ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR | 3. ročník | číslo 7 | duben 2021

Monitoring zaměstnanců vs. GDPR

Kamery na pracovišti, kontrola elektronické pošty nebo nahrávání telefonických hovorů – to všechno jsou způsoby, jak kontrolovat zaměstnance. Nesmíte přitom však zapomenout na ochranu soukromí a osobních údajů! Jaké zásady musíte při monitoringu zaměstnanců dodržovat?

Kontrola zaměstnanců představuje nedílnou součást výkonu řídicí činnosti zaměstnavatele. Zaměstnavatelé kontrolují zaměstnance v souvislosti s ochranou svých oprávněných zájmů i za účelem **zajištění efektivního výkonu práce**. Mezi rozšířené nástroje kontroly patří i ty, které jsou označovány jako monitoring. Uplatnění sledovacích nástrojů při kontrole zaměstnanců není zakázáno, ale musí být dodrženy **podmínky stanovené zákoníkem práce**. Monitoring navíc představuje i formu zpracování osobních údajů, a tak musí zaměstnavatel dodržet i pravidla vyplývající z obecného nařízení o ochraně osobních údajů (GDPR).

Základní podmínky monitoringu

Zákoník práce upravuje možnosti zaměstnavatele při využití sledovacích nástrojů za účelem kontroly zaměstnanců v § 316 odst. 2 a 3. Mezi sledovací nástroje, jejichž uplatnění je označováno za monitoring zaměstnanců, je řazeno otevřené nebo skryté sledování, odposlech a **záznam telefonických hovorů a kontrola elektronické pošty** nebo listovních zásilek adresovaných zaměstnanci. Za nejčastější formu monitoringu lze **označit kamerové sledování pracovišť** zaměstnavatele, v jehož rámci se ještě rozlišuje sledování bez pořízení a s pořízením a uchováním záznamu.

Za neoprávněný monitoring můžete dostat pokutu až 1 milion Kč

Zaměstnavatel, který je oprávněn a současně i povinen své zaměstnance při výkonu práce kontrolovat, musí zvolit, **který z kontrolních nástrojů uplatní**. Zajištění kontroly zaměstnanců rozhodně neznamená, že by každý zaměstnavatel musel nebo měl provádět monitoring. Při úvaze o tom, jak bude zaměstnance kontrolovat, musí brát zaměstnavatel v úvahu vedle svých právem chráněných zájmů i právo zaměstnanců na zachování jejich lidské důstojnosti a na **ochranu soukromí**.

Klíčovými pojmy při zvažování toho, jaký kontrolní nástroj uplatnit, jsou **přiměřenost a proporcionalita**.

Přiměřenost a proporcionalita

Hledisko proporcionality (úměrnosti) je třeba vnímat tak, že **míra narušení soukromí**, kterou způsobí kontrolní mechanismus, musí být úměrná významu a hodnotě zájmů zaměstnavatele. Mechanismy, jež umožňují důkladnou kontrolu, ale současně znamenají velmi **intenzivní zásah do soukromí zaměstnanců** (například kamerové sledování se záznamem), mohou být uplatněny jen tam, kde zaměstnavatel musí chránit zájmy vysokého významu či hodnoty.

Z hlediska přiměřenosti v souvislosti s veškerými formami kontroly vyplývá, že pokud k oprávněnému cíli (například k dosažení ochrany majetkových zájmů zaměstnavatele) vede **několik možných způsobů**, musí zaměstnavatel zvolit ten, který představuje nejméně intenzivní zásah do soukromí zaměstnanců. Přiměřenost je třeba **zvažovat vždy individuálně** s ohledem na míru zásahu do soukromí a efektivitu uplatněného kontrolního mechanismu.

K monitoringu nepotřebujete souhlas zaměstnance

PŘÍKLAD:

Ochrana majetku představuje pro každého zaměstnavatele důležitý zájem. Zaměstnavatel proto může kontrolovat, jak zaměstnanci s jeho majetkem nakládají a zda se nedopouštějí jednání, které jeho majetkové zájmy ohrožuje (poškozování, zpronevěra, krádež a podobně). Uplatněný kontrolní mechanismus musí být nicméně úměrný povaze a hodnotě zaměstnavatelova majetku. Obecně lze shrnout, že čím vyšší škoda zaměstnavateli hrozí, tím intenzivnější zásah do soukromí musí být zaměstnanci připraveni při výkonu kontroly snést.

PŘÍKLAD:

Nejvyšší soud v rámci své rozhodovací činnosti dovodil, že si zaměstnavatel počíná přiměřeně, pokud za účelem kontroly dodržování zákazu používat internetové stránky s pochybným nebo citlivým obsahem sleduje, jaké webové stránky zaměstnanec z prohlížeče na zaměstnavatelově počítači otevírá.

Závažný důvod

Zákoník práce spojuje možnost uplatnění kontrolních mechanismů, které zahrnují sledování zaměstnance a jeho projevů osobní povahy, s **existencí závažných důvodů**. Pokud tedy například zaměstnavatel uvažuje o aplikaci kamerového sledování spojeného s pořizováním záznamu, musí být připraven vysvětlit, na základě jakého závažného důvodu chce tuto formu monitoringu uplatnit a proč není možné dosáhnout téhož cíle jinými prostředky. Nutno totiž připustit, že **kamerové sledování a následné ukládání záznamů** představuje z pohledu zaměstnance velmi výrazný zásah do jeho soukromí.

Zaměstnavatel musí **být připraven zdůvodnit i dobu**, po kterou jsou pořízené záznamy dále ukládány. Toto zdůvodnění musí pochopitelně odrážet specifické důvody a okolnosti, které zaměstnavatele vedly k rozhodnutí sledovací mechanismus zavést.

Sledování elektronické pošty

Zvláštní pozornost musí být věnována také souvislostem případného **sledování obsahu elektronické pošty**, případně listovních zásilek určených zaměstnanci. Listovní tajemství a tajemství jiných písemností a záznamů zasílaných poštou nebo jiným způsobem totiž požívá zvláštní ochrany zakotvené v čl. 13 Listiny základních práv a svobod.

PŘÍKLAD:

Provozuje-li zaměstnavatel kamerový systém za účelem ochrany svého majetku, měl by být schopen vysvětlit, jak konkrétně provoz kamery zlepší úroveň ochrany určitých majetkových zájmů, a také zdůvodnit, proč k ochraně majetku není dostatečný jiný nástroj, který by méně zasahoval do soukromí dotčených zaměstnanců (například bezprostřední dohled ze strany vedoucích zaměstnanců nebo důsledná kontrola při odchodu zaměstnanců z pracoviště).

Lze si představit, že bude zaměstnavatel argumentovat například rozlohou výrobních prostor, v jejímž důsledku nelze uplatnit jiný efektivní kontrolní nástroj než právě kamerový systém. Pro zdůvodnění mohou zaměstnavateli posloužit třeba i případy narušení majetkových zájmů, k nimž došlo nebo dochází, případně jiné specifické okolnosti.

Pokud má být pořízený záznam uchováván například po dobu tří dnů, musí zaměstnavatel zdůvodnit, že právě taková doba je k efektivní ochraně majetkových zájmů nezbytná (například proto, že případy narušení majetkových zájmů se mohou na určitém pracovišti projevit právě až s odstupem několika dnů).

Při existenci závažných důvodů je možné připustit, že zaměstnavatel nebo jiný zaměstnanec otevře listovní či elektronickou zásilku směřovanou zaměstnanci jen v případě, kdy je z okolností zjevné, že **jde o zásilku pracovní a nikoliv soukromé povahy**, a kdy je tento postup nezbytný z hlediska ochrany oprávněných zájmů zaměstnavatele (například tehdy, pokud je zaměstnanec, jemuž byla zásilka adresována, v dlouhodobé dočasné pracovní neschopnosti a z důvodu rizika prodlení nelze čekat na jeho opětovný nástup do práce).

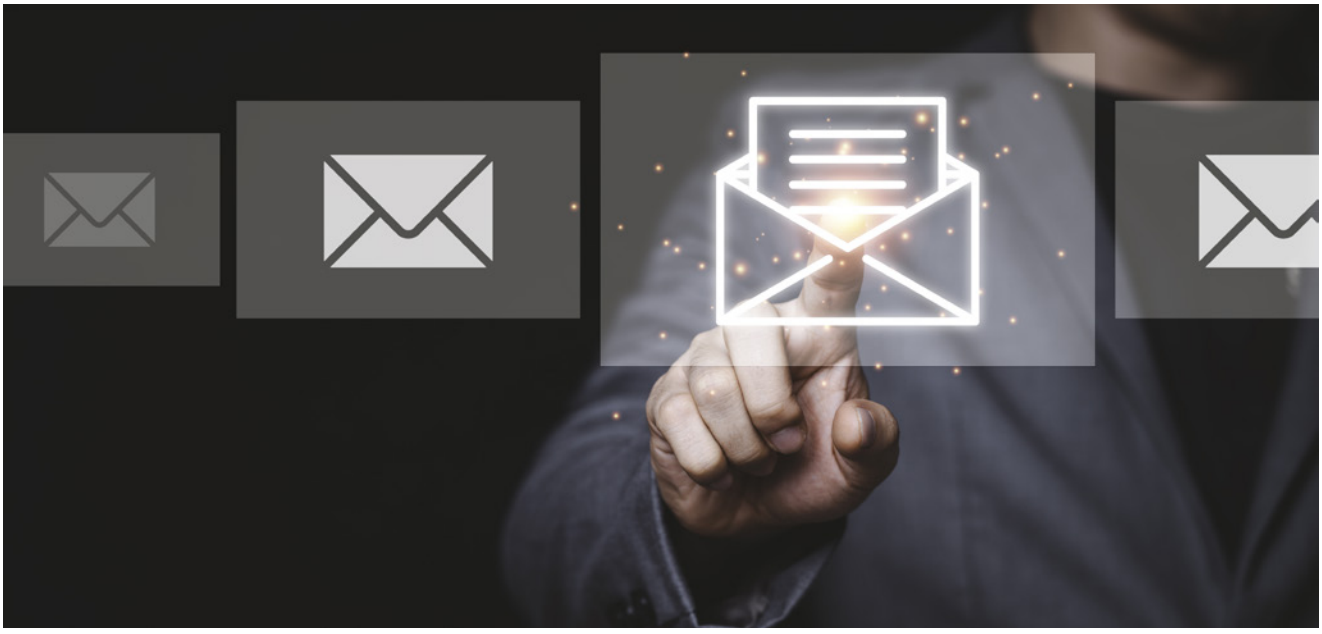
Přímé informování o monitoringu

Jako další podmínku uplatnění sledovacích mechanismů stanovuje zákoník práce **předchozí informování zaměstnanců o rozsahu kontroly** a způsobech jejího provádění. Zaměstnavatel tedy musí zajistit, aby byli zaměstnanci vždy přímo seznámeni s tím, zda je vůči nim aplikován sledovací mechanismus, jakým způsobem a v jakém rozsahu jsou sledováni.

Volba konkrétního způsobu informování záleží na zaměstnavateli. Za dostatečnou formu lze jistě považovat například **popis uplatněných sledovacích mechanismů** ve směrnici o zpracování a ochraně osobních údajů nebo v jiném, zaměstnancům přístupném vnitropodnikovém dokumentu. Nově nastupující zaměstnanci budou s tímto dokumentem seznámeni v rámci plnění informační povinnosti zaměstnavatele při založení základního pracovněprávního vztahu.

Zákoník práce netrvá na tom, aby zaměstnanci **uplatnění sledovacího mechanismu odsouhlasili**. Zaměstnavatel tedy nemusí případnou listinu, která obsahuje popis způsobu a rozsahu sledování, předkládat zaměstnancům s tím, aby ji svým podpisem odsouhlasili.

Ačkoliv monitoring zaměstnanců představuje formu zpracování osobních údajů, na něž se vztahují i pravidla obsažená v GDPR, neznamená to, že by museli zaměstnanci s tímto zpracováním vyslovit souhlas. Zpracování totiž probíhá **na základě jiné-**



CHYBA:

Udělení souhlasu nelze považovat za nahrazení právními předpisy stanovených a výše popsaných podmínek pro sledování. Nelze se tedy domnívat, že pokud zaměstnanec vysloví souhlas, může zaměstnavatel provádět jakékoliv sledování. Ochrana soukromí představuje ústavně garantované právo, jehož se nelze vlastním projevem vůle vzdát. Rozhodující pro soulad monitoringu s právní úpravou je splnění popsaných podmínek, tedy zejména existence závažného důvodu a přiměřenost.

ho právního titulu, uvedeného v čl. 6 odst. 1 písm. f) GDPR. Jde o příklad zpracování, které je **nezbytné pro účely oprávněných zájmů správce**. Pokud zaměstnavatel provádí monitoring v souladu s § 316 odst. 2 zákoníku práce na základě vážného důvodu, poslouží tento důvod i pro doložení existence oprávněného zájmu zaměstnavatele jako správce podle čl. 6 odst. 1 písm. f) GDPR.

Povinnost informovat zaměstnance o monitoringu, zakotvená v zákoníku práce, koresponduje s povinnostmi správce vůči subjektům údajů podle GDPR. I z tohoto předpisu lze jednoznačně dovodit **povinnost správce informovat subjekty údajů** o tom, jaké jejich osobní údaje jsou zpracovávány, jakým způsobem, za jakým účelem a podobně.

Kontroly ze strany inspekce práce

Případy, kdy zaměstnavatelé provádějí například kamerové sledování svých zaměstnanců, aniž jsou u nich dány okolnosti úměrné takto intenzivnímu zásahu do soukromí, **představují porušení zákona**, v souvislosti s nímž může dojít i k **uložení pokuty ze strany orgánů inspekce práce**.

Podle § 24a zákona o inspekci práce představuje narušení soukromí zaměstnanců monitorováním bez splnění stanovených podmínek správní delikt, za jehož spáchání může být uložena **pokuta až do výše jednoho milionu korun**. Zaměstnavatel, který vůči sledovaným zaměstnancům nesplnil informační povinnost, riskuje uložení pokuty až do výše sto tisíc korun. ▪▪▪

JUDr. Jaroslav Stránský, Ph.D.

Ověřovací certifikát o očkování proti covidu obsahuje nechráněné osobní údaje

Každý, kdo absolvuje druhou dávku očkování proti covidu-19, obdrží elektronické potvrzení, kterým by v budoucnu mohl prokázat, že dostal vakcínu, a získat tak určité úlevy či výhody. Očkovací certifikát, jehož vydávání má na starosti Ústav zdravotnických informací a statistiky, však obsahuje osobní údaje očkovaného, které nejsou nijak chráněny. Certifikát je opatřen QR kódem pro ověření pravosti, který obsahuje webový odkaz na ověřovací stránku ústavu s číslem certifikátu, ale také jménem a příjmením očkovaného, jeho datem narození, rodným číslem a číslem občanského průkazu či pasu. Žádný z těchto údajů přitom není nijak zašifrován, a hrozí tak, že se tyto údaje budou automaticky ukládat do historie prohlížeče či čtečky QR kódů na zařízení, na němž bude certifikát kontrolován. Adresa navštívených stránek se navíc obvykle zaznamenává i do takzvaných přístupových logů serverů, kde nejsou osobní údaje nijak chráněny.

Zdroj: iRozhlas

Jak dopadly kontroly ÚOOÚ v oblasti školství i obchodu

Co odhalily kontroly ÚOOÚ ve školství a obchodu? Je třeba logovat přístup k osobním údajům i při malém počtu zaměstnanců? A lze zveřejnit fotografii zaměstnance na základě oprávněného zájmu?

V minulém čísle jsme se věnovali kontrolním závěrům ÚOOÚ z oblasti IT technologií a státní správy, aby se ze zjištěných chyb poučili i ostatní a aby nahlédli pod pokličku právních názorů ÚOOÚ. V tomto čísle se podíváme na kontrolní závěry z **oblasti prodeje zboží a služeb a školství**. Tyto oblasti mohou na první pohled vypadat nudně, ÚOOÚ se však věnoval i takovým otázkám, jako je **logování přístupu či právní titul pro zpracování fotografií** zaměstnanců. Pojďme tedy na to.

