Dopady GDPR na organizace a jejich ICT systémy

Praha, 1. února 2018

Mgr. Zbyněk Loebl, LLM
PRK Partners advokátní kancelář

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

Zásady zpracování OÚ dle GDPR

- **Čl. 5 GDPR**
  - Možnost omezení aplikace zásad a práv subjektů OÚ za účelem výslovného veřejného zájmu - čl. 23 GDPR

- **Zásada zákonnosti zpracování**
  - Zpracování OÚ výlučně zákonným způsobem a ze zákonných důvodů
  - Čl. 6 GPDR Zákonnost zpracování + Čl. 7 GDPR Podmínky udělení souhlasu
  - Čl. 9 GDPR Zpracování zvláštních kategorií OÚ

- **Zásada korektnosti a transparentnosti zpracování**
  - Zpracování OÚ korektně
  - Zpracování OÚ transparentním způsobem
  - Čl. 12 – 14 GDPR
    - Požadavek transparentnosti
    - Informační povinnosti při získání OÚ od/bez subjektů

Zásady zpracování OÚ dle GDPR

- **Zásada účelového omezení shromažďování osobních údajů**
  - Určité, výslovně vyjádřené a legitimní účely
  - Zpracování pouze způsoby, které jsou slučitelné s účelem
  - Zpracování pro účely archivace, vědeckého výzkumu či statistické účely
  - Další zpracování (čl. 5 GDPR)

- **Zásada minimalizace zpracovávaných osobních údajů**
  - OÚ přiměřené a v relevantním rozsahu
  - OÚ jen v nezbytném rozsahu ve vztahu k účelu

- **Zásada přesnosti osobních údajů**
  - Přesné OÚ
  - V případě potřeby aktualizované
  - Veškerá rozumná opatření k vymazání / opravě nepřesných OÚ

Zásady zpracování OÚ dle GDPR

- **Zásada omezeného uložení osobních údajů**
  - Ve formě umožňující identifikaci subjektu OÚ jen na dobu nezbytně nutnou pro dané účely zpracování
  - Na delší dobu pro účely archivace ve veřejném zájmu, výzkumu a statistické účely (čl. 89 GDPR)

- **Zásada integrity a důvěrnosti zpracování**
  - Požadavek náležitého zabezpečení OÚ
  - Ochrana pomocí vhodných technických nebo organizačních opatření
    - Neoprávněné a protiprávní zpracování
    - Náhodná ztráta
    - Zničení a poškození
  - Čl. 32 GDPR

- **Zásada odpovědnosti**
  - Povinnost správce dodržet všechny povinnosti vyplývající ze zásad
  - Povinnost správce dodržení shody prokázat

Právní tituly zpracování OÚ

- **Čl. 6 GDPR**
  - Průmět zásady zákonnosti
  - Správce musí mít pro zpracování aspoň jeden právní titul; časté souběhy
  - Další zpracování

- **Splnění smlouvy**
- **Splnění právní povinnosti**
- **Ochrana životně důležitých zájmů subjektu údajů anebo jiné fyzické osoby**
- **Úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci správcem**
- **Oprávněné zájmy příslušného správce anebo třetí strany**
  - Možná přednost zájmů, základních práva a svobod subjektu OÚ dítě

- **Souhlas subjektu údajů**
  - Vždy zákonné zpracování

Dopady GDPR na organizaci

- Rozšíření informačních povinností správce OÚ vůči subjektu OÚ
- Zavedení povinnosti vést záznamy o činnostech zpracování
- Zpřísnění požadavků na poskytovaný souhlas se zpracováním OÚ
- Zavedení institutu posouzení vlivu na ochranu OÚ (DPIA)
- Povinnost některých správců a zpracovatelů jmenovat pověřence pro ochranu OÚ (DPO)
- Explicitní zakotvení práva na výmaz údajů (právo být zapomenut)
- Zavedení práva na přenos údajů k jinému správci (data portability)
- Zpřísnění a zpřesnění úpravy obsahu smlouvy o zpracování OÚ
- Přísná úprava ohlašovací povinnosti v případě porušení zabezpečení OÚ (data breaches)
- Rozšíření výčtu identifikátorů (OÚ) o síťové identifikátory a lokační údaje
- Významné zvýšení sankcí

Zpracování OÚ

- **Základní kategorie zpracování (podle účelu) a odpovědnosti v rámci organizace**
  - Marketing → CCO
  - Produkty / Služby → Obchodní ředitel
  - Dodavatelé → Pověřená osoba
  - HR → Personální ředitel
  - Správa a řízení práv subjektů OÚ → General Counsel / DPO
  - Archivace, likvidace → CIO
  - Ostatní → CO

Zpracování OÚ

- **Zpracování OÚ**
  - Evidence existujícího zpracování OÚ
  - Příprava nového zpracování osobních údajů
  - Změna schválené přípravy nového zpracování OÚ
  - Změna stávajícího zpracování OÚ včetně ukončení zpracování

- **Práva subjektů OÚ**
  - Čl. 13, 15, 17, 21 a 22 GDPR
  - Právo na informace o zpracování OÚ
  - Právo na přístup subjektu k OÚ
  - Právo získat od správce OÚ potvrzení o zpracování OÚ
  - Právo poskytnout kopii zpracovávaných OÚ
  - Právo subjektu na vyžádaný výmaz jeho OÚ („právo být zapomenut“)
  - Právo subjektu OÚ vznést námitku
  - V případě, že zpracování provádí správce na základě svých oprávněných zájmů
  - Právo subjektu nebýt předmětem automatizovaného rozhodnutí

