ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR | 3. ročník | číslo 10 | květen 2021

Evidence testovaných a očkovaných zaměstnanců vs. GDPR

Jak vést evidenci testovaných zaměstnanců v souladu s GDPR? Jaké údaje uchovávat a po jakou dobu? A platí stejná pravidla i pro evidování očkovaných zaměstnanců, kteří uplatňují výjimku z povinného testování?

V současné době v souvislosti s onemocněním covid-19 probíhá povinné pravidelné antigenní testování zaměstnanců a dobrovolné očkování, což má dopady na povinnosti zaměstnavatelů (zejména povinnost dle mimořádného opatření Ministerstva zdravotnictví č. j. MZDR 47828/2020-16/MIN/KAN, ve znění pozdějších mimořádných opatření, umožnit osobní přítomnost na pracovišti pouze negativně testovaným zaměstnancům). Zaměstnavatelé tak zcela logicky za účelem řádného plnění svých povinností **přistupují k vedení příslušné evidence** zaměstnanců, případně o tom minimálně uvažují. Je však vedení takové evidence v souladu s nařízením GDPR?

Údaj o testování na onemocnění covid-19 včetně údaje o očkování proti němu lze nepochybně řadit mezi **údaje související se zdravotním stavem** jedince. Toto potvrzuje i nařízení GDPR, které regulaci těchto údajů (mimo jiné) upravuje a obecně je definuje jako *„veškeré údaje související se zdravotním stavem subjektu údajů, které vypovídají o minulém, současném či budoucím tělesném nebo duševním zdraví subjektu údajů“*. Nařízení dokonce výslovně uvádí, že údaje o zdravotním stavu zahrnují informace získané během provádění testů nebo vyšetřování části těla nebo tělesných látek a jakékoliv informace například o nemoci, postižení, riziku onemocnění, anamnéze, klinické léčbě nebo fyziologickém či biomedicínském stavu subjektu údajů nezávisle na jejich původu. Přímo tak označuje informace o testování jako údaje o zdravotním stavu. Informace o očkování pak lze zahrnout pod **informace související s rizikem onemocnění** (výčet navíc není uzavřený a údaj o očkování, byť ne výslovně uvedený, zcela jistě naplňuje definici osobních údajů o zdravotním stavu tak, jak s ní nařízení pracuje).

Dle nařízení GDPR údaje o zdravotním stavu **patří do zvláštní kategorie osobních údajů**, jejichž zpracování je až na výjimky zakázáno. Pro zpracování údajů o zdravotním stavu zaměstnance zaměstnavatelem, tedy včetně údajů o testování nebo očková-

ní, lze vzít v úvahu aplikaci především následujících výjimek:

- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva; a
- zpracování je nezbytné z důvodu významného veřejného zájmu.

Vnitrostátní právní úprava přitom může zavést další podmínky, včetně omezení, a tyto výjimky ještě zúžit, případně vyloučit. Toto je aktuální zejména s ohledem na mimořádná opatření Ministerstva zdravotnictví ČR.

Evidence testovaných zaměstnanců

V případě vedení evidence testovaných zaměstnanců na onemocnění covid-19 se situace zdá být poměrně jasná. Mimořádné opatření Ministerstva zdravotnictví č. j. MZDR 47828/2020-27/MIN/KAN totiž zaměstnavatelům, kteří pro své zaměstnance zajišťují antigenní testy k použití laickou osobou, přímo **nařizuje vést evidenci provedených testů**. Toto mimořádné opatření je přitom obecně závazné a zaměstnavatelé jsou povinni se jím řídit.

Nutno dodat, že během přípravy tohoto čísla Nejvyšší správní soud zrušil mimořádné opatření ukládající zaměstnavateli vést evidenci provedených testů s tím, že **odložil účinnost tohoto rozhodnutí**. Ministerstvo zdravotnictví má nyní pro vydání nového mimořádného opatření čas do 15. května. Lze však předpokládat, že nové opatření bude věcně shodné a bude doplněno pouze o podrobnější odůvodnění.