Katalogové služby

Obdrželi jste někdy jako podnikatelé **dopis, k němuž byla přiložena složenka** a v záhlaví dopisu bylo uvedeno například „Rejstřík obchodu a živnosti“ či jiný nadpis, jenž by mohl působit matoucím způsobem? Pokud ne, věřte, že když začínajícímu podnikateli takový přípis přijde, často má nakročeno k tomu, aby **naletěl možným podvodníkům a platil** za něco, co je vlastně úplně zbytečné.

Dopis totiž vypadá, jako by přišel od státní instituce, která žádá o uhrazení běžného poplatku, aby vás mohla zařadit do rejstříku – což se po zaplacení skutečně stane, nicméně **nejedná se o živnostenský či obchodní rejstřík**, ale rejstřík (lépe řečeno katalog) soukromé společnosti, jenž většinou nemá žádný dosah. Ve většině případů se pro takový business model zažil název **katalogový podvod**, a kdo se s ním ještě neseznámil, může se o něm dozvědět více například **zde**.

Právě jednoho z provozovatelů katalogu „Rejstřík obchodu a živnosti“ kontroloval i ÚOOÚ, a to v reakci na stížnost subjektu údajů, jehož **námitky proti zpracování osobních údajů** na základě oprávněného zájmu nebyly ze strany kontrolované osoby reflektovány. Stěžovatel totiž obdržel od této společnosti výzvu, kterou ÚOOÚ při kontrole kvalifikoval jako **nevyžádanou a adresnou nabídku služeb**. Stěžovatel však nebyl dle textace ÚOOÚ schopen doložit, že skutečně podal námitky proti danému zpracování na základě oprávněného zájmu, a ÚOOÚ tudíž celou situaci vyhodnotil jen jako porušení čl. 6 odst. 1 GDPR, nikoliv čl. 12 GPDR. Společnost proti kontrolním zjištěním podala námitky, ty však byly předsedou ÚOOÚ zamítnuty.

> **Pozor na katalogové podvody a soukromé rejstříky**

Prodejci energií

ÚOOÚ se věnoval taktéž oblasti prodeje energií, což si předsevzal **v rámci kontrolního plánu** pro rok 2020. V této oblasti máme informace o dvou provedených kontrolách.

V rámci první ÚOOÚ nezjistil nic mimořádného, nicméně přece jen otevřel jednu klíčovou otázku zabezpečení osobních údajů – **logování přístupů k osobním údajům**. V daném případě totiž kontrolovaná osoba vyhodnotila, že má malý počet zaměstnanců a zpracování nevykazuje příliš riziko pro práva subjektů údajů.

ÚOOÚ tuto skutečnost okomentoval tak, že ačkoliv povinnost logování přístupu nemá svoji výslovnou oporu v GDPR, stává se již **standardní ochranou a nezbytnou součástí zabezpečení** osobních údajů, ale že je to na volbě správce, přičemž zdůraznil, že nelogování přístupu s sebou nese větší odpovědnost. Doslova ÚOOÚ řekl: *„V případě, že dojde k neoprávněnému přístupu k osobním údajům, popřípadě k jejich zneužití a správce nebude v daném případě schopen prokázat, kdo, kdy a za jakým účelem k osobním údajům neoprávněně přistoupil, bude odpovídat za vzniklé protiprávní následky v plném rozsahu.“*

V tomto konkrétním případě tak ÚOOÚ přihlédl **k argumentu malých rizik a malého počtu zaměstnanců**, nicméně můžeme to chápat také jako jemné naznačení, jak k této problematice bude příště přistupovat.

Druhá kontrola v této oblasti si ani nezaslouží bližší komentář, neboť ÚOOÚ se omezil na konstatování, že nezjistil žádné porušení.

Kontroly ve školství

Kontrolní činnost ve školství nebyla nikterak plodná, alespoň pro naše po-

třeby. V této oblasti se v souladu se svým kontrolním plánem ÚOOÚ věnoval kontrole zpracování osobních údajů v rámci **informačního systému Bakaláři**, a to celkem dvakrát – ani jednou však neodhalil porušení GDPR.

Třetí kontrola byla věnována základní škole, a to na základě **stížnosti na protiprávní předání osobních údajů** ze strany základní školy Spolku ZUŠ. Tento závěr však ÚOOÚ nepotvrdil.

Zaměstnanecká agenda

To nejzajímavější přichází na samotný konec – ÚOOÚ kontroloval **státní příspěvkovou organizaci** na základě stížnosti, která mířila proti zpracování osobních fotografií zaměstnanců na internetových stránkách zaměstnavatele.

Původně zaměstnavatel na svém webu uveřejňoval fotografie zástupců regionálních poboček a činil tak na základě uděleného souhlasu. Nicméně okamžikem, kdy byl daný souhlas ze strany stěžovatelky odvolán a byl požadován výmaz fotografií, **přehodnotila kontrolovaná osoba právní základ** pro dané zpracování a sdělila, že se jedná o zpracování osobních údajů na základě oprávněného zájmu, a dokonce k tomu stěžovatelce předložila i balanční test.

Kontrola ze strany ÚOOÚ toto neakceptovala, připustila nicméně poměrně zásadní věc, a sice že zpracování osobních údajů prostřednictvím fotografie by bylo **možno schovat pod oprávněný zájem**, v daném případě ovšem **neobstál balanční test**, který měl prokázat přednost oprávněného

Logování přístupu může být nezbytnou součástí zabezpečení osobních údajů

zájmu před právy subjektu údajů. ÚOOÚ k tomu obecně připojil doplňující informace: *„Ačkoli obecné nařízení nestanoví závaznou podobu balančního testu, musí tento prokázat oprávněné zájmy pro dané zpracování, které převažují nad zájmy nebo základními právy a svobodami subjektů údajů. Jestliže oprávněný zájem prokázán není, nelze pro toto zpracování využít právní titul ve smyslu čl. 6 odst. 1 písm. f) obecného nařízení. V rámci balančního testu se nikdy nebude možné spokojit s prostým konstatováním, že ve vztahu k subjektu údajů žádná rizika neexistují, tak jak bylo uvedeno v balančním textu kontrolované osoby. Jestliže jsou rizika určitými opatřeními minimalizována, pak právě balanční test poskytuje pro tyto úvahy a informace vhodný prostor.“*

Je tedy otázkou, zda možnost zpracování osobních údajů na základě oprávněného zájmu v této formě není spíše teoretickou možností, která bude v praxi vždy vyloučena tím, že předmětné **zpracování neprojde balančním testem**.

Závěr

Závěry ze zmíněných kontrol **otevřely dvě poměrně zásadní otázky**, jako je povinnost logovat přístupy k osobním údajům (což se z počátku účinnosti GDPR velmi často zaměňovalo za povinnost dle čl. 30 GDPR), ale i užívání fotografií na webu. V dalším díle se můžete těšit na závěry z kontrol, které se týkají zdravotnictví a dalších oblastí.

▪▪▪

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

Poradna

Do jaké kategorie osobních údajů spadají údaje o odměnách za práci a další údaje vyplývající z pracovněprávního vztahu (délka čerpané dovolené, počet odpracovaných hodin a podobně)? Kdy je délka čerpané dovolené a počet odpracovaných hodin osobním údajem?

Předně nutno uvést, že GDPR neobsahuje taxativní výčet kategorií osobních údajů a ani podnikatelská veřejnost se není schopna shodnout na tom, co je „kategorií" osobních údajů myšleno. Na výše položenou otázku tak lze odpovědět, že samy údaje o odměnách za práci jsou kategorií osobních údajů. Dlužno dodat, že samotné pojmenování kategorie není tak důležité a vždy bude záležet na kontextu (zejména ve vztahu k informování subjektů údajů či obecným parametrům zpracovatelské smlouvy). Důležitější než myslet na to, jak se kategorie jmenuje, je tak přemýšlet, co je jejím obsahem a zda se jedná o zvláštní kategorii osobních údajů (dle čl. 9 GDPR) – pokud se totiž jedná o zvláštní kategorie osobních údajů, jsou s jejich zpracováním spojeny dodatečné povinnosti, na které je potřeba dávat pozor. Ve vztahu k otázce lze však bezpečně říct, že uvedené kategorie (či příklady osobních údajů) nespadají do zvláštní kategorie osobních údajů.

