HAVEN
ADVOKÁTNÍ KANCELÁŘ

PŘEHLED K PROBLEMATICE OSOBNÍCH ÚDAJŮ 2021

V následujícím článku si Vás dovolujeme seznámit s nedávnými rozhodnutími Úřadu pro ochranu osobních údajů (ÚOOÚ). O závěrech některých kontrol provedených ÚOOÚ a dalších aktualitách ze světa ochrany osobních údajů Vás budeme nadále informovat v dalším vydání tohoto přehledu nebo přehledu právních aktualit.

+ Vysoká pokuta za spam

Úřad pro ochranu osobních údajů (ÚOOÚ) upozornil na svém webu na případ 11 společností, které zpracovávaly tisíce adres datových schránek fyzických osob a související osobní údaje. Tyto společnosti, aniž by mezi nimi a příjemci obchodních sdělení existoval jakýkoli zákaznický nebo obdobný vztah, který by z pohledu obecného nařízení na ochranu osobních údajů (GDPR) zakládal titul pro zasílání obchodních sdělení, zasílaly přímo do datových schránek nevyžádaná obchodní sdělení. ÚOOÚ shledal, že společnosti nesdělily adresátům, že jejich osobní údaje budou použity pro zasílání obchodních sdělení. Se společnostmi zahájil správní řízení, přičemž za přestupek uložil pokutu v souhrnné výši 3 111 000 Kč.

+ SDEU se vyslovil pro individuální posuzování lhůt pro uchovávání dat

Soudní dvůr Evropské unie (SDEU) vydal dne 6. 10. 2020 dva rozsudky týkající se ochrany osobních údajů. Jde o věc *Privacy International* (C-623/17) a spojené věci *La Quadrature du Net a další proti Francii a Belgii* (C-511/18, C-512/18, C-520/18). Oba rozsudky potvrzují dosavadní trend v judikatuře SDEU a nadto rozšiřují působnost práva EU i na zadržení údajů zpravodajskými službami.

Rozsudky SDEU uložily zákaz preventivního plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů, ledaže by toto shromažďování osobních údajů bylo v zájmu národní bezpečnosti a boje proti závažné trestné činnosti. I v těchto případech však podle ÚOOÚ bude nezbytné stanovit individuálně přiměřené lhůty pro uchovávání dat (pro jednotlivé účely a pro jednotlivé komunikační kanály tak, aby budoucí vytěžování zadržených osobních údajů bylo pro dotčené subjekty údajů předvídatelné a mohlo obstát).

+ ÚOOÚ k povinnému testování zaměstnanců

Úřad pro ochranu osobních údajů zveřejnil na svých webových stránkách stanovisko k povinnému testování zaměstnanců na přítomnost nemoci COVID-19. ÚOOÚ potvrzuje, že pokud dochází ke shromažďování osobních údajů přímo ze strany zaměstnavatele, dostává se ten tím ve smyslu GDPR do role správce osobních údajů. Z důvodu veřejného zájmu v oblasti veřejného zdraví je při testování zaměstnanců zpracovávána navíc také zvláštní kategorie osobních údajů o zdravotním stavu. Proto zaměstnavatelé musejí zajistit, aby osobní údaje byly zpracovávány s co nejvyšší ochranou soukromí, tedy aby nebyly zpřístupněny neomezenému počtu osob. Samotná evidence provedených testů zaměstnanců musí být náležitě zabezpečena a přístup k ní by měly mít pouze osoby pověřené plněním úkolů k dodržování mimořádného opatření. Každý ze zaměstnavatelů musí přihlédnout ke svým organizačním a technickým možnostem, aby evidenci provedených testů řádně zabezpečil před možnou ztrátou nebo zpřístupněním neoprávněným osobám. Záznamy o zpracování osobních údajů zaměstnanců za účelem testování jsou součástí záznamů o činnostech zpracování podle čl. 30 GDPR. Doba uchování

++ HAVEN ++

evidence provedených testů zaměstnanců nebyla stanovena. Lze dovodit, že zaměstnavatelé mají povinnost vést evidenci provedených testů zaměstnanců nejméně do zrušení mimořádného opatření k provádění povinného testování zaměstnanců.

