16. 8. 2017

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

GDPR

GDPR, v překladu obecné nařízení o ochraně osobních údajů[1], je v současnosti nejvíce skloňovaným tématem, co se týče evropského práva. Zatímco novou směrnici o ochraně obchodního tajemství[2], která má být implementována do 9. 6. 2018, nebo návrh nařízení o zajištění přeshraniční přenositelnosti on-line služeb poskytujících obsah v rámci vnitřního trhu (se zamýšlenou účinností od 17.5.2018)[3], přešla veřejnost, až na odborné spektrum zaměřující se na právo duševního vlastnictví, více méně bez povšimnutí, odpočet do účinnosti GDPR nezadržitelně pokračuje a plní stránky denního tisku.

ADVOKÁTNÍ KANCELÁŘ
KŘÍŽ A PARTNEŘI

Přibývá množství více či méně spolehlivých výkladů a rozborů, brožur, seminářů a školení a roste i nabídka možností, jak se s požadavky GDPR v praxi vypořádat. Rostoucí zájem o tuto problematiku je však zcela na místě. Mnoha správcům osobních údajů po zjištění rozsahu konkrétních opatření, které musí zavést, se květnová lhůta už nyní zdá být příliš krátká, byť zbývá bezmála rok.

GDPR se prezentuje jako pokroková legislativa k ochraně práva na informační sebeurčení ve složitém prostředí kyberprostoru a jednotící rámec povinností správců osobních údajů na jednotném digitálním trhu. Ve svých důsledcích jde ale především o praktické cvičení, jímž bude muset projít každý správce osobních údajů vždy individuálně podle typu, rozsahu a způsobu zpracování osobních údajů, se kterými při své činnosti pracuje. Nejčastější z argumentů proti GDPR, hned vedle výše hrozících sankcí, jsou právě náklady, které bude muset každý správce vynaložit na soulad s GDPR, a nejasnost požadavků nařízení.

Cílem tohoto článku je krátce připomenout několik způsobů, jak náklady omezit a zároveň poukázat na některé základní problémy, které GDPR v praxi přináší. Problematické mohou být nejasnosti, daná jednak nutností výkladu některých ustanovení a vedle toho i možností odchylek v rámci národních právních úprav jednotlivých členských států. Jednotlivé členské státy mají prostor zejména dále zpřísnit požadavky GDPR, čehož využilo mezi dalšími například Německo. Nová německé legislativa mimo jiné rozšiřuje okruh správců, které musí jmenovat pověřence pro ochranu osobních údajů („DPO“), nebo zpřísňuje pravidla pro nakládání s osobními údaji zaměstnanců. [4]

Jedním z nejméně sporných a zároveň nejvíce přehlížených faktů je skutečnost, že GDPR se vztahuje nejen na správu osobních údajů v digitální podobě, ale také na fyzické, „papírové“ databáze v podobě kartoték a archivů. Ty dnes již nejsou právě běžné, to však neznamená, že správci údajů s nimi nemusí nakládat v souladu s GDPR.

Ačkoliv nařízení je zaměřeno především na řešení postupů a bezpečnostních rizik, majících technickou povahu, konkrétní řešení, která uvádí, jsou ponejvíce administrativního charakteru. I doporučovaná ISO jsou jen obecným návodem, jak zajistit úvodní audit a další organizační postupy pro implementaci GDPR. Každý správce osobních údajů by měl v první řadě bezpodmínečně provést právní posouzení postupů při zpracování osobních údajů a v rámci něj nechat vypracovat návrhy nutných změn pro zajištění souladu s GDPR.

V zásadě vždy je nutné revidovat smlouvy se subjekty údajů a znění získávaných souhlasů se zpracováním osobních údajů od subjektů údajů, ať už zaměstnanců, zákazníků nebo obchodních partnerů. Nezbytné je rovněž provést revizi interních směrnic a postupů při zpracování osobních údajů a zajistit jejich soulad s nařízením a rovněž připravit dokumenty, potřebné pro prokazování souladu s GDPR na základě principu odpovědnosti.

V neposlední řadě je pak potřebné nastavit pravidla nejen pro zpracování osobních údajů, ale také pro komunikaci se subjekty údajů a pro řešení a komunikaci bezpečnostních incidentů.

