ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR

3. ročník | číslo 8 | duben 2021

Můžete **sledovat firemní auta** i po pracovní době?

Máte ve firemních vozech GPS lokátory? Pokud ano, mohlo by vás zajímat, zda a za jakých podmínek můžete sledovat firemní auta i po pracovní době.

V předchozím čísle jsme se zaměřili na oblast monitoringu zaměstnanců, která je relativně problematická a přirozeně přitahuje pozornost Úřadu pro ochranu osobních údajů. Možná se k vám donesla informace, že ÚOOÚ říká, že **sledovat služební vozidla i po pracovní době** je v souladu se zákonem, neboť je to oprávněným zájmem správce. To však není tak úplně pravda. Pojďme se podívat na to, jak je to ve skutečnosti.

Monitoring a stanovisko ÚOOÚ

Na začátku je vhodné říct, že v zákoníku práce i GDPR bychom definici monitorování (respektive sledování) nacházeli jen velmi obtížně. Minimálně z předchozího článku však víme, že pokud chceme vystavit zaměstnance sledování (bez ohledu na to, jestli otevřenému, nebo skrytému), můžeme tak činit **pouze na základě závažného důvodu**, který spočívá ve zvláštní povaze zaměstnavatele. Mimo to však platí obecná pravidla dle GPDR – pokud chceme zpracovávat osobní údaje, musíme mít stanoven účel zpracování, maximálně nezbytný rozsah osobních údajů a vhodný právní titul. A pochopitelně se musí jednat o zpracování nezbytné.

> **Zaměstnanec by měl mít právo sledování polohy vypnout**

Zase tak jednoduché to ale není, a proto ÚOOÚ přispěchal s návodem a odpovědí, jak GDPR dopadá na GPS lokátory ve služebních vozech (stanovisko naleznete **zde**). Bohužel, problematika GPS v autech je o něco složitější, než jak ji maluje ÚOOÚ.

ÚOOÚ k GPS lokátorům v autech

Úřad věnoval na svých stránkách v oddíle Často kladené otázky zaměstnavatelům vlastní sekci. V obecné rovině doporučujeme tyto stránky sledovat, neboť se zde obyčejně dozvíte cenné rady – v tomto případě to však **nemusí být úplně pravda**.

ÚOOÚ na otázku, zda lze monitorovat služební vozidla pomocí GPS, **odpovídá, že ano** – v tomto se s ÚOOÚ shodnou asi úplně všichni. V čem se však již neshodneme, je **rozsah takového zpracování**.

ÚOOÚ sděluje, že *„monitorování služebních vozidel při pracovních cestách pomocí GPS v rozsahu a způso-*

bem potřebným pro ochranu a správu majetku je oprávněným zájmem zaměstnavatele, tedy zpracováním osobních údajů dle článku 6 odst. 1 písm. f) GDPR". S tímto se v zásadě shodujeme, s odůvodněním už nikoliv. To však nechme stranou, protože důležitější je další věta: „*Umožní-li zaměstnavatel využívat služební vozidlo zaměstnanci i k soukromým účelům, jde o určitý druh benefitu. Úprava vzájemných práv a povinností se bude řídit dohodou o použití vozidla. Zaměstnanec by měl být na použití GPS sledování upozorněn, a to v rozsahu informace podle čl. 13 GDPR. Využije-li zaměstnanec vozidlo i v rámci svých soukromých aktivit, je nadále oprávněným zájmem zaměstnavatele chránit svůj majetek prostřednictvím GPS. Pokud podmínku zaměstnavatele ohledně GPS zaměstnanec neakceptuje, nedojde k uzavření smlouvy o použití vozidla, a nebude tak oprávněn předmětný benefit čerpat.*"

Byť následně Úřad upozorňuje, že **intenzivní či stálá kontrola zaměstnanců** by byla v rozporu se zákoníkem práce (jmenovitě § 316 odst. 2 a 3 zákoníků práce), nelze se ubránit pocitu, že tento text ÚOOÚ někteří fakticky chápou jako bianco šek zaměstnavatelům na **nadbytečné sledování zaměstnanců**.

Co si o tom myslí ministerstvo?

Ministerstvo průmyslu a obchodu má na tuto oblast trochu jiný, respektive přesnější pohled. V rámci své Příručky pro přípravu malých a středních firem na GDPR (dostupné **zde**) totiž jako příklad špatné praxe uvádí to, když jsou GPS lokátory v provoze nepřetržitě a **monitorují každé použití služebního automobilu** kterýmkoliv zaměstnancem firmy (včetně služebních jízd). Nadto dokonce ministerstvo zkritizovalo **uchování záznamů z GPS lokátorů** v případě, kdy to po zaměstnavateli vyžadoval správce daně jako důkaz v rámci evidence jízd.

Údaje ze sledování vozu uchovávejte pouze do vyúčtování služební cesty

Jako správnou praxi ministerstvo naopak uvádí **sledování prostřednictvím nahodilé kontroly**, a to na základě klíče, který není zaměstnancům znám a podle kterého vše probíhá namátkově. Tyto údaje je však možno uchovávat **pouze po dobu, než dojde k vyúčtování služební cesty** a pracovník správy vozového parku vše ověří, a následně dojde k výmazu.

Tedy trochu odlišný a opatrnější přístup, než jak by bylo možno na první přečtení chápat ze stanoviska ÚOOÚ.

Co na to říká WP29?

V oblasti ochrany osobních údajů se nemusíme spoléhat pouze na stanoviska ÚOOÚ. V minulosti totiž vznikla takzvaná Pracovní skupina podle čl. 29 (anglicky Working Party, proto zkráceně WP29), která byla následně s příchodem GDPR nahrazena Evropským sborem pro ochranu osobních údajů (tedy European Data Protection Board, proto EDPB). Společné pro tyto orgány je to, že jsou/byly **složeny z jednotlivých kontrolních úřadů** napříč členy Evropské unie, tedy i český ÚOOÚ zde měl své zástupce.

WP29 vydalo **stanovisko** 2/2017 ke zpracování osobních údajů na pracovišti, které je s ohledem na aktualizaci platné i po účinnosti GDPR. V tomto stanovisku zástupci kontrolorů uvádí, že zaměstnavatel může mít oprávněný zájem na tom, aby **mohl kdykoliv zjistit polohu vozidel**. Nicméně jedním dechem dodává, že „*i kdyby zaměstnavatelé měli oprávněný zájem k dosažení těchto účelů, měli by nejprve posoudit, zda je zpracování pro tyto účely nezbytné a zda zavedení těchto opatření bude v souladu se zásadami proporcionality a subsidiarity*".

V případě využití GPS lokátorů a současného užití vozidla k soukromým účelům například WP29 uvádí, že zaměstnanec by měl mít naopak **možnost dočasně vypnout sledování polohy v případě zvláštních okolností**. Tou může být například návštěva lékaře.

Co se týče soukromých účelů a užití vozidla mimo pracovní dobu, zde **je situace ještě komplikovanější**.

WP29 přímo uvádí: *„Vzhledem k citlivosti údajů o poloze je málo pravděpodobné, že by existoval právní důvod k monitorování polohy služebních aut řízených zaměstnancem mimo pracovní hodiny.“*

To neznamená, že by WP29 užití GPS pro tyto účely vylučovala, nicméně uvádí, že je **nutno brát v úvahu proporcionalitu** a že finální řešení musí být přiměřené rizikům. Jako příklad pak WP29 uvádí, že pokud by **účelem byla prevence krádeže aut**, neměla by být poloha auta mimo pracovní dobu zaznamenávána, dokud vůz neopustí široce definovaný územní okruh (oblast, nebo dokonce zemi). *„Kromě toho by poloha měla být zobrazována jen způsobem, kdy zaměstnavatel aktivuje ‚viditelnost‘ polohy přistoupením k systémem již uloženým datům, když vozidlo opustí předem definovanou oblast.“*

Jak to tedy je?

Z výše uvedeného je tedy zřejmé, že používání GPS lokátorů ve služebních autech obecně **není zakázáno**, a to ani v případě, kdy je vůz používán pro soukromé účely. Situace je však o něco komplikovanější, než by se po nepozorném přečtení stanoviska ÚOOÚ mohlo zdát. V případě instalace takového systému je totiž nutno zajistit, že **práva zaměstnanců nepřijdou k úhoně**.