+ ÚOOÚ k tzv. očkovacím pasům

Úřad pro ochranu osobních údajů zveřejnil své stanovisko k možnému národnímu využití digitálního zeleného certifikátu, tzv. očkovacího pasu (CovidPass), který sám o sobě představuje zásadní zásah do ochrany soukromí. Úřad tímto upozorňuje na možná rizika, která vyplývají ze zavedení tzv. očkovacích pasů. Podstatou digitálního zeleného certifikátu je doložení, že jeho držitel byl na COVID-19 očkován, testován, nebo se z nej uzdravil. Jeho účelem je usnadnění volného pohybu během pandemie COVID-19, nikoliv jím volný pohyb podmínit. Dle Úřadu pro ochranu osobních údajů je v každém případě třeba respektovat základní zásady ochrany osobních údajů, a to i v případě zpracování osobních údajů v souvislosti s opatřeními v rámci boje s COVID-19. Osobní údaje, jejich zpracování a k tomu využívané technologie by měly být používány spíše k posílení pozice jednotlivců než k jejich kontrole, stigmatizaci nebo utlačování. Ohledně otázky dalšího možného využití digitálního zeleného certifikátu v ČR se Úřad pro ochranu osobních údajů tak, že v širokém měřítku nelze zavádět jakákoliv opatření či výhody, pokud nebude zároveň široce dostupná možnost získat požadované potvrzení či srovnatelnou alternativu, a to pro celou společnost, v opačném případě by se mohlo jednat o zásadní odepření ochrany práv a neúměrné omezování práv některých osob.

Společné stanovisko k očkovacím pasům vydal také Evropský sbor pro ochranu osobních údajů a Evropský inspektor ochrany údajů. Zejména upozorňují na to, že používání digitálního zeleného certifikátu nesmí v žádném případě vést k přímé nebo nepřímé diskriminaci fyzických osob a musí být plně v souladu se zásadami nezbytnosti, účelnosti a přiměřenosti. Využívání tzv. očkovacích pasů nesmí vést k vytvoření jakéhokoliv druhu centrální databáze osobních údajů na úrovni EU.

+ ÚOOÚ k prokazování totožnosti a zpracování osobních údajů

Úřad pro ochranu osobních údajů zveřejnil souhrnný materiál k prokazování totožnosti a zpracování osobních údajů. Odpovídá například na některé z níže uvedených otázek:

Komu, kdy a jakým způsobem musím prokazovat svou totožnost?

K prokazování totožnosti i dalších osobních údajů občana ČR je určen občanský průkaz. Skutečnosti zapsané v občanském průkazu není občan povinen prokazovat jiným způsobem, pokud tak nestanoví zákon o občanských průkazech. Jako průkaz lze využít i cestovní doklad, popřípadě jiné doklady. Samotné zjištění totožnosti fyzické osoby není zpracováním osobních údajů podle obecného nařízení o ochraně osobních údajů. Zpracováním osobních údajů je až jejich uložení na nosič informací, prováděné za účelem jejich zpracování v evidenci, které musí dodržovat zásadu minimalizace údajů, tedy ukládat pouze ty údaje, které jsou pro určitý účel nezbytně potřebné. Prokázat svou totožnost je zákonná povinnost občana vůči orgánům veřejné moci i vůči fyzickým a právnickým osobám (např. pro poskytnutí nějaké služby – banky, pojišťovny, auditoři, účetní, daňoví poradci, zdravotnický pracovník, městská hromadná doprava a další). Kromě zákonem stanovených případů je prokazování totožnosti potřebné i v soukromoprávních vztazích, zejména při uzavření a plnění smluv.

Jaké moje osobní údaje přitom mohou být zaznamenány?

Na občanském průkazu je několik typů údajů. Jednak jsou to údaje bezprostředně čitelné člověkem, dále to jsou údaje uvedené ve strojově čitelné podobě jako 2D kód (dvoudimenzionální čarový kód) a údaje uvozené kódem IDCZE, kde je kód dokladu, číslo dokladu, datum narození, pohlaví, datum

platnosti, státní občanství; a dále to jsou data elektronicky uložená v občanském průkazu (tzn. s využitím nosiče dat – bezkontaktního elektronického čipu). Platí zákaz zpracovávat údaje uvedené v občanském průkazu a data pro elektronické využití občanského průkazu bez souhlasu držitele.

Kdo je oprávněn pořídit kopii mého průkazu totožnosti?

Vzhledem ke zneužitelnosti občanského průkazu a cestovního dokladu ke krádeži identity fyzické osoby stanovují příslušné zákony zákaz pořizovat jakýmikoliv prostředky kopie těchto průkazů bez prokazatelného souhlasu občana, kterému byl průkaz vydán, pokud není stanoveno jinak. Nicméně v praxi je často souhlasem s pořízením kopie dokladu totožnosti podmiňováno poskytnutí nějaké služby, kdy pak tento souhlas nenaplňuje podmínku svobodného projevu vůle. Je proto podstatné, aby byl držitel dokladu výslovně informován o možnosti nesouhlasit s pořízením kopie a důsledcích takového odmítnutí. Neoprávněné pořízení kopie občanského průkazu nebo cestovního dokladu je přestupkem.

Závěrem

Každý, kdo je požádán o to, aby umožnil pořídit kopii svého průkazu totožnosti, by se tak měl v prvé řadě dotázat, zda jde o požadavek na základě zákona, či zda má jít o pořízení kopie na základě dobrovolného souhlasu, jaké jsou pro to důvody a jaké jsou důsledky odmítnutí. Může se dotázat, zda je pořízení kopie pro ověření jeho totožnosti nezbytné, např. pokud není možné předložení originálu dokladu v osobním styku k nahlédnutí. Měl by si být také vědom, že k projednání stížnosti na neoprávněné pořízení kopie občanského průkazu nebo cestovního dokladu je příslušný obecní úřad obce s rozšířenou působností. Případné porušení zásady minimalizace ukládáním kompletních kopií dokumentů do evidence fyzických osob je již porušením GDPR, k jehož posouzení je příslušný Úřad pro ochranu osobních údajů.

+ Reakce ÚOOÚ k evidenci zákazníků v provozovnách a k prokazování výsledků testů na SARS-CoV-2 ze strany zákazníků

V odůvodnění mimořádného opatření Ministerstva zdravotnictví ČR týkající se evidence a prokazování výsledků testů zákazníků v provozovnách (č. j. MZDR 14601/2021-7/MIN/KAN ze dne 29. dubna 2021) byl zmíněn rozsah zpracovávaných osobních údajů a doba jejich uchování. Podle opatření je evidence údajů poskytovatele služby na dobu nezbytnou k provedení epidemiologického šetření orgánem ochrany veřejného zdraví, a v nezbytném rozsahu. Taková evidence by měla zároveň obsahovat identifikaci zákazníka (zejm. jméno, příjmení), kontaktní údaje zákazníka (nejlépe telefonní číslo), informaci o čase poskytnutí služby (od kdy, do kdy) a informaci, který zaměstnanec poskytoval služby tomuto zákazníkovi. Tuto evidenci by měl poskytovatel uchovávat 30 dnů.

Poskytovatelům služeb se doporučuje, aby nepřekračovali předepsaný rozsah údajů a dobu jejich uchování. Zvláště je nutno zdůraznit, že součástí evidence nemá být originál či kopie listiny, kterou se osvědčují skutečnosti, jimiž je vstup do provozovny podmíněn (potvrzení, prohlášení, certifikáty). Poskytovatelé služeb mají informační povinnost vůči zákazníkům, že údaje obsažené v seznamu zákazníků (identifikační a kontaktní údaje) mohou být předány orgánům ochrany veřejného zdraví za účelem trasování nákazy COVID-19.

