ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

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

Porušuje aplikace Clubhouse GDPR?

Aplikace Clubhouse nabírá poslední dobou v českém prostředí na popularitě. K čemu slouží a jak zachází s osobními údaji uživatelů? Některé její funkce jsou z pohledu GDPR problematické – zpracování osobních údajů neuživatelů či nahrávání hovorů. Porušuje Clubhouse nařízení GDPR?

Pokud sledujete sociální sítě a pohybujete se na internetu, určitě vám neuniklo, že se v rámci České republiky stále častěji hovoří o sociální síti Clubhouse. Popsat tuto aplikaci tomu, kdo ji nikdy neviděl a nepoužíval, není jednoduché. Pokud však znáte například Discord, nebude vám fungování tohoto nového fenoménu až tak cizí. Oproti Discordu **nemůžete v rámci aplikace Clubhouse psát či posílat soubory jiným uživatelům – můžete s nimi jen mluvit**. Aplikaci si představte jako virtuální hospodu, kde se posadíte k libovolnému stolu (pokud není privátní), poslouchate rozhovor a popřípadě se i do hovoru zapojíte. Ostatně v médiích je této aplikaci věnován čím dál větší prostor, proto není těžké si o ní a o jejím fungování zjistit více.

Proč si toto téma zaslouží vaši pozornost? Počet českých uživatelů aplikace se sice stále pohybuje v řádu nižších tisíců, nicméně například na internetových stránkách vlády se objevila informace, že **v rámci marketingové kampaně proti dezinformacím budou probíhat diskuze právě i na sociální síti Clubhouse**, což svědčí minimálně o její možné budoucí relevanci, a to i přes to, že aktuálně není dostupná pro uživatele Androidu. Jistě tedy není od věci **nahlédnout na otázky zpracování osobních údajů i v rámci této aplikace**.

Samotný přístup k aplikaci není úplně jednoduchý, neboť musíte splnit dvě podmínky – mít iPhone, respektive zařízení s iOS, a zároveň obdržet pozvánku (popřípadě se zařadit na takzvaný waiting list a počkat na schválení jiným uživatelem). V tomto bodě pravidelné čtenáře Zpravodaje zaujmou minimálně dvě věci – **způsob zasílání pozvánek do aplikace a následná možnost nahrávání rozhovorů**.

Způsob zasílání pozvánek

Pokud chcete do služby někoho přidat, kliknete v aplikaci na funkci „invite“. Objeví se kontakty z vašeho adresáře seřazené podle toho, kolik má daný uživatel již na Clubhousu přátel. Následně máte možnost si jednotlivé uživatele vybrat a **prostřednictvím iMessage jim zaslat pozvánku na jejich telefonní číslo** – aplikace totiž umožňuje tvořit pouze jeden účet, který je s telefonním číslem propojen. Vašemu kamarádovi pak od vás přijde zpráva s odkazem, kde si Clubhouse stáhnout. Zdá se vám to povědomé?

Ano, **jedná se o variaci funkce tell-a-friend**, kterou známe již z jiných sociálních sítí a která se vymstila sociální platformě Twoo – za užívání této funkce obdržela od belgického úřadu pro ochranu osobních údajů **pokutu padesát tisíc eur**. O tomto případu jsme informovali v minulých číslech Zpravodaje.

Co se tehdy belgickému úřadu nelíbilo? Primárně to, že má aplikace **přístup k vašim kontaktům a kontroluje, zda je daný kontakt již uživatelem aplikace**, či nikoliv. V případě Clubhousu aplikace nadto ukáže i počet „společných přátel", kteří již Clubhouse využívají. Problém je v tomto případě relativně jednoduše popsatelný z pohledu neuživatele služby. Aniž byste cokoliv udělali, **aplikace má informace o tom, kteří uživatelé mají vaše telefonní číslo ve svém adresáři**, a zná celkový počet těchto uživatelů (v současné době implicitně s informací, že máte mobilní zařízení s operačním systémem iOS). To vše pak zobrazuje uživatelům, kteří mají uložené vaše telefonní číslo.