Druhá část otázky se týká povahy a pojetí definice osobního údaje jako takového. Definici osobního údaje nalezneme přímo v čl. 4 odst. 1 GDPR, přičemž za osobní údaje je nutno považovat takovou informaci, kterou zpracováváme o identifikované či identifikovatelné osobě. Zjednodušeně řečeno – informace se stává osobním údajem okamžikem, kdy jsme pomocí ní schopni identifikovat osobu, ale je to také informace, kterou vedeme o již identifikované osobě. Pokud tedy o svém zaměstnanci ukládáme nějaké informace (velikost bot, jména dětí, datum narození ale i oblíbenou barvu nebo cokoliv jiného), splňují takové informace definiční znak osobního údaje.

Je samotné poskytnutí informací žadateli podle zákona 106/1999 nebo zastupiteli podle zákona 128/2000 o zaměstnancích úřadu (subjektech údajů) zpracováním osobních údajů? Případně za jakých okolností?

Definici zpracování osobních údajů nalezneme v čl. 4 odst. 2 GDPR, který hovoří o tom, že zpracováním je jakákoliv operace (či soubor operací), která je prováděna pomocí či bez pomoci automatizovaných postupů. S trochou nadsázky je tak možno říct, že stejně jako je nutno široce vykládat definici samotných osobních údajů, je nutno vykládat i definici zpracování – tedy v podstatě jako cokoliv, co s osobními údaji uděláme. Co se týče otázky poskytnutí informací, zmíněné ustanovení čl. 4 odst. 2 GDPR obsahují příklady operací zpracování, mezi které řadí i *„použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění"*. Výše zmíněné poskytnutí informací je tak vhodné chápat jako operaci zpracování. Dlužno dodat, že sám zákon (zejména zákon č. 106/1999 Sb.) upravuje, kdy má veřejný zájem nad kontrolou fungování orgánů veřejné správy (ve formě práva na informace) přednost před právy fyzických osob na soukromí. Pokud tedy musí povinný subjekt žádosti o informaci vyhovět, lze na takové zpracování pohlížet zpravidla jako na nezbytné pro splnění právní povinnosti, popřípadě zpracování osobních údajů ve veřejném zájmu.

Jsme zdravotnické zařízení pečující o onkologické pacienty. Zhruba dvě třetiny našich zaměstnanců jsou již po očkování, zbývající nyní podrobujeme antigenním testům. Je v souladu s GDPR vyžádat si a uchovat pro případnou kontrolu od očkovaných zaměstnanců certifikáty o očkování? Nebo je možné si jej pouze nechat ukázat a provést záznam o kontrole?

I v této nelehké situaci platí základní pravidla ochrany osobních údajů, které bychom měli mít stále na paměti. Klíčová je tak zásada minimalizace dle čl. 5 odst. 1 GDPR, která nám přikazuje zpracovávat pouze nezbytně nutný rozsah osobních údajů, který je nezbytný pro splnění daného účelu zpracování osobních údajů. Je tak nutné si nejprve položit otázku, proč dané osobní údaje potřebuji a následně v jaké formě.

Certifikát o provedeném očkování sám o sobě dosvědčuje skutečnost, že osobě byla podána vakcína – takový certifikát však obsahuje mnohem více informací. Alespoň ze **vzoru** uvedeného na stránkách covid.gov.cz vyplývá, že součástí certifikátu jsou nejen identifikační údaje (včetně data narození), ale i údaje o čísle pojištěnce, čísle občanského průkazu či čísle pasu. Kromě toho takový dokument obsahuje i informace týkající se podané vakcíny, včetně šarží jednotlivých dávek.

Pokud bychom k tomu přistupovali v rámci myšlenkového cvičení od konce, měli bychom si položit otázku, zda existuje účel, který by ospravedlňoval naše zpracování všech těchto údajů v takovém rozsahu (včetně například ověřené kopie certifikátu). Kupříkladu dne 1. 3. 2021 vydalo Ministerstvo zdravotnictví mimořádné opatření č. j. MZDR 47828/2020-16/MIN/KAN, kterým se zavedlo (zjednodušeně řečeno) povinné testování zaměstnanců, přičemž doplnění tohoto mimořádného opatření ze dne 5. 3. 2021 (č. j. MZDR 47828/2020-21/MIN/KAN) uvádí z tohoto pravidla výjimku, a to sice pro osoby *„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 dnů a očkovaná osoba nejeví žádné příznaky onemocnění covid-19".

