

GDPR – evoluce v ochraně osobních údajů

Petr Habarta,
OBP MV

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 (někdy vnitrostátní zákon prostě platí, jindy se oznamují dotčená ustanovení Komisi)



- vztah mezi nařízením a vnitrostátními předpisy může být poměrně **nepřehledný**

Evolve, not revolution

- 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
- Nemění se ani právní tituly ke zpracování údajů
- 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

Zákon o zpracování osobních údajů

- MV ve spolupráci s ÚOOÚ předložilo vládě 22. ledna 2018 návrh **adaptačního zákona**
- Vláda jej schválila **21. března 2018**
- Nahradí zákon 101/2000 Sb., o ochraně osobních údajů
- 4 hlavní části:
 - **Adaptace** na Obecné nařízení
 - **Transpozice** větší části směrnice pro policejní a trestní zpracování
 - Základní pravidla ochrany údajů v oblasti národní bezpečnosti (mimo působnost práva EU)
 - Postavení a struktura ÚOOÚ, pravomoci a přestupky
- Změnový zákon – řada dílčích úprav různých zákonů (cca 35) kvůli nařízení nebo směrnici

Zákon o zpracování osobních údajů

Přináší některá upřesnění a vyjasnění, např.:

- Pokud má správce zákonem stanovenou povinnost, vykonává veřejnou moc nebo plní úkol ve veřejném zájmu, je **oprávněn** kvůli tomu **zpracovávat** osobní údaje
- Správce zajišťující některé chráněné zájmy **nemusí posuzovat slučitelnost** účelů
- Subsidiární **výjimky z práv subjektu údajů** za kvůli zajištění některých chráněných zájmů **kompensovány dozorem ÚOOÚ**
- **Oznamovat** změny a výmazy **lze aktualizací evidence**
- Věk pro **samostatný on-line souhlas dítěte** na **15 let**
- **Omezení** zpracování **nestaví** zákonnou **ohlašovací povinnost**
- Prolomení některých mlčenlivostí pro kontrolní činnost ÚOOÚ
- **Omezení pokut** pro veřejnou sféru na současných 10 mil. Kč

Co zákon **ne**obsahuje

- Vlastní definice základních pojmů – z práva EU
 - **Zpřísňování** pravidel Obecného nařízení nad rámec stávajícího zákona, např.:
 - Kvalifikace **pověřence**, rozšíření povinnosti pověřence jmenovat
 - Další omezení nakládání s **údaji o zdravotním stavu** aj.
 - Další omezení **přenosu osobních údajů** do třetí země
 - Další povinnosti provádět **posuzování** dopadů
 - Další **přestupky** (přebírají se však delikty ze 101/2000)
- ⇒ Kdo dodržuje zákon 101/2000 a je připraven na Obecné nařízení, je připraven i na nový zákon

Praktické dopady – podobné nynějším

- Standardní povinnosti správce nebo zpracovatele zůstávají zachovány (bezpečnost, **technicko – organizační opatření**)
- Správce musí být schopen splnění svých povinností **doložit**
- Standardní práva subjektu údajů (na přístup, na opravu apod.) se použijí podobně jako nyní
- Důraz na zabezpečení osobních údajů

Praktické dopady - nové

- *Standardní a záměrná ochrana osobních údajů*
- Hlášení porušení zabezpečení osobních údajů
- Posouzení vlivu na ochranu osobních údajů
- Konzultace s ÚOOÚ
- Pověřenec pro ochranu osobních údajů
- *Více podmínek pro udělení souