Obecné nařízení o ochraně osobních údajů (GDPR)

S přihlédnutím ke Smart Cities

Petr Habarta, OBPPK MV

Evoluce, nikoli revoluce

- Obecné nařízení o ochraně osobních údajů č. 2016/679(EU) bude účinné od 25. května 2018
- Nahrazuje směrnici 95/46(ES) o ochraně osobních údajů, kterou implementoval zákon 101/2000 Sb.
- Obecné nařízení vychází z definic, zásad a struktury této směrnice
- Proto je řada povinností správce a práv subjektu údajů stejná nebo podobná jako podle zákona 101/2000 Sb.
- Na rozdíl od směrnice je Obecné nařízení téměř celé přímo použitelné – nepotřebuje český zákon

Nařízení z pohledu právní formy

- Většina ustanovení platí přímo a „nepřekládá“ se do vnitrostátních zákonů → odchylky a rozdíly jen ve vymezených oblastech
- Cílem je zajistit jednotný právní režim v celé EU → ušetřit podnikům právní náklady na plnění různých národních předpisů
- Povolené odchylky se ale vymezují různým způsobem

- vztah mezi nařízením a vnitrostátními předpisy je poměrně nepřehledný

Nový zákon – pro informaci

- Připravuje MV ve spolupráci s ÚOOÚ
- Do vlády předložen v polovině ledna 2018
- Nahradí zákon 101/2000
- Přináší některá usnadnění a vyjasnění, např.
  - Pokud má správce úkol, může k němu zpracovávat osobní údaje
  - Správce může o zpracování podle předpisu informovat i na webu, ne jednotlivě
  - Výjimky z práv subjektu údajů za účelem bezpečnosti státu, boje proti trestné činnosti a podobně
  - Omezení počtu správců, kteří potřebují pověřence

Právní základ zpracování

- Stále je 6 právních základů pro zpracování osobních dat
  - Souhlas subjektu údajů (toho člověka, kterého se údaje týkají)
  - Smlouva nebo příprava smlouvy
  - Právní povinnost správce
  - Životně důležitý zájem subjektu údajů nebo jiného člověka
  - Úkol správce ve veřejném zájmu, výkon veřejné moci správcem
  - Oprávněný zájem správce či jiné osoby, ledaže převažuje zájem subjektu údajů
- Omezení a posuny může přinést nařízení o soukromí v elektronických komunikacích (přenášený obsah, metadata, koncová zařízení)

Některé změny

- Větší důraz na (technické) zabezpečení údajů a hlášení jeho narušení
- Větší důraz na přizpůsobení se riziku zpracování
- Právo na přenositelnost
- Posouzení vlivu na ochranu osobních údajů
- Konzultace s ÚOOÚ
- Pověřenec pro ochranu osobních údajů

Zabezpečení údajů – zase evoluce

- Na bezpečnost se klade velký důraz, nově je to jedna ze zásad činnosti správce a zpracovatele:
  - Principy zabezpečení zůstávají stejné či velmi podobné
  - Mění se částečně jejich vyjádření
  - Klade se větší důraz na to, aby povinnosti správce včetně zabezpečení odpovídaly riziku
  - Řešení incidentů formou hlášení narušení
  - Zohledňuje se i cena a technologické možnosti
  - Klade se důraz na proces hodnocení a zlepšování

Riziko zpracování

- Nový princip: povinnosti správce a zpracovatele mají odpovídat riziku zpracování
- Formálně se posuzuje jen u nových nebo podstatně upravených zpracování podle čl. 35. Podrobnosti ve vodítku WP 29 č. WP 248/17 na webu www.uoou.cz
- Ve skutečnosti na něj navazují jiné parametry, takže je vhodné se nad ní zamyslet aspoň orientačně
- Riziko má pravděpodobnost a závažnost
- Riziko může být nízké (malé), normální či vysoké

Posouzení rizika

- riziko zpracování = pravděpodobnost a závažnost hmotné nebo nehmotné újmy včetně diskriminace, zneužití identity, poškození pověsti nebo porušení práv subjektu údajů apod.
- Přihlíží se k
  - rozsahu (např. rozsah zpracovávaných údajů a rozsah využití zvláštních kategorií údajů nebo údajů týkajících se rozsudků v trestních věcech a trestných činů),
  - kontextu (např. využití údajů shromážděných za různými účely a jejich kombinace nebo porovnání, zvláštní zranitelnost nebo významně nerovnovážné postavení subjektu údajů, předávání mimo EU),
  - povaze (např. využití nových technologií, automatizovanost rozhodování, hodnocení osobních aspektů včetně porovnávání nebo predikce, systematičnost nebo pravidelnost zpracování, inovativní prostředky nebo povaha zpracování), a
  - účelům zpracování.

Riziko a povinnosti

- Pokud je riziko újmy při úniku nebo narušení bezpečnosti dat vysoké, nutno ohlašovat narušení bezpečnosti subjektu údajů.
- Pokud je vysoké riziko připravovaného zpracování pravděpodobné, je nutno provést posouzení vlivu, např.:
  - scoring, automatizované rozhodování, systematické monitorování, citlivé údaje, jiné rizikové údaje (finanční), velký rozsah, kombinace dat shromážděných za různými účely, zranitelné subjekty, inovativní použití, předávání z EU, zpracování brání subjektu ve využití služby)
- Pokud je riziko zpracování vysoké, nutno konzultovat s UOOU.
- Pokud je riziko nízké, v určitých výjimečných případech podle čl. 30 odst. 5 není nutné provádět obecný popis zpracování.
- Stupeň rizika ovlivňuje zejména technicko-organizační opatření správce, parametry ochrany údajů, úroveň zabezpečení a priority pověřence.

