KPMG

GDPR

Přehled nejvýznamnějších změn

Viktor Dušek, KPMG Legal

Praha, 28. února 2017

Co, kdy, kdo

Co se mění?

— Obecné nařízení o ochraně osobních údajů EU 2016/679 ze dne 27. dubna 2016 a o zrušení směrnice 95/46/ES

— Osud současného zákona č. 101/2000 Sb., o ochraně osobních údajů, nejasný, může dojít ke zrušení zákona nebo jeho novelizaci (zachování vymezení a pravidel jednání ÚOOÚ)

Od kdy?

— 25. května 2018

Na koho dopadá?

— Zpracování osobních údajů v souvislosti s činností provozovny správce/zpracovatele v EU (i když zpracování probíhá mimo EU)

— Činnosti zpracování související s nabídkou zboží nebo služeb subjektům údajů z EU nebo monitorováním jejich chování, pokud k němu dochází v rámci EU

Účel a titul

Principy

— Zákonnost, korektnost a transparentnost

— **Účelové omezení**

— **Minimalizace údajů**

— **Omezení uložení**

— Integrita a důvěrnost

— Přesnost

— **Proporcionalita**

— **Odpovědnost správce za zpracování**

Tituly (důvody) pro zpracování

- **Nezbytnost pro plnění smlouvy**
- **Nezbytnost pro splnění právní povinnosti**
- **Oprávněné zájmy správce či třetí osoby**
- Ochrana životně důležitých zájmů subjektu údajů
- Veřejný zájem nebo výkon veřejné moci
- **Souhlas subjektu údajů**
  - Musí být svobodný (zákaz *„take it or leave it“),* určitý, informovaný a jednoznačný
  - Žádost o vyjádření souhlasu musí být srozumitelná
  - Pokud je souhlas součástí jiného dokumentu (např. smlouvy), musí být zřetelně oddělen
  - Správce musí být schopen udělení souhlasu doložit
  - Možnost souhlas kdykoli odvolat

Potřebujeme (nové) souhlasy?

KPMG

Práva subjektů

Práva subjektů údajů

Dosavadní práva zůstávají zachována

- Právo na přístup k údajům
- Právo na informace
- Právo na vysvětlení
- Právo na odstranění závadného stavu
- Právo na opravu údajů
- Právo na omezení zpracování (dnes *blokování* osobních údajů)

Vznikají **nová práva**

- Právo na výmaz
- Právo na přenositelnost údajů
- Právo vznést námitku
- Právo na lidský zásah v případě rozhodnutí na bázi automatizovaného zpracování a profilování

Obecná pravidla pro výkon práv

— Informace o právech subjektů musí být **transparentní, srozumitelné a snadno přístupné** (jasný a jednoduchý jazyk)

— Správce **usnadňuje výkon práv subjektu** údajů (např. formuláře žádostí atp.)

— Správce je povinen **informovat subjekt údajů** o opatřeních přijatých na základě podnětu subjektu bez zbytečného odkladu, **nejpozději do 1 měsíce**

— V případě nevyhovění informuje ve stejné lhůtě, takový postup musí správce odůvodnit a poučit o možnosti obrátit se na dozorový úřad či soud

— **Uplatnění práv musí být bezplatné** (pokud nejsou žádosti) zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují

— Má-li správce důvodné pochybnosti o totožnosti subjektu, může požádat o poskytnutí informací k ověření totožnosti

Právo na informace

O čem informovat?

- Povinnost správce informovat např.:
  - o době, po kterou budou osobní údaje uloženy
  - zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy
  - zda má subjekt údajů povinnost osobní údaje poskytnout
  - o možných důsledcích neposkytnutí těchto údajů
  - o existenci práva podat stížnost u dozorového úřadu
- V případě získání informací z jiných zdrojů může být rozsah informační povinnosti omezen

Kdy informovat?

- Osobní údaje získány od subjektu údajů – v okamžiku jejich získání
- Osobní údaje získány z jiných zdrojů
  - do jednoho měsíce
  - v okamžiku první komunikace nebo při prvním zpřístupnění osobních údajů

Právo na výmaz (právo být zapomenut)

- Dovozováno judikaturou již v současném režimu
- Uplatní se pouze ve stanovených případech, např. pominul účel, subjekt odvolá souhlas
- Nutno vždy vyvažovat rovněž s oprávněnými zájmy správce (z tohoto pohledu je nutné správně identifikovat zákonný titul pro zpracování)
- Správce je povinen učinit přiměřené kroky, aby o žádosti o výmaz informoval další správce

Právo na přenositelnost údajů

- Pouze v případech, kdy je zpracování prováděno automatizovaně a je založeno na souhlasu subjektu údajů nebo na smlouvě
- Osobní údaje musí být předány přímo jedním správcem správci druhému, je-li to technicky proveditelné
- Nutnost poskytnout údaje ve strukturovaném, běžně používaném a strojově čitelném formátu
- Nejasný je rozsah údajů, které je správce nucen předat

Právo vznést námitku

- **Právo subjektů vznést námitku** proti zpracování založeného na oprávněném zájmu a v případě přímého marketingu
- Subjekt údajů musí být **výslovně upozorněn na toto právo** již v okamžiku první komunikace se subjektem údajů

Automatizované zpracování a profilování

- Profilování představuje **hodnocení aspektů chování fyzických osob**
- **Právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování**, včetně profilování, které má pro subjekt údajů právní účinky nebo se ho obdobným způsobem významně dotýká
- Kdy je dovoleno?
  - Nezbytné k uzavření nebo plnění smlouvy
  - Výslovný souhlas subjektů
- Zachováno právo na lidský zásah, vyjádřit svůj názor a napadnout rozhodnutí

KPMG

Povinnosti správců

Zabezpečení

Princip **odpovědnosti** správce za celkový soulad s GDPR (accountability)

Záměrná a standardní ochrana (tzv. privacy by design & privacy by default)

- Již při úmyslu začít zpracovávat údaje by měl správce navrhnout systém zpracování tak, aby bral ohled na práva subjektů údajů a jejich ochranu obecně
- Správce musí již v době určení prostředků pro zpracování určit a zavést vhodná technická a organizační opatření, jako je pseudonymizace nebo šifrování údajů
- Tato opatření je nutné pravidelně vyhodnocovat a případně aktualizovat

Posouzení vlivu zpracování při vysokém riziku (tzv. privacy impact assessment)

- Posouzení musí obsahovat alespoň popis operací zpracování, vyhodnocení rizik či plánovaná opatření
- Pokud z posouzení vyplyne vysoké riziko, správce konzultuje opatření ke zmírnění těchto rizik s dozorovým úřadem

Data Protection Officer

- Povinný pro **orgány veřejné moci a vybrané správce a zpracovatele** (pokud pravidelně a systematicky monitorují subjekty údajů, rozsáhle zpracovávají citlivé osobní údaje apod.)
- Hlavní úkoly:
  - poskytovat **interní poradenství** ohledně zpracování osobních údajů
  - **monitorovat soulad s GDPR**
  - **spolupracovat s dozorovým úřadem** (plní také roli kontaktního místa, i ve vztahu k subjektům údajů)
- Může jít o **zaměstnance i externího poskytovatele služeb**
- Musí být přímo podřízen vrcholovému vedení a nesmí dostávat pokyny týkající se výkonu svých pravomocí

Záznamy o zpracování

— Správce **musí vést záznamy o činnostech zpracování**, které obsahují zejména identifikaci správce, účely zpracování, popis kategorií subjektů údajů a kategorií osobních údajů

— Záznamy je nutné vést **písemně a na vyžádání je zpřístupnit dozorovému úřadu**

Oznamovací povinnost

— Zavádí se **oznamovací povinnost porušení zabezpečení osobních údajů** (dozorovému úřadu, v některých případech i subjektům údajů)

— Správce musí **popsat incident, pravděpodobné důsledky porušení zabezpečení a přijatá o**patření

— Lhůta pro oznámení bez zbytečného odkladu, **nejdéle 72 ho**din

— Správce musí vést **dokumentaci veškerých případů** porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření

Zpracovatel

- **Koncept správce a zpracovatele zůstává zachován**
- **Správce určuje účel a prostředky** zpracování, **zpracovatel zpracovává osobní údaje pro správce**
- Zpracovatel musí poskytovat dostatečné **záruky zavedení vhodných technických a organizačních opatření**
- Nové náležitosti smlouvy o zpracování – tyto smlouvy bude nutné revidovat a aktualizovat
- Výslovné umožnění řetězení zpracovatelů

KPMG

Dozor a sankce

Dozor

— Vytvoření „one-stop shopu“ pro správce (jeden kontaktní dozorový úřad)

— Vznik Evropského sboru pro ochranu osobních údajů

Sankce

— Nyní maximálně 10 mil. Kč

— Nově v případě méně závažného porušení až do výše 10 mil. eur nebo u podniku až 2 % celkového ročního světového obratu

— Nově v případě závažnějšího porušení až do 20 mil. eur nebo u podniku až 4 % celkového ročního světového obratu

KPMG

Školení GDPR

Školení GDPR

http://skolenikpmg.cz/skoleni/pravni-skoleni

GDPR: Nová pravidla ochrany osobních údajů

Školitelé: Ing Pavel Kohout, Mgr. Viktor Dušek, Mgr. Filip Horák, Ing. Radek Koudela, Ing. Jan Reich

V roce 2018 nabude účinnosti Obecné nařízení o ochraně osobních údajů (GDPR). Školení je proto zaměřeno nejen na nejvýznamnější novinky a právní aspekty, které nová regulace přináší, ale i na související praktické změny v oblasti zpracování osobních údajů včetně nastavení vnitřních procesů a IT infrastruktury.

Viktor Dušek
Advokát, KPMG Legal
vdusek@kpmg.cz
@KPMG_Legal