ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR | 3. ročník | číslo 1 | leden 2021

Privacy Notice – jak se vyhnout likvidační pokutě

Nechcete dopadnout jako Google, který dostal pokutu 100 milionů eur? Zásady ochrany soukromí neboli Privacy Notice by měly být součástí každého webu nebo e-shopu, který zpracovává či shromažďuje údaje o svých uživatelích. Potřebujete je i vy? Jaké informace v nich uvést?

Google dostal ve Francii na konci minulého roku **pokutu 100 milionů eur za porušení ochrany osobních údajů při používání cookies** a dalších online trackerů (sledovačů) využívaných při zobrazování relevantní reklamy. Jedná se o nejvyšší pokutu, jakou francouzský úřad dohlížející na ochranu osobních údajů CNIL dosud udělil. Americký maloobchodní gigant **Amazon dostal za porušení stejných pravidel pokutu 35 milionů eur**.

CNIL uvedl, že francouzské weby Google a Amazon si od návštěvníků nevyžádaly souhlas s uložením reklamních cookies do jejich počítačů. V odůvodnění se píše, že Google a Amazon **neposkytly jasné informace o tom, jak budou online trackery použity** a jak mohou návštěvníci francouzských webových stránek cookies odmítnout. Technologičtí giganti dostali tři měsíce na změnu informačních bannerů zobrazovaných při návštěvě jejich webových stránek. Pokud tyto podmínky nedodrží, bude jim **do provedení změn uložena pokuta dalších 100 000 eur denně**.

> **100 tis. eur pokuta DENNĚ čeká Google i Amazon, pokud nebudou plnit informační povinnosti**

Zjednodušeně řečeno, uvedené **společnosti dostatečně nesplnily svou informační povinnost**, kterou jim GDPR ukládá. Kromě „cookie banneru“ s tím velmi úzce souvisí i Privacy Notice, tedy zásady ochrany soukromí (osobních údajů) nebo veřejné prohlášení správce o tom, jakým způsobem se k osobním údajům staví a jak s nimi zachází.

Co jsou zásady ochrany soukromí?

Zásady ochrany soukromí neboli **Privacy Notice je veřejné prohlášení nebo právní dokument**, který uvádí, jak organizace, e-shop nebo web shromažďuje a zpracovává osobní údaje svých zákazníků a návštěvníků a jak s nimi nakládá. Dokument by měl výslovně popisovat, **zda jsou shromažďované informace považovány za důvěrné, zda jsou sdíleny nebo poskytovány třetím stranám**.

Tento dokument musí být podle obecného nařízení GDPR:

- stručný, transparentní, srozumitelný a snadno dostupný;
- psán jasným a pochopitelným jazykem, zejména je-li určen dítěti; a
- poskytnut zdarma.

Stručně řečeno, Privacy Notice je místo na webu, kde svým uživatelům sdělíte vše o tom, jak zajistíte, **aby obchodní praktiky vaší organizace respektovaly soukromí zákazníků** a návštěvníků webu. V současné době lze považovat za best practice užití takzvaných „Privacy Hub", tedy míst, kde může uživatel **nastavit všechny své preference v oblasti osobních údajů** při využívání vámi poskytované služby. Cookie banner je jen jednou částí takového Privacy Hubu.

Zákazník může vidět a nastavit například:

- jak jsou jeho osobní údaje a generovaná data využívána;
- kde se používají;
- jak jsou data shromažďována;
- jaký typ dat povolí shromažďovat;
- podmínky, za jakých jsou sdílena;
- kde mohou subjekty údajů odvolat udělený souhlas.

Potřebujete zásady ochrany soukromí?

Ochrana soukromí, a tedy i osobních údajů, není nic nového. S digitalizací našeho života a sběrem všemožných údajů a dat však získala ochrana osobních údajů významnou prioritu. Je třeba si uvědomit, že **v současné době už umělá inteligence dokáže předjímat vaše budoucí chování** s téměř bezchybným úsudkem, pokud má dostatek informací o vašem předchozím chování. Tyto předpovědi se nevztahují jen na nákupní chování, ale také například na volební preference, a má tedy i možnost vaše rozhodnutí zásadně ovlivnit, či dokonce změnit.

Příkladem může být stížnost jednoho z rodičů na internetový obchod ohledně toho, že jeho nezletilé dceři primárně nabízí věci pro novorozence. Dotyčný e-shop se omluvil, že umělá inteligence špatně vyhodnotila chování jeho dcery, aby se vzápětí ukázalo, že se počítač nemýlil a dceři nabízel opravdu zboží, které v blízké budoucnosti potřebovala. Následovala pokorná omluva dotyčného otce.

PŘÍKLAD:

Výňatek ze zásad o ochraně osobních údajů společnosti Pinterest jasně popisuje informace, které společnost Pinterest shromažďuje jak od svých uživatelů, tak i z jakéhokoli jiného zdroje. Pinterest za osobní údaje považuje v zásadě všechny informace, které uživatel dobrovolně poskytne. Jedná se například o jména, fotografie, špendlíky (piny), tabule (boardy), kategorie, lajky, e-mailové adresy a/nebo telefonní číslo, geolokační data či platební údaje včetně dopravy při koupi nějakého produktu. Na uvedeném příkladu je vidět, že se nejedná jen o klasicky vnímané osobní údaje jako jméno, telefon a e-mail, ale také o informace, které uživatel prostřednictvím služby Pinterest teprve vytváří jejím užitím.

Organizace nebo webové stránky, které zpracovávají informace o zákaznících, **jsou povinny zveřejňovat zásady ochrany soukromí osobních údajů na svých komerčních webech**. Pokud provozujete web, webovou, mobilní nebo desktopovou aplikaci, která shromažďuje či zpracovává údaje o svých uživatelích, budete s největší pravděpodobností muset transparentně zveřejnit zásady ochrany soukromí osobních údajů na svém webu nebo **poskytnout v dané aplikaci přístup k zásadám ochrany osobních údajů**.

Existuje několik důvodů, proč webová stránka zveřejňuje na svém webu prohlášení o zásadách ochrany osobních údajů. K těmto důvodům například patří:

- vyžaduje to zákon;
- vyžadují to služby třetích stran;
- zvyšujete tím transparentnost.

Vyžadování zákonem

Státy po celém světě si začaly uvědomovat potřebu ochrany dat a soukromí svých občanů. Organizace a weby, které shromažďují a/nebo zpracovávají informace o zákaznících, jsou povinny zveřejňovat a dodržovat zásady o ochraně soukromí osobních údajů. Většina zemí již **přijala zákony na ochranu osobních údajů a soukromí svých uživatelů**, které vyžadují, aby organizace získaly souhlas od svých klientů, pacientů, uživatelů a návštěvníků, jejichž údaje budou ukládat nebo zpracovávat. Příkladem těchto zákonů jsou:

- obecné nařízení GDPR v EU;
- zákon č. 110/2019 Sb., o zpracování osobních údajů;
- CalOPPA v USA;
- PIPEDA v Kanadě.

Pro firmu nebo weby, které shromažďují a zpracovávají informace o uživateli v určité oblasti nebo zemi, je velmi důležité mít **úplný přehled a znalost zákonů o ochraně osobních údajů v dané zemi**, ve které se nacházejí zákazníci a koncoví uživatelé.

V některých případech musí podniky **dodržovat zákony specifické pro jednotlivé státy** (Kalifornie) nebo **předpisy specifické pro průmyslová odvětví** (kodexy). Příkladem může být společnost General Motors dodržující CalOPPA v USA tím, že do svých zásad ochrany osobních údajů zahrnula samostatnou sekci specifickou pro Kalifornii.

Při psaní zásad ochrany soukromí **je třeba si odpovědět na následující otázky**:

- Je má organizace správce nebo zpracovatel?
- Musím jmenovat pověřence, a tedy uvést kontakt?
- Jaké informace se shromažďují?
- Kdo údaje ve skutečnosti sbírá?
- Jak se shromažďují?
- Proč se shromažďují?
- Jak budou používány?
- S kým jsou data dále sdílena?

- Jaký to bude mít dopad na dotčené osoby?
- Je pravděpodobné, že zamýšlené použití způsobí námitky nebo stížnosti osob?

Jaké informace uvést?

Pokud již máte jasno v tom, zda jste správcem nebo zpracovatelem, a také znáte právní základ, který je třeba uvést ve vašich zásadách ochrany osobních údajů, můžeme si říct, co by takový dokument měl obsahovat. Existují dvě jasné kategorie, které vám pomohou určit, **jaké informace musíte poskytnout**. Týkají se způsobu, jakým informace shromažďujete – přímo, nebo nepřímo.

Pokud potřebujete podrobnější vysvětlení kategorií v níže uvedené tabulce, najdete jej v obecném nařízení GDPR, čl. 13 odst. 1 a 2, které pojednávají o tom, **co musí být subjektu údajů poskytnuto v okamžiku získání osobních údajů**.

V příštím díle

Nyní byste měli mít jasno, k čemu zásady ochrany soukromí neboli Privacy Notice slouží a zda byste je měli umístit i na svůj web či e-shop. Vyjasnili jsme si také, jaké informace by měly zásady ochrany soukromí obsahovat. V příštím čísle se dozvíte několik tipů, jak napsat oznámení o ochraně osobních údajů a jak ho upravit pro specifické případy, například pro mobilní aplikace, děti či cizince. Nabídneme také recenze na dostupné generátory zásad o ochraně osobních údajů. ▪▪▪

