

15. 6. 2016

Veźměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Evropská unie schválila konečnou podobu obecného nařízení o ochraně osobních údajů

Evropská unie po několikaletém vyjednávání definitivně přijala obecné nařízení o ochraně osobních údajů, které vstoupilo v platnost dne 24. května 2016.[1] Podniky se musí přizpůsobit novým pravidlům nejpozději do 25. května 2018, kdy nařízení nabude účinnosti a začne se aplikovat na celém území EU. Na co všechno se musí firmy adaptovat a jaké sankce jim hrozí v případě neplnění povinností? Odpovědi naleznete v tomto článku.



Jednotná pravidla ve všech zemích EU

Na úvod je třeba říci, že nařízení přinese pro podniky i řadu výhod. Zejména umožní volný pohyb osobních údajů v rámci jednotného digitálního trhu EU. Nařízení je totiž přímo účinné a sjednocuje právní úpravu regulující ochranu osobních údajů ve všech členských státech EU. Dosavadní národní zákony budou zrušeny a odstraní se tak rozdíly v právní regulaci ochrany osobních údajů v členských státech EU, která se nyní v mnohém liší, přestože vnitrostátní předpisy jsou harmonizovány směrnici.[2]

Evropská unie usiluje o to, aby stejná pravidla pro zpracování osobních údajů platila také pro konkurenci ze třetích zemí mimo EU. Proto by se nařízení mělo vztahovat i na zpracování osobních údajů, které provádí společnosti neusazené na území EU, pokud zpracování údajů souvisí s nabídkou zboží nebo služeb osobám s bydlištěm v EU anebo pokud zpracování údajů souvisí s monitorováním osob s bydlištěm v EU, k němuž dochází v rámci EU. Záměr je to vskutku ambiciózní, nicméně o jeho skutečné realizaci lze pochybovat, neboť kompetence orgánů EU jsou ve vztahu k subjektům z nečlenských států dosti omezené.

Nové povinnosti

Mnoho povinností stanovených nařízením vyplývá již ze současné české právní úpravy obsažené v zákoně č. [101/2000](#) Sb., o ochraně osobních údajů. Nařízení je však upřesňuje nebo rozšiřuje. Nadále bude platit, že osobní údaje lze zpracovávat pouze na základě souhlasu subjektu údajů nebo jiného legitimního důvodu (např. je-li zpracování nezbytné pro splnění smlouvy, právní povinnosti nebo pro účely oprávněných zájmů správce údajů apod.). Souhlas se zpracováním osobních údajů musí být podle nařízení svobodný, konkrétní, informovaný a jednoznačný. Povinnost předem informovat subjekt údajů o zpracování údajů a o jeho právech tedy rovněž zůstane zachována, ale částečně se mění její obsah především s ohledem na některá nová práva subjektů údajů (např. právo na přenositelnost údajů[3]).

Nařízení dále mění povinné náležitosti smlouvy o zpracování osobních údajů, kterou musí správce údajů uzavřít se zpracovatelem, kterému předal údaje ke zpracování. Ovšem na rozdíl od současného českého zákona nařízení nevyžaduje písemnou formu této smlouvy a umožňuje, aby byla uzavřena i v elektronické podobě bez zaručeného elektronického podpisu.

Podle nového nařízení správci údajů již nebudou muset splnit tzv. oznamovací povinnost (povinnost registrace) u příslušného orgánu dozoru (v ČR u Úřadu pro ochranu osobních údajů) před zahájením zpracování osobních údajů. Tato povinnost však bude nahrazena tím, že každý správce údajů anebo jeho případný zástupce musí vést záznamy o všech činnostech zpracování údajů, za něž odpovídají. Nově budou správci údajů také povinni ohlásit každé závažnější porušení ochrany osobních údajů, a to jak orgánu dozoru bez zbytečného odkladu (nejpozději do 72 hodin), tak dotčeným subjektům údajů bez zbytečného odkladu.