Přestože audit a následná řešení je nezbytné provádět individuálně a nelze se bez dalšího spoléhat na obecné rady, čas a finance lze šetřit například tak, že někteří správci s povinností jmenovat DPO se mohou rozhodnout pro sdíleného DPO. Pro sdružení nebo jiné subjekty zastupující různé kategorie správců nebo zpracovatelů osobních údajů lze pak doporučit postup podle článku 40 GDPR, tedy vypracování kodexů chování, které sjednotí postupy v souladu s GDPR. Do budoucna bude možné se obracet také na certifikované poskytovatele pečetí, známek a osvědčení o ochraně údajů, které budou prokazovat soulad s GDPR, když v České republice pravidla pro poskytování osvědčení o ochraně osobních údajů aktuálně připravuje Úřad pro ochranu osobních údajů.[5]

Více než doporučit lze také monitoring dalšího vývoje výkladu GDPR a jeho faktické aplikace i po 25. 5. 2018, neboť stanoviska WP29 a jednotlivých národních orgánů dohledu, ale také první právní spory, jak ve správním, tak v civilním řízení, budou přinášet cenná zpřesnění odpovědí na praktické otázky ohledně GDPR.

Aktuálně je vhodné věnovat pozornost činnosti WP29, a to zejména vydaným vodítkům k implementaci GDPR, týkajících se přenositelnosti osobních údajů[6] a institutu DPO[7], a stanovisku ke zpracovávání osobních údajů v souvislosti se zaměstnáním[8]. S ohledem na skutečnost, že zaměstnanecké údaje zpracovává v zásadě každý správce údajů bez výjimky, a to i společnosti, které by jinak neměly důvod se domnívat, že by je GDPR mohlo zasáhnout, budeme se nyní blíže věnovat tomuto stanovisku.

Stanovisko WP29 ke zpracovávání osobních údajů v souvislosti se zaměstnáním

Nové stanovisko představuje aktualizaci stanoviska z roku 2001[9], zejména s ohledem na nové technologie, a zabývá danou problematikou i s ohledem na GDPR. Stanovisko používá pouze výraz „work“ a nikoli „employment“ jako dřívější dokument, aby byly pokryty i instituty obdobné pracovnímu poměru. I zde je důležitý důraz, kladený na princip minimalizace, který je jedním ze základních principů zpracování osobních údajů podle GDPR, v tomto případě požadavek výběru opatření, které nejméně narušuje soukromí zaměstnance a také minimalizace shromažďovaných dat.

Zpracovávání tohoto typu údajů je podle GDPR jednou z oblastí, kterou mohou dále upravovat členské státy, ať už právními předpisy či v kolektivních smlouvách. Pravidla však dle požadavku GDPR vždy musí obsahovat zvláštní a vhodná opatření, zajišťující ochranu lidské důstojnosti, oprávněných zájmů a základních práv subjektů údajů, především pokud jde o transparentnost zpracování, předávání osobních údajů v rámci skupiny podniků a systémy monitorování na

pracovišti. Stanovisko se zabývá zpracováním osobních údajů ve fázi výběru zaměstnanců a celosvětově právně spornými otázkami jako jsou např. monitorování aktivit zaměstnanců na sociálních sítích, monitorování používání informačních technologií mimo pracoviště (v kontextu stále častějších případů práce z domova, využívání vlastních přístrojů zaměstnanců při práci nebo dálkového přístupu do zařízení), a to například také v souvislosti s přeshraničním předáváním osobních údajů třetím stranám.

JUDr. Veronika Křížová, LL.M.,
advokátka

Gabriela Kadlecová,
studentka

Advokátní kancelář Kříž a partneři s.r.o.

Rybná 9
110 00 Praha 1

Tel.: +420 224 819 334
Fax: +420 224 819 343
e-mail: info@ak-kp.cz

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ("GDPR" nebo "nařízení").
[2] Směrnice Evropského parlamentu a Rady (EU) 2016/943, ze dne 8. června 2016, o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich neoprávněným získáním, využitím a zpřístupněním.
[3] Návrh nařízení Evropského parlamentu a Rady o zajištění přeshraniční přenositelnosti on-line služeb poskytujících obsah v rámci vnitřního trhu, COM/2015/0627 - 2015/0284 (COD).
[4] Novela zákona č. 204-03, Bundesdatenschutzgesetz ze dne 9.3.2017.
[5] Sdělení Úřadu pro ochranu osobních údajů o postupu při vydávání osvědčení o ochraně osobních údajů podle GDPR, dostupné na www, k dispozici >>> zde.
[6] Article 29 Data Protection Working Party Guidelines on the right to data portability, ze dne

13.12.2016, v revizi ze dne 5.4.2017
[7] Article 29 Data Protection Working Party Guidelines on Data Protection Officers (‘DPOs’), ze dne 13.12.2016, v revizi ze dne 5.4.2017
[8] Article 29 Data Protection Working Party Opinion 2/2017 on data processing at work, ze dne 8.6.2017
[9] Article 29 Data Protection Working Party Opinion 8/2001 on the processing of personal data in the employment context, zed ne 13.9.2001

Další články:

- Novinky z české a evropské regulace finančních institucí za měsíc duben 2026
- Dvě kiwi denně: EU schválila první zdravotní tvrzení pro čerstvé ovoce
- 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