Co je potřeba vědět o nařízení GDPR

Mgr. Radomír Pivoda

1. 2. 2018, Hotel Olympik

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

Co je vlastně GDPR?

- Co je GDPR a jak se na něj připravit.
- Jaká data zpracováváme v rámci organizace?
- Provádíme zpracování v souladu se zákonem?
- A bude současný stav vyhovovat GDPR?
- Jaká opatření přijmout?
- Co nám hrozí, když se nepřipravíme?

Jaké základní změny GDPR přinese

- Rovnocenná vymahatelnost v celé EU
- Stejné sankce
- Spolupráce dozorových orgánů
- Rozšíření definice osobních údajů
- Nová práva subjektů údajů
- Oznamovací povinnost v případě narušení bezpečnosti údajů

Sankce a rizika

- Až 20 milionů Euro nebo 4% z celosvětového obratu skupiny (vyšší z obou možností)
- Podle návrhu zákona:

  - Porušení zákazu zveřejnění OÚ – pokuta do 1.000.000Kč

  (do 5.000.000 Kč pokud spácháno tiskem, filmem, rozhlasem, televizí…)

  - Ostatní porušení – pokuta do 10.000.000 Kč

Sankce a rizika

- Výše sankce se stanovuje podle řady faktorů:
  - povaha, závažnost a délka porušování,
  - počet poškozených občanů a míra škody,
  - kroky podniknuté správcem či zpracovatelem ke zmírnění škod,
  - kategorie osobních údajů dotčené porušením atd.
- Nebezpečí žalob ze strany fyzických osob
  - nárok na náhradu škody v případě hmotné či nehmotné újmy
- Ztráta důvěry a reputační riziko

Osobní údaj

- Veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě
- Údaj, který umožňuje identifikovat konkrétní osobu, je osobním údajem
- To, co je u jedné fyzické osoby osobním údajem, protože ji to jasně identifikuje, nemusí být osobním údajem pro další fyzickou osobu
- Osobním údajem může být jeden údaj nebo i více údajů, které teprve dohromady umožňují konkrétní osobu určit
- Např. adam.novak@seznam.cz / adam.novak@hotelolypmik.cz
- Obecné / zvláštní kategorie / genetické a biometrické OÚ

Údaje nepožívající ochrany

- Všechny údaje o právnických osobách, orgánech veřejné moci a institucích
- Údaje **zemřelých osob**
- Údaje získané v rámci **činnosti čistě osobní povahy**, které nemají obchodní či institucionální charakter
- **Anonymizované údaje -** nelze ani nepřímo přidělením dalších identifikátorů určit subjekt údajů

Zásady zpracování osobních údajů

- Zákonnost, korektnost a transparentnost
- Účelové omezení
- Minimalizace údajů
- Přesnost
- Omezení uložení
- Integrita a důvěrnost
- Odpovědnost

Právní titul zpracování

- Plnění smlouvy, jejíž smluvní stranou je subjekt údajů
- Opatření před uzavřením smlouvy na žádost subjektu údajů
- Splnění právní povinnosti
- Ochrana životně důležitých zájmů
- Splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
- Oprávněný zájem příslušného správce (přednost základních práv a svobod)
- Souhlas

Souhlas

- **Svobodný, konkrétní, informovaný a jednoznačný** projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů
- Povinnost správce doložit, že subjekt údajů udělil souhlas se zpracováním svých údajů
- Aktivní a dobrovolný projev vůle subjektu údajů, ke kterému nesmí být nucen

Práva subjektu údajů

- právo na přístup
- právo na opravu
- právo na výmaz
- právo být zapomenut
- právo na omezení zpracování
- právo na přenositelnost údajů
- právo vznést námitku

Posouzení vlivu na ochranu osobních údajů

- „Data Protection Impact Assessment“
- Pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob
- Povinnost provést před zahájením zpracování
- Správce si vyžádá posudek pověřence pro ochranu osobních údajů
- Možnost „předchozí konzultace“ s ÚOOÚ

Předávání údajů do ciziny

- Předpoklad odpovídající úrovně ochrany
- Existence vhodných záruk a zajištění vymahatelnosti práva v případě předání mimo EU
- Seznam třetích zemí zveřejňuje Komise v ústředním věstníku
- Závazná podniková pravidla
- Dostatečné záruky (standardní smluvní doložky)

Vnitřní předpisy

- Vyřizování stížností
- Ochrana osobních údajů
- Ochrana dat
- Systém řízení rizik
- Směrnice k provádění kontroly dodržování léčebného režimu zaměstnanců dočasně práce neschopných

Kamerový systém

- Důvody pro instalaci – účel zpracování
  - Bezpečnost
  - Ochrana majetku správce
  - Prevence vandalismu
  - Zamezení přístupu cizích osob
- Zakázaný účel – sledování zaměstnanců a dalších fyzických osob
- Monitorované prostory – právo na soukromí
- Kamera se záznamem
  - Uchovávání záznamu
  - Zabezpečení záznamu / pravidla pro přístup k záznamu

Osobní spis zaměstnance

- Obsah určuje zaměstnavatel
- Pouze písemnosti nezbytné pro výkon práce v pracovněprávním vztahu
- Nelze pořizovat kopie libovolných dokladů, ani se souhlasem nebo je nutné zamezit zpracování údajů o třetích osobách (např. rodný list – údaje o rodičích dítěte)

Osobní údaje zaměstnance po skončení pracovního poměru

- Archivace dle zákona
- Uschování odůvodněno předpokladem vzájemného uplatňování nároků z pracovněprávního vztahu
- Postupná likvidace složky po uplynutí lhůt pro archivaci:
  - Životopis – ztrácí relevanci ukončením pracovního poměru
  - Stejnopisy evidenčních listů (3 roky)
  - účetní podklady (5 let)
  - záznamy o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti (6 let)
  - mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění (30 let)

Závěrečné shrnutí

- Proveďte důkladnou inventuru
- Posuďte, kdo má k datům přístup
- Ověřte si bezpečnost dat
- Zvažte jmenování pověřence
- Aktualizujte vnitřní předpisy a procesy
- Vzdělávejte personál

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