Národné centrum zdravotníckych informácií
Lazaretská 26, 811 09 Bratislava 1

Vážený pán
doc. JUDr. Robert Fico, CSc.
Národná rada Slovenskej republiky
Námestie Alexandra Dubčeka 1
812 80 Bratislava

Váš list číslo/zo dňa	Naše číslo	Vybavuje/linka	Mesto
	NCZI- 00842-2021-1130		Bratislava, 25.08.2021

Vec
Oznámení porušenia ochrany osobných údajov dotknutej osobe

Vážený pán doc. JUDr. Robert Fico, CSc.,

dňa 03.08.2021 Národné centrum zdravotníckych informácií (ďalej len „**NCZI**“) na základe oznámenia z CSIRT.SK (Vládna jednotka pre riešenie počítačových incidentov v Slovenskej republike) o existencii zraniteľnosti informačného systému Moje ezdravie (ďalej len „**IS MeZ**“), resp. formulára eHranica analyzovalo, identifikovalo a potvrdilo incident, ktorý má charakter porušenia ochrany osobných údajov v zmysle čl. 4, ods. 12 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), (ďalej len „**GDPR**“).

Na základe následného analyzovania a vyšetrovania bolo špecifikované k akým osobným údajom mala tretia strana (ďalej len „**tretia strana**“ alebo aj ako „**útočník**“) prístup:

- Meno a priezvisko – útočník mal k dispozícii z otvorených zdrojov – k zmene nedošlo
- Rodné číslo – útočník mal k dispozícii z otvorených zdrojov – k zmene nedošlo
- Dátum narodenia – útočník mal k dispozícii z otvorených zdrojov – k zmene nedošlo
- Telefónne číslo – útočník nemal prístup k originálnemu údaju – k zmene došlo, uviedol vlastné
- Email – útočník nemal prístup k originálnemu údaju – k zmene došlo, uviedol vlastný
- Covid pass – útočník mal prístup k originálnemu údaju – ide o neoprávnené získanie údaju – zmena nie je technicky možná
- Digitálny COVID preukaz EÚ – 1 ks Potvrdenie o vykonaní testu (Certifikát o teste PCR) – útočník mal prístup k údaju – neoprávnené získanie osobných údajov citlivého charakteru vygenerovaním certifikátu – zmena údajov nie je technicky možná

  (rozsah údajov certifikátu: 1. meno a priezvisko, 2. dátum narodenia, 3. ochorenie alebo pôvodca ochorenia, 4. typ testu, 5. názov testu, 6. výrobca testu, 7. dátum a čas odberu testovanej vzorky, 8. výsledok testu, 9. testovacie centrum alebo zariadenie, 10. krajina testovania, 11. certifikát vystavil)

Po analýze konštatujeme, že ide o nasledovný typ porušenia ochrany osobných údajov:

- porušenie dôvernosti – neoprávnený prístupu k osobným údajom.

NCZI po klasifikovaní incidentu prijalo technické, ochranné a organizačné opatrenia na zabezpečenie osobných údajov. Vaše osobné údaje a formulár eHranica ako súčasť IS MeZ boli špecifickú dobu počas analýzy incidentu nedostupné, aj pre vás ako dotknutú osobu. Aktuálne sú všetky vaše osobné údaje zabezpečené a po obnove pôvodných dát sú pre Vás dostupné.

Úrad verejného zdravotníctva SR (ďalej len „**UVZSR**") ako prevádzkovateľ IS MeZ v zmysle Zmluvy o spracúvaní osobných údajov[1] oznámil incident Úradu pre ochranu osobných údajov po tom čo NCZI definitívne potvrdilo, že tretia strana mala prístup a pozmenila osobné údaje dotknutých osôb.

NCZI ako prevádzkovateľ v zmysle ustanovenia § 12, ods. 8 zákona 153/2013 Z.z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov, taktiež oznámilo incident Úradu pre ochranu osobných údajov, že tretia strana mala prístup a odcudzila osobné údaje dotknutých osôb prostredníctvom elektronickej podoby Digitálny COVID preukaz EÚ.

Po prevzatí kontroly útočníkom nad autorizačnými údajmi bolo možné získať digitálne certifikáty danej dotknutej osoby (potvrdenia o očkovaní, PCR testovaní), autorizačné správy atď., ktoré sa posielali už na nový email a nové mobilné číslo, ktoré útočník pre dané rodné číslo pozmenil pri zneužití formulára eHranica.

Aktuálne je vec zneužitia prístupu k vašim osobným údajom, ich pozmenenie a odcudzenie prostredníctvom Digitálny COVID preukaz EÚ vyšetrované Orgánmi činnými v trestnom konaní (ďalej len „**OČTK**"), nakoľko NCZI podalo trestné oznámenie na neznámeho páchateľa. Po konzultácii s vyšetrovateľom týmto bezodkladne pristupujeme k informovaniu vás ako dotknutej osoby o vzniknutej udalosti. Trestné oznámenie je k dispozícii u OČTK a evidované pod evid. č. ORPZ-BAI-OPP2-910/2021.

Opis pravdepodobných dôsledkov porušenia:

- Je potenciálne možné zneužiť získaný certifikát a ako?
    - Kontrolný účel – je možné zneužiť certifikát pri kontrole (bez overenia totožnosti osoby, ktorá sa falošne vydáva za niekoho iného) na vstup do prevádzok, alebo na podujatia.
    - Politický účel – v prípade politicky exponovaných osôb je možné zneužiť informácie o (ne)očkovaní na politické ciele, pripadne voči dotknutým osobám.
    - Registračný účel – registrácia na očkovanie, vykonávanie zmien v registrácii na očkovanie, upravovanie osobných informácií, možnosť vytvoriť nové prístupové údaje do GreenPass aplikácie.

Opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom riešiť porušenie, prípadne vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov:

- Stiahnuté certifikáty boli znefunkčnené?
    - všetky certifikáty boli znefunkčnené.
- Je možné ich znefunkčniť a ako?
    - certifikáty vie znefunkčniť len NCZI,
    - dotknutá osoba nemá možnosť priamo ovplyvniť znefunkčnenie certifikátov.
- Aké sme prijali opatrenia aby sa to neopakovalo, keďže je eHranica naďalej funkčná?
    - zablokovali sme zmenu kontaktných údajov v IS MeZ (telefón, email) na základe vyplnených informácii na formulári eHranica,

[1] http://www.nczisk.sk/Documents/ochrana_osobnych_udajov/UVZSR_zmluva_z_23122020.pdf