Březen 2017

Škola ochrany osobních údajů

advokátní kanceláře Balcar, Polanský & Spol. s.r.o.

Nařízení EP a Rady (EU) 2016/679 z 27. dubna 2016, tzv. Všeobecné nařízení o ochraně údajů („Nařízení") zrušilo směrnici 95/46/ES („Směrnice"), která je nyní transformována do českého právního řádu zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Nařízení vstoupí v účinnost dnem 25. května 2018, kdy se stane přímo účinným rovněž v České republice a dotkne se všech, kteří osobní údaje zpracovávají, jakož i fyzických osob, jejichž osobní údaje jsou předmětem zpracování, tedy téměř každého.

Vzhledem k dosud nejvýznamnější legislativní změně evropského rozměru v oblasti ochrany osobních údajů Vám s týdenní frekvencí přinášíme pravidelné informace pro snadnější a efektivnější orientaci v množství povinností, které Nařízení přináší.

Pokud si přejete odebírat Školu osobních údajů přímo do Vaší e-mailové schránky, prosím přihlaste se na adrese office@bapol.cz, popř. na tel. čísle +420 251 009 111.

Lekce 2 z 16

Zásady ochrany osobních údajů

V textu se dozvíte:

Důležité změny

- V důsledku nově zavedené zásady odpovědnosti budou společnosti/instituce zpracovávající si samy osobní údaje (správci) povinny nejen dodržovat, ale také prokázat, že osobní údaje zpracovávají v souladu se zásadami ochrany osobních údajů

Compliance: Akční plán

Správci by měli před nabytím účinnosti Nařízení:

- provést audit zpracovávání osobních údajů, zaměřený na nové povinnosti;
- vytvořit (resp. aktualizovat existující) vnitřní předpisy upravující zpracovávání, aktualizovat pracovní řád v rozsahu monitorování zaměstnanců a ochrany jejich osobních údajů, zrevidovat pracovní smlouvy zaměstnanců oprávněných zpracovávat osobní údaje a všechny ostatní dokumenty týkající se zpracovávání;
- zajistit a moci prokázat vyškolení svých zaměstnanců, kteří mají přístup k osobním údajům, ohledně jejich práv a povinností a poučit je o následcích porušení jejich povinností.

K zásadám ochrany osobních údajů

Zásady ochrany osobních údajů ve smyslu Nařízení jsou podobné těm, které upravovala Směrnice a které jsou obsaženy také v aktuálním znění zákona č. 101/2000 Sb., o ochraně osobních údajů. Nařízení je však podrobněji specifikuje a rozšiřuje.

Zákonnost, korektnost, transparentnost

Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem.

Pro účely splnění podmínky transparentnosti se společnosti / instituce budou muset vypořádat s povinností poskytnout subjektům údajů, jejichž osobní údaje zpracovávají, rozsáhlý balík informací. Subjekty údajů by měly být dostatečně jasně a srozumitelně informovány o podmínkách zpracovávání a o právech, která mají v této souvislosti.[1]

Seznam informací, které budou správci povinni prokazatelně oznámit subjektům údajů před zahájením zpracovávání, je v porovnání se Směrnici podstatně širší a zahrnuje kromě jiného právo na vymazání (tj. „právo být zapomenut"[2]), právo napadnout zpracovávání nebo podat stížnost orgánu dohledu nebo právo, aby se na subjekt údajů nevztahovalo rozhodnutí založené výhradně na automatizovaném zpracovávání včetně profilování[3]. Subjekty údajů musí být také vedle poučení o jejich právech informovány o specifické povaze zpracovávání včetně toho, k jakým účelům se údaje budou zpracovávat a na jakém právním základě (např. souhlas, zákonné ustanovení apod.). Oznamovací povinnosti se budeme podrobněji věnovat v samostatné lekci.

Účelové omezení

Osobní údaje musí být získávány ke konkrétně určeným, výslovně uvedeným a legitimním účelům a nesmí se dále zpracovávat způsobem, který je s těmito účely neslučitelný[4]. Další zpracovávání za jiným účelem, než pro který byly osobní údaje získány, bude oproti stávající úpravě za určitých podmínek již dovolené. Toto je podstatná změna v českých podmínkách zpracovávání a znamená, že i když správce získá osobní údaje ke konkrétnímu účelu, za splnění určitých podmínek může tyto údaje zpracovávat i k jiným než původním účelům.

Další zpracovávání pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu nebo pro statistické účely se ve smyslu Nařízení nepovažuje za neslučitelné s původním účelem, za předpokladu, že zpracovatel zajistí přiměřené záruky pro práva a svobody subjektů

---

[1] Za nelegitimní zpracovávání je z logiky věci považováno utajené a neviditelné instalování spywaru (viz případ provozovatele webových stránek, který zveřejňoval e-mailové adresy účastníků internetové diskuse; WP 29 - Pracovní skupina pro ochranu jednotlivců v souvislosti se zpracováváním osobních údajů (čl. 29)

[2] Dosud pouze judikatorně zakotveno SDEU, viz věc C-131/12, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Spor mezi skupinou Google a P. Gonzálezem, který si přál vymazat z veřejného povědomí nepříjemnou epizodu, kdy byla v tisku zveřejněna informace o nuceném prodeji jeho nemovitosti z důvodu nesplaceného dluhu na sociálním pojištění, který byl následně splacen. Španělský úřad nařídil společnosti Google Inc., aby přijala opatření nezbytná k odstranění osobních údajů týkajících se p. Gonzáleze ze svého indexu a zabránila přístupu k těmto údajům v budoucnosti.

[3] Viz čl. 4 odst. 4 Nařízení, tj. „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;".

[4] Tzn., že jde o obecný zákaz dalšího zpracovávání pro sekundární účely, neslučitelné s primárním účelem, přičemž „slučitelností" se rozumí „přímá souvislost" s primárním účelem.

údajů. Správce resp. zpracovatel by měl zavést technická a organizační opatření, která mohou zahrnovat minimalizaci údajů, pseudonymizaci[5] či anonymizaci.

Za neslučitelné s primárním účelem tak bude podle našeho názoru nadále považováno zpracovávání osobních údajů shromážděných při projednávání přestupku k sekundárnímu účelu, kterým bude např. zveřejnění v místním periodiku nebo prostřednictvím internetu, anebo zveřejnění údajů o existenci dluhů majitele bytu, zpracovávaných primárně v souvislosti se správou bytového domu, anebo zpřístupnění shromážděných osobních údajů jednotlivých účastníků zájezdu bez jejich souhlasu všem ostatním cestujícím, aj.

Minimalizace údajů

Osobní údaje musí být přiměřené, relevantní a omezené na rozsah, který je nezbytný vzhledem k účelům, ke kterým se zpracovávají.

Přiměřenost osobních údajů ve vztahu k účelu zpracovávání není vždy jednoznačně určitelná. Zjištění, zda je zpracovávání konkrétních osobních údajů přiměřené, bude vyžadovat posouzení, zda je zásah do práv subjektu údajů, ke kterému v důsledku zpracování dojde, přiměřený legitimnímu účelu zpracovávání. Pokud se zpracovávání konkrétního osobního údaje k určitému účelu ukáže jako nadbytečné, nebude takové zpracovávání v souladu s Nařízením. Nepřiměřené by bylo např. zpracovávání rodného čísla osoby k marketingovým účelům, jelikož k těmto účelům není nezbytné tento údaj zpracovat.

Přesnost

Osobní údaje musí být přesné a podle potřeby aktualizované. Správce je povinen zajistit, aby se osobní údaje, které jsou nepřesné, bezodkladně vymazaly nebo opravily.

Minimalizace uchovávání

Osobní údaje musí být uchovávány v podobě, která umožňuje identifikaci subjektů údajů nejdéle po dobu, po kterou je to potřebné k účelům, ke kterým se údaje zpracovávají.