▪▪▪

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

Poradna

Naše organizace Svazek obcí XY zaměstnává osoby se zdravotním postižením. Některé naše administrativní pracovníky „umisťujeme“ na městský úřad, kde mají na starost spisovou službu. Při své práci tedy pracují s osobními údaji. Svazek figuruje jako zaměstnavatel, se kterým mají zaměstnanci uzavřené pracovní smlouvy, městský úřad pak figuruje jako zadavatel práce (ošetřeno smluvně mezi městem a svazkem). Domníváme se, že v případě úředníků územních samosprávných celků není nutné vytvářet formulář na mlčenlivost zaměstnanců či ustanovení o mlčenlivosti uvádět do pracovních smluv. Vycházíme zde ze zákona o úřednících, zákona o obcích a nařízení GDPR. Jak ale postupovat v našem případě, kdy zaměstnanci svazku vykonávají pracovní činnost na městském úřadu, kde přicházejí do styku s osobními údaji?

Bez detailních znalostí případu si dovolím k tomu přistoupit z jiné strany. Předpokládám, že smluvní ošetření mezi zadavatelem (městským úřadem) a svazkem také řeší otázku zpracování osobních údajů. Co se týče vykonávaných činností, lze předpokládat, že pro tyto účely bude svazek zpracovatelem osobních údajů a smlouva by tak měla obsahovat i zpracovatelskou smlouvu v souladu s čl. 28 GDPR. Tato smlouva by dle čl. 28 odst. 3 písm. b) GDPR měla svazek zavázat k tomu, aby zajistil, že osoby oprávněné zpracovávat osobní údaje se zaváží k mlčenlivosti nebo že se na ně bude vztahovat zákonná povinnost mlčenlivosti.

A zde nastává problém. Zatímco minulý zákon č. 101/2000 Sb., o ochraně osobních údajů, v rámci § 15 odst. 1 obsahoval zákonnou povinnost mlčenlivosti, a nebylo proto nutno tuto otázku dál řešit, zákon č. 110/2019 Sb., o zpracování osobních údajů, tuto otázku vlastně neřeší. Není však bez zajímavosti, že prakticky totožné ustanovení, které bylo v § 15 odst. 1 starého zákona, se ve skutečnosti objevuje v § 47 zákona nového, nicméně (nejspíše) chybou zákonodárce toto ustanovení na tento případ nedopadá. Ustanovení § 47 se totiž nachází v Hlavě IV zákona, která se vztahuje pouze na zpracování osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky.

Nabízí se tak otázka, zda vlastně tuto okolnost neřeší sám zákon č. 262/2006 Sb., zákoník práce, ale bez dalšího natahování můžeme říct, že prakticky nikoliv. Pravdou je, že ve vztahu k zaměstnancům územních samosprávných celků zařazených dle § 303 odst. 1 písm. e) zákoníku práce se povinnost zachovávat mlčenlivost částečně vztahuje (viz § 303 odst. 2 písm. b) zákoníku práce), nicméně pouze pokud takové důvěrné informace „v zájmu zaměstnavatele nelze sdělovat jiným osobám“. Chtě nechtě tak ve vašem případě zůstává poslední možnost – smluvní závazek dodržovat mlčenlivost.

▪▪▪

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

Pokuta 100 tisíc eur za pozdní ohlášení porušení zabezpečení

Španělská letecká společnost musí zaplatit pokutu 100 tisíc eur za to, že neohlásila porušení zabezpečení včas. Jaké jsou tedy lhůty pro ohlášení porušení zabezpečení osobních údajů?

Nesplnění ohlašovací povinnosti může správce vyjít draze. Nedávno se o tom přesvědčila španělská letecká společnost, která povinnost ohlásit porušení zabezpečení osobních údajů **splnila se značným zpožděním**. Za dané zpoždění ji byla dozorovým úřadem uložena **pokuta ve výši 100 tisíc eur**.

Ohlášení porušení zabezpečení

Podle ustanovení čl. 33 GDPR má správce povinnost ohlásit jakékoliv porušení zabezpečení osobních údajů bez zbytečného odkladu a **pokud možno do 72 hodin** od okamžiku, kdy se o něm dozvěděl, příslušnému dozorovému úřadu. Jako příklad podobného porušení zabezpečení osobních údajů uvádí Úřad pro ochranu osobních údajů na svých webových stránkách následující situace: „*… útok proti počítači, ve kterém jsou osobní údaje zpracovávány, jehož důsledkem je únik osobních údajů, jejich pozměnění nebo jiné zneužití. Může jít také například o ztrátu listinných dokumentů obsahujících osobní údaje, které byly součástí manuálně vedené evidence (kartotéky) fyzických osob nebo byly vytištěny z počítače, ve kterém je taková evidence vedena a obsah těchto dokumentů zakládá riziko pro dotčené osoby (například ztráta zdravotnické dokumentace).*“

Ohlašovací povinnost však správce nemá, pokud je nepravděpodobné, že by toto porušení mělo za následek **riziko pro práva a svobody fyzických osob**. Dle ÚOOÚ může například jít „*… o momentální nemožnost dohledat listinný dokument, který byl nebo měl být součástí manuálně vedené evidence (kartotéky) fyzických osob nebo byl vytištěn z počítače, ve kterém je taková evidence vedena, přičemž je nepravděpodobné, že se dostal do nepovolaných rukou, ale jde spíše o jeho momentální chybné založení*“.

Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním **uvedeny důvody tohoto zpoždění**. Za porušení ustanovení čl. 33 GDPR (výše popsané ohlašovací povinnosti) lze uložit správní **pokuty až do výše deseti milionů eur**, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší. Pokuty v uvedené výši, ač zní sebevíc hrozivě, budou ukládány jen **ve výjimečných případech**. Dá se očekávat, že ve většině případů budou řádově nižší. V jakých výškách to bude, se však dá jenom těžce odhadovat. Jako vodítko nám mohou posloužit případy z praxe. Nejnověji byla pokuta za porušení čl. 33 GDPR uložena španělské letecké společnosti.

Případ španělské letecké společnosti

Společnost Air Europa Lineas Aereas, třetí největší španělská letecká společnost, nesplnila povinnost uloženou výše uvedeným čl. 33 GDPR. Porušení zabezpečení osobních údajů ohlásila španělskému dozorovému úřadu (Agencia Española de Protección de Datos) **se zpožděním 41 dnů**. Společnost přitom neodůvodnila, proč ohlašovací povinnost splnila s takovým zpožděním. Za toto pochybení ji byla dozorovým úřadem uložena pokuta ve výši 100 tisíc eur.

V daném případě došlo k **neoprávněnému přístupu ke kontaktním údajům** a údajům týkajícím se bankovních účtů asi 489 tisíc subjektů údajů. Za nezajištění dostatečné úrovně zabezpečení uložil dozorový úřad letecké společnosti zároveň i **pokutu ve výši 500 tisíc eur**. Podle čl. 32 GDPR má totiž správce povinnost provést, s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, **vhodná technická a organizační opatření**, aby zajistil úroveň zabezpečení odpovídající danému riziku. Této povinnosti však společnost Air Europa Lineas Aereas nedostála. Celkově tak byla letecké společnosti uložena pokuta ve výši 600 tisíc eur. Rozhodnutí Agencia Española de Protección de Datos sp. zn. PS/00179/2020 je dostupné z webových stránek dozorového úřadu **zde** (pouze ve španělském jazyce).

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

Zdravotnictví pod lupou ÚOOÚ

Jak obstála zdravotnická zařízení při kontrolách Úřadu pro ochranu osobních údajů? Úřad zkoumal nejen zdravotnickou dokumentaci, e-recepty a informační systémy, ale řešil i kuriózní případ ztráty osobních dokladů.

Pokud jste pověřencem či správcem v oblasti zdravotnictví, měli byste při čtení následujících řádků zbystřit. V našem seriálu o kontrolách ÚOOÚ budeme tentokrát rozebírat poznatky z kontrolní činnosti ÚOOÚ ve zdravotnictví. Díky nim se můžete lépe **připravit na případnou kontrolu** a ověřit si, že vaše zpracování osobních údajů netrpí žádnou vadou. Oblast zdravotnictví je specifická tím, že se v ní zpracovávají **zvláštní kategorie osobních údajů**. Pojďme se tedy podívat na to, co kontroly odhalily.