Ing. Mgr. Luděk Nezmar, MBA

Klikněte a stáhněte si vzor

Jaké informace uvést v Privacy Notice

	Údaje shromážděné	
	přímo	nepřímo
Totožnost a kontaktní údaje vašeho pověřence pro ochranu osobních údajů	Ano	Ano
Účel zpracování včetně právního základu	Ano	Ano
Oprávněné zájmy vaší společnosti nebo organizace	Ano	Ano
Kategorie shromažďovaných osobních údajů	Ne	Ano
Příjemci nebo kategorie příjemců osobních údajů	Ano	Ano
Informace o předávání třetím stranám a přijatá bezpečnostní opatření	Ano	Ano
Jak dlouho budete uchovávat data a na základě čeho byla lhůta stanovena	Ano	Ano
Informace o existenci práv na ochranu osobních údajů každého subjektu údajů	Ano	Ano
Právo odvolat souhlas (je-li relevantní)	Ano	Ano
Právo podat stížnost u dozorového úřadu	Ano	Ano
Zdroj dat – pochází z veřejně přístupných zdrojů?	Ne	Ano
Zákonné a smluvní závazky a jejich důsledky	Ano	Ne

Nejhorší hesla roku 2020

Uhodnete, jaká byla nejhorší hesla roku 2020? Řady posloupných čísel, jména rodinných příslušníků a přátel nebo jen „heslo“ – ty všechny útočník prolomí během zlomku sekundy. Používáte je také? A ví vaši zaměstnanci, jak vytvořit těžce prolomitelné heslo? Naučte je šest základních pravidel pro bezpečné heslo.

Heslo je jedním ze základních bezpečnostních prvků používaných správci osobních údajů, respektive jejich zaměstnanci. Správci osobních údajů, případně jejich zaměstnanci, se (ve většině případů) **pomocí hesla přihlašují do počítače, telefonu, jednotlivých aplikací a systémů**… Je důležité, aby přitom dodržovali určité zásady, které povedou k vytvoření dostatečně silného (těžce prolomitelného) hesla. Správce osobních údajů by tudíž měl své zaměstnance pravidelně upozorňovat na jedné straně na to, jaké jsou nejčastější chyby při vytváření hesla, a na straně druhé na to, jak bezpečné heslo vytvořit.

Společnost NordPass provedla analýzu jednotlivých hesel uniklých na internet v roce 2020 a **sestavila žebříček 200 nejhorších hesel loňského roku**. Nejhorším heslem za minulý rok bylo podle předmětné společnosti heslo „123456“, hned za ním následovala hesla „123456789“ a „picture1“. Prolomit první dvě hesla by podle společnosti NordPass trvalo méně než jednu sekundu, prolomit třetí by trvalo asi tři hodiny (což však rovněž není možné považovat za ideální stav). Kompletní seznam nejhorších hesel za rok 2020 vytvořený společností NordPass je dostupný na webových stránkách společnosti **zde**. První desítku najdete v tabulce.

10 nejhorších hesel za rok 2020 podle společnosti NordPass

pořadí	heslo	doba potřebná k prolomení hesla
1.	123456	méně než 1 sekunda
2.	123456789	méně než 1 sekunda
3.	picture1	3 hodiny
4.	password	méně než 1 sekunda
5.	12345678	méně než 1 sekunda
6.	111111	méně než 1 sekunda
7.	123123	méně než 1 sekunda
8.	12345	méně než 1 sekunda
9.	1234567890	méně než 1 sekunda
10.	senha	10 sekund

Je patrné, že uvedená tabulka nejspíš nebude úplně věrným odrazem hesel používaných v České republice nebo na Slovensku. Dá se však předpokládat, že s určitými obměnami je aplikovatelná i na české a slovenské prostředí. Autor článku si například dokáže živě představit, že mnoho českých a slovenských uživatelů sáhne namísto hesla „password“ po heslu „heslo“. Že by tím ale dosáhli větší bezpečnosti, se však rozhodně říci nedá.

Proč lidé volí slabá hesla?

Většina lidí používá jednoduchá a snadno zapamatovatelná hesla, protože je to pro ně pohodlné. Sahají tudíž po **jménech svých rodinných příslušníků a přátel, názvech oblíbených sportů nebo jídel**, nadávkách, takzva-

ných pozitivních slovech (například „iloveyou“, „love“, „family“, „princess“, „sunshine“) nebo názvech filmů, seriálů, komiksů, knih či po jménech postav z nich. Problém však je, že většina jednoduchých a snadno zapamatovatelných hesel je vysoce zranitelná vůči prolomení.

Jak na bezpečné heslo?

Co by měl správce naučit své zaměstnance a jaké zásady by případně měl sám dodržovat? Cesta k bezpečnému heslu není (alespoň teoreticky) nikterak složitá. Je nutné dodržet několik základních pravidel. Můžete si je stáhnout jako vzor a vyvěsit například v kanceláři, aby je vaši zaměstnanci měli stále na očích.

