4.1 Záznamy o činnostech zpracování[1]

Správci i zpracovatelé osobních údajů jsou povinni dokumentovat, jaká zpracování osobních údajů provádí, za jakým účelem, a jaké jsou některé další parametry zpracování. GDPR ukládá, aby správci i zpracovatelé tuto povinnost plnili formou písemně vedených záznamů o činnostech zpracování. Ty mají sloužit nejen správci a zpracovateli k tomu, aby měl přehled o své činnosti, ale správce a zpracovatel je povinen záznamy kdykoliv na vyžádání předložit dozorovému úřadu, Úřadu pro ochranu osobních údajů, který je může využít pro monitorování souladu činnosti dané organizace s GDPR.

Tato povinnost se nevztahuje na správce či zpracovatele osobních údajů, kteří mají méně než 250 zaměstnanců a zároveň:

- Neprovádějí zpracování, které může představovat riziko pro práva dotčených osob; riziko může být spatřováno např. ve větším rozsahu zpracovávaných údajů, prostředcích zpracování (profilování, dlouhodobé sledování dotčené osoby) či účelu zpracování (přiznávání práv či povinnosti, uzavření smlouvy atd.).
- Jimi prováděné zpracování osobních údajů není pouze příležitostné; pokud je zpracování osobních údajů nezbytné pro hlavní předmět činnosti správce (např. poskytování či zprostředkování nebankovních úvěrů nebo pojištění fyzickým osobám, monitorování veřejně přístupných prostor, poskytování cloudových služeb pro zpracování osobních údajů), tato výjimka se neuplatní, i pokud by organizace měla méně než 250 zaměstnanců.
- Nezpracovávají citlivé osobní údaje (informace o národnostním či etnickém původu, zdravotním stavu, genetické či biometrické údaje atd.). Pokud je součástí hlavní činnosti správce nebo zpracovatele zpracování citlivých osobních údajů (např. provádí genetické testy, nebo se podílí na zpracování biometrických údajů), výjimka z povinnosti vést záznamy o činnostech zpracování se rovněž neuplatní.

GDPR výslovně vypočítává, jaké informace musí v záznamech vést správce a jaké zpracovatel osobních údajů.

U správce se jedná o:

- Jméno (identifikaci) a kontaktní údaje správce a jméno a kontaktní údaje pověřence pro ochranu osobních údajů, pokud byl u správce jmenován.
- Účely zpracování. O pojmu účel zpracování bylo pojednáno výše, i v rámci záznamů o činnostech zpracování je vhodné účely definovat šířeji pro související operace zpracování. Typickými účely zpracování tak bude např. shromažďování osobních údajů pro marketing, zasílání marketingových nabídek, uzavírání a plnění smluv s klienty, ověřování klientů, vymáhání pohledávek, ale i ochrana majetku (kamerovým nebo jiným sledovacím systémem), personální agenda, mzdová agenda atd.
- Ke každému účelu zpracování je správce povinen uvést kategorii dotčených osob (klienti, bývalí klienti, zaměstnanci, návštěvníci kamenné pobočky) a kategorii zpracovávaných údajů (identifikační údaje, kontaktní, popisné, údaje o spotřebitelském chování atd.)
- Kategorie příjemců, kterým budou nebo mohou být osobní údaje předávány. Typicky půjde o další členy podnikatelské skupiny, orgány státní správy a dále zpracovatele podílející se na některých částech zpracování (shromažďování údajů, poskytovatel cloudových či obecně IT služeb, externí archiv, externí účtárny atd.).

[1] Čl. 30 GDPR.

- Informace o předání osobních údajů do třetí země, její určení a označení záruk pro ochranu osobních údajů v některých specifických situacích, kdy nejsou využity běžné nástroje (standardní smluvní doložky, závazná podniková pravidla atd.).[2]
- Je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií osobních údajů. Pokud není možné konkrétní lhůtu uvést, lze ji definovat obecně, např. tři roky po skončení smluvního vztahu.
- Je-li to možné, obecný popis technických a organizačních bezpečnostních přijatých k ochraně zpracovávaných osobních údajů. Pokud jsou bezpečnostní opatření dokumentována jinde, ve vnitřních předpisech, technické dokumentaci atd., lze na tyto dokumenty v rámci záznamů jenom odkázat nebo je k záznamům přiložit.

