



DIAPX002N8EG

prvotní identifikátor

ČÍSLO JEDNACÍ

DIA- 7950-2/EG-2024

(osobní údaje žadatele anonymizovány)

> Váš dopis značky / ze dne

> Číslo jednací

> Počet příloh

Místo odeslání / dne

Praha / datum uvedeno
v doložce elektronického podpisu

Poskytnutí informace k žádosti podle zákona č. 106/1999 Sb.

Digitální a informační agentura obdržela dne 17. 4 2024 žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, podanou žadatelem (osobní údaje žadatele anonymizovány)

Žadatel požaduje informaci k jednotlivým bodům jeho dotazu v následujícím znění:

- 1) *Jakým způsobem je zabezpečeno datové úložiště, ve kterém se nachází moje datové zprávy, ke kterým lze přistupovat prostřednictvím webového rozhraní www.mojedatovaschranka.cz, vůči riziku ztráty dat, nebo jejich kompromitace jinou osobou?*
- 2) *Jakým způsobem jsou data (pokud jsou) v datovém úložišti zašifrována? Jaký šifrovací protokol je používán?*
- 3) *Kdo/jaké osoby/jaké role mají přístup k šifrovacím klíčům a zda jako provozovatel ISDS dokážete rozpoznat, že byly klíče použity?*
- 4) *Je datové úložiště provozováno vlastními prostředky DIA, nebo je pro tyto potřeby najímán jeden, nebo více poskytovatelů cloudových služeb? Pokud ano, prosím o výčet takových poskytovatelů.*
- 5) *Prosím o sdělení geografické polohy fyzického umístění serverů, na kterých jsou data uložena?*
- 6) *Prosím o sdělení hraničních hodnot pro RPO (Recovery Point Objective) a RTO (Recovery Time Objective)?*
- 7) *Prosím o sdělení počtu a délce výpadků znamenajících uživatelskou nedostupnost portálu www.mojedatovaschranka.cz za posledních 12 měsíců*

Digitální a informační agentura **poskytuje** k jednotlivým bodům položeného dotazu následující informaci:

- 1) Úložiště jsou redundantní. Data jsou v nich také uložena redundantně. Redundantně jsou data rovněž zálohována. Obnovitelnost ze záloh je testována.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

- 2) Obsahy datových zpráv jsou šifrovány ještě před jejich uložením. K dešifrovanému obsahu zpráv mají přístup jen úspěšně autentizovaní a k tomu oprávnění uživatelé mající účet pro přístup do schránky odesílatele nebo příjemce dané datové zprávy. Obsahy zpráv jsou šifrovány algoritmem, jehož odolnost splňuje požadavky Národního úřadu pro kybernetickou společnost kladené na informační systémy kritické infrastruktury.
- 3) K šifrovacím klíčům, které slouží pro šifrování obsahů datových zpráv nemají přístup žádné osoby. Provozovatel dokáže rozpoznat události používající šifrovací klíče a také jejich původce.
- 4) Datová úložiště jsou v majetku provozovatele systému. Datová úložiště jsou umístěna v datových centrech. Nikde v Informačním systému datových schránek (dále jen „ISDS“) nejsou používány cloudové služby.
- 5) ISDS je aktuálně provozováno v datových centrech, která mají potřebnou certifikaci a jsou na území ČR.
- 6) Data jsou zálohována s parametry, které garantují, že budou v případě potřeby obnovena v co nejkratší době a že nedojde k jejich ztrátě.
- 7) V dotazovaném období evidujeme jednu událost, která mohla mít vliv na uživatelskou dostupnost webového portálu ISDS, a to v trvání 2 minut

Závěrem si dovoluujeme upřesnit, že správce ISDS byl nucen v souladu s § 11 odst. 1 písm. f) zákona č. 106/1999 Sb. ve spojení s § 10a zákona č. 184/2001 Sb. (zákon o kybernetické bezpečnosti) zohlednit skutečnost, že předmětem shora uvedené žádosti (dotazů) jsou závažné okolnosti bezpečnostní povahy, které se týkají ISDS, jakožto kritické infrastruktury státu, kdy poskytování požadovaných informací v detailnějším či vyšším rozsahu by mohlo významně ohrozit bezpečnost systému, proto jsou poskytovány pouze v takovém rozsahu, v jakém jsou poskytovány.

S pozdravem

MGR. ING. ONDŘEJ MENOŠEK_

POVĚŘENÝ ŘÍZENÍM ODBORU SLUŽEB EGOVERNMENTU

ODBOR SLUŽEB EGOVERNMENTU_