Předmětné mimořádné opatření však neupravuje povinnost vedení evidence v případě, že zaměstnavatel zajišťuje antigenní testování **prostřednictvím poskytovatelů zdravotní péče**, tedy nejde o testy pro laické osoby. I v této situaci nicméně považujeme vedení evidence testovaných zaměstnanců zaměstnavatelem za oprávněné, a to z důvodu povinnosti zaměstnavatelů

umožnit osobní přítomnost na pracovišti pouze negativně testovaným zaměstnancům. Zaměstnavatelé by tedy měli mít **přehled o testování svých zaměstnanců**, aby byli schopni tuto povinnost řádně plnit.

Vedení evidence testovaných zaměstnanců tak považujeme za zcela ospravedlnitelné a **v souladu s nařízením GDPR**. Plyne totiž přímo z právních předpisů a takové zpracování údajů o zdravotním stavu lze podřadit pod výjimku zahrnující plnění povinností v oblasti pracovního práva a dále významný veřejný zájem spočívající v prevenci šíření onemocnění covid-19. Bližší podmínky pro zpracování údajů o testovaných zaměstnancích jsou uvedeny níže.

Zaměstnavatel i poskytovatel lékařských služeb jsou dva samostatní správci

K testování prostřednictvím poskytovatelů zdravotní péče nutno dodat, že zaměstnavatel a poskytovatel zdravotní péče jsou **v postavení dvou samostatných správců** osobních údajů se všemi povinnostmi z toho plynoucími. Dle Úřadu pro ochranu osobních údajů by zaměstnavatel měl informaci o provedeném testování obdržet prostřednictvím **potvrzení o provedeném testu** vystaveném daným poskytovatelem. K takovému předání údajů o zdravotním stavu zaměstnavateli, a to za účelem řádného plnění jeho povinností dle předmětného mimořádného opatření, přitom musí dojít na základě smluvního ujednání mezi zaměstnavatelem a poskytovatelem zdravotní péče (nejde však o smlouvu o zpracování osobních údajů mezi správcem a zpracovatelem).

Evidence očkovaných zaměstnanců

V případě vedení evidence očkovaných zaměstnanců proti onemocnění covid-19 však situace tak jasná není. Povinnost vedení této evidence totiž není mimořádnými opatřeními přímo dána. Oporu pro vedení evidence očkovaných zaměstnanců však spatřujeme v mimořádném opatření Ministerstva zdravotnictví č. j. MZDR 47828/2020-16/MIN/KAN, ve znění pozdějších mimořádných opatření, které mimo jiné uvádí, že zaměstnanci jsou povinni na výzvu zaměstnavatele podstoupit testování, s výjimkou *„osob, které mají vystavený certifikát Ministerstva zdravotnictví ČR o provedeném očkování proti onemocnění covid-19, a od aplikace druhé dávky očkovací látky v případě dvoudávkového schématu podle souhrnu údajů o léčivém přípravku (dále jen „SPC“) uplynulo nejméně 14 dní, nebo od aplikace první dávky očkovací látky v případě jednodávkového schématu podle SPC uplynulo nejméně 14 dní, a očkovaná osoba nejeví žádné příznaky onemocnění covid-19“.*

Pokud tedy zaměstnavatel povede evidenci o zaměstnancích s vystaveným

certifikátem Ministerstva zdravotnictví ČR (toto se bude pravděpodobně týkat pouze EU či ČR schválených vakcín), případně i s datem aplikace poslední dávky očkování proti covidu-19, máme za to, že toto bude na základě předmětného mimořádného opatření, které vedení takové evidence v podstatě nepřímo ukládá, zcela ospravedlnitelné a důvodem pro zpracování takového údaje tedy bude **plnění povinností v oblasti pracovního práva**. Bližší podmínky pro zpracování údajů o očkovaných zaměstnancích následují níže.

Zpracování údajů a související povinnosti

V případě vedení evidence testovaných a očkovaných zaměstnanců je zaměstnavatel při zpracování takových údajů **v pozici správce osobních údajů** se všemi povinnostmi vyplývajícími z nařízení GDPR, a to zejména:

- poskytnout subjektům údajů (zaměstnancům) konkrétní informace o zpracování osobních údajů souvisejících s vedením evidence testovaných a očkovaných zaměstnanců (účel a právní důvod zpracování, rozsah zpracovávaných údajů, doba uchování atd.);
- vést záznamy o činnostech zpracování podle článku 30 nařízení GDPR; a
- zajistit, aby osobní údaje byly zpracovávány s odpovídající ochranou soukromí (přijmout technická a organizační opatření, aby byly osobní údaje řádně zabezpečeny před možnou ztrátou, neoprávněným zpřístupněním nebo nepovolenými úpravami).