Další administrativní zatížení bude pro některé firmy představovat povinnost vypracovat posouzení vlivu na ochranu osobních údajů a povinnost předchozí konzultace s orgánem dozoru. Tato povinnost dopadne především na společnosti, které provádí ve velkém rozsahu tzv. profilování[4] nebo zpracování citlivých údajů (např. banky, pojišťovny) anebo systematické monitorování veřejně přístupných prostorů.

Nařízení zavádí v ČR novou funkci pověřence pro ochranu osobních údajů. Obligatočně ho musí jmenovat každý správce nebo zpracovatel, pokud zpracování provádí orgán veřejné moci nebo jejich hlavní činnosti spočívají ve zpracování, které kvůli své povaze, rozsahu nebo účelům vyžaduje rozsáhlé, pravidelné a systematické monitorování subjektů údajů, anebo jejich hlavní činnosti spočívají v rozsáhlém zpracování citlivých údajů. Ostatní správci nebo zpracovatelé mohou pověřence jmenovat dobrovolně. Pověřencem může být zaměstnanec podniku nebo i externista, který uzavře s podnikem smlouvu o poskytování služeb. Jeho úkoly zahrnují především poskytování informací a poradenství správcům nebo zpracovatelům údajů a jejich zaměstnancům, monitorování souladu zpracování údajů s nařízením a spolupráci s dozorovým orgánem.

Nařízení dále zakotvuje právo subjektů údajů na výmaz údajů („právo být zapomenut“), které bylo dovozeno již v rozsudku Soudního dvora EU z května 2015 týkajícího se španělského Googlu (C-131/12). Toto právo umožňuje jednotlivcům, aby na základě jejich žádosti provozovatelé webových prohlížečů odstranili některé osobní údaje z vyhledávače a zároveň informovali správce údajů, kteří údaje zpracovávají, aby vymazali veškeré odkazy na tyto osobní údaje včetně jejich kopií.

Cookies

Dlouhou dobu diskutovanou otázku, zda mezi osobní údaje patří i cookies, řeší nařízení tak, že výslovně stanoví, že osobními údaji mohou být i síťové identifikátory jako například IP adresa nebo právě cookies. Jestliže prostřednictvím cookies nebo i jiných údajů bude možné identifikovat konkrétní osobu, tak si provozovatelé webových stránek musí podle nařízení vyžádat předchozí souhlas s používáním takových cookies (až na některé výjimky). Stávající česká právní úprava naproti tomu souhlas s používáním cookies nevyžaduje, nýbrž postačí pouze jasně a srozumitelně informovat uživatele webových stránek a umožnit mu odmítnout používání cookies. Je však nutné říci, že český Úřad pro ochranu osobních údajů již nyní upozorňuje na to, že cookies mohou být považovány za osobní údaje a v takovém případě musí být dán předchozí souhlas s jejich používáním.

Transfer údajů mimo EU

Úprava předávání osobních údajů do zemí mimo EU zůstane víceméně stejná. Údaje mohou být předány do třetí země bez zvláštního povolení, pokud Evropská komise rozhodla tzv. rozhodnutím o

přiměřenosti, že daná země splňuje požadovanou úroveň ochrany osobních údajů. Těmito státy jsou například Švýcarsko, Izrael nebo Kanada. Na podzim minulého roku Soudní dvůr EU zrušil rozhodnutí upravující zvláštní režim „Safe Harbor“ („bezpečný přístav“) pro transfer dat do USA. Safe Harbor má být nahrazen novým režimem nazvaným „Privacy Shield“ („štít soukromí“).[5] Jeho schválení se očekávalo již v červnu, ovšem nyní se zřejmě pozdrží, jelikož pracovní skupina WP 29 vydala stanovisko, ve kterém nový režim Privacy Shield zásadně kritizuje a požaduje jeho doplnění.

Pokud není pro třetí zemi, kam mají být údaje předány, schváleno rozhodnutí Komise o přiměřenosti, tak podle nařízení bude možné předávat údaje do těchto zemí bez zvláštního povolení dozorového orgánu za předpokladu, že subjektům údajů budou poskytnuty vhodné záruky. Těmi jsou především standardní smluvní doložky a závazná podniková pravidla („binding corporate rules“) schválená dozorovým orgánem, jež se používají již podle současné právní úpravy.[6]

Sankce

Přestože podniky mají dva roky na to, aby se na nové nařízení připravily, tak by se s ním měly seznámit co nejdříve. Za porušení povinností vyplývajících z nařízení totiž hrozí vysoké pokuty. Příslušný dozorový orgán může uložit peněžitou pokutu v případě méně závažného porušení až do výše 10 mil. EUR nebo u podniku až 2 % celkového ročního světového obrátu a v případě závažnějšího porušení až do 20 mil. EUR nebo u podniku až 4 % celkového ročního světového obrátu.

Vysokým sankcím mohou firmy účinně předejít tím, že aktualizují svoji stávající dokumentaci týkající se osobních údajů (zejm. ustanovení smluv se zákazníky, smlouvy o zpracování údajů a interní předpisy) a že začnou vést řádnou evidenci o všech zpracovávaných údajích. Současně musí zavést další vhodná technická a organizační opatření, která zajistí bezpečnost zpracovávaných údajů a soulad zpracování s nařízením. Splnění požadovaného standardu ochrany osobních údajů mohou firmy prokázat například tím, že se přihlásí k dodržování kodexů chování nebo osvědčení schválených příslušným dozorovým orgánem anebo že ve svých podnicích vytvoří funkci pověřence pro ochranu osobních údajů.



JUDr. Martin Kartner,
partner

Mgr. Bc. Jiří Prouza,
advokátní koncipient

[CHSH Kališ & Partners s.r.o., advokátní kancelář](#)

Týn 639/1
110 00 Praha 1 - Staré Město

Tel.: +420 221 111 711
Fax: +420 221 111 725
e-mail: office@chsh.cz

-
- [1] Celé znění nařízení - dostupné na [www](#), k dispozici >>> [zde](#).
- [2] Dosavadní směrnice č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů bude s účinností nařízení zrušena.
- [3] Na základě tohoto práva bude mít subjekt údajů právo získat osobní údaje, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a právo předat tyto údaje jinému správci.
- [4] Profilováním se podle nařízení rozumí „jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.“ Typicky se jedná o cílenou reklamu, kdy dochází ke sledování chování zákazníka, na základě něhož se vyhodnocují jeho preference.
- [5] O novém režimu Privacy Shield a procesu jeho přijetí jsme již informovali v dřívějším článku Privacy Shield – Nový režim pro transfer osobních údajů z EU do USA, který je dostupný na [www](#), k dispozici >>> [zde](#).
- [6] Více informací o pravidlech pro předávání osobních údajů do zemí mimo EU najdete v našem článku Změna způsobu předávání osobních údajů do USA, který je dostupný na [www](#), k dispozici >>> [zde](#).

© EPRAVO.CZ – Sběrka zákonů, judikatura, právo | www.epravo.cz

Další články:

- [Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?](#)
- [Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor](#)
- [Novinky z české a evropské regulace finančních institucí za měsíc březen 2026](#)
- [Novelizace nařízení EU o odlesňování \(EUDR\)](#)
- [Zneužití práva na přístup podle GDPR](#)
- [Doručování soudních písemností ze zahraničí do ČR](#)
- [Novinky z české a evropské regulace finančních institucí za měsíc únor 2026](#)
- [Digital Fairness Act a influencer marketing – cesta ke konci roztříštěnosti regulace?](#)
- [Novinky z české a evropské regulace finančních institucí za měsíc leden 2026](#)
- [IATA Travel & Cargo akreditace v letectví – v čem spočívají její výhody?](#)
- [Digital Omnibus o AI: návrh nařízení o zjednodušení pravidel pro umělou inteligenci](#)