Časovaná bomba GDPR: Jak se změní nová pravidla ochrany osobních údajů

JUDr. Anna Bartůňková, advokátka Weinhold Legal

Místo konání, 5. 12. 2017

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Obecné nařízení o ochraně osobních údajů (GDPR) I.

- **3 důvody přijetí GDPR**
  - vývoj v oblasti zpracování osobních údajů - zejména digitalizace a profilování uživatelů internetu
  - zastaralost směrnice 95/46/ES
  - sjednocení v rámci EU a EHP – dosud roztříštěnost ochrany OÚ způsobená rozdílnou implementací
- GDPR přebírá všechny dosavadní zásady ochrany a zpracování osobních údajů
- GDPR klade systematicky důraz na vymahatelnost práv lidí a povinností správců

Obecné nařízení o ochraně osobních údajů (GDPR) II.

- **Místní působnost**: univerzální
- **Časová působnost**: od **25.5.2018** plně použitelné
- **Osobní působnost**: subjekt nakládající s údaji občanů EU
- **Věcná působnost**:
  - věrnostní programy, zákaznické a zaměstnanecké údaje
  - platební informace
  - distribuce přes internet
  - retail
  - veřejný sektor atd.
  - mimo věcnou působnost: výkon výlučně osobních nebo domácích prací, atd.

Další relevantní právní předpisy

- **Nařízení o soukromí a elektronických komunikacích (ePrivacy nařízení)**
  - schválen EP v listopadu, plánovaná účinnost jako GDPR
  - stávající právní úprava se vztahuje pouze na telekomunikační operátory – nově i OTT služby jako Messenger, Skype, WhatsApp apod.
- **Nový zákon o zpracování osobních údajů**
  - důvodem je adaptace na GDPR
  - aktuálně v připomínkovém řízení, má zrušit zákon č. 101/2000 Sb., o ochraně osobních údajů
  - navrhovaná účinnost společně s GDPR

Hlavní novinky GDPR
Povinnosti správce a zpracovatele I.

„Papírové“ povinnosti

- Širší informační povinnost
- Zpracování OÚ pouze ze zákonných důvodů – souhlas subjektu údajů a přísnější požadavky na něj
- **Zabezpečit soulad s GDPR** - dokumentovat zásady zpracování údajů, procesy a operace, a zpřístupnit je na žádost dozorujícímu úřadu – **záznamy o zpracování OÚ, kodexy, certifikace**

Hlavní novinky GDPR
Povinnosti správce a zpracovatele II.

Procesní povinnosti

- Posouzení vlivu zpracování na ochranu OÚ před započetím zpracování **(analýza rizik)**
- Přijímání technických a organizačních opatření k ochraně údajů
- **Záměrná a standardní ochrana údajů**
- **Zabezpečení** údajů – pseudonymizace, šifrování atd.
- **Oznamování narušení zabezpečení** údajů
- Ustavení **pověřence** pro ochranu údajů

Pověřenec pro ochranu osobních údajů I.

Správce i zpracovatel jsou povinni jmenovat vždy, kdy:

- zpracování provádí orgán veřejné moci či veřejný subjekt
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování vyžadujících rozsáhlé, pravidelné a systematické monitorování subjektů údajů (s ohledem na povahu, rozsah a účel operace)
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování citlivých údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů

– Vyhodnocení povinnosti jmenovat pověřence je na každém správci a zpracovateli - není-li zřejmé, zda vzniká povinnost jmenování, měla by být zpracována interní analýza

Pověřenec pro ochranu osobních údajů II.

Pojmy „hlavní činnosti“ a „rozsáhlé zpracování“

- Hlavní činnosti správce
  - souvisejí s jeho základními činnostmi a nevztahují se na zpracování osobních údajů jakožto pomocnou činnost
  - klíčové operace nezbytné k dosažení cílů správce / zpracovatele
  - např. hlavní činností nemocnice je poskytování zdravotní péče, která ji nemůže poskytovat bezpečně a účinně bez zpracování záznamů o pacientovi
- Rozsáhlé zpracování – dle množství zpracovávaných dat, počtu dočtených jednotlivců

Pověřenec pro ochranu osobních údajů III.

Role pověřence

- Kontaktní bod a komunikace s dozorovým orgánem
- Posouzení rizik při zpracování osobních údajů
- Rady a doporučení správci/zpracovateli
- Dohled nad vedením záznamů o činnostech zpracování
- Zajištění souladu zpracování osobních údajů s GDPR
  - pověřenec není odpovědný za nesoulad s požadavky ochrany OÚ
  - správce / zpracovatel musí vždy zajistit a doložit, že zpracování osobních údajů probíhá v souladu s GDPR

Pověřenec pro ochranu osobních údajů IV.

Forma spolupráce

- Musí být **reálně dostupný** (doporučení, aby pověřenec sídlil v EU bez ohledu na sídlo správce / zpracovatele)
- Může být jeden v rámci skupiny společností, pokud bude snadno dosažitelný z každé z nich
- Zaměstnanec x Spolupráce na externí bázi

Profesní kvality

- Musí být jmenován na základě svých **profesních kvalit** - odborné znalosti práva a praxe v oblasti ochrany údajů a schopnost plnit úkoly stanovené v GDPR
- Nemusí mít právnické vzdělání

Širší informační povinnost

- Již dnes, GDPR tuto povinnost dále rozšiřuje
- Vždy informace o správci, účelu a právním základu zpracování
- Pokud jsou – informace o příjemci osobních údajů, úmyslu správce předat osobní údaje do třetích zemí, pověřenci, oprávněných zájmech správce
- Případně informace o automatizovaném zpracování OÚ (vč. profilování), důsledcích takového zpracování, úmyslu zpracování OÚ, právu souhlas kdykoli odvolat, právech subjektů údajů
- V době shromáždění údajů, v případě získání z jiného zdroje pak v přiměřené lhůtě po získání

Souhlas se zpracováním OÚ

- Oproti nynějšku se souhlas jako titul posouvá z prvního místa na poslední

– nejprve zkoumat, zda nenajdu jiný právní titul (oprávněný zájem?); pouze pokud nelze, využívat souhlas

- Svobodný, konkrétní, informovaný a jednoznačný, kdykoli odvolatelný
- Prohlášení nebo jasné souhlasné jednání odlišitelné od ostatních informací poskytovaných subjektu údajů
- Vyloučení implicitního souhlasu a opt-out souhlasu
- Musí být doložitelný po celou dobu zpracování
- **Nutno zrevidovat stávající souhlasy – zohlednit GDPR**

Ohlašovací a oznamovací povinnost, Pseudonymizace

Ohlášení narušení bezpečnosti osobních údajů ÚOOÚ

- bezodkladně, nejpozději do 72 hodin od zjištění
- co ohlásit: povaha porušení, kdo je ovlivněná osoba, možné důsledky, dosavadní kroky k odvrácení

Oznamovací povinnost narušení bezpečnosti osobních údajů

- dotčeným subjektům

Pseudonymizace osobních údajů

- OÚ nemohou být přičitatelné konkrétnímu subjektu OÚ, jednoznačná identifikace subjektu údajů není možná bez „klíče“ (např. kód subjektu údajů přiřazený správcem)

Posuzování vlivu na ochranu OÚ

„Privacy Impact Assessment“

- Nahrazuje registrační povinnost správců u ÚOOÚ, správce vede záznamy
- Nutné zejména při systematickém a rozsáhlém zpracování údajů a systematickém monitorování veřejně přístupných prostorů
- Posouzení rizik z hlediska práv a svobod subjektů údajů
- Provedení testu proporcionality
- Možnost předchozí konzultace s ÚOOÚ před započetím se zpracováním osobních údajů x povinná konzultace - zpracování je vysoce rizikové a riziko nelze zmírnit přiměřenými prostředky

Posuzování vlivu na ochranu OÚ – příklad

Kamerový monitoring na pracovišti

– pokud správce zamýšlí ukládat záznamy z kamer, dochází ke zpracování osobních údajů a správce musí posoudit vlivy uchovávání těchto údajů, jejich zabezpečení, možnost přístupu cizích osob atd.

Záměrná a standardní ochrana

Privacy by design

- Správce/zpracovatel musí implementovat technicko-organizační opatření k zajištění ochrany osobních údajů (např. i vnitřní předpisy zaměstnavatele)

Privacy by default

- Nastavení systému zpracování pouze takových osobních údajů, jež jsou nezbytné pro dosažení specifikovaného účelu,
- minimalizace rozsahu zpracovávaných údajů,
- vymezení přístupových práv a subjektů oprávněných ke zpracování osobních údajů

Zabezpečení ochrany OÚ

Každý správce musí přijmout **adekvátní bezpečnostní opatření**

- odlišné s ohledem na rozsah, účel a povahu zpracování

Krytá rizika

- náhodné nebo protiprávní zničení, ztráta nebo pozměnění údajů, neoprávněné zpřístupnění údajů třetím osobám
- neoprávněný přístup k údajům při přenosu, uložení nebo jiném zpracování

Bezpečnostní opatření

- šifrování, pseudonymizace, opatření pro zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování, proces pravidelného testování opatření

Hlavní novinky GDPR
Posílení práv subjektů údajů I.

Právo být zapomenut

- Rozšířené právo na výmaz osobních údajů, pokud

  (i) osobní údaje nejsou již potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,

  (ii) subjekt údajů odvolal svůj souhlas se zpracováním,

  (iii) subjekt údajů vznesl námitku proti zpracování OÚ

  (iv) osobní údaje jsou zpracovávány protiprávně atd.
- Smyslem je zamezit řetězení osobních údajů a šíření nepravdivých či škodlivých údajů např. na sociálních sítích
- Výjimky: může být omezeno právem na svobodný přístup k informacím či dalšími právem chráněnými zájmy

Hlavní novinky GDPR
Posílení práv subjektů údajů II.

Právo vznést námitky proti zpracování údajů

- Nástroj pro omezení zpracování osobních údajů; limitováno závažnými oprávněnými důvody správce převažujícími nad právy subjektu údajů
- Zpracování pro účely přímého marketingu: právo vznést kdykoli, absolutní

Právo na přenositelnost osobních údajů

- Za splnění dvou podmínek:

  (i) zpracování osobních údajů je založeno na souhlasu občana nebo na smlouvě, a

  (ii) zpracování je prováděno automatizovaně

Děkuji za pozornost!

Tuto konferenci pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz