Odpověď Ministerstva zdravotnictví na žádost o informaci dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Dne 18. srpna 2021 obdrželo Ministerstvo zdravotnictví (MZ) Vaši žádost o informaci dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, evidovanou pod č.j. xxx, s prodlouženou lhůtou přípisem č.j. xxx, kterou jste požádala o následující informace *ve věci povinnosti občana při návratu ze zahraničí vyplnit příjezdový formulář, konkrétně pak:*

1.dle nařízení Evropského parlamentu a Rady (EU) 2016/679 má stát povinnost konzultovat legislativní opatření a regulační opatření, která souvisejí se zpracováním osobních údajů. Kdy, jakou formou a s jakými pracovníky Úřadu pro ochranu osobních údajů bylo výše uvedené ochranné opatření konzultováno a jaký je závěr této konzultace? Prosím připojit zápis z jednání příp. jiný výstup.

2. sdělte konkrétní rozsah a způsob zpracování požadovaných údajů, konkretizujte všechny subjekty zpracovávající jednotlivé údaje (kdo konkrétně má k čemu přístup), způsob a místo jejich uložení, způsob ochrany před zneužitím, jakož i specifikujte další nařízením a UOOU určené povinnosti a parametry spojené se zpracováním, vykazováním údajů a také jak a kým je prováděna následná kontrola dodržování pravidel pro zpracování, nakládání údajů.

3. sdělte, jak je s údaji po uplynutí 2 měsíců, po které jsou údaje uchovávány naloženo a jaký záznam dokládající likvidaci údajů je pořízen.

4. Připojte prováděcí předpis určující pravidla zpracování osobních údajů požadovaných od občanů vyplněním příjezdového formuláře.

5. sdělte, proč je doba uchování osobních údajů stanovená na 2 měsíce, jestliže potenciálně rizikovým je občan 14 dnů. Co se s údaji děje po uplynutí doby potenciální "nebezpečnosti" občana?

K Vaší žádosti uvádím:

Ad 1

Speciální konzultace s ÚOOÚ výhradně k Příjezdovému formuláři neproběhly, nicméně doplňujeme, že komunikace s příslušným úřadem probíhá komplexně ohledně systému Chytré karantény a to od 31. 3. 2020 doposud.

Ad 2

Předně bychom Vás rádi ujistili, že veškerým nástrojům tzv. „Chytré karantény“ je v oblasti ochrany dat věnovaná patřičná pozornost, a to již od jejich samotné přípravy. Probíhá průběžná komunikace s Úřadem pro ochranu osobních údajů i s dalšími odborníky v této oblasti. Veškerá data sbíraná prostřednictvím PLF (Příjezdového formuláře) jsou ukládána v zabezpečeném datovém úložišti, které provozuje ÚZIS ČR ve vlastních datových centrech v rámci České republiky. Přístup k datům mají výhradně pověřené osoby, které jsou za účelem výkonu svých pracovních povinností řádně proškoleni a poučeni. Systém PLF je součástí vyššího infomačního systému, který je určen a provozován jako Významný informační systém dle zákona 181/2014 Sb. o Kybernetické bezpečnosti.

Rozsah zpracování: Dle formuláře na stránce: https://plf.uzis.cz/

Způsob zpracování:
Základní operace zpracování

- shromažďování údajů
- zaznamenávání údajů
- uspořádání údajů
- strukturování údajů
- uložení údajů
- přizpůsobení údajů
- pozměnění údajů
- vyhledání údajů
- nahlížení na údaje
- použití údajů
- zpřístupnění údajů přenosem
- šíření údajů či jiná forma jejich zpřístupnění
- seřazení údajů
- zkombinování údajů
- omezení, výmaz nebo likvidace údajů

Zpracování související se zajištěním provozu registru včetně zajištění bezpečnosti údajů zpracovávaných v registrech zajištění HW, SW infrastruktury pro provoz informačního systému

- správa, konfigurace a provoz HW, SW infrastruktury a sítě
- zajištění, provoz a údržba koncových stanic pro přístup ke službě informačního systému
- správa informačního systému (maintenance, patche, hotfix)
- zajištění bezpečnosti informačního systému
- zajištění disaster recovery
- zajištění Help a Service desku pro příjem a poskytování informací od uživatelů
- zajištění služeb datového centra pro umístění technologií pro provoz informačního systému včetně potřebné konektivity

Konkretizujte všechny subjekty zpracovávající jednotlivé údaje (kdo konkrétně má k čemu přístup),

- Ministerstvo zdravotnictví ČR, krajské hygienické stanice, Ústav zdravotnických informací a statistiky ČR
- Všechny výše uvedené subjekty mají přístup ke všem údajům

Způsob a místo jejich uložení, způsob ochrany před zneužitím, jakož i specifikujte další nařízením a UOOU určené povinnosti a parametry spojené se zpracováním, vykazováním údajů a také jak a kým je prováděna následná kontrola dodržování pravidel pro zpracování, nakládání údajů:

Obecná technická opatření dle čl. 32 odst. 1. GDPR	☑ pseudonymizace a šifrování osobních údajů	Nativní šifrování všech uložených dat v rámci databázových prostředků MS SQL Enterprise. Anonymizační a pseudonymizační služby zajišťují pseudynomizaci nebo anonymizaci dat, ke kterým přistupuje běžný uživatel z dat osobních, ke kterým mají přístup pouze vybraní pověření uživatelé.
	☑ schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování	Zpracování je realizováno na redundantním nativním vysoce dostupném řešení v clusteru na vyšších vrstvách od hypervizoru, v rámci infrastruktury aplikační farma s balancery (od hypervizoru výše, aplikační farma s balancery), databáze zpracování je tvořena nativním clusterem (A-A) na úrovni dvou fyzických serverů.
	☑ schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů	Je uplatňována metodika disaster recovery plan s popisem postupu zálohování a plánem obnov. Pro zálohování je využit Data Protector na diskové pole a pásky.
	☑ řízení přístupových oprávnění	Uživatelská práva jsou řízena prostřednictvím Jednotné správy uživatelů (součást JTP) se systémy atomického oprávnění a generovanými přístupovými kódy.
	☑ proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování	
Organizační opatření	☑ Směrnice o zpracování osobních údajů UZIS ☑ Pravidlo čistého stolu ☑ Školení všech zaměstnanců v oblasti ochrany osobních údajů	

	☑ Proces pravidelného testování, posuzování a hodnocení účinnosti zavedených organizačních opatření pro zajištění bezpečnosti zpracování dle Směrnice o nakládání s osobními údaji UZIS

Dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů provádí Úřad pro ochranu osobních údajů.

Ad 3)

Údaje se likvidují aktuálně po roce, a to na základě rozhodnutí správce údajů, Ministerstva zdravotnictví ČR (vizte https://plf.uzis.cz/). Lhůta není určena zákonem ani jiným právním předpisem, jde o preventivní technické opatření. Pokud jsou osobní údaje vymazány z rozhodnutí správce, záznam o vymazání osobních údajů se nepořizuje.

Ad 4

Pokud jste svým dotazem měla na mysli právní základ zpracování údajů, pak se jedná o zákon č. 258/2000 Sb. § 79.

Ad 5

Data se skladují příslušnou dobu s tím, že na potenciálnost využití se tato doba nedělí, tedy jsou bezpečně uloženy po celou dobu, viz politika bezpečnosti citovaná ad 2.

S pozdravem

Mgr. Daniela Kobilková
ředitelka odboru Kancelář ministra
podepsáno elektronicky