▪▪▪

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

Klikněte a stáhněte si vzor

6 základních pravidel pro bezpečné heslo

1. Nepoužívejte stejná hesla pro více účtů nebo zařízení. Pro každý účet nebo zařízení je nutné si vytvořit jedinečné a složité heslo. Pokud dojde k úniku jednoho hesla, nebudou ohrožena všechna zařízení či účty.
2. Nepoužívejte „snadno zapamatovatelná hesla“ vytvořená podle jmen svých rodinných příslušníků nebo přátel, názvů oblíbených sportů nebo jídel, nadávek, takzvaných pozitivních slov („family“, „love“) nebo názvů filmů, seriálů, komiksů či knih nebo jmen postav z nich. Stejně tak není vhodné používat řady po sobě jdoucích číslic či písmen nebo osobní údaje (jako je například datum narození, rodné číslo, adresa).
3. Nepoužívejte krátká hesla. Heslo by mělo mít minimálně 12 (někdy se uvádí až 15) znaků.
4. Ideální je kombinace velkých a malých písmen, písmen s háčky, dlouhých hlásek, čísel a speciálních znaků. Dojde tím ke snížení rizika prolomení hesla. Avšak nestačí pouhé přidání čísla, velkého písmena, písmena s háčkem či speciálního znaku na začátek nebo konec jinak slabého hesla (například jména filmu).
5. Nepoužívejte běžné náhrady znaků. Heslo, které využívá nahrazování písmen podobnými číslicemi a naopak, je rovněž slabé. Ať už si jako heslo nastavíte výraz „INTERNET“ nebo „1NT3RN3T“, útočník používající hrubou sílu jej prolomí stejně snadno.
6. Ideální je využívat dvoustupňové (vícestupňové) ověření.

Už jste se podívali na návrh nových standardních smluvních doložek?

Do půlnoci 10. prosince 2020 bylo možné zasílat připomínky k **návrhu nového rozhodnutí Evropské komise o standardních smluvních doložkách** pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle GDPR a rovněž i k návrhu samotných standardních smluvních doložek.

Standardní smluvní doložky (Standard Contractual Clauses, zkráceně SCC) představují nástroj, který umožňuje vytvořit **vhodné záruky ochrany osobních údajů ve třetí zemi** s nedostatečnou úrovní ochrany osobních údajů. Standardní smluvní doložky jsou vzorovým textem smlouvy (smluvní doložky) mezi správcem osobních údajů, který má v plánu předat osobní údaje do třetí země mimo EU, respektive mimo EHP, a příjemcem osobních údajů v této třetí zemi s nedostatečnou úrovní ochrany osobních údajů. V případě, že **správce osobních údajů uzavře s tímto příjemcem osobních údajů smlouvu**, jejíž součástí budou i standardní smluvní doložky, vytvoří tak v této třetí zemi vhodné záruky ochrany osobních údajů. K této problematice viz blíže čl. 46 GDPR.

Návrh rozhodnutí Evropské komise o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle GDPR a draft samotných standardních smluvních doložek je dostupný ke stažení z webových stránek Evropské komise **zde** (k dispozici pouze v anglickém jazyce).

Samotné rozhodnutí Evropské komise (tedy prozatím jeho návrh) lze označit za poměrně jednoduchý právní předpis, který čítá pouze šest článků a jehož prostudování nezabere mnoho času ani úsilí. O to větší **pozornost si naopak zaslouží samotný návrh standardních smluvních doložek**, jejichž znění může v budoucnu výrazně ovlivnit proces předávání osobních údajů do třetích zemí s nedostatečnou úrovní ochrany osobních údajů.

Evropská komise slibuje, že zaslaná zpětná vazba bude při dokončování výše popsané iniciativy zohledněna. Všechny obdržené připomínky budou zveřejněny na internetových stránkách Evropské komise.

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

Videokonference vs. ochrana osobních údajů

Ani v novém roce se videokonferencím zřejmě nevyhneme. Ujistěte se proto, že postupujete správně. Na jakém právním základě postavit zpracování osobních údajů během videokonference? Kdy použít souhlas subjektů údajů a kdy vás opravňuje plnění smlouvy? Jak zacházet se zvláštní kategorií osobních údajů či údaji třetích stran?

V minulém čísle jsme si objasnili, jaké osobní údaje jsou během videokonferencí zpracovávány a že za jejich ochranu odpovídá vždy organizátor. Popsali jsme tři možnosti provozování systému videokonference a povinnosti, které se k nim váží. Dnes se blíže podíváme na to, jaký právní základ lze využít ke zpracování osobních údajů během videokonference.

Právní základ

Pro zákonné zpracování osobních údajů osob účastnících se videokonference **potřebuje odpovědná osoba právní základ** v souladu s čl. 6 GDPR. V závislosti na kontextu zpracování je třeba použít některé z ustanovení čl. 6 odst. 1 písm. a), b), e), f) GDPR, případně další ustanovení ze zákona č. 110/2019 Sb., o zpracování osobních údajů.

Zpracování osobních údajů tedy může být **založeno na uděleném, dobrovolném a informovaném souhlasu**. Kromě souhlasu přichází v úvahu jako právní základ čl. 6 odst. 1 písm. b) GDPR – **plnění smlouvy**. Pokud v rámci plnění smlouvy neexistují alternativy k videokonferencím nebo se videokonference účastní zaměstnanci jiných společností a jiných osob, **zpracování osobních údajů může také legitimizovat oprávněný zájem** podle čl. 6 odst. 1 písm. f) GDPR, přičemž je třeba zdůraznit, že v tomto případě musí odpovědná osoba **informovat o právu vznést námitku** v souladu s čl. 21 odst. 4 GDPR.

Orgány státní správy se však nemohou spoléhat na čl. 6 odst. 1 písm. f) GDPR. V případě orgánů veřejné moci je právním základem čl. 6 odst. 1 písm. e) GDPR v souvislosti s příslušnou normou českého práva, například školský zákon.

Pro distanční výuku ve školách nemůžete využít souhlas

Souhlas subjektů údajů

Má-li být jako právní základ pro zpracování osobních údajů použit souhlas subjektů údajů, je třeba zdůraznit následující: Souhlas je účinný, pouze pokud **byl udělen informovaným způsobem a dobrovolně** (viz čl. 4 a bod 11 GDPR). Dobrovolnou účast lze předpokládat pouze tehdy, pokud k účasti na videokonferenci existuje reálná alternativa.

V profesním nebo školním kontextu je dobrovolnost často pochybná, zejména pokud jsou informace nezbytné pro výkon odborné činnosti nebo pro školní výuku sdělovány pouze v rámci videokonference. V takovém případě **nebude účast na videokonferenci obvykle dobrovolná**, takže jako právní základ **je vyloučen souhlas subjektů údajů**.

V takových případech lze o účinném souhlasu uvažovat pouze tehdy, je-li dobrovolnost zajištěna dalšími opatřeními, například **poskytnutím odpovídajících znalostí těm, kteří se nechtějí účastnit** videokonferencí, v odpovídající formě jinými prostředky nebo nabídkou jiných komunikačních prostředků (například telefonické připojení ke konferenci). Nelze-li těmito opatřeními zajistit dobrovolnost, využití videokonference nemůže být založeno na souhlasu jako právním základu, a odpovědná osoba tak musí ověřit, zda lze **založit využití videokonference na jiném právním základu**.

Odpovědnost zaměstnavatele

Pokud je osobou odpovědnou za ochranu osobních údajů zaměstnavatel, na jehož pokyn zaměstnanci používají videokonferenční systém **za účelem plnění svých smluvních a pracovních povinností**, je právní základ pro zpracování údajů **založen na zákoníku práce**. Musí však být vždy zkontrolována nutnost přenosu obrazových dat.

V kontextu pracovněprávních vztahů existuje možnost upravit zpracování osobních údajů zaměstnanců

konkrétněji prostřednictvím kolektivních smluv. Dohody mohou být použity zejména ke specifikaci obecných právních ustanovení v konkrétních případech použití, tedy **zda a jak jsou videokonference prováděny**. Úroveň ochrany GDPR však nesmí být podhodnocena.

Zvláštní kategorie osobních údajů

Pokud jsou během videokonference projednávány zvláštní kategorie osobních údajů, **například údaje o zdraví a zdravotním stavu**, musí být toto zpracování osobních údajů přípustné také podle čl. 9 odst. 2 GDPR, případně ve spojení s vnitrostátním právem. Totéž platí, pokud se videokonference týká údajů ve smyslu čl. 9 GDPR, **například náboženská výchova nebo teologická studia**.

V těchto případech **může být vyžadován samostatný souhlas**. Je však účinný pouze tehdy, pokud se jedná o výslovný souhlas. Musí tedy být informovaný, dobrovolný, předchozí, aktivní, jednoznačný pro konkrétní případ a samostatně deklarovaný a kdykoli přiměřeně odvolatelný.

Videokonference z domova

Pokud se zaměstnanci účastní videokonference z domova, nastává **problém s vhledem ostatních účastníků do soukromí** prostřednictvím obrazů nebo zvuku bez souhlasu zaměstnanců. Zaměstnavatel proto musí přijmout technická a organizační opatření (čl. 25 odst. 1 GDPR) tak, aby zajistil, že takové poznatky nebude možné získat. Toho lze například dosáhnout **vyrovnáním kamery nebo aktivací virtuálního pozadí**. Jako alternativa k těmto technickým a organizačním opatřením se nabízí souhlas zaměstnanců, přičemž by musela být zajištěna zejména dobrovolná povaha souhlasu. Vzhledem k pracovněprávnímu vztahu je však tato dobrovolnost značně problematická.

Při přenosu ze soukromí je třeba se vyhnout nevhodnému nastavení (zarovnání) kamery, **přemístění zařízení do nevhodných místností** nebo místností obsazených třetími stranami, nepřipravenému vizuálnímu a/nebo akustickému vzhledu třetích osob ve videokonferenci a podobným „poruchám".

Zpracování ze strany poskytovatelů

Pokud by poskytovatel videokonferenčních služeb zpracovával osobní údaje pro své vlastní účely, nemůže se spoléhat na právní základ, ze kterého organizátor konference vychází při svém vlastním zpracování. Potřebuje **svůj vlastní právní základ**. Totéž platí i pro školní online výuku.

Zpřístupnění osobních údajů poskytovateli služby pro jeho vlastní účely je spojeno se změnou účelu zpracování. Taková změna účelu je povolena pouze v úzkých mezích dle čl. 5 odst. 1 písm. b), čl. 6 odst. 4 GDPR. Kompatibilita účelů ve smyslu těchto požadavků obvykle nebude existovat. Kromě toho **musí být poskytnutí informací poskytovateli rovněž založeno na právním základě**. Pokud jde o zpracovatele, ve smlouvě o zpracování osobních údajů musí být zajištěno, že zpracovává osobní údaje zúčastněných osob pouze na pokyny odpovědné osoby, a nikoli pro vlastní účely.

Zpracování údajů třetích stran

Pokud jsou v rámci konference diskutovány osobní údaje **třetích osob, které se neúčastní videokonference**, a jsou tedy také zpracovávány, je třeba použít obecné právní základy. Kromě toho musí být jasně definován druh a účel zpracování osobních údajů, aby byly **splněny požadavky na transparentnost**.

Zpracování se v zásadě omezuje na účel videokonference, protože **další zpracování a vyhodnocení dat konference obvykle není nutné**. To platí zejména pro záznamy. Právní základ musí být ověřen samostatně. Výjimky jsou možné u otevřených akcí nebo veřejných seminářů a přednášek, pro které může být v jednotlivých případech nutný záznam řečníka. Pokud neexistuje žádný zvláštní požadavek opravňující záznam, **je nutné souhlas pravidelně vyžadovat** (případně dodatečně, nezávisle na souhlasu se zpracováním údajů spojeným s účastí na videokonferenci). Při plnění informačních povinností musí být zmíněna možnost záznamu.

Zvuková, obrazová a rámcová data konference **mohou být zpracovávána pouze tak dlouho, jak je to nezbytné pro přenos zpráv poskytovatelem služeb** nebo v souvislosti s potřebnou dokumentací. Uložení záznamu po ukončení konference není nutné ani slučitelné s původním účelem (čl. 5 odst. 1 písm. b), čl. 6 odst. 4 GDPR). To znamená, že jakákoli stávající **funkce nahrávání musí být ve výchozím nastavení deaktivována**. Uživatelé by měli být informováni, že nahrávání (zejména tajné) obrazových a/nebo zvukových dat, ukládání a distribuce těchto záznamů může být trestné.

Účastník videokonference musí být informován o pořizování záznamu

Odpovědnost a povinnosti organizátora

Při provozu nebo používání služby videokonference je **za zpracování osobních údajů odpovědný organizátor** a musí splnit povinnosti podle GDPR. Zodpovědné osoby musí osobám účastnícím se konference **poskytnout jasné a jednoznačné informace o zpracování osobních údajů** souvisejících s využíváním služby v souladu s články 13, 14 GDPR.

Pro zajištění transparentnosti zpracování musí být informace prezentovány tak, aby jim průměrný uživatel služby rozuměl bez zbytečného úsilí (čl. 12 a čl. 5 odst. 1 písm. a) GDPR). Je třeba **vyvarovat se příliš složitých jazykových, technických nebo právních výrazů**. Pokud se používání technických výrazů jeví jako nevyhnutelné, musí být vysvětleny srozumitelným způsobem. Zejména v případě rozsáhlých prohlášení o ochraně osobních údajů je rovněž třeba zajistit, aby byla srozumitelnost udržována prostřednictvím pochopitelné struktury a smysluplných záhlaví tak, aby dotyčné osoby mohly získat konkrétní informace.

Informační povinnosti podle čl. 13 a 14 GDPR zahrnují zejména informace o účelech, pro které a na jakém právním základě se osobní údaje zpracovávají, o tom, zda o nich může poskytovatel videokonferenční služby nebo softwaru získat informace, **po jakou dobu jsou uchovávány po ukončení konference** a zda mohou být předány do třetí země. S ohledem na své povinnosti týkající se transparentnosti (čl. 5 odst. 1 písm. a) GDPR) by odpovědné osoby měly rovněž informovat zúčastněné o typu šifrování, který se při provozu systému použije. Tyto informace jsou zvláště důležité pro účastníky, kteří se účastní videokonference na základě uděleného souhlasu.

Kromě toho musí odpovědná osoba **informovat účastníky o právním základu jednotlivých zpracovatelských operací**. Pokud se jedná o oprávněný zájem, pak musí být účastník navíc informován o svém právu vznést námitku v souladu s čl. 21 odst. 4 GDPR. Pokud se použijí různé právní základy, mělo by se zejména objasnit, **jaké operace zpracování jsou založeny na souhlasu zúčastněné osoby**. Pouze pokud si jsou účastníci vědomi své pravomoci nakládat se svými údaji, mohou také právo uplatnit (například pokud zaměstnanec neví, že použití funkce videa v rámci obchodních jednání je dobrovolná, pak pro něj nemá žádný ochranný účinek). Z pohledu odpovědné osoby existuje také riziko u operací zpracování založených na souhlasu, že **nedostatečné informace od zúčastněných osob povedou k nezákonnosti zpracování údajů**, protože zpracování osobních údajů může odůvodnit pouze informovaný souhlas (viz čl. 4 bod 11 GDPR).