Účel a rozsah zpracovávaných údajů

Údaje o testovaných a očkovaných zaměstnancích je možné zpracovávat a používat výhradně v souvislosti s **plněním povinností zaměstnavatele** dle příslušných mimořádných opatření. Zejména se jedná o povinnost zaměstnavatele umožnit osobní přítomnost na pracovišti pouze negativně testovaným zaměstnancům s výjimkou mimo jiné těch, kteří mají vystavený certifikát Ministerstva zdravotnictví ČR o provedeném očkování proti onemocnění covid-19, od poslední dávky očkovací látky uplynulo nejméně 14 dní a očkovaná osoba nejeví příznaky onemocnění covid-19.

Rozsah údajů o testovaných a očkovaných zaměstnancích je pak striktně omezen pouze na takové údaje, které jsou pro plnění výše uvedené povinnosti nezbytné:

- **základní identifikační údaje zaměstnance** (jméno, příjmení, datum narození, které je možno nahradit identifikátorem zaměstnance přiděleným zaměstnavatelem),
- **údaje o přesném čase provedení testu** (u většiny zaměstnavatelů postačí datum provedení testu, ve specifických provozech může být evidován i přesný čas),
- **výsledek testu**,

Údaje o provedených testech lze uchovávat po dobu 3 let

- **údaj o provedeném očkování** (respektive vystaveném certifikátu Ministerstva zdravotnictví ČR o provedeném očkování) a
- **datum aplikace poslední dávky očkovací látky**.

Vzhledem k tomu, že vedení evidence provedených testů je dle mimořádných opatření povinné, lze ze strany testovaných zaměstnanců při vedení takové evidence zaměstnavatelem očekávat spíše součinnost. U evidence očkovaných však poskytnutí součinnosti zaměstnancem, tedy **poskytnutí informace o provedeném očkování** (respektive předložení certifikátu Ministerstva zdravotnictví ČR o provedeném očkování), tak samozřejmé být nemusí. Očkování proti onemocnění covid-19 je totiž dobrovolné a zaměstnanci ho (ať už z objektivních, nebo subjektivních důvodů) podstoupit nemusejí a mohou být méně svolní sdělit takovou informaci zaměstnavateli. Pokud zaměstnavatel tuto informaci nemá, jelikož zaměstnanec není povinen mu ji sdělit, měl by k zaměstnanci **přistupovat jako k neočkovanému** a vyžadovat pro jeho osobní přítomnost na pracovišti negativní test. Lze nicméně předpokládat, že zaměstnanci informaci o svém očkování zaměstnavateli sdělí dobrovolně, aby povinné testování absolvovat nemuseli.

Doba pro uchování

V souladu se zásadou minimalizace zpracování osobních údajů by mělo být zpracování údajů o testovaných a očkovaných zaměstnancích přiměřené a uskutečněné **pouze na nezbytně nutnou dobu**.

Dle stanoviska Úřadu pro ochranu osobních údajů, který se vyjádřil k době uchování evidence testování, se s ohledem na související povinnosti zaměstnavatelů jeví jako maximální doba uchování osobních údajů v evidenci testování **3 roky od doby jejich pořízení**, pokud nebude zjištěno, že pro uvedené účely postačuje doba kratší. Tuto dobu Úřad váže na nutnost prokázání plnění uložených povinností vůči orgánům ochrany veřejného zdraví (respektive na promlčecí dobu přestupku spočívajícího v neplnění příkazu testovat zaměstnance a jiné pracovníky, za který je možné uložit sankci do výše 500 tisíc korun). Stejnou dobu pro uchování je z našeho pohledu vhodné aplikovat i **v případě evidence očkovaných zaměstnanců**, aby byl zaměstnavatel případně schopen orgánům ochrany veřejného zdraví prokázat, že na tyto zaměstnance dopadá výjimka z povinnosti testování.