Že je taková operace z pohledu GDPR i ePrivacy komplikovaná, už dobře víme. Můžete si to připomenout v **článku** Problém jménem tell-a-friend v digitálním marketingu. Problém tkví zejména v tom, že **aplikace zpracovává osobní údaje ještě předtím, než k tomu potenciální uživatel udělí souhlas**. Neméně komplikované je pak i stanovení právního titulu, respektive **podmínek podle směrnice ePrivacy, které se týkají zasílání obchodních sdělení**. Sociální platforma Twoo tuto funkci následně odebrala, což svědčí o tom, že tento problém nemá úplně jednoduché řešení. Ačkoliv v tomto případě je situace možná lehce odlišná, z pohledu vyřešení mechanismu zpracování osobních údajů je to výzva.

Aplikace využívá funkci tell-a-friend, za níž byla v minulosti udělena pokuta 50 tisíc eur

Nahrávání hovoru

Jak již bylo zmíněno v úvodu, celá **interakce uživatelů této aplikace probíhá v rámci hlasové komunikace**. Moderátor a jím připuštění uživatelé mohou hovořit na takzvané „stage" (označováni jsou jako „speakers") a ostatní, tedy prakticky kdokoliv, pokud místnost není uzamčena, mohou jejich hovor poslouchat (označováni jsou jako „listeners").

To samo otevírá novou výzvu s ohledem na ochranu soukromí, a sice **nahrávání hovoru aplikací a zároveň i jednotlivými uživateli**. Co se týče poskytovatele aplikace, samotný **hovor je nahráván vždy po dobu jeho trvání**, a to ryze z bezpečnostních důvodů, přičemž pokud nedojde k nahlášení porušení podmínek služby, měl by být záznam hovoru smazán. Aplikace tedy sama o sobě **neumožňuje uživatelům nahrávat konverzaci**, děje se tak pouze nepřímo v případě, kdy jednotliví uživatelé nahlásí jednání, které považují za závadné, a poskytovatel si uchová záznam, aby mohl toto nařčení přezkoumat.

Co však nahrávání ze strany uživatelů prostřednictvím jiných aplikací? Clubhouse k tomuto problému při-

stupuje podle pravidla „co se stane ve Vegas, zůstane ve Vegas“. V souladu s tímto pravidlem v rámci **Community Guidelines** (pravidla komunity) stanovuje, že **uživatel není oprávněn přepisovat, nahrávat či jakkoliv jinak reprodukovat či sdílet informace**, které získal v rámci užívání Clubhousu – pokud to není předem umožněno (doslovný překlad by byl „bez předchozího souhlasu“).

Samotná pravidla komunity již tuto otázku neřeší, je tedy nutno nahlédnout do **Terms of Services** (podmínky užívání služby), které jsou taktéž závazným dokumentem pro všechny uživatele. Tyto podmínky zavazují uživatele souhlasit s tím, že **nebude nahrávat ani část konverzace bez předchozího písemného souhlasu všech zúčastněných** „hovořících uživatelů“ („speakers“) a dále že uživatel nebude sdílet (ať už na Clubhousu, či kdekoliv jinde) informaci, o níž „speaker“ prohlásil, že s ní má být zacházeno, jako by byla vyřčena „mimo záznam“ (tedy off the record).

Pokud chce tedy kdokoliv nahrávat konverzaci na Clubhousu, je postaven před veskrze nemožný úkol – **je nucen si od všech, kteří aktivně vystupují v konverzaci, obstarat písemný souhlas**. Avšak jak již bylo řečeno dříve, aplikace neumožňuje jiným uživatelům napsat. Navíc je nutné upozornit, že stále platí zákony, které se týkají ochrany soukromí (ať už občanský zákoník v části týkající se ochrany osobnosti, či GDPR). Přesto však někteří uživatelé daný obsah nahrávají a následně jej zveřejňují jako podcasty, čímž se mohou dopouštět porušení pravidel. Sám Clubhouse trestá případné přešlapy nekompromisně, druhou šanci zpravidla nedává, lze tedy předpokládat, že **v případě zjištění porušení svá pravidla vynucuje poměrně přísně**.

Závěrem

Zda si Clubhouse získá srdce všech uživatelů jiných sociálních sítích a jeho popularita vzroste, těžko říct. Využívání aplikace určitě otevírá nové možnosti v rámci mezilidské interakce, ale tvoří i staronové výzvy z pohledu ochrany osobních údajů.

▪▪▪

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

Lhůty pro uchovávání dat musejí být určovány individuálně, rozhodl SDEU

Podle nových rozsudků Soudního dvora Evropské unie (SDEU) týkajících se uchovávání a dalšího poskytování provozních a lokalizačních údajů o elektronické komunikaci by se lhůty pro uchovávání dat měly pro různé subjekty stanovovat individuálně. Rozhodnutí by se mohla dotknout i české legislativy. SDEU vydal 6. října 2020 rozsudek ve věci Privacy International v. UK (C-623/17) a spojený rozsudek La Quadrature du Net a další v. Francie a Belgie (C-511/18, C-512/18 a C-520/18), v nichž mimo jiné obecně zakazuje národní legislativní opatření založená ustanovením čl. 15 směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, pokud preventivně ukládají plošné a nerozlišující uchovávání provozních a lokalizačních údajů. Připouští však výjimky v případě reálné a vážné hrozby národní bezpečnosti a boje proti závažné trestné činnosti. Úřad pro ochranu osobních údajů upozorňuje, že závěry těchto rozsudků mohou rozporovat ustanovení § 97 zákona č. 127/2005 Sb., o elektronických komunikacích a související předpisy založené na preventivním šestiměsíčním zadržování provozních a lokalizačních údajů, přestože Ústavní soud ve svém nálezu č. 161/2019 Sb. uvádí, že k zadržování takových dat docházet musí. Podle ÚOOÚ je proto nutné zvážit, jak naplnit požadavky obsažené v předmětných rozsudcích SDEU, případně zda je nutné změnit zákon.

Zdroj: ÚOOÚ

Jak napsat oznámení o ochraně osobních údajů

Napsat oznámení o ochraně údajů je možná snazší než napsat knihu, ale je tu několik věcí, na které byste si měli dát pozor. Jakých formulací se raději vyvarovat? Je lepší napsat oznámení svépomocí, nebo využít online nástroj? A jak ho upravit pro děti či cizince?

Zásady ochrany soukromí neboli Privacy Notice není dobré brát na lehkou váhu, může vás to totiž stát až likvidační pokutu, jak jsme si vyjasnili v **článku** Privacy Notice – jak se vyhnout likvidační pokutě. Už tedy víte, jaké informace musí Privacy Notice obsahovat. Jak ale napsat samotné oznámení? Máme pro vás **praktické rady, jak postupovat, a několik tipů na užitečné online nástroje**, které vám můžou zásadně usnadnit práci.

Co byste měli zahrnout

Teď, když víte, co musíte do zásad ochrany soukromí zahrnout, je třeba myslet i na několik věcí, které byste zahrnout měli. Nezapomeňte, že **v ideálním případě by lidé měli se shromažďováním údajů souhlasit**. Zejména pokud nemáte žádný jiný zákonný základ pro jejich shromažďování, je důležité být uživatelsky přívětivý a přátelský.

Různé druhy sběru dat si obecně zaslouží různé druhy oznámení. V tomto případě předpokládáme, že vaše organizace již **provedla audit a disponuje katalogem zpracování osobních údajů**, aby identifikovala procesy, kde jsou osobní údaje shromažďovány, a způsob, jakým organizací procházejí, kde jsou uloženy, kdo k nim má přístup a podobně. Měli byste tedy vědět, **komu případně budete muset zasílat oznámení o existenci zpracování**.

V jiných případech, **například pokud shromažďujete údaje od třetích stran**, možná budete muset někoho přímo kontaktovat. V takovém případě byste měli postupovat následovně:

1. Začněte tím, **kdo je správcem údajů**. Ideálně se sami představte a v případě, že nejste správcem, informujte, pro koho pracujete.
2. Zjistěte, **k čemu slouží účel zpracování dat**, a lidem sdělte, co s jejich daty děláte.
3. Nezapomeňte zahrnout dostatek informací k **prokázání zákonného, korektního a transparentního zpracování**.