Pokud poskytovatel služby zpracovává údaje pro své vlastní účely (pokud vůbec může), platí informační povinnosti také pro samotného poskytovatele služby. Organizátor by měl též **informovat účastníky o možnostech upravit nastavení aplikace** týkající se ochrany osobních údajů (například použitím pseudonymu, nastavením virtuálního pozadí a podobně). Účastníci by měli být zejména informováni o tom, zda konferenci může organizátor nahrát a uložit. Účastníci **musí být informováni o probíhajícím záznamu**, pokud je aktivována funkce nahrávání.

Kromě toho musí být zaručena práva subjektů údajů dle čl. 15 až 21 GDPR. Pokud je organizátor konference rovněž odpovědný za údaje, které služba shromažďuje i bez toho, aby k nim mohl sám organizátor přistupovat, měl by při výběru služby věnovat pozornost tomu, do jaké míry to služ-

DALŠÍ POVINNOSTI SPRÁVCE:

- **Katalog zpracování – organizace videokonference by měla být zahrnuta do seznamu zpracovatelských činností v souladu s čl. 30 GDPR.**
- **Povinnost hlásit porušení osobních údajů – v případě porušení ochrany osobních údajů v souvislosti s videokonferencí musí odpovědná osoba dodržet povinnosti podle čl. 33 a 34 GDPR.**
- **Posouzení dopadu na ochranu osobních údajů – DPIA – odpovědná osoba musí ověřit, zda je třeba zpracovat posouzení dopadu na ochranu osobních údajů v souladu s čl. 35 GDPR. Může tomu tak být zejména tehdy, jsou-li ve videokonferenci rozsáhle zpracovány zvláštní kategorie osobních údajů zúčastněných osob nebo jiných osob podle čl. 9 GDPR.**

ba umožňuje a jaké údaje ukládá. Vymazání obsahu a metadat o ukončené konferenci **musí být rovněž provedeno bezprostředně po skončení videokonference** bez ohledu na žádost subjektů údajů podle čl. 17 GDPR, protože bylo dosaženo účelu zpracování osobních údajů a **další uchovávání údajů není vyžadováno** z důvodu právní povinnosti, které odpovědná osoba podléhá dle práva Unie nebo práva jejího členského státu.

Zpracovatelská smlouva

GDPR nabízí vysokou úroveň ochrany údajů, která nesmí být ohrožena zapojením poskytovatelů služeb. Pokud je systém videokonference provozován poskytovatelem nebo má poskytovatel možnost získat přístup k osobním údajům, **musí být uzavřena smlouva o zpracování osobních údajů**. V závislosti na použitém řešení může taková možnost přístupu existovat také v systémech provozovaných odpovědnou osobou. Podle čl. 5 odst. 2 GDPR musí být odpovědná osoba schopna kdykoli prokázat, že dodržuje zásady ochrany osobních údajů. Smlouva o zpracování proto musí bezpochyby pokrývat všechny požadavky článku 28 GDPR. Nejasnosti ve smlouvě o zpracování osobních údajů jsou proto jasnými vylučovacími kritérii pro využití příslušného poskytovatele.

Přenos do třetích zemí

Za podmínek stanovených v čl. 3 odst. 2 GDPR se nařízení vztahuje také **na poskytovatele systémů videokonferencí usazených mimo EU**. Na poskytovatele ze zemí mimo EU se obvykle rovněž vztahují zákonná ustanovení jejich domovské země, a za určitých okolností tedy přístupová práva orgánů ze třetích zemí, což **ztěžuje soulad s požadavky GDPR** na ochranu osobních údajů, nebo s nimi může být v jednotlivých případech dokonce v rozporu.

Pokud jsou zvoleny videokonferenční systémy, které **povedou k přenosu dat do třetích zemí**, tedy

do zemí mimo EU nebo do Evropského hospodářského prostoru, musí přenos odpovídat zvláštním podmínkám. K těmto převodům může dojít zejména u poskytovatelů, kteří sami sídlí ve třetích zemích nebo kteří využívají subdodavatele ze třetích zemí. Údaje se také přenášejí do třetích zemí, pokud poskytovatel nebo dílčí zpracovatel přistupuje k údajům zpracovávaným v EU ze třetí země.

Evropská komise rozhodla, že v některých třetích zemích existuje odpovídající úroveň ochrany údajů. V takovém případě už nemusí být splněny žádné další **podmínky pro přípustnost přenosu osobních údajů** (čl. 45 GDPR). Vzhledem k tomu, že rozsudkem ESD C-311/18 (Schrems II) bylo rozhodnutí Komise EU o tzv. Privacy Shieldu prohlášeno za neplatné, tak již není k dispozici jako prostředek k zajištění odpovídající úrovně ochrany v USA. Podmínky pro přenos mohou být nadále **dodrženy prostřednictvím standardních smluvních doložek** Komise EU, které správce uzavírá s poskytovatelem jako zpracovatelem.

