Zkušenosti z implementace GDPR

Tomáš Nielsen

NIELSEN MEINL, advokátní kancelář, s.r.o.

Standardní výchozí stav

- Často první kontakt s ochranou OÚ
- Neznalost nových povinností
- Neznalost vlastního prostředí
- Chybný pohled na výklad „zpracovatele“
- Povědomí o GDPR aneb mýty a legendy 2018

Neznalost nových povinností

- Informační povinnost i pro zpracování bez souhlasu
- Vedení záznamů o zpracování
- Proces na realizaci práv subjektů údajů
- Hlášení incidentů
- Odpovědnost za aktuálnost údajů
- Existence podrobné smlouvy o zpracování
- Analýza rizik zpracování / DPIA
- DPO

Neznalost prostředí - stav

- Jen rámcový přehled o zpracovávaných OÚ a o formách zpracování
- Absence kategorizace OÚ, důvodů a účelů zpracování, stanovení doby archivace
- Neurčité povědomí o příjemcích údajů (zpracovatelé)

Neznalost prostředí - řešení

- Správné (funkční) zmapování operací s OÚ
- Definice kategorií OÚ, důvodů a účelů zpracování, stanovení doby archivace
- Identifikace třetích osob, které přicházejí do styku s OÚ, a ověření (příp. nastavení) správných vztahů

Chybný pohled na výklad „zpracovatele“ – stav

- Nemožnost přístupu k datům nemusí znamenat, že nejsem zpracovatelem (viz cloudové služby)
- Nejasné vymezení role při zpracování (správce / zpracovatel)
- Výsledkem může být zpracování OÚ v roli zpracovatele bez právního důvodu (smlouvy)

Chybný pohled na výklad „zpracovatele“ – řešení

- V rámci mapování operací určit, zda v našich systémech existují OÚ získané od třetích osob (příp. pro třetí osoby)
- Pokud ano, identifikovat, co se s OÚ děje
- Zjistit, kdo určuje účely a prostředky zpracování
- Pokud 3. osoba, jsme zpracovatelem (povinnost mít smlouvu o zpracování, ale odpovědnost jde primárně za správcem)

Povědomí o GDPR aneb mýty a legendy 2018 - stav

- Víra v mýtické informace
  - reálně nám hrozí pokuty 10-20 mio Eur
  - je povinnost vše šifrovat
  - je nutné implementovat IS, které přesně logují veškeré operace s OÚ
  - aktuálně zpracovávané OÚ musíme po 25. 5. smazat
  - do 25. 5. musíme sehnat nové souhlasy
  - profilování zákazníků je zakázáno
- Podceňování skutečnosti
  - stačí včas rozeslat oznámení subjektům OÚ
  - fakticky se nic nemění

NIELSEN MEINL

Povědomí o GDPR aneb mýty a legendy 2018 - řešení

- Zorientovat se v operacích, při nichž dochází ke zpracování OÚ
- Získat informace o nových povinnostech z relevantních zdrojů
- Aplikovat standardní pravidla tam, kde je to možné
- Individuálně řešit složitější případy

NIELSEN MEINL

Co dělat?

Základní principy

- Zákonnost, korektnost, transparentnost
- Legitimní účel
- **Přiměřenost** a minimalizace (rozsahu i doby)
- Správnost a aktuálnost
- Integrita a důvěrnost
- Odpovědnost a schopnost ji doložit

Právní základy zpracování

SOUHLAS	**PLNĚNÍ ČI UZAVÍRÁNÍ SMLOUVY**
PLNĚNÍ PRÁVNÍ POVINNOSTI	OCHRANA ŽIVOTNĚ DŮLEŽITÝCH ZÁJMŮ FO
VEŘEJNÝ ZÁJEM NEBO VÝKON VEŘEJNÉ MOCI	**OPRÁVNĚNÝ ZÁJEM** (SPRÁVCE ČI TŘETÍ OSOBY)

NIELSEN MEINL

Účel a doba zpracování

- GDPR nestanoví účel ani dobu zpracování
- Obojí stanoví správce v souladu s:
  - Právním základem zpracování
  - Svými potřebami
  - Principy GDPR
  - Právními předpisy (např. v oblasti HR apod.)

Informační povinnost

- Informovat řádně subjekty údajů
- Informace musí být:
  - Stručné
  - Transparentní
  - Srozumitelné
  - Snadno přístupné
  - Používat jasné a jednoduché jazykové prostředky

Záznamy o zpracování

- Kontaktní údaje správce, zástupce a pověřence
- Účely zpracování
- Kategorie subjektů údajů a kategorie údajů
- Kategorie příjemců osobních údajů (minulých i budoucích)
- Údaje o předání do třetích zemí
- Pokud je to možné, předvídanou dobu uložení osobních údajů
- Pokud je to možné, popis technických a organizačních bezpečnostních opatření

Hlášení incidentů

- Nově – oznamovací povinnost porušení zabezpečení osobních údajů (dozorovému úřadu, v některých případech i subjektům údajů)
- Správce musí popsat incident, odhad důsledků porušení zabezpečení a přijatá opatření
- Lhůta: bez zbytečného odkladu, **nejpozději do 72 hodin**
- Povinnost evidovat případy porušení, účinky i přijatá opatření

Jak postupovat?

- Mapa procesů / transakcí
- Určení role při zpracování
- Vymezení kategorií osobních údajů
- Vymezení způsobu zpracování
- Identifikace právního základu pro zpracování, účelu a doby
- Identifikace všech příjemců (zpracovatelé, další správci apod.)
- Seznam seznamů, další vnitřní předpisy a dokumentace
- Nastavení funkčních vnitřních procesů (práva subjektů údajů apod.) a jejich kontrola
- Odpovědná osoba (kvaziDPO)
- Smlouvy, souhlasy, další dokumentace směrem ven

Další doporučení

- Sledujte stránky www.uoou.cz a WP29
- Sledujte články (epravo.cz, google apod.)
- Konzultujte nejasné věci s ÚOOÚ
- V případě nouze kontaktujte právníka

NIELSEN MEINL

www.nielsenmeinl.cz

Kontakt

Tomáš Nielsen
+420 602 463 507
tnielsen@nielsenmeinl.com

NIELSEN MEINL, advokátní kancelář, s.r.o.
Žatecká 55/14, Praha 1