Zjednodušeně řečeno v takovém případě, i když zaměstnavatel vyzve zaměstnance k tomu, aby se nechal otestovat, zaměstnanec tuto povinnost nemá. Otázkou zůstává, jakým způsobem toto má zaměstnanec doložit. Odpověď na tuto otázku nepodává ani Ministerstvo zdravotnictví v rámci odůvodnění svého opatření, ani Ministerstvo průmyslu a obchodu na svých internetových stránkách (viz **zde**). Bližší informace k tomu nepodal ani Úřad pro ochranu osobních údajů (viz **zde**), který se této okolnosti věnoval spíše okrajově v souvislosti s testováním: *„Vlastní záznamy o provedení testů u zaměstnanců mohou obsahovat pouze základní identifikační údaje zaměstnance (jméno, příjmení, číslo pojištěnce), údaje o zdravotní pojišťovně zaměstnance, údaje o přesném čase provedení testu a výsledek testu na nákazu covid-19. Stejné omezení rozsahu pouze na nezbytné osobní údaje platí i pro případné dokumenty prokazující výjimku z povinného testování daného zaměstnance (identifikační údaje zaměstnance, důvod výjimky z testování)."*

Variant, jak k této otázce přistupovat, je tedy několik – můžete uvažovat o tom, že si ponecháte originál či úředně ověřenou kopii certifikátu, obyčejnou kopii certifikátu, částečně anonymizovanou kopii certifikátu, popřípadě si zapíšete jen nezbytné údaje (datum vakcinace, číslo certifikátu a podobně), nebo si jen ověříte pravost certifikátu a kromě informace, že osobu není potřeba testovat, nebudete zpracovávat už vůbec nic. Při tomto rozhodování musíte zohlednit všechny okolnosti, včetně minimalizace, možného zásahu do práv subjektů údajů, případná rizika a všechny související povinnosti.

V případě běžného zaměstnavatele si dovedeme představit, že postačí částečně anonymizovaná podoba certifikátu či jen opsané údaje. V případě poskytovatele zdravotních služeb je možné, že s přihlédnutím k všeobecnému riziku v daném prostředí bude mít zaměstnavatel extrémní zájem na tom, aby osoby, které tvrdí, že jsou očkovány, toto skutečně prokázaly, a pro účely tohoto prokázání si zaměstnavatel ponechá důkaz. S ohledem na stávající situaci lze připustit, že nepřiměřeným zásahem do práv zaměstnanců by pravděpodobně nebylo, pokud by si zaměstnavatel ponechal částečně anonymizovanou kopii certifikátu, a to za předpokladu, že dodrží veškeré technické a organizační opatření, které je nutno s přihlédnutím k takovému „certifikátu" zavést. A to vše alespoň do chvíle, než budou upřesněny informace týkající se kontrol či bude vydáno bližší stanovisko Úřadu pro ochranu osobních údajů, z nějž lze aktuálně usoudit, že se k této problematice staví spíše rezervovaně a preferuje co nejmenší rozsah shromažďovaných osobních údajů. Pokud tedy nechcete udělat chybu, můžete se odpíchnout od toho a pro případ kontroly odkázat kontrolující subjekt na informace z Očkovacího portálu občana, v rámci kterého by měl být každý z certifikátu evidován.

JOSEF BÁTRLA ADVOKÁT

Nevíte si s něčím rady? Pošlete nám svůj dotaz a my vám zprostředkujeme odpověď! Dotazy pokládejte e-mailem na:
zpravodaj.poverenec@forum-media.cz

V příštím čísle Zpravodaje se dozvíte:
- **Sledování firemních vozů pomocí GPS vs. GDPR**
- **Co odhalily kontroly ÚOOÚ ve zdravotnictví?**

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: 25. 3. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.