Ztracené doklady

První z kontrol, o které nás ÚOOÚ informuje, byla věnována nemocnici, a to na základě ohlášení porušení zabezpečení osobních údajů. Ačkoliv z prvotního oznámení tato skutečnost nebyla dle slov ÚOOÚ úplně zřejmá, v rámci kontrolovaného případu šlo nakonec o **ztrátu osobních dokladů pacienta**. Svoje doklady neměl uložené v úschovně, ale ponechal si je v nočním stolku na pokoji, odkud je neúmyslně vyzvedla zdravotní sestra. Ta je následně omylem **předala jinému pacientovi**, jenž byl v té době propouštěn. Záměny dokladů si všiml až rodinný příslušník propuštěného pacienta, nahlásil to a doklady předal jinému zdravotnímu středisku, kde si je měl vyzvednout řidič a převézt je zpět původní nemocnici – kontrolované osobě. K tomu však nikdy nedošlo. **Dle slov ÚOOÚ se doklady ztratily** a nebylo objasněno, v kterém okamžiku se tak stalo.

Na daném případu jsou pozoruhodné dvě skutečnosti. Zaprvé, že ÚOOÚ danou kontrolu uzavřel, aniž posuzoval aplikaci čl. 33 GDPR (tedy **povinnost ohlášení porušení zabezpečení**), neboť dle jeho slov tato konkrétní ztráta osobních dokladů **nespadá pod věcnou působnost GDPR** tak, jak je stanovena v čl. 2 odst. 1 GDPR. Co k tomuto závěru ÚOOÚ vedlo, není zcela jisté. My si z toho nicméně můžeme dovodit to, že ne každou **ztrátu dokladu, který obsahuje osobní údaje**, ÚOOÚ považuje za zpracování osobních údajů.

Naši pozornost si dále zaslouží i to, že ÚOOÚ si na závěr neodpustil upozornit na jednu věc, týkající se ohlášení porušení zabezpečení. Dle slov Úřadu totiž nebylo úplně jednoduché **z ohlášení vyčíst, co se vlastně stalo**. ÚOOÚ tak apeluje na všechny správce, aby v případě ohlášení porušení zabezpečení **podali co nejucelenější popis události** tak, aby řešení daného incidentu mohlo být co nejrychlejší a nejefektivnější.

> **V ohlášení porušení zabezpečení přesně a jednoznačně popište událost**

Zabezpečení zdravotnické dokumentace

Druhá z kontrol byla zahájena na základě kontrolního plánu a směřovala na zabezpečení osobních **údajů zpracovávaných ve zdravotnické dokumentaci** u poskytovatele ambulantních zdravotních služeb.

Z popisu kontroly nejsou zcela zřejmé okolnosti zpracování, lze dovodit jedině to, že kontrola směřovala na zpracování osobních údajů **jak v listinné, tak i elektronické podobě**. Zaměřila se na okolnosti zpracování osobních údajů a plnění povinností, jako je přijetí technických a organizačních opatření, zvolení správného právního titulu a dodatečné podmínky ke zpracování dle čl. 9 GDPR.

Jelikož však kontrola **nezjistila žádné porušení** a proběhla na základě kontrolního plánu, nelze z výše uvedeného učinit žádný závěr.

Dodavatel ambulantního informačního systému

Jako dobrou zprávu pro uživatele informačního systému PC DOKTOR lze považovat závěr z kontroly tohoto dodavatele. Systém je dodáván poskytovatelům zdravotních služeb, přičemž ÚOOÚ se v rámci kontroly zaměřil na **plnění povinností dle GDPR** (zejména pak povinností uvedených v čl. 5, čl. 6, čl. 12 až 23, čl. 25 a čl. 28 až 32 GDPR), aniž odhalil porušení povinností tohoto zpracovatele.

E-recept

V souvislosti s e-recepty provedl ÚOOÚ jednu kontrolu. Ta byla zahájena na základě stížnosti, kterou ÚOOÚ postoupil **inspektorát České obchodní inspekce**. Stěžovatelce se totiž nelíbilo, že při vyzvednutí e-receptu v červenci 2020 byla v lékárně požádána o **předložení občanského průkazu**, z něhož si lékárnice opsala údaje, a následně stěžovatelku informovala, že daný lék nemají. Dle slov ÚOOÚ stěžovatelka považovala samotné opi-

sování údajů za poměrně **nestandardní postup**, jejž lékárnice neuměla hodnověrně vysvětlit.