Při přenosu dat do třetích zemí musí odpovědné osoby zkontrolovat, zda zvolené nástroje předávání zaručují, že osobní údaje, které mají být předány do třetí země, požívají v zásadě **stejné ochrany během přenosu a v samotné třetí zemi jako v EU**, případně přijmout další opatření k zajištění této ochrany. Pokud nedostatečná úroveň ochrany vyplývá z možností oficiálního přístupu třetí země k ochraně osobních údajů, je obtížné si představit dostatečná dodatečná opatření v oblasti videokonferenčních služeb, protože alespoň určité rámcové údaje o konferencích musí být poskytovateli z technických důvodů přístupné.

Podle čl. 5 odst. 2 GDPR musí být osoby odpovědné za používání videokonferenčních služeb schopny **prokázat, že provedly tuto kontrolu** a že údaje ve třetí zemi jsou odpovídajícím způsobem chráněny v souladu s těmito normami. Dne 23. července 2020 již Evropský výbor pro ochranu údajů (EDSA) rozhodl o často kladených otázkách týkajících se účinků rozsudku obecně a důsledků pro jednotlivé přenosové nástroje.

▪▪▪

Ing. Mgr. Luděk Nezmar, MBA

Poradna

V rámci roční kontroly dodržování povinností stanovených GDPR pro zpracování a ochranu osobních údajů bychom chtěli pořídit zprávu o provedení této kontroly, jejíž součástí by byl i případný výčet zjištěných nedostatků, jakož i návrh na vhodná řešení. Můžete nám poskytnout nějaký vzorový checklist s položkami a oblastmi, které by měla daná kontrolní zpráva obsahovat?

V případě, že se provádí tzv. „re-audit", měla by na jeho závěru skutečně být závěrečná zpráva. Co se týče jejího obsahu, v ideálním případě by měla obsahovat alespoň zjištěné nedostatky a jejich klasifikaci podle rizika (a to jak z hlediska práv subjektů údajů, tak i z hlediska případné kontroly ze strany ÚOOÚ). V ideálním případě by taková zpráva měla obsahovat rovnou i implementační plán s návrhy, jak zjištěné nedostatky odstranit a v jakém pořadí.

Co se týče oblastí, na které by se tento re-audit měl zaměřit, v zásadě se nemění od původního auditu. Způsobů, jak k auditu přistupovat, je poměrně dost, nicméně nejvíce efektivní je následující postup.

V první řadě je nutno zkontrolovat, zda jsou záznamy o činnostech zpracování kompletní a neprobíhá operace zpracování, která by nebyla v takových záznamech (popřípadě v jiné dokumentaci) zanesena. První fáze auditu se tak musí týkat toho, zda je seznam všech operací kompletní a správce je schopen doložit, jaké osobní údaje jsou skutečně zpracovávány. Ačkoliv vedení záznamů o činnostech zpracování může být v některých případech dobrovolné, pravdou je, že platí doporučení, aby byly vedeny vždy.

Pokud zkontrolujete, že dané záznamy jsou úplné, můžete pokračovat dále. Pokud úplné nejsou, je přirozeně potřeba je doplnit.

Jak tedy pokračovat dále? Nejúčinnější metoda je prověřit každý záznam zpracování osobních údajů zvlášť, a to z následujících hledisek, která vycházejí z jednotlivých zásad:

- Zásada zákonnosti, korektnosti a transparentnosti
  - Právní základ (Je zvolen správně, je vše dobře definováno?)
  - Plnění informační povinnosti
  - Kontrola evidence zpracovatelů, existence zpracovatelských smluv
- Zásada účelového omezení
  - Jak je definován účel a zda není překračován
- Zásada minimalizace údajů
  - Kontrola rozsahu údajů
  - Kontrola přístupů k údajům (privacy by default)
- Zásada přesnosti
  - Kontrola mechanismu oprav údajů
- Zásada omezení uložení
  - Kontrola dob uchování
- Zásada integrity a důvěrnosti
  - V případě bezpečnosti záleží na velikosti organizace a povahy zpracování, někdy stačí udělat kontrolu dodržování organizačních opatření, někde je vhodné provést komplexní bezpečnostní audit.
- Zásada odpovědnosti
  - Kontrola veškeré interní dokumentace (zda existuje a pokud ano, zda je aktuální);
  - Kontrola ostatních povinností dle GDPR (například ve vztahu k pověřenci a podobně).

Důležité samozřejmě je to, s čím se skutkový stav porovnává. Proto doporučuji obohatit své znalosti o aktuální rozhodovací praxi, relevantní podklady ze strany WP29, potažmo EDPB, a mít přehled o stavu ochrany osobních údajů v rámci EU.

Pokud se budete držet výše uvedených oblastí, objevíte další detailní povinnosti, u nichž je nutno zhodnotit, zda jsou splněny, či nikoli. ▪▪▪

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:
- **Jak na reaudit?**
- **Předávání údajů do VB po Brexitu – co se změní?**

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. 12. 2020 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.