O povinnostech správce souvisejících s testováním zaměstnanců jsme také informovali v mimořádném čísle, které si můžete přečíst **zde**. ▪▪▪

Mgr. Veronika Odrobinová
Mgr. Martina Šumavská

Klikněte a stáhněte si návod

JAK ZPRACOVÁVAT A EVIDOVAT OSOBNÍ ÚDAJE ZAMĚSTNANCŮ TESTOVANÝCH NA COVID-19

1. Co nás jako zaměstnavatele opravňuje osobní údaje zpracovávat?

- právní titul splnění právní povinnosti dle čl. 6 odst. 1 písm. c) GDPR
- pro zpracování údajů o zdraví navíc veřejný zájem v oblasti veřejného zdraví dle čl. 9 odst. 2 písm. i) GDPR

2. Za jakými účely můžeme údaje zaměstnanců zpracovávat?

- předcházení dalšího šíření onemocnění covid-19
- zvýšení bezpečnosti pracovního prostředí
- prokázání plnění povinností uložených správci právními předpisy a jejich kontrola
- prokázání nároků správce vůči zdravotním pojišťovnám při čerpání finančních prostředků na testování poskytované zdravotními pojišťovnami z fondu prevence (tento účel jen pokud se vás týká)

3. Jaké osobní údaje můžeme v rámci testování zpracovávat?

Rozsah uchovaných údajů závisí na konkrétních podmínkách. Zpravidla jde ale o:

- jméno a příjmení,
- datum narození (možné nahradit tak, že zaměstnavatel přidělí jiný identifikátor),
- přesný čas provedení testu,
- výsledek testu (pozitivní / negativní).

Pokud čerpáte finanční prostředky od zdravotní pojišťovny, je třeba uvést i číslo pojištěnce a zdravotní pojišťovnu (případně jiné údaje vyžadované pojišťovnou).
Pokud se na zaměstnance vztahuje výjimka z testování (home office, očkování a podobně), je třeba do příslušných dokumentů rovněž zahrnout i důvod výjimky z testování.

4. Testuje zaměstnance zdravotnické zařízení?

Pokud ano, nezapomeňte s příslušným provozovatelem zařízení uzavřít smlouvu, která dostatečně zajistí plnění právní povinnosti zaměstnavatele (předávání osobních údajů, jejich rozsah, zabezpečení, možnost záměny a podobně). Nejde o smlouvu mezi správcem a zpracovatelem, protože i provozovatel zařízení je v postavení správce.

5. Jak informovat zaměstnance o zpracování?

Obdobně jako v jiných případech. Jednoduše, jasně a srozumitelně. Můžete vyjít z **formuláře** připraveného ze strany ÚOOÚ.

6. Jak máme získané osobní údaje evidovat a po jak dlouhou dobu?

Aktualizujte záznamy o činnostech zpracování. Vzor **záznamu** opět poskytl ÚOOÚ. Zároveň dbejte na to, aby údaje v evidenci testovaných zaměstnanců byly přesné a abyste evidenci s přihlédnutím ke svým možnostem zabezpečili před zneužitím, neoprávněným zpřístupněním, ztrátou či zničením.

✘ Sešit se jmény zaměstnanců položený na recepčním stole není správná volba.

✓ Sešit svěřte klidně recepční, která testované eviduje, ale zamykejte ho do šuplíku v uzamčené místnosti, k němuž mají přístup jen pověřené osoby, které například komunikují s pojišťovnou nebo KHS. Pověřené osoby nezapomeňte proškolit.

✓ Pracujete-li v zabezpečených systémech, vytvořte si evidenci elektronicky, zálohujte ji a nastavte k ní přístup pomocí hesla, které má pouze zapisující osoba a pověřené osoby. Zaměstnanec může mít přístup pouze ke svým záznamům.

Uchovejte si evidenci nejdéle tři roky od provedení záznamu. Porušení povinnosti testovat zaměstnance může být posouzeno jako přestupek, u něhož se stanoví tříletá promlčecí doba.
Orgány mohou stanovit i delší dobu uchování (například ve vztahu ke kontrole evidence v rámci programu zdravotních pojišťoven).