> **Nepoužívejte odborné termíny, napište to polopaticky**

4. Korektnost je v GDPR nesmírně důležitá a není jen prázdným slovem. Existují **tři hlavní složky korektnosti**:
   - využití získaných dat způsobem, který lidé rozumně očekávají,
   - úvaha o dopadu a důsledcích zpracování,
   - transparentnost a poskytnutí informací, jak jsou data využívána.

Důvěra na prvním místě

Důvěra se prolíná celým obecným nařízením GDPR. Pokud jde o oznámení o ochraně osobních údajů, je snazší vytvořit si důvěru přímým sdělením o tom, **jaké údaje máte, proč je budete používat a jak je budete udržovat v bezpečí**. Je také důležité přidat informaci, jak dlouho si data ponecháte.

Tipy pro psaní zásad o ochraně osobních údajů

Osvojte si jednoduchý styl, který bude pro vaše publikum snadno srozumitelný. Buďte jasní a výstižní – **jděte přímo k věci**. Nepředpokládejte, že čtenář má stejnou úroveň porozumění jako vy. Snažte se **držet stranou od průmyslového žargonu** a tam, kde je nutné ho použít, vysvětlete, co to znamená. Matoucí terminologie je zaručený způsob, jak od čtení odradit.

Zkuste si udělat průzkum, **jak zásady o ochraně osobních údajů řeší jiní, včetně vaší konkurence**. Pokud jste data shromáždili nepřímo, můžete také zahrnout prohlášení o hodnotě, které vám pomůže budovat důvěru. Ujistěte se ale, že jste již vysvětlili, co s osobními údaji děláte, než začnete mluvit o sobě.

Nakonec je dobré zajistit, aby oznámení o ochraně osobních údajů byla **konzistentní napříč všemi vašimi platformami**, abyste měli jejich změny pod kontrolou. Britské ICO doporučuje informace podávat v jednotlivých úrovních, tedy strukturovaně, nebo v momentě, kdy je na to vhodný čas, tedy těsně před sběrem informací v podobě cookies banneru.

Do oznámení zahrňte také **informace o následujících službách**, pokud některou z nich využíváte:

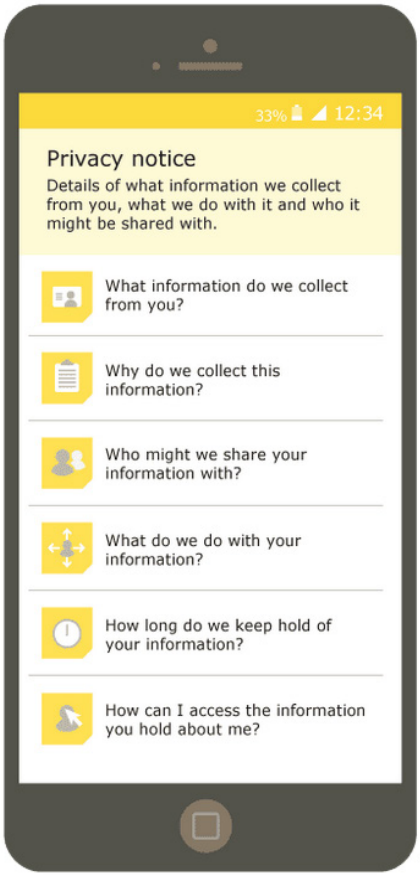
- sociální sítě (Facebook, Instagram, Twitter, Youtube…)
- kategorie shromažďovaných osobních údajů
- jak vás mohou subjekty údajů kontaktovat
  - e-mail
  - webová stránka
  - telefon
  - poštovní adresa
  - datová schránka
- zda využíváte Google Analytics či jiné analytické nástroje (záleží na nastavení)
- rozesílání e-mailů – mailChimp a podobně
- zda zobrazujete cílenou reklamu
- zda přijímáte platby přes web
  - PayPal
  - bankovní převod
  - WePay
  - Google Pay
  - Apple Pay
  - platební brána (konkrétní)
- zda využíváte získaná data pro retargeting
- zda využíváte služby jako například:
  - reCaptcha
  - Google places
  - Mouseflow
  - FreshDesk
- zda sbíráte osobní údaje dětí (s tím velmi opatrně)
- využití Fan Page na Facebooku

