PČR je nasazen systém DataFactory české společnosti FF GROUP. Server / koncentrátor je instalován on-premise.

K bodu 7 uvádí povinný subjekt, že veškerá data (záznamy z kamerového systému a analytická metadata) budou po zprovoznění ukládána na infrastrukturu, resp. na serverech v zabezpečené serverovně Městské policie Děčín s omezeným fyzickým i kybernetickým přístupem pouze pro pověřené osoby MP Děčín. Záznamy z kamerových systémů mohou být v souladu se zákonem na písemnou žádost poskytnuty orgánům činným v trestním řízení.

K bodu 8 uvádí povinný subjekt, že po zprovoznění MKDS nebude docházet k přenosu ani zpracování dat v cloudech mimo území ČR nebo EU.

K bodu 9 uvádí povinný subjekt, že jsou implementovány metody a nástroje šifrování na úrovni komunikace mezi komponentami, využívána je zabezpečená síť pro datové přenosy (mimo veřejnou síť internet), šifrovány a zabezpečeny jsou rovněž samotné záznamy. Přístupy a změny konfigurace jsou logovány. Data se systematicky mažou cyklicky.

K bodu 10 uvádí povinný subjekt, že doba uchovávání záznamů je max. 14 dnů.

K bodu 10b uvádí povinný subjekt, že MKDS jako celek a jeho jednotlivé komponenty budou po zprovoznění provozovány v souladu se zákonným rámcem. Instalované komponenty nenaplňují rizikové znaky s ohledem na publikovaná varování NÚKIB. Provoz kamerového systému jako celku podléhá pravidelným kontrolám, profylaxi, revizím, aktualizacím firmwaru, úpravám konfigurací a dalším standardním úkonům.

K bodu 11 uvádí povinný subjekt, že správcem osobních údajů je povinný subjekt, který nemá v kontextu budoucího provozu MKDS zpracovatele osobních údajů.

K bodu 12 uvádí povinný subjekt, že právním základem je výkon veřejné moci podle ustanovení § 24b zákona č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů, (dále jen „zákon o obecní policii“), jehož účelem je zajištění veřejného pořádku, ochrana bezpečnosti osob a majetku a prevence kriminality.

Zpracování osobních údajů prostřednictvím MKDS se tedy opírá o zákonný právní základ ve smyslu čl. 6 odst. 1 písm. e) GDPR („zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu“).

K bodu 13 uvádí povinný subjekt, že k datu podání žádosti je MKDS ve fázi přípravy instalace, tudíž data nejsou nikomu zpřístupňována nebo předávána.

K bodu 14 uvádí povinný subjekt, že smlouvy o předávání nebo zpracování dat k datu podání žádosti neexistují.

K bodu 15 uvádí povinný subjekt, že bezpečnostní dohled bude po zprovoznění MKDS prováděn MP ve spolupráci s oddělením informačních technologií Magistrátu města Děčín. Přístupovými právy k datům a záznamům budou disponovat pouze k tomu pověřeni pracovníci MP.

K bodu 16 uvádí povinný subjekt, že projekt byl iniciován ze strany MP ve spolupráci s PČR, nadále byl podpořen, schválen a realizován na úrovni Magistrátu města Děčín. Garantem je odbor strategií a informačních technologií.

K bodu 17 uvádí povinný subjekt, že z důvodu přiměřenosti zásahu do soukromí bude nastavení kamer probíhat na základě podkladů Ministerstva vnitra ČR, metodických pokynů ÚOOÚ, dobré praxe provozu MKDS, preferencí PČR a pro potřeby výkonu služby MP v souladu se zákonem o obecní policii za účelem posilování nástrojů prevence kriminality a zvyšování bezpečnosti města.

Po konečném zprovoznění MKDS bude za pomoci kamer docházet k dohledu veřejně přístupných prostranství (primárně pozemních komunikací), prováděn sběr statistických dat (neobrazových) o průjezdu vozidel pro rozvojové potřeby města v souladu se schválenými cíli 5G projektu - bez sběru citlivých informací či osobních údajů.

K bodu 18 uvádí povinný subjekt, že alternativně bylo zvažováno častější nasazení hlídek MP, manuální sběr dat a fyzický dohled v dotčených oblastech.

K bodu 19 uvádí povinný subjekt, že v současné době není plánováno rozšíření systému.

S pozdravem

**Ing. Martin Kříž**  
tajemník Magistrátu města Děčín

otisk úředního razítka  
podepsáno elektronicky