7. Kdo může mít k údajům přístup?

- zpracovatel osobních údajů (například dodavatel softwaru; dbejte ale na uzavření smlouvy o zpracování osobních údajů)
- orgány veřejného zdraví (typicky hygienická stanice) za účelem kontroly plnění uložených opatření
- zdravotní pojišťovny při uplatnění nároku k proplacení nákladů na test

Závěry z kontrol ÚOOÚ a pokuta půl milionu korun

Půlmilionová pokuta za nezákonné zpracování dat z veřejných rejstříků, odstranění kamerového systému a pokuty za neposkytnutí součinnosti – to přinesly další kontroly ÚOOÚ. Co si z nich máte odnést vy?

V posledním díle seriálu o kontrolách ÚOOÚ se podíváme na kategorii, do níž Úřad zařadil kontroly, které nepasovaly do jiných oblastí. To však neznamená, že bychom jim neměli věnovat pozornost. Právě naopak – se seriálem se rozloučíme ve velkém stylu, a to půlmilionovou pokutou.

Zpracování dat z veřejných rejstříků

Pokutu ve výši 600 tisíc korun si od ÚOOÚ vykoledoval správce, který **překlápěl data z veřejných rejstříků** (ARES, obchodní rejstřík, živnostenský rejstřík…) na svou webovou stránku. ÚOOÚ totiž obdržel celkem šest stížností, které vedly k zahájení kontroly.

Závěr ÚOOÚ je v tomto poměrně zajímavý, neboť konstatuje celkem pět porušení. Jako první (a potažmo i druhé) jmenuje **porušení zákonnosti s ohledem na právní titul**, jímž měl být oprávněný zájem. ÚOOÚ vyhodnotil, že pro něj nebyly splněny podmínky, a sdělil, že *„v případě prostého překlápění živnostenského rejstříku a obchodního rejstříku kontrolovanou společností je takové zpracování nezákonné, neboť pouhé ‚překlápění' veřejného rejstříku nesplňovalo podmínku nezbytnosti ve vztahu k účelu zpracování osobních údajů deklarovaného společností"*. Za druhý přešlap ÚOOÚ považuje to, že zpracování **probíhalo bez zákonného právního titulu**.

Třetí, čtvrté a potažmo i páté porušení se mělo týkat **porušení zásady transparentnosti**. Kontrolovaná osoba nejen že nevyrozuměla stěžovatele o způsobu vyřízení jejich žádostí o výmaz, ale zároveň neusnadňovala výkon práv tak, jak požaduje čl. 12 odst. 3 GDPR. A právě pátý prohřešek je pro nás nejvýznamnější, neboť ÚOOÚ konstatoval, že pouhé uveřejnění informací o zpracování osobních údajů na webových stránkách **pro splnění informační povinnosti nestačí**.

Pro splnění informační povinnosti nestačí dát informace o zpracování na web

Společnost proti protokolu o kontrole nepodala námitky a pravděpodobně s ÚOOÚ komunikovala velmi nedostatečně, neboť jí Úřad uložil **smluvní pokutu za nesoučinnost ve výši 100 tisíc korun** a v samotné věci uložil opatření k nápravě a pokutu 500 tisíc korun.

Porušení zabezpečení

ÚOOÚ v minulém roce kontroloval provozovatele rozhlasového vysílání, protože proti němu obdržel stížnost i vlastní oznámení kontrolované osoby, které se týkalo porušení zabezpečení.

V zásadě se tak mělo jednat o dva incidenty, ale ani jeden z nich ÚOOÚ nevyhodnotil jako porušení povinností dle GDPR. První se týkal vlastního oznámení porušení zabezpečení ve věci **zaměstnance ve výpovědní lhůtě**, který tvrdil, že nadřízený měl přístup k jeho osobním údajům tím, že se mu **přihlásil do počítače a využíval jeho identity** (nespecifikováno jak). Incident měl být prošetřen interně, přičemž dle slov ÚOOÚ nebylo shledáno porušení zabezpečení. To vše bylo oznámeno samotnou kontrolovanou osobou.