Oznámení na mobilních zařízeních

Při plánování a zveřejnění zásad o ochraně osobních údajů nezapomeňte na svůj mobilní web. Mnoho uživatelů webu je na mobilních zařízeních, což znamená, že **vaše oznámení musí odpovídat potřebám mobilních uživatelů**. Na obrázku výše je příklad oznámení o ochraně osobních údajů od ICO. Takový design lze považovat za velmi srozumitelný a pochopitelný. Britské ICO nabízí zpracované příklady, jak by zveřejněné zásady měly, nebo naopak neměly vypadat.

Oznámení pro děti

Web používá každý a v současné době i děti. Může dojít k situaci, kdy děti



zveřejní osobní údaje, aniž chápou důsledky takového zveřejnění. Obecné nařízení GDPR je v oblasti ochrany osobních údajů dětí velmi jasné. Děti jsou považovány za zranitelné jedince a musíte s nimi zacházet korektně a spravedlivě.

To znamená, že oznámení o zásadách ochrany osobních údajů by mělo být zaměřeno na věkovou skupinu a **úroveň srozumitelnosti by měla odpovídat zamýšlenému publiku**. To také může znamenat přidání dalších ochranných a bezpečnostních opatření.

Především byste se nikdy neměli snažit využít něčího nepochopení. To platí i pro dospělé subjekty údajů, ale vzhledem k postavení dětí jako zranitelných osob budou případné tresty v tomto případě ještě přísnější. V České republice platí, že **děti mladší 15 let musí mít výslovný souhlas rodiče nebo zákonného zástupce**. Při kontrole údajů musí správce vyvinout dostatečné a přiměřené úsilí k ověření, zda souhlas skutečně udělil rodič nebo zákonný zástupce.

Oznámení pro různé skupiny

Podniky a organizace často komunikují s širokou škálou lidí. Budete tedy muset přemýšlet o tom, **jaké typy vztahů máte s různými skupinami** a zda je některá z vámi poskytovaných oznámení nemohou zmást nebo být ve vztahu k nim přinejmenším irelevantní. Jinými slovy: **plošné prohlášení nemusí stačit**.

V této souvislosti je vhodné segmentovat zákazníky a **poskytnout každé kategorii přizpůsobené oznámení o ochraně osobních údajů**. To pomůže zákazníkům lépe pochopit, jak se k nim vztahují vaše postupy a procesy v oblasti ochrany osobních údajů.

Oznámení pro cizince

Podnikání se stalo globálním, takže vaše společnost může shromažďovat údaje od osob, které nehovoří česky. Je vhodné **poskytnout oznámení o ochraně osobních údajů v jazyce vašich zákazníků**, ale obecné nařízení GDPR to výslovně ve vztahu k cizincům nevyžaduje. V případě souladu s obecným nařízením GDPR je však vždy lepší chybovat na straně opatrnosti.

Generátory zásad o ochraně osobních údajů

V současné době si vytvoření oznámení o zásadách zpracování osobních údajů můžete **ulehčit některým z existujících nástrojů**. V češtině zatím existuje pouze jeden generátor, a to jako modul nástroje DPO Tools pro správu agendy související se správou ochrany osobních údajů. Pokud nemáte problém s anglickou verzí, nebo ji dokonce přímo potřebujete, pak máte výběr podstatně širší. Tipy na další generátory zásad o ochraně osobních údajů najdete na následující straně.