Organizace je povinna záznamy o činnostech zpracování vést i pro ta zpracování, kde vystupuje jako zpracovatel, která osobní údaje zpracovává dodavatelsky – tzn. pro někoho jiného.
V takovém případě musí záznamy obsahovat následující položky:

- Jméno (identifikaci) a kontaktní údaje zpracovatele a jméno a kontaktní údaje pověřence pro ochranu osobních údajů, pokud byl u zpracovatele jmenován.
- Identifikaci správce, pro kterého zpracovatel osobní údaje zpracovává
- U každého správce potom kategorii (druh) zpracování, které pro něj zpracovatel provádí. Může se jednat např. shromažďování kontaktních údajů zájemců o produkt a jejich předávání správci, provozování cloudových služeb, zajišťování kamerové ostrahy budovy správce, likvidace nosičů osobních údajů atd.
- Informace o předání osobních údajů do třetí země, její určení a označení záruk pro ochranu osobních údajů v některých specifických situacích, kdy nejsou využity běžné nástroje (standardní smluvní doložky, závazná podniková pravidla atd.).
- Je-li to možné, obecný popis technických a organizačních bezpečnostních přijatých k ochraně zpracovávaných osobních údajů. I pro zpracovatele platí, že pokud jsou bezpečnostní opatření, která pro ochranu zpracovávaných údajů přijal, dokumentována jinde, lze tyto další dokumenty k záznamům přiložit nebo na ně odkázat.

Záznamy musí být vedeny písemně, aby mohly být kdykoliv předloženy dozorovému úřadu. Písemnou formou se rozumí i elektronické vedení záznamů, ať už v některém z obecných nástrojů (textový editor, tabulkový editor), nebo jako samostatné aplikace na správu a udržování záznamů o zpracování.

Věděli jste, že:

GDPR ruší tzv. registrační povinnost pro nová zpracování osobních údajů? Podle zákona o ochraně osobních údajů byl správce povinen většinu nových zpracování předem oznámit Úřadu pro ochranu osobních údajů. Tato povinnost se však v praxi příliš neosvědčila, a proto od ní bylo upuštěno a je zčásti nahrazena právě povinností vést záznamy o činnostech zpracování.

Co si odnést do praxe:

- Záznamy o činnostech zpracování jsou povinni vést všichni správci a zpracovatelé, kteří mají více než 250 zaměstnanců. Ti, kteří mají zaměstnanců méně, jsou povinni záznamy vést tehdy, pokud provádějí zpracování představující významné riziko pro dotčené osoby, pravidelné a systematické zpracování osobních údajů či zpracovávají citlivé osobní údaje.

[2] Ke specifický pravidlům pro předávání osobních údajů do třetích zemí a možných zárukách pro ochranu práv dotčených osob srov. kapitolu 4.4.

- I pokud na správce či zpracovatele povinnost vést záznamy o činnostech zpracování nedopadá, lze doporučit, aby měl alespoň základní přehled o tom, za jakými účely údaje zpracovává, na základě jakých právních důvodů a o jaké údaje se jedná.
- Je nezbytné určit odpovědnou osobu či útvar, který záznamy povede a bude je průběžně aktualizovat. Pokud je u správce či zpracovatele zřízen pověřenec pro ochranu osobních údajů, je vhodné tuto agendu svěřit jemu.
- Aby záznamy byly aktuální, je vhodné všem útvarům správce či zpracovatele uložit povinnost průběžně informovat o změně v jimi prováděných zpracováních. Stejně tak je vhodné, aby pověřenec pro ochranu osobních údajů či jiná osoba, která za záznamy odpovídá, v pravidelných intervalech dotčené útvary vyzývala k potvrzení aktuálnosti, správnosti a úplnosti záznamů o jimi prováděných činnostech zpracování údajů.
- Správce či zpracovatel může v záznamech ke každému zpracování evidovat i další informace, aby pro něj záznamy byly využitelnější, například interní předpis, ve kterém je dané zpracování popsáno, odpovědnou osobu, související produkt, použité IT systémy či aplikace atd.