ÚOOÚ k tomu uvedl: *„Kontrolou nebylo zjištěno, že by kontrolovaná osoba zpracovávala osobní údaje stěžovatelky ve své vlastní evidenci, tedy ani číslo jejího občanského průkazu.“* Na jiném místě nicméně uvedl, že kontrolovaná osoba **využívá lékárenský systém Lekis** a ten má být napojen na Centrální úložiště elektronických receptů, který provozuje Státní ústav pro kontrolu léčiv. Zároveň k tomu ÚOOÚ uvádí: *„Při výdeji léčivých přípravků vydávaných na základě vystaveného receptu shromažďuje a zpracovává informace o pacientech/klientech v rámci výkonu řádné lékárenské praxe, a to minimálně v rozsahu jméno, příjmení, číslo pojištěnce (rodné číslo), evidenční číslo receptu, název léčivého přípravku a jméno vydávajícího lékaře.“*

Je tedy otázkou, zda se lze ztotožnit s předpokládanou skutečností, že zadávání osobních údajů do systému Lekis, jehož prostřednictvím lékárna komunikuje s Centrálním úložištěm elektronických receptů, není ze strany ÚOOÚ považováno za **zpracování v rámci vlastní evidence**. Daná premisa by totiž měla poměrně zásadní **dopady v případě využívání některých cloudových služeb**. Jedná se však o domněnky, které jsou založeny na krátkém textu zveřejněném na stránkách ÚOOÚ.

Tak či tak z uvedeného vyplývá, že Úřad v rámci daného zpracování **nezjistil žádné porušení GDPR**, neboť číslo občanského průkazu je jedna z možností přístupu do Centrálního úložiště elektronických receptů. Svou kontrolu tedy ÚOOÚ uzavřel tak, že v daném případě se neprokázalo porušení GDPR a že *„lékárna, v souvislosti s online připojením do Centrálního úložiště elektronických receptů, se jako zpracovatel osobních údajů řídí předpisy a metodikami pro provoz úložiště. Státní ústav pro kontrolu léčiv podle zákona o léčivech jako správce osobních údajů zodpovídá za jejich bezpečnost při shromažďování, zpracování a ukládání.“*

> **V roce 2021 můžeme očekávat další kontroly ve zdravotnictví**

ePortál

Posledním kontrolovaným subjektem v rámci této oblasti byla Pražská správa sociálního zabezpečení (PSSZ), a to na základě kontrolního plánu. ÚOOÚ se zaměřil na kontrolu dodržování povinností stanovených GDPR v souvislosti se zpracováním osobních údajů klientů PSSZ, včetně jejich zpracování při **poskytování online služeb prostřednictvím ePortálu**, který však provozuje Česká správa sociálního zabezpečení (ČSSZ). PSSZ je pouze územní organizační jednotky ČSSZ, nicméně ÚOOÚ ji dle závěrů z kontroly **považuje za samostatného správce**.

ÚOOÚ se pak v rámci kontroly zaměřil na plnění povinností dle čl. 6, 13 a 14, ale také 25 až 32 GDPR a neodhalil jakékoliv pochybení.

Závěr

Zdravotnictví aktuálně patří k **jedné z nejdiskutovanějších oblastí** s ohledem na ochranu osobních údajů jednak kvůli současné pandemii, jednak z důvodu digitalizace některých služeb, jako je **registrace do očkovacích systémů**, databáze očkovaných osob, ale i zavádění nových opatření jako například **povinného testování**. Proto si můžeme být jistí, že se tato oblast objeví i v závěrech z **kontrolní činnosti za rok 2021** – nyní však můžeme být připraveni lépe.

V příštím díle tohoto miniseriálu se zaměříme na zpracování osobních údajů v oblasti, kterou ÚOOÚ označil jako „ostatní“, a podíváme se na **zpracování osobních údajů z veřejných rejstříků** či využívání kamerového systému v rámci veřejného prostranství v pražských Řeporyjích.