Naopak blíže neurčený stěžovatel zaslal před koncem roku 2019 ÚOOÚ stížnost, podle níž **mělo dojít k porušení důvěrnosti dat**, a to externím útokem u 45 subjektů údajů v rámci služby Office 365. ÚOOÚ se v tomto případě spokojil s odpovědí kontrolované osoby, že přijala řadu technicko-organizačních opatření, a ÚOOÚ je označil za dostačující.

Registr dlužníků

Třetí z kontrol se týkala zpracování osobních údajů z registru dlužníků. O této problematice jsme psali už v **článku** Registr dlužníků vs. GDPR. Vzhledem k tomu, že ÚOOÚ v rámci kontroly nereferuje o žádných dalších skutečnostech, nebudeme se k tomu nyní vracet.

Kamery na veřejném prostranství

Poměrně smutnou zprávu máme pro fanoušky fenoménu takzvané slow TV.

Souvisí to totiž s kontrolou provozovatele televizního/internetového vysílání, a to na základě několika podnětů, které si stěžovaly na **kamery zabírající prostor železničního přejezdu** v městské části Praha-Řeporyje, jejichž *„záznam je zveřejňován v reálném čase na webových stránkách mall.tv“*, přičemž části záznamu jsou taktéž zveřejňovány v rámci pořadu Extrémní starosta a jsou dále přejímány jinými zpravodajskými médii.

ÚOOÚ toto počínání **kvalifikoval jako porušení GDPR**, neboť mělo docházet ke zpracování osobních údajů bez právního titulu, což vedlo k odstranění kamer.

Další katalogový podvod

Jako katalogový podvod bychom mohli označit počínání osoby, která z veřejného rejstříku Úřadu průmyslového vlastnictví **stáhla blíže neurčený seznam držitelů patentů**, jimž pak předkládala faktury *„za zveřejnění jejich patentů na blíže nestanoveném seznamu patentů“*.

Alespoň takovému případu se ÚOOÚ věnoval na základě podnětu Úřadu průmyslového vlastnictví, což následně vedlo k vydání příkazu a **uložení sankce ve výši 80 tisíc korun za neposkytnutí součinnosti**. Oproti jiným případům však kontrolující osoby uvedly, že *„vzhledem k nesoučinnosti kontrolované osoby bylo hodnocení dodržování dalších povinností stanovených kontrolované osobě obecným nařízením bezpředmětné“*.

> **Neposkytnutím součinnosti se kontrole nevyhnete**

Těžko říct, co si z toho závěru odnést, dlužno dodat, že ÚOOÚ na svých internetových stránkách informuje poměrně v krátkém rozsahu, a proto doporučujeme nechápat výše uvedené tak, že neposkytnutím součinnosti se vyhneme kontrole (protože by ji ÚOOÚ měl považovat za bezpředmětnou).

Závěr

Tímto se loučíme se s naším seriálem o kontrolní činnosti ÚOOÚ za rok 2020, ve kterém jsme se vám snažili přiblížit nejdůležitější závěry z provedených kontrol. Díky těmto informacím byste měli mít přehled o tom, na co se ÚOOÚ při kontrolách zaměřuje, a na případnou kontrolu ve vaší společnosti být zase o něco více připraveni. Zatím můžeme vyhlížet konec pololetí a s ním zveřejnění závěrů z kontrolní činnosti za první pololetí roku 2021.

▪▪▪

Mgr. Josef Bátrla,
advokát v oblasti ICT
www.josefbatrla.cz

Deset mýtů o anonymizaci osobních údajů

Je anonymizace osobních údajů vždy trvalá? Jaký je rozdíl mezi anonymizací, pseudonymizací a šifrováním? A proč dva stejné procesy anonymizace nemusí vést vždy ke stejnému výsledku? Ověřte si, zda jste nepodlehli některému z nejčastějších mýtů o anonymizaci osobních údajů.

Evropský inspektor ochrany údajů (European Data Protection Supervisor neboli EDPS) vydal společně se španělským Úřadem pro ochranu osobních údajů (Agencia Española de Protección de Datos neboli AEPD) stanovisko k **nejčastějším nedorozuměním týkajícím se anonymizace**.