Bezpečnostní opatření

- Čl. 32 odst. 1 Obecného nařízení (oproti § 13 odst. 4 ZOOÚ):

  S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

  a) pseudonymizace a šifrování osobních údajů;

  b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

  c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

  d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Hlášení porušení zabezpečení

- Pokud správce zjistí, že bylo narušeno zabezpečení osobních údajů, například hackerským útokem, nebo vloupáním, nebo ztrátou nosiče dat (ne dílčí neoprávněné přístupy)
- Musí to vždy a co nejdříve ohlásit na ÚOOÚ a navrhnout způsoby řešení rizik
- V případě, že narušení vede k velkému riziku pro subjekty údajů (např. data nejsou šifrována), musí to oznámit subjektům údajů (případně veřejně)

Právo na přenositelnost a Smart City

- Nové právo na to, aby správce připravil údaje, které subjekt údajů dříve poskytl, v používaném strukturovaném a strojově čitelném formátu
- Má posílit konkurenci a vstřícnost k uživatelům sociálních a podobných sítí
- Platí jen pro zpracování založená na souhlasu nebo smlouvě, pokud jsou data uložena digitálně
- WP 29 do „poskytl“ zahrnuje i data získaná pozorováním subjektu údajů, tj. včetně chytrých měřičů, zdravotních náramků, lokalizace, logů atd., ale ne analýzu těchto dat

Posouzení vlivu na ochranu osobních údajů a Smart City

- Platí pro zpracování zahájená po květnu 2018
- Pokud je pravděpodobné, že zpracování povede k vysokému riziku pro subjekt údajů, musí se provést hodnocení dopadů, posoudit rizika a kompenzovat je
- Také vždy, pokud zpracování zahrnuje:
  - Rozsáhlé a systematické profilování a automatizované rozhodování se závažným dopadem na fyzické osoby
  - Rozsáhlé zpracování citlivých údajů
  - Rozsáhlé systematické monitorování veřejně přístupných prostor

- Pokud zpracování vychází z podrobné právní úpravy, není nutné hodnocení dopadů či konzultace s ÚOOÚ
- Pro podobná zpracování postačí jedno posouzení (např. podobné kamerové systémy v různých obcích nebo na nádražích)
- Lze kombinovat hodnocení připravené dodavatelem s konkrétním způsobem nasazení u správce (chytrý měřič a dodavatel energie atd.)

Příklady evropských metodologií pro posouzení vlivu na ochranu údajů

- Privacy and Data Protection Impact Assessment Framework for RFID Applications http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Konzultace s ÚOOÚ

- Není tak úplně nové, ÚOOÚ u rizikových zpracování může vést řízení z vlastního podnětu již nyní
- Platí pro zpracování zahájená po květnu 2018
- Pokud zpracování přináší vysoké riziko, má správce před jeho zahájením konzultovat s ÚOOÚ, který má na posouzení asi ¼ roku a může doporučit další opatření

Pověřenec pro ochranu osobních údajů a Smart City

- Je povinný pro správce a zpracovatele:
  - orgány veřejné moci (vč. obcí) a „veřejné subjekty“ (v návrhu zákona je zužující definice „veřejných subjektů“, protože široký výklad „veřejné instituce“ podle zákona 106/1999 nemá smysl)
  - Hlavní činnosti vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů:
    - Za „pravidelné a systematické“ se považují např. chytré měřiče, auta podobná propojená zařízení, sledování lokace (např. v městské HD nebo operátory), monitory kondice, CCTV. „Monitorování“ není definováno, patří sem např. sledování a profilování na internetu.
  - Hlavní činnosti vyžadují rozsáhlé zpracování citlivých údajů nebo údajů o trestné činnosti (např. nemocnice, ne jeden doktor v ordinaci)
- Lze jmenovat jednoho pověřence pro více orgánů nebo subjektů (například pro všechny základní školy v kraji), záleží na rozsahu, intenzitě a komplexnosti zpracování
- Může to být i externí subjekt (praktické spíše pro soukromý sektor)

Pověřenec pro ochranu osobních údajů

- Má jít o „svědomí“ správce z hlediska ochrany osobních údajů, jeho role je:
  - Poradní, informační a metodická
  - Kontrolní ohledně předpisů na ochranu údajů
  - Kontaktní pro ÚOOÚ a částečně pro subjekty údajů
- Pověřenec má rozumět ochraně osobních údajů přiměřeně rozsahu, komplexnosti a citlivosti zpracování, ale nemusí to mít jako jedinou činnost
- Náměstek MV pro státní službu vydal metodická vodítka pro ústřední orgány
- Náměstek MV pro veřejnou správu vydal spolu s ÚOOÚ metodickou pomoc pro obce

Kontext a podrobnosti

- Ministerstvo vnitra Obecné nařízení o ochraně osobních údajů legislativně implementuje, ale nevykládá ani nekontroluje.
- Praktické vymáhání je v kompetenci ÚOOÚ
- Výklad spočívá zejména na Sboru, nyní na Pracovní skupině 29, která svá výkladová vodítka k jednotlivým oblastem zveřejňuje a jsou k dispozici i na www.uoou.cz