+ Pokuty za porušení povinností z GDPR

Společnost, která provozuje pro své zákazníky call centrum, identifikovala volajícího podle toho, z jakého čísla volal. Pokud se jednalo o telefonní číslo udělené společností, zobrazily se pracovníkovi call centra i údaje volajícího. Problematická byla zejména identifikace členů rodiny, neboť sdělil-li volající, že volá jako člen rodiny (aniž by byl uveden jako zákazník v zákaznické smlouvě) a uvedl-li základní identifikační údaje uvedené v zákaznické

++ HAVEN ++ HAVEN ++ HAVEN ++

smlouvě, společnost měla za to, že volající člen rodiny je oprávněn jednat i za člena uvedeného v zákaznické smlouvě. Tak se stalo, že ochotný pracovník call centra sdělil volající ženě telefonní číslo bývalého partnera, který si však toto číslo změnil právě proto, aby nemohl být svou bývalou partnerkou nadále kontaktován, neboť z její strany docházelo k jednání charakterizovanému jako stalking. Dozorový orgán uložil společnosti správní pokutu ve výši 9 550 000 EUR za nezajištění přiměřené úrovně ochrany osobních údajů. Soud výši správní pokuty výrazně snížil na 900 000 EUR. Argumentoval zejména tím, že nebyly dotčeny ani ohroženy žádné citlivé osobní údaje a že riziko neoprávněného zpřístupnění osobních údajů bylo a je malé. Snížená bezpečnostní úroveň při identifikaci volajících existovala z důvodu zajištění co nejvyššího komfortu zákazníků společnosti pro případy kontaktování společnosti.

+ Kontrola využití biometriky u klientů

Kontrolovaná obchodní společnost využívala v rámci smluvní dokumentace dynamický biometrický podpis (tj. nahrazení tradičního podepisování se na papír za podepisování se na speciální zařízení pro snímání podpisu). Pro účely uzavření a uchování smluvní dokumentace však není nezbytné využívat dynamický biometrický podpis, neboť není vyžadován ani v případě podpisu dokumentů v listinné podobě. Jako dostatečný je pro stanovené účely prostý obraz podpisu klienta na dematerializované smluvní dokumentaci, který je srovnatelný s podpisem smluvní dokumentace v listinné podobě. Kontrolovaná společnost tímto nedodržela zásadu minimalizace údajů stanovenou v nařízení, když shromažďovala a následně uchovávala dynamické biometrické podpisy svých klientů.

+ Zpracování osobních údajů při přímém marketingu

Kontrola byla provedena na základě několika stížností stěžovatelů, kteří měli být kontaktováni obchodní společností, aniž by jí poskytli své osobní údaje. Podle stěžovatelů měla kontrolovaná osoba k dispozici minimálně jejich jméno, telefonní číslo, rodné číslo, číslo účtu a informace o provizích. Bylo zjištěno, že kontrolovaná osoba použila osobní údaje, které jí byly známy z její předchozí obchodní činnosti za účelem přímého marketingu (telefonické hovory). Kontrolovaná osoba nedisponovala žádným legitimním titulem (tj. zákonným důvodem) pro další zpracování těchto osobních údajů, takové zpracování není ani nezbytné pro účely oprávněných zájmů kontrolované osoby. Jedná se o neoprávněné (protizákonné) zpracování osobních údajů.

+ Kontrola používání cookies

Během kontroly povinností provozovatele televizního vysílání jako správce osobních údajů uživatelů v souvislosti s využíváním cookies v rámci provozování webových stránek s multimediálním obsahem bylo zjištěno, že i když kontrolovaná osoba vůči subjektu údajů plnila informační povinnost tím, že zpracovala dokument Zásady ochrany osobních a dalších zpracovávaných údajů, který byl uložen na webové stránce, uživatel/návštěvník na to však nebyl upozorněn a informace nebyly poskytnuty snadno přístupným způsobem, neboť bylo nezbytné je hledat. Kromě toho, informace nebyly úplné, některé údaje nebyly aktuální (zejména odkazy na právní předpisy). Kontrolovaná osoba se tímto dopustila přestupku, za což jí byla uložena pokuta.

+ Kontrola zpracování osobních údajů v aplikaci Mobilní rozhlas

V rámci zprovoznění městské aplikace Mobilní rozhlas bylo ohlášeno, že došlo k vědomému zneužití osobních údajů starostou města. Údajně měl neoprávněně získanou databázi kontaktů zaměstnanců a zákonných zástupců žáků místní základní školy použít pro registraci jednotlivců do aplikace Mobilní rozhlas, bez jejich udělení souhlasu se zpracováním

osobních údajů. Před samotným udělením souhlasu se zpracováním osobních údajů musí kontrolovaná osoba subjekt údajů informovat o možnosti souhlas odvolat. Starosta dále nedisponoval řádným právním titulem (tj. zákonným důvodem) ke zpracování výše uvedených osobních údajů, čímž jednal v rozporu s obecným nařízením o ochraně osobních údajů. Úřad pro ochranu osobních údajů dále doplňuje, že při výběru a jmenování pověřence pro ochranu osobních údajů je nutno pamatovat na to, aby byl jmenován na základě svých profesních kvalit, odborných znalostí práva a praxe v oblasti ochrany osobních údajů.

+ Kontrola zveřejňování fotografií zaměstnanců na internetových stránkách zaměstnavatele – balanční test

Kontrolovaná osoba původně zveřejňovala fotografie zaměstnanců na základě údajně uděleného souhlasu. Stěžovatelka se proti tomu vyhradila a požadovala výmaz fotografie z internetových stránek. Na základě této skutečnosti kontrolovaná osoba přehodnotila právní základ pro dané zpracování a stěžovatelku informovala, že fotografie je zveřejněna na základě oprávněného zájmu kontrolované osoby. Stěžovatelce následně předložila na vyžádání provedený balanční test (ten provádí správce ještě před zahájením zpracování osobních údajů, aby vyhodnotil, zda jeho oprávněný zájmem převažuje nad zájmy (tj. práva a svobody) subjektů osobních údajů, správce musí zároveň posoudit přiměřenost jeho oprávněného zájmu vzhledem k právům subjektů údajů).

Balanční test svým obsahem neprokázal oprávněné zájmy pro zpracování, které by převážily nad zájmy nebo základními právy a svobodami subjektů údajů. Kontrolovaná osoba tak neprokázala, že by jí pro zveřejňování fotografií zaměstnanců svědčil uvedený právní základ a předmětné zpracování bylo nezákonné. Ačkoli obecné nařízení nestanoví závaznou podobu balančního testu, musí tento test 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 obecného nařízení. Správce je povinen provést balanční test pro každé zpracování osobních údajů, které hodlá vykonávat na základě právního důvodu oprávněného zájmu.

+ Kamery na veřejném prostranství

Záznam kamery zabírající prostor železničního přejezdu v městské části Praha-Řeporyje je zveřejňován v reálném čase na webových stránkách www.mall.tv a části záznamů jsou také zveřejněny v rámci pořadu Extrémní starosta, nebo přejímány jinými zpravodajskými médii. Před zahájením kontrolního šetření kontrolující zjistili, že na webových stránkách www.mall.tv je mimo záznamu z železničního přejezdu v Řeporyjích také záznam z kamery, která snímá prostranství kolem památníku vlasovců na Řeporyjském náměstí v městské části Praha-Řeporyje. Kontrolou bylo zjištěno porušení povinností správce tím, že kontrolovaný zpracovával osobní údaje z výše uvedených kamer bez právního titulu (právního důvodu zpracování). Vzhledem k tomu, že kontrolovaný odstranil v průběhu kontroly obě kamery, a ze svých webových stránek odstranil záznamy z těchto kamer, Úřad kontrolovanému neuložil nápravná opatření.