GDPR chápe anonymní informace jako ty, které se **netýkají identifikované či identifikovatelné fyzické osoby**, a jako osobní údaje anonymizované takovým způsobem, že subjekt údajů není nebo již přestal být identifikovatelným (viz bod 26 odůvodnění GDPR). Anonymní informace hrají důležitou roli ve výzkumu v oblasti medicíny, demografie, marketingu, ekonomiky, statistiky a mnoha dalších.

Aby se osobní údaje staly anonymními informacemi, musí tudíž **projít procesem anonymizace**. V průběhu několika posledních let jsme mohli pozorovat více příkladů neúplných nebo nesprávně provedených anonymizačních procesů, které vedly k opětovné identifikaci subjektů údajů. Dokument s názvem *10 Misunderstandings Related to Anonymisation* shrnuje deset největších nedorozumění týkajících se anonymizace, vysvětluje fakta kolem daných nedorozumění a poskytuje odkazy na další literaturu zabývající se touto problematikou. Dokument je dostupný z webových stránek Evropského inspektora ochrany údajů **zde** (v anglickém a španělském jazyce). Stručný přehled nejčastějších omylů týkajících se anonymizace si můžete přečíst níže. ▪▪▪

JUDr. Andrej Lobotka, Ph.D.
www.smart-law.cz

1. PSEUDONYMIZACE JE TO SAMÉ CO ANONYMIZACE

Pseudonymizace a anonymizace jsou dva rozdílné procesy. V čl. 4 GDPR je pseudonymizace definována jako zpracování osobních údajů tak, že již nemohou být **přiřazeny konkrétnímu subjektu** údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě. Použití dodatečných informací tedy může vést k identifikaci fyzických osob. Právě proto je nutné pseudonymizované údaje pořád považovat za osobní údaje. Anonymizovaná data naopak není možné spojit s konkrétní fyzickou osobou. Jakmile jsou údaje skutečně anonymní, nespadají pod GDPR.

2. ŠIFROVÁNÍ JE ANONYMIZACE

Šifrování není anonymizační technikou, ale může být mocným **nástrojem pro pseudonymizaci**. Dešifrovací klíče je totiž nutné chápat jako dodatečnou informaci, jejíž použití často vede k identifikaci fyzických osob (viz výše uvedená definice pseudonymizace). Ani smazání dešifrovacího klíče nemusí být nutně zárukou, že data nebude možné časem dešifrovat. Ani bez dešifrovacího klíče není vyloučeno, že se časem povede data dešifrovat.

3. ANONYMIZACE ÚDAJŮ JE MOŽNÁ VŽDY

Ne vždy je možné snížit riziko opětovné identifikace pod definovanou hodnotu při zachování užitečného souboru údajů pro další konkrétní zpracování. Může se jednat například o situaci, kdy je celkový **počet možných subjektů údajů příliš malý** (například anonymizovaný soubor údajů týkajících se pouze 705 členů Evropského parlamentu) nebo kdy jsou kategorie údajů mezi subjekty údajů natolik odlišné, že tyto subjekty údajů lze vyčlenit.

4. ANONYMIZACE JE NAVŽDY

Existuje riziko, že v budoucnu bude možné některé **anonymizační procesy zvrátit**. Okolnosti, díky nimž jsme mohli určité údaje považovat za anonymizované, se mohou časem změnit a nový technický vývoj (například v oblasti kvantových počítačů) a dostupnost dalších informací (jiných osobních údajů, které v budoucnu uniknou na veřejnost) potenciálně ohrozí předchozí anomymizační procesy.

5. ANONYMIZACE VŽDY SNIŽUJE PRAVDĚPODOBNOST OPĚTOVNÉ IDENTIFIKACE NA NULU

Proces anonymizace a způsob jeho implementace má přímý vliv na pravděpodobnost opětovné identifikace subjektů údajů, jejichž osobní údaje byly anonymizovány. Ačkoliv nezvratná (stoprocentní) anonymizace je z hlediska ochrany osobních údajů nejžádanějším cílem, **v některých případech ji nelze dosáhnout** (pokud chceme zachovat použitelnost anonymizovaných údajů) a je vždy nutné zvážit riziko možnosti opětovné identifikace subjektů údajů, jejichž osobní údaje byly anonymizovány (viz blíže předchozí bod).