Tipy na generátory zásad o ochraně osobních údajů

DPO Tools ➤ ZDE	Online nástroj na celkovou správu agendy související s ochranou osobních údajů v češtině a dalších jazycích. K dispozici mají buď generátor jako modul, který vychází z katalogu zpracování organizace a dalších dat, nebo šablony ve formátu MS Word. Užitím modulu získáte zcela personalizovaný dokument.
TermsFeed ➤ ZDE	Generátor vám umožní vytvářet vlastní právní dokumenty, které mohou být pro vaše uživatele právně závazné – snadno a online. TermsFeed umožňuje vytvářet zásady ochrany osobních údajů, obchodní podmínky, EULA a zásady používání cookies.
Free Privacy Policy ➤ ZDE	Zásady ochrany osobních údajů vygenerujete za méně než 15 minut jednoduchým postupem podle pokynů. Společnost poskytuje několik nástrojů pro ověřování souladu.
Privacy Policies.com ➤ ZDE	Zdarma pro osobní použití. Pokud podnikáte, zaplatíte jednorázový poplatek. To, co získáte, není jen šablona. Zadáte své informace a základní šablona bude změněna tak, aby odrážela vaše konkrétní potřeby, což je zásadní, protože každý web a podnik jsou jedinečné.
Shopify ➤ ZDE	Shopify má bezplatný generátor zásad ochrany osobních údajů. Použití generátoru je intuitivní a poskytne vám přizpůsobené zásady týkající se produktů a služeb vaší společnosti.
Privacy Policy Online ➤ ZDE	Generátor nabízí mimo jiné prohlášení o zásadách ochrany osobních údajů a také pokrývá požadavky přidružených společností, včetně Google AdSense a dalších populárních webů.
Iubenda ➤ ZDE	Iubenda vám sdělí, jak a proč možná budete muset vygenerovat zásady pro konkrétní služby, jako jsou Google AdSense a AdWords, stejně jako Mailchimp, Facebook, seznamy adresátů a soubory cookie. Zásady můžete generovat v deseti jazycích včetně angličtiny.
Trust Guard ➤ ZDE	Společnost poskytuje pečeť důvěryhodnosti, kterou můžete umístit na svůj web. Říká lidem, že váš web je bezpečný. Trust-Guard zajišťuje, že získáte nejpřesnější dostupné zásady ochrany osobních údajů.
Seq Legal ➤ ZDE	Na svých webových stránkách zveřejňují bezplatné i prémiové šablony právních dokumentů. Můžete si z nich stáhnout profesionální šablonu zásad ochrany osobních údajů (v dokumentu Word).
Virginia Tech ➤ ZDE	Tento web velmi podrobně vysvětluje potřebu zásad ochrany osobních údajů. Vysvětlení je jasné a stručné.
Get Terms ➤ ZDE	Generátor vám umožní získat pro váš web velmi jednoduše podmínky služby a prohlášení o zásadách ochrany osobních údajů. Vyplníte několik polí a můžete si zdarma vytvořit vlastní zásady ochrany osobních údajů.
Auto Terms Of Service And Privacy Policy ➤ ZDE	Pokud používáte WordPress, můžete si zásady ochrany osobních údajů vygenerovat pomocí pluginu. Stáhněte si bezplatný plugin z adresáře pluginů WordPress a okamžitě máte základní zásady ochrany osobních údajů.
3dcart Personalized Privacy & Return Policy Generator ➤ ZDE	Společnost nabízí e-commerce software a vytvořila užitečný nástroj pro generování zásad ochrany osobních údajů a vrácení zboží.

Kdy je třeba poskytnout oznámení?

Podle článku 14 GDPR, pokud získáváte údaje přímo od subjektu údajů, musíte všechny výše uvedené skutečnosti **oznámit v době, kdy byly získány**. Je tedy zřejmé, že budete muset všechny informace uvést nejen na stránce se zásadami ochrany osobních údajů, ale například **v případě cookies v momentě, kdy chcete sběr dat zahájit**. Tedy před vytvořením cookies. V tomto případě pouhá informace v zásadách o ochraně osobních údajů nestačí.