+ Operátor dostal za opakované porušování GDPR pokutu až 8 milionů euro

Společnost Vodafone España opakovaně kontaktovala subjekty údajů s marketingovými nabídkami bez předchozího souhlasu. Údajně obtěžovala nevyžádanými obchodními sděleními i ty subjekty, kteří se předem vyjádřili, že o zasílání sdělení nemají zájem. Španělský dozorový úřad (AEPD) udělil společnosti Vodafone España pokutu ve výši 8 150 000 euro. Vysoká míra využití zpracovatelů (externích společností) také zapříčinila, že docházelo k velkému mezinárodnímu přenosu dat, který společnost

neměla plně pod kontrolou a nebyla tak schopna zajistit dostatečná technická a bezpečnostní opatření. Společnost sama jako správce ani velký počet zpracovatelů nevedli společnou evidenci kontaktovaných osob, což následně vedlo k opakovanému kontaktování osob, které tato marketingová sdělení již dříve odmítly. Takové kontaktování osob pak samozřejmě nebylo v souladu s Nařízením GDPR.

+ Od srpna budou součástí občanských průkazů i otisky prstů

Tuto povinnost zavedlo Nařízení Evropského parlamentu a Rady 2019/1157 již v roce 2019 s účinností od 2. srpna letošního roku. Cílem Nařízení je omezit padělání a zneužívání občanských průkazů napříč Evropskou unií. Česká republika na tuto novinku zareagovala minulý rok přijetím novely zákona o občanských průkazech. Dle informací Ministerstva vnitra ČR se od 2. srpna 2021 začne vydávat nový typ občanského průkazu, který bude obsahovat vysoce zabezpečený bezkontaktní čip, na kterém budou uloženy biometrické údaje. Návrh schválila Sněmovna 2. června 2021 ve třetím čtení, tento nový typ občanského průkazu umožní například i cestování bez nutnosti mít u sebe pas. Biometrické údaje se povedou v informačním systému evidence občanských průkazů nejdéle po dobu 90 dnů od vyrobení dokladu, a to pro účely vyřízení jeho případné reklamace. Poté dojde k jejich smazání, protože vytvářet jakékoliv databáze, které by biometrické údaje shromažďovaly, není povoleno. Dosud platné občanské průkazy budou platit do skončení jejich platnosti, nejdéle do 3. srpna 2031. Občanské průkazy, které neobsahují strojově čitelnou zónu, musí být vyměněny do pěti let, jinak s nimi nebude možné cestovat.

+ Nařízení ePrivacy – Rada EU schválila svou variantu

ePrivacy neboli *návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)* bude doplněním Obecného nařízení o ochraně osobních údajů (GDPR) a bude se dotýkat úpravy zpracování osobních údajů. Podstatou ePrivacy je, aby měli občané možnost vědomě odsouhlasit, že o nich smějí poskytovatelé elektronických komunikací shromažďovat data, cílem je tedy zajištění větší ochrany soukromí na internetu. Oproti stávající úpravě ve směrnici o soukromí a elektronických komunikacích 2002/58/ES, která se vztahuje pouze na tradiční telekomunikační operátory, budou nová pravidla závazná i pro poskytovatele služeb jako je WhatsApp, Facebook Messenger, Skype, Gmail, iMessage nebo Viber.

Nové nařízení se dotkne například ochrany před nevyžádanou poštou nebo telemarketingu, zjednodušit a sjednotit by mělo také pravidla spojená se zpracováním souborů cookies. Pro cookies třetích stran by měl být nově vyžadován souhlas uživatelů, zatímco pro cookies poskytovatele by neměl být souhlas vyžadován. Nabýt účinnosti mělo nařízení původně zároveň s GDPR, tedy od května 2018, nicméně konečné datum se stále odkládalo. Úřad pro ochranu osobních údajů však v dubnu tohoto roku informoval, že v následujících týdnech lze očekávat zahájení trialogu Rady EU, Evropského parlamentu a Evropské komise o návrhu nařízení o soukromí a elektronických komunikacích.