6. ANONYMIZACE JE BINÁRNÍ STAV A NELZE U NÍ MĚŘIT STUPEŇ

Informace nelze vnímat jako nacházející se v jednom z binárních stavů: anonymní/neanonymní. Je totiž možné **analyzovat a měřit stupeň anonymizace**. U anonymizovaných údajů vždy existuje určitá míra pravděpodobnosti opětovné identifikace subjektů údajů, jejichž osobní údaje byly anonymizovány. S výjimkou specifických případů, například když jsou údaje velmi zobecněné (třeba informace o počtu návštěvníků webových stránek v určité zemi za rok), není míra pravděpodobnosti opětovné identifikace nikdy nulová.

7. ANONYMIZACI LZE PLNĚ AUTOMATIZOVAT

Během procesu anonymizace je možné použít automatizované nástroje, avšak vzhledem k důležitosti procesu anonymizace je **nutný zásah člověka** – odborníka. Je totiž nutné provést analýzu údajů, které mají být anonymizovány, definovat účel následného použití údajů (poté, co projdou anonymizací) a zvážit riziko opětovné identifikace subjektů údajů, jejichž osobní údaje byly anonymizovány.

8. ANONYMIZACE ČINÍ DATA NEPOUŽITELNÝMI

Správný proces anonymizace udržuje údaje použitelné pro předem definovaný účel. Cíl, pro nějž mají být údaje použity, je však nutné stanovit předem a podle toho zvolit správný proces anonymizace a způsob jeho implementace (přičemž je ovšem nutné zvažovat i riziko opětovné identifikace subjektů údajů, jejichž osobní údaje byly anonymizovány).

9. PROCES ANONYMIZACE, KTERÝ JIŽ POUŽILI JINÍ, POVEDE KE STEJNÉMU VÝSLEDKU

Jak plyne z výše uvedeného, před samotnou anonymizací je nutné provést analýzu údajů, které mají být anonymizovány, definovat účel jejich následného použití poté, co projdou anonymizací, a zvážit riziko možnosti opětovné identifikace subjektů údajů, jejichž osobní údaje byly anonymizovány. Na základě daného posouzení je možné vybrat vhodný způsob anonymizace údajů. Proces, který fungoval pro jednoho správce, **nemusí fungovat pro správce jiného**. I pokud by se jednalo o správce zpracovávající zcela shodné údaje, a povedlo by se tím pádem dosáhnout stejné míry anonymizace, každý z nich může mít jinou představu o tom, co chce s údaji po anonymizaci dále dělat. Zatímco pro jednoho tak anonymizované údaje mohou mít i nadále použití, pro dalšího správce budou zcela bezcenné.

10. NEEXISTUJE ŽÁDNÉ RIZIKO ANI ZÁJEM ZJISTIT, KOHO SE ANONYMIZOVANÉ ÚDAJE TÝKAJÍ

Osobní údaje mají hodnotu samy o sobě, mají hodnotu pro samotné subjekty údajů i pro třetí strany. Opětovná identifikace subjektů údajů by mohla mít vážný **dopad na jejich práva a svobody**. K opětovné identifikaci subjektů údajů, jejichž osobní údaje byly anonymizovány, může dojít v důsledku úmyslných pokusů o opětovnou identifikaci (například s cílem údaje zneužít pro nezákonné jednání, pro výzkum nebo čistě z důvodu zvědavosti a bez záměru je jakkoliv zneužít a podobně) i neúmyslného jednání či v rámci úniku dat.

Elektronický zpravodaj pro pověřence | Vydavatel: Nakladatelství FORUM, s. r. o. | Adresa redakce: Střelničná 1861/8a, 182 00 Praha 8 | Šéfredaktorka: Mgr. Anna Zavadilová | Editorka: Anna Pěkná | Zákaznický servis: Petra Pokojová, office@forum-media.cz, tel.: +420 251 115 576, fax: +420 251 512 422 Jazyková redakce: Bc. Vendula Pazderová | Fotografie: www.bigstockphoto.com | Zlom časopisu: Renata Brtnická | Roční předplatné: 2 490 Kč bez DPH Objednávka předplatného: office@forum-media.cz, fax: +420 251 512 422, informace o předplatném: +420 251 115 576 | Redakční uzávěrka: 6. 5. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.