▪▪▪

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

Klikněte a stáhněte si vzor

Záznam o činnostech zpracování správce podle článku 30 odst. 1 GDPR

Název předmětného zpracování:	
Údaje o správci	
Název/Jméno a příjmení:	
Právní forma:	
IČO:	
Adresa:	
Telefon:	
E-mailová adresa:	
Webové stránky:	
Údaje o společném správci (* pokud je relevantní)	
Název/Jméno a příjmení:	
Právní forma:	
IČO:	
Adresa:	
Telefon:	
E-mailová adresa:	
Webové stránky:	
Údaje o zástupci správce (* pokud je ustanoven)	
Název/Jméno a příjmení:	
Právní forma:	
IČO:	
Adresa:	
Telefon:	
E-mailová adresa:	
Webové stránky:	
Údaje o pověřenci pro ochranu osobních údajů (* pokud je ustanoven podle čl. 37 GDPR)	
Název/Jméno a příjmení:	
Právní forma:	
IČO:	
Adresa:	
Telefon:	
E-mailová adresa:	
Pokud je pověřencem pro ochranu osobních údajů právnická osoba, pak doplňte údaje také o fyzické osobě, která činnost pověřence pro ochranu osobních údajů vykonává:	

Klikněte a stáhněte si vzor

Jméno, příjmení:			
Telefon:			
E-mailová adresa:			
Popis činnosti zpracování			
Zahájení zpracování:		Datum poslední změny:	
Odpovědné oddělení:			
Kontaktní osoba:			
Telefon:			
E-mailová adresa:			
Popis činnosti zpracování:			
Účel(y) zpracování:			
Právní základ zpracování:			
Kategorie subjektů údajů dotčených předmětným zpracováním:	☐ Uchazeči o zaměstnání ☐ Zaměstnanci ☐ Bývalí zaměstnanci ☐ Zájemci o poskytnutí služeb/produktů ☐ Zákazníci ☐ Uživatelé webových stránek ☐ Odběratelé ☐ Dodavatelé ☐ Pacienti ☐ Široká veřejnost (například v případě instalace kamer na veřejných prostranstvích) ☐ Jiný:		
Kategorie zpracovávaných osobních údajů:			
Zpracovávání zvláštní kategorie osobních údajů (čl. 9 GDPR):	☐ ANO ☐ NE		
Kategorie zpracovávaných osobních údajů spadajících pod zvláštní kategorie osobních údajů (čl. 9 GDPR):			
Právní základ zpracování zvláštní kategorie osobních údajů (čl. 9 odst. 2 GDPR):			
Způsob získávání (zdroj) zpracovávaných osobní údajů:			
Způsob aktualizace zpracovávaných osobní údajů:			
Které listinné a elektronické evidence (spisovny, archivy, IT systémy, datová uložiště a podobně) jsou v rámci předmětného zpracování využívány?			
Způsob zajištění práv subjektů údajů dle čl. 13–14 GDPR:			
Způsob zajištění práv subjektů údajů dle čl. 15–23 GDPR:			
Kategorie příjemců, kterým budou nebo byly osobní údaje sděleny nebo jinak zpřístupněny:	V rámci organizace Oddělení/Funkce:		

Klikněte a stáhněte si vzor

	Příjemci mimo organizaci včetně příjemců ve třetích zemích a mezinárodních organizacích
	Název/Jméno a příjmení:
	Právní forma:
	IČO:
	Adresa:
	Telefon:
	E-mailová adresa:
	Postavení příjemce: ☐ zpracovatel ☐ samostatný správce
	Dohoda o zpracování osobních údajů: ☐ ANO ☐ NE ☐ N/A
Předávání osobních údajů do třetích zemí a mezinárodním organizacím:	☐ Osobní údaje nejsou předávány do třetích zemí ani mezinárodním organizacím a jejich předávání se do budoucna neplánuje.
	☐ Osobní údaje jsou předávány následovně: Třetí země: Mezinárodní organizace: Dokumentace vhodných záruk (pokud se jedná o předání podle čl. 49 odst. 1 pododstavce 2 GDPR):
Lhůty pro výmaz jednotlivých kategorií osobních údajů:	
Technická a organizační opatření podle čl. 32 odst. 1 GDPR:	

Správce ..... Datum ..... Podpis .....

V příštím čísle Zpravodaje se dozvíte:

- **Jak naložit s osobními údaji po propuštění zaměstnance?**
- **Koho bude Úřad kontrolovat v roce 2021?**

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: 8. 4. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.