+ Nová populární síť Clubhouse by mohla představovat riziko pro osobní údaje

Clubhouse je americká sociální síť založená na vzájemné diskusi uživatelů ve skupinkách, bez možnosti sdílet své fotografie, videa či psané statusy. Uživatelem se můžeme stát pouze tehdy, pokud nás jiný uživatel do této sociální sítě pozve, a to je vzhledem k ochraně osobních údajů problematické zejména z toho důvodu, že uživatel musí v rámci rozeslání pozvánky nejprve sdílet s aplikací veškeré své kontakty. Jde o značně nepřiměřené zpracování dat, síť Clubhouse by neměla mít možnost zpracovávat kontakty lidí, kteří nejsou jejím členem.

Dochází k porušení zásady přiměřenosti zpracování osobních údajů a nelegitimnímu sbírání kontaktních údajů osob, které k tomu nedali souhlas. Mezi další riziko patří i možný únik dat nebo útok na servery Clubhouse, který může představovat velký zásah do práv jednotlivých uživatelů. I při dojmu sebevětšího soukromí je důležité nezapomínat na ochranu svých osobních dat, zejména tak činit v případě, sdílíme-li o sobě či svých blízkých osobní informace na kterékoli sociální síti či kdekoliv veřejně.

+ ÚOOÚ rozdal pokuty za zneužití datových stránek

Usnesení Vlády ČR ze dne 31. 10. 2020 č. 1110, které umožňovalo po dobu nouzového stavu dočasně využívat službu datové schránky zdarma, zneužilo několik subjektů tím, že bez jakéhokoliv právního titulu rozesílaly obchodní sdělení prostřednictvím datové schránky. Subjekty se tímto dopustily nezákonného zpracování osobních údajů. Úřad pro ochranu osobních údajů mimo jiné konstatoval i porušení správce osobních údajů, a to z toho důvodu, že pokud správce osobních údajů neobdrží osobní údaje přímo od subjektů údajů, má povinnost tyto osoby informovat o všech náležitých informacích týkajících se zpracování jeho osobních údajů (totožnost a kontaktní údaje správce a pověřence pro osobní údaje, účel zpracování, oprávněný zájem správce, případné další příjemce osobních údajů, doba, po kterou budou osobní údaje uloženy).

+ Ministerstvo zdravotnictví navrhuje rozsáhlé zpracování dat o poloze

Bývalý ministr zdravotnictví Jan Blatný navrhl v době legislativní nouze novelu zákona o ochraně veřejného zdraví, která by mohla představovat významný zásah do soukromí každého z nás. Hlavním cílem zmíněné novely je vytvoření centrální Státní hygienické služby, která má nahradit dosavadní decentralizovanou soustavu hygienických stanic. Ta by mohla být mimo jiné oprávněna zavírat školy, omezovat pohyb a možnost setkávání osob, zavírat provozovny a nařizovat krajům a obcím karanténní opatření. Nejzásadnější pravomocí Státní hygienické služby z pohledu ochrany osobních údajů je možnost vyžádat si od telefonních operátorů údaje o poloze pozitivně nakažených, a to až tři týdny nazpět. Doposud je možné podobné údaje o nakažených zpracovávat pouze na základě jimi uděleného souhlasu nebo soudního příkazu, nicméně nevolený úředník v čele Státní hygienické služby by tak mohl činit bez jakéhokoliv povolení či souhlasu. S narůstající kritikou ze strany veřejnosti i opozice se z původního znění novely začíná ustupovat. Nová varianta novely by měla být o poznání mírnější, části týkající se sledování nakažených budou vyňaty zcela. S účinností příslušných změn v zákoně se nyní počítá od ledna 2022.

NEJSTE
NA TO
SAMI

++ HAVEN ++ HAVEN ++ HAVEN ++