Osobní údaje se mohou uchovávat déle, pokud se budou zpracovávat výhradně pro účely archivace ve veřejném zájmu, pro vědecký nebo historický výzkum nebo pro statistické účely za předpokladu přijetí přiměřených technických a organizačních opatření požadovaných Nařízením k ochraně práv a svobod subjektů údajů.

Nadále tak bude platné stanovisko českého ÚOOÚ, že při provozování kamerového systému u trvale střeženého soukromého objektu je přípustným časovým limitem např. doba 24 hod., v zásadě však nepřesahující několik dnů. Omezení se však neuplatní při pořízení záznamů Policií ČR podle zvláštního zákona nebo v případě bezpečnostního incidentu, kdy záznam bude poskytnut jako důkaz příslušným orgánům pro další řízení.

Integrita a důvěrnost

Osobní údaje musí být zpracovávány způsobem, který zaručuje přiměřenou bezpečnost osobních údajů, včetně ochrany před neoprávněným nebo nezákonným zpracováváním a náhodnou ztrátou, zničením nebo poškozením, a to pomocí přiměřených technických nebo organizačních opatření.

---

[5] Viz čl. 4 bod 5) Nařízení, tj. zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;".

Odpovědnost

Správce je odpovědný za zpracovávání osobních údajů v souladu s výše uvedenými zásadami a musí být schopen tento soulad také prokázat. K prokázání souladu je možno např. vypracovat písemné podklady o tom, že všechny aspekty zpracovávatelských operací v rámci společnosti či instituce byly interně posouzeny a výsledkem tohoto posouzení je soulad s ustanoveními Nařízení.

Nařízení zavádí nový koncept ochrany osobních údajů, a to specificky navrženou („*data protection by design*") a standardní („*data protection by default*") ochranu osobních údajů.

Specificky navržená ochrana osobních údajů znamená, že správce je před začátkem zpracovávání povinen, se zřetelem na různé aspekty zpracovávání (např. nejnovější poznatky, povahu, rozsah a účel zpracovávání, rizika pro práva subjektů údajů), přijmout přiměřená technická a organizační opatření a záruky na ochranu osobních údajů a tyto přiměřeně přizpůsobit aktuálním podmínkám zpracovávání. Tento koncept tedy zavazuje všechny společnosti / instituce zpracovávající osobní údaje, aby provedly vnitřní audit zpracovávání osobních údajů. Je nezbytné, aby se ochranou osobních údajů aktivně zabývaly, vyčlenily lidské, finanční a technické zdroje pro účely posouzení zákonnosti zpracovávání a zavedly opatření na jejich ochranu.

Standardní ochrana osobních údajů znamená, že správce zajistí, aby se zpracovávaly pouze osobní údaje nezbytné pro každý konkrétní účel zpracovávání. Je též povinen zajistit, aby osobní údaje nebyly bez zásahu fyzické osoby běžně dostupné neomezenému počtu fyzických osob.

Pokud správce zpracovává osobní údaje prostřednictvím třetí osoby – zpracovatele, je tento oprávněn zpracovávat osobní údaje pouze na základě pokynů správce s výjimkou případů, kdy je to vyžadováno unijním právem nebo právem členského státu.

Co dále

Společnosti / instituce, kterých se to týká, jsou povinny provést audit zpracovávání osobních údajů a zajistit jednak soulad, ale také možnost prokázání, že osobní údaje zpracovávají zákonně a s odbornou péčí, a k tomuto účelu přijmout organizační a technická opatření a záruky. Návrhy na zajištění uvedeného najdete výše v části *Compliance*.

Další informace

Recitály 39, 40, 22

Články 5, 6, 24, 25, 29, 89 odst. 1

Kontaktní osoba

Pro další informace prosím kontaktujte:

Česká republika:

JUDr. Jaroslav Srb
Advokát

Tel.: +420 220 251 111
Mobil: +420 731 609 510

jaroslav.srb@bapol.cz

Slovensko:

JUDr. Helga Maďarová, CIPP/E
Advokátka | Certified Intl. Privacy Professional/Europe

Tel.: +421 220 251 311
Mobil: +421 917 092 076

helga.madarova@bapol.sk