



DIAPX001ZOQT

první identifikátor

ČÍSLO JEDNACI

DIA- 1975-2/ORR-2024

Vážená paní



VYŘIZUJE



TELEFON



E-MAIL



POČET PŘÍLOH

0

MÍSTO ODESLÁNÍ / DNE

Praha / datum uvedeno v doložce
elektronického podpisu

Poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Digitální a informační agentura (dále jen „DIA“) jakožto povinný subjekt ve smyslu ustanovení § 2 odst. 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „InfZ“), obdržela žádost o poskytnutí informací paní [redacted] trvale bytem [redacted] [redacted] doručenou dne 24. ledna 2024.

Žadatelka podala žádost tohoto znění:

ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím Vás žádám o zpřístupnění následujících informací týkajících se uložení osobních dat občana a bezpečnosti:

v souvislosti s digitalizací je pro občany k dispozici služba Identita občana, která mě zaujala z důvodu zjednodušení komunikace s úřady. Jako občan jsem vlastníkem Datové schránky, kterou k těmto účelům již nějakou dobu používám. Ještě jsem se ale nerozhodla, zda budu chtít využívat i dalších služeb, které jsou nám občanům nabízeny, jako např. zmíněná Identita občana. Ráda bych se proto informovala na některé otázky, které jsem bohužel nikde na internetu nebyla schopna najít a vyčíst. V první řadě mě zajímá, kde jsou fyzicky uložena má osobní data, zda jsou v datovém centru na území ČR nebo jsou uložena v zahraničí. Dále mě zajímá, kdo má k datům přístup, zda se jedná pouze o státní organizace a subjekty nebo jsou data ve správě zahraniční společnosti. A nakonec bych ráda ještě před zřízením výše uvedených služeb věděla, jak jsou data zabezpečena, jak často a jaký subjekt vede kontroly a zda je vedena evidence kybernetických útoků, potažmo zda je možno se s informacemi tohoto typu jako občan seznámit, zda jsou někde zveřejňovány. Neunikl mi ani článek na zpravodajském serveru iDnes (<https://www.idnes.cz/zpravy/domaci/edoklady-prihlaseni-identita-obcana-problemy-pretizeni-nia-aplikace-A240121-110408-domaci-hovo?>), týkající se aplikace eDoklady. Tuto aplikaci, pokud článek rozumím správně, má ve správě společnost Microsoft. Prosím Vás o informaci, kde tato společnost uchovává data,

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

zda má své datové centrum na území ČR, případně využívá služeb jiných tuzemských datových center nebo jsou data fyzicky v zahraničí a dochází tedy k výměně těchto osobních dat mezi ČR a zařízením v zahraničí.

V reakci na tuto žádost DIA poskytuje následující informace:

Data v Identitě občana, která jsou podle zákona 250/2017 Sb., o elektronické identifikaci vedena v informačním systému národního bodu pro identifikaci a autentizaci (dále jen „NIA“), jsou uložena v datových centrech na území České republiky. Data nejsou přenášena ani uchovávána v zahraničí.

K datům má přístup oprávnění zaměstnanci správce NIA, kterým je DIA. Dále je k datům umožněn přístup definovaným zaměstnancům Národní agentury pro informační a komunikační technologie s.p. (dále jen „NAKIT“), která je smluvním dodavatelem informačního systému (NIA) a zajišťuje podporu provozu tohoto systému.

Aplikace eDoklady technicky funguje nezávisle na informačním systému NIA a využívá vlastní poskytované cloudové služby, které byly před spuštěním aplikace kapacitně navýšeny. Společnost Microsoft není správce ani provozovatel aplikace eDoklady. Aplikaci má ve správě rovněž DIA a provozuje jí NAKIT. Data jsou uložena v datovém centru na technologii MS Azure v Nizozemí od společnosti Microsoft, tedy probíhá výměna nezbytných dat mezi ČR a zahraničím.

Pro NIA i pro aplikaci eDoklady platí požadavky na bezpečnost dle ZoKB č. 181/2014 Sb., relevantních požadavků dle vyhlášky č. 82/2018 Sb. a vyhlášky č. 529/2006 Sb. Dále splňuje podmínky stanovené zákonem pro používání eDokladů (zákon, kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony).

Data jsou zabezpečena šifrováním, autentizací, zálohováním a dalšími technickými a organizačními prostředky. Pravidelně se provádějí kontroly a testy bezpečnosti dat a systémů. V případě kybernetických útoků nebo incidentů se vede evidence a podávají se hlášení příslušným orgánům. Tyto informace nejsou veřejné.

Poučení:

Proti rozhodnutí je možné podat ve smyslu § 16 odst. 3) zákona o svobodném přístupu k informacím rozklad, a to do 15 dnů ode dne doručení rozkladu. Rozklad se podává Digitální a informační agentuře, o rozkladu rozhoduje vedoucí jiného správního úřadu.

S pozdravem

Mgr. Petr Frendlovský
vedoucí oddělení správy informačních
systémů referenčního rozhraní