MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MVCRX089VHZD
prvotní identifikátor

odbor archivní správy a spisové služby
Nad Štolou 3
170 34 Praha 7

Č. j. MV-188332-3/AS-2024

Praha 17. prosince 2024

Vážená paní
Xxxxxxxxxxx
xxxxxxxxxxx

# Rozhodnutí

Ministerstvu vnitra jako povinnému subjektu podle § 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon č. 106/1999 Sb.“), byla dne 5. 12. 2024 doručena žádost xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx(dále jen „žadatelka“) o zaslání informace, týkající elektronického systému spisové služby Ministerstva vnitra.

Ministerstvo vnitra žádost posoudilo a v souladu s § 15 odst. 1 zákona č. 106/1999 Sb. rozhodlo takto:

**žádost o poskytnutí informací se odmítá**.

## Odůvodnění:

Žádost žadatelky o poskytnutí informací podle zákona č. 106/1999 Sb. byla Ministerstvu vnitra doručena dne 5. 12. 2024. Žadatelka ve své žádosti požaduje informaci, formulovanou jako dotaz „*Pokud zprávy archivujete na vlastním serveru, kde se server nachází a jaká je jeho kapacita vyjádřena v Gb*“ (dále jen „žádost“).

Povinný subjekt zaslanou žádost posoudil a vzhledem k tomu, že požadované informace se týkají elektronického systému spisové služby Ministerstva vnitra, který je významným informačním systémem ve smyslu ustanovení § 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (*významným informačním systémem informační systém spravovaný*

*orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci*) a ustanovení § 2 odst. 1, písm. a) a d) vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů (*významný informační systém podle § 2 písm. d) zákona je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při výkonu působnosti orgánu veřejné moci k zajištění mj. elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci a výkonu spisové služby*) s tím, že podle ustanovení § 2 odst. 4 citované vyhlášky platí, že významný informační systém uvedený v odstavci 1 naplňuje určující kritéria, tedy že narušení bezpečnosti informací v informačním systému, který není uveden v § 2 odst. 1, by mohlo způsobit omezení či narušení poskytování služeb nebo informací orgánem veřejné moci veřejnosti, případně jiné omezení či narušení fungování orgánu veřejné moci, jedná se o žádost o poskytnutí informací smyslu ustanovení § 2 odst. 3 zákona č. 106/1999 Sb., na něž se informační povinnost nevztahuje.

Ustanovení § 2 odst. 3 zákona č. 106/1999 Sb. stanoví, že se tento zákon nevztahuje mimo jiné na poskytování informací, pokud zvláštní zákon upravuje jejich poskytování. V tomto konkrétním případě platí ustanovení § 10a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů stanoví, že informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, se podle předpisů upravujících svobodný přístup k informacím neposkytují. Důvodová zpráva k tomuto ustanovení zákona mj. uvádí: *„V současné době, kdy již bylo určeno 155 významných informačních systémů, spravovaných 58 subjekty, a 48 systémů kritické informační infrastruktury, jejichž správci jsou orgány veřejné správy, tedy potenciálních povinných subjektů podle zákona o svobodném přístupu k informacím, a kdy roste počet útoků v kybernetickém prostoru, je zapotřebí přistoupit k opatření i v obecnější rovině zajišťování kybernetické bezpečnosti. Je zapotřebí zdůraznit, že v současnosti účinná výjimka uvedená v § 11 odst. 4 písm. f) zákona o svobodném přístupu k informacím nenaplňuje požadavky na ochranu citlivých informací, zejména těch, které se vztahují k přijatým bezpečnostním opatřením podle zákona o kybernetické bezpečnosti. Potenciální útočník by tak v současné době mohl požádat podle tohoto zákona správce informačních nebo komunikačních systémů kritické informační infrastruktury nebo správce významných informačních systémů o poskytnutí informací o přijatých bezpečnostních opatřeních, přičemž tento povinný subjekt by byl povinen je poskytnout. Z tohoto důvodu se předkladatel rozhodl, i v souladu s čl.*

*1 odst. 6 směrnice (Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti.) a recitály č. 2 (Rostoucí rozsah, četnost výskytu a dopad bezpečnostních incidentů představují pro fungování sítí a informačních systémů významnou hrozbu. Uvedené systémy se rovněž mohou stát snadným cílem úmyslných škodlivých akcí za účelem poškození nebo narušení provozu systémů. ...) a č. 8 (Touto směrnicí by neměla být dotčena možnost jednotlivých členských států přijmout nezbytná opatření, aby zajistily ochranu podstatných zájmů své bezpečnosti, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů. ...) směrnice pro doplnění výjimky z povinnosti poskytovat informace na základě zákona o svobodném přístupu k informacím o údaje, které se týkají zajišťování kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti.“*

Na základě výše uvedených skutečností rozhodl povinný subjekt tak, jak je uvedeno ve výroku.

**Poučení:**

Proti tomuto rozhodnutí lze, ve lhůtě 15 dnů ode dne jeho doručení, podat rozklad k ministru vnitra prostřednictvím povinného subjektu.

PhDr. Daniel Doležal, Ph.D.
ředitel odboru

Vyřizuje: Mgr. Alena Štětková
tel. č.: 974847613
e-mail: alena.stetkova@mvcr.cz