Příkladem jde i britské ICO, které, byť ze zákona nemusí, tak souhlas v tomto případě preferuje a informa-

ČEMU SE VYHNOUT A CO NAOPAK ZDŮRAZNIT

Je snadné něco zamlčet či mlžit, takovou praxi však dozorové orgány nemilosrdně trestají.

NEVHODNÉ FORMULACE:

- **„Vaše osobní údaje můžeme použít k vývoji nových služeb.“ (Není jasné, co to jsou „služby“ nebo jak je tyto údaje pomohou rozvíjet.)**
- **„Vaše osobní údaje můžeme použít pro výzkumné účely.“ (Není jasné, o jaký „výzkum“ se jedná.)**
- **„Vaše osobní údaje můžeme použít k nabízení personalizovaných služeb.“ (Není jasné, co je „personalizací“ míněno.)**

MNOHEM LEPŠÍ FORMULACE:

- **„Uchováme vaši historii nákupů a použijeme podrobnosti o výrobcích, které jste si dříve zakoupili, abychom vám mohli navrhnout další produkty, o kterých si myslíme, že vás také zajímají.“ (Je jasné, jaké typy údajů budou zpracovávány, že subjekt údajů bude předmětem cílené reklamy na produkty a že údaje budou použity k tomu, aby to bylo možné.)**
- **„Budeme uchovávat a vyhodnocovat informace o vašich nedávných návštěvách našeho webu a o tom, jak se pohybujete v různých částech webových stránek pro analytické účely, abychom pochopili, jak uživatelé používají náš web, a my jej mohli udělat intuitivnějším.“ (Je jasné, jaké typy údajů budou zpracovány, a je uveden typ analýzy, kterou se správce chystá provést.)**
- **„Budeme vést záznamy o článcích na našem webu, na které jste klikli, a tyto informace použijeme k cílení reklamy na tomto webu, která souvisí s vašimi zájmy, jež jsme identifikovali na základě článků, které jste si přečetli.“ (Je zřejmé, co zahrnuje personalizace a jak byly identifikovány zájmy připisované subjektu údajů.)**

ci poskytuje nejen v zásadách ochrany osobních údajů, ale i formou oznámení prostřednictvím cookies banneru. Informace by měly být strukturované. Jinými slovy, pokud například žádáte o datum narození, měla by se po jeho zadání **změnit informace pro osoby starší 15 let a naopak mladší 15 let**.

Klíčem úspěšně napsaných zásad o zpracování osobních údajů je rozumné očekávání subjektů údajů. V každém případě zveřejněte zásady ochrany osobních údajů, pokud:

- shromažďujete citlivé informace;
- zamýšlené použití informací bude pravděpodobně neočekávané nebo nevhodné;
- poskytnutí nebo neposkytnutí osobních údajů bude mít na subjekt údajů významný vliv; nebo
- informace budou sdíleny s jinou organizací způsobem, který by subjekt údajů neočekával.

Nezapomeňte upravit oznámení pro mobilní web

Nezapomeňte, že kdykoliv poprvé shromažďujete údaje novým způsobem, musíte o tom okamžitě informovat subjekt údajů. A opět, pokud vaším právním základem bude souhlas, zakažte používání souborů cookie, dokud tento souhlas neobdržíte. Mějte

na mysli, že **zásady o ochraně osobních údajů jsou vždy součástí udělovaných souhlasů**.

Na druhou stranu, pokud shromažďujete údaje ze zdrojů třetích stran, a ne přímo od subjektu údajů, musíte na to **upozornit nejen ve svých zásadách, ale i do jednoho měsíce subjekt údajů**. Pokud používáte údaje ke kontaktování subjektu údajů, musíte to oznámit při prvním kontaktu. Pokud sdělujete údaje třetí straně, musíte to subjektu údajů oznámit před zveřejněním.

Rada na závěr

S vytvořením vlastního dokumentu ochrany osobních údajů vám pomůže celá řada webů. Je však důležité, abyste ve svých zásadách zohlednili všechny věci, které chcete a které zohlednit musíte. Zatímco většina webů používá standardní šablony, vy zřejmě budete potřebovat takovou **šablonu upravit, aby vyhovovala všem potřebám vaší organizace**. Pokud je to třeba, vyhledejte radu odborníka a nechte si vytvořit profesionální zásady ochrany osobních údajů. Mít je nesprávně je stejně špatné, ne-li horší, než nemít vůbec žádné. Použijte online nástroj zásad ochrany osobních údajů, ale proveďte i svůj průzkum a v případě potřeby vyhledejte právní radu. Nepředpokládejte, že jste vytvořili zásady, které mohou pokrýt všechny scénáře.

▪▪▪

Ing. Mgr. Luděk Nezmar, MBA

Jsou trestné body za dopravní přestupek osobním údajem?

Kam spadají informace o trestných bodech udělených řidičům z pohledu GDPR? Jde o osobní údaje zvláštní kategorie? A může být taková informace zpřístupněna třetím stranám?

Generální advokát Soudního dvora EU Maciej Szpunar zveřejnil v polovině prosince 2020 své stanovisko k několika předběžným otázkám položeným lotyšským ústavním soudem (na které bude Soudní dvůr EU odpovídat v řízení pod sp. zn. C-439/19). Ten se v první položené otázce zajímal o to, **zda je nutné považovat informace o trestných bodech udělených řidičům za osobní údaje** ve smyslu čl. 10 GDPR.

Údaje o trestných činech

Článek 10 GDPR blíže upravuje **zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů** či souvisejících bezpečnostních opatření: *„Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření na základě čl. 6 odst. 1 se může provádět pouze pod dozorem orgánu veřejné moci nebo pokud je oprávněné podle práva Unie nebo členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů. Jakýkoli souhrnný rejstřík trestů může být veden pouze pod dozorem orgánu veřejné moci.“*

Údaje týkající se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření **nejsou součástí zvláštních kategorií osobních údajů** (čl. 9 GDPR). Namísto toho je pro ně stanovena speciální kategorie. Článek 10 GDPR obsahuje odlišné podmínky pro jejich zpracování. Uvedené ustanovení nařízení dopadá na osobní **údaje o odsouzení za trestný čin, na informace o podmíněném zastavení trestního stíhání, narovnání**… Otázkou však je, zda předmětné ustanovení nařízení dopadá i na informace o trestných bodech udělených řidičům.

Podle názoru generálního advokáta Soudního dvora EU Macieje Szpunara informace o trestných bodech **udělených řidičům pod čl. 10 GDPR nespadají**. Jedná se tudíž o „běžné“ osobní údaje.

> **Informace o trestných bodech nesmí být veřejně přístupné**

Zpřístupnění třetím stranám

Ve své druhé otázce se lotyšský ústavní soud (*Latvijas Republikas Satversmes tiesa*) zajímal o to, zda informace o trestných bodech udělených řidičům **mohou být zpřístupněny třetím stranám a případně využity k dalšímu zpracování** (tedy ke zpracování pro jiné účely, než jsou ty, pro které byly osobní údaje původně shromážděny).

Generální advokát Soudního dvora EU Maciej Szpunar ke druhé položené otázce sdělil, že **informace o trestných bodech udělených řidičům nemohou být veřejně přístupné**. Zpřístupnění informací o trestných bodech udělených řidičům třetím stranám a jejich případné další zpracování je v rozporu se zásadami účelového omezení (čl. 5 odst. 1 písm. b) GDPR) a minimalizace údajů (čl. 5 odst. 1 písm. c) GDPR).

Zásada účelového omezení a minimalizace

Zásada účelového omezení říká, že osobní údaje **musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely** a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Zásada minimalizace údajů zase říká, že osobní údaje **musí být přiměřené, relevantní a omezené na nezbytný rozsah** ve vztahu k účelu, pro nějž jsou zpracovávány.

Stanovisko generálního advokáta (v anglickém jazyce) je dostupné z webových stránek Soudního dvora EU **zde**. Nyní nezbývá než počkat, zda se bude Soudní dvůr EU daným názorem generálního advokáta řídit. ▪▪▪

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

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: 28. 1. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.