Zpracování OÚ

- **Povinnosti správců a zpracovatelů**
  - Čl. 30 a násl. GDPR
  - Povinnost vést záznamy o činnostech zpracování
    - Písemné záznamy, dostupné na vyžádání dozorovému úřadu
    - Výjimka pro malé a střední podniky do 250 zaměstnanců
  - Povinnost zajistit odpovídající zabezpečení OÚ
    - Povinnost přijmout vnitřní koncepce a opatření pro zabezpečené zpracování OÚ
    - Zásady záměrné a standardní ochrany osobních údajů
    - Neustálá důvěrnost, integrita, dostupnost a odolnost systémů a služeb
    - Pravidelné testování, posuzování a hodnocení bezpečnosti opatření
  - Povinnost ohlašovat bezpečnostní incidenty (data breaches)
    - Bez zbytečného odkladu, nejpozději do 72 hodin dozorovému orgánu
    - Bez zbytečného odkladu v případě závažného úniku i subjektům OÚ
  - Povinnost provést posouzení vlivu na ochranu OÚ (DPIA) a předchozí konzultace
    - Povinnost preemptivně posoudit vliv konkrétních operací při zpracování OÚ, které představují vysoké riziko pro práva a svobody FO
    - Povinnost předběžné konzultace s dozorovým orgánem

Zpracování OÚ

- **Bezpečnostní incidenty**
  - Návrh notifikace o incidentu
  - Odsouhlasení notifikace
  - Podání notifikace
  - Přijatá opatření
  - Další

- **Vztahy s ÚOOÚ**
  - Registrace zpracování u ÚOOÚ
  - Stížnosti SÚ u ÚOOÚ
  - Inspekce
  - Hlášení bezpečnostních incidentů
  - Posouzení vlivu

Záměrná ochrana OÚ

- **Záměrná ochrana osobních údajů (Privacy / Data protection by design)**
  - Soukromí jako ústavní právo (USA) × základní lidské právo (Evropa)
  - Report Privacy-enhancing technologies
  - Teledienstedatenschutzgesetz (Německo, červenec 1997)

- **Principy návrhu systémové / datové architektury organizace**
  - Návrh systémové / datové architektury od počátku tak, že data nepotřebují dodatečnou externí ochranu
  - Organizační a technologická opatření
  - Technologie pro podporu ochrany soukromí (privacy enhancing technologies - PETs)

- **7 pravidel**
  - Proaktivní, ne reaktivní ochrana /
    Prevence před odstraňováním škod
  - Ochrana soukromí jako standardní nastavení
  - Ochrana soukromí součástí návrhu
  - Ochrana údajů přes všechny funkce
  - Zabezpečení end-to-end /
    Ochrana po celý životní cyklus údaje
  - Transparentnost a otevřenost
  - Respekt a nastavení služby k uživateli

Záměrná ochrana OÚ

- **Čl. 25 odst. 1 GDPR – Záměrná ochrana OÚ**
  - Vhodná technická opatření a organizační opatření (např. pseudonymizace) k ochraně OÚ
    - S přihlédnutím ke stavu techniky, nákladům, povaze, rozsahu, kontextu, účelům a rizikům zpracování OÚ
    - V době určení prostředků × v době zpracování OÚ

- **Účelem provádět zásady ochrany OÚ a začlenit nezbytné záruky k ochraně práv subjektů**
  - Zásada zákonnosti
  - Zásada minimalizace OÚ
  - Zásada přesnosti, integrity a důvěrnosti

Záměrná ochrana OÚ

- **ENISA – Osm strategií záměrné ochrany soukromí**
  - Minimalizace
  - Skrývání
  - Oddělování
  - Agregace
  - Informování
  - Kontrola
  - Prosazování
  - Prokazování omezení shromáždění pro veřejné účely

Záměrná ochrana OÚ

- **Čl. 25 odst. 2 GDPR – Standardní ochrana OÚ**
  - Vhodná technická opatření a organizační opatření k minimalizaci zpracovávaných OÚ
    - Průmět zásady minimalizace
    - Povinnost standardně zpracovávat jen OÚ
      - Nezbytně nutné pro specifikovaný účel
      - V nezbytně nutném rozsahu
      - Uchovávat po nezbytně dlouhou dobu
  - OÚ nelze volně zpřístupňovat neomezenému počtu osob

Praktické zkušenosti s implementací GDPR

- **Důraz na následující aspekty ochrany osobních údajů:**
  - Záznamy zpracování
  - Vyčištění systémů o duplicitní data, resp. data bez účelu
  - Revize souhlasů a smluv se zpracovateli osobních údajů
  - Bezpečnost zpracování osobních údajů
  - Plnění informačních povinností vůči subjektům údajů
  - Hladký výkon práv subjektů údajů
  - Vyřizování stížností a podnětů subjektů údajů
  - Nastavené interní procesy DPO

Děkuji za pozornost!

© Zbyněk Loebl, 2018

Zbyněk Loebl je Off Counsel advokátní kanceláře PRK Partners; zbynek.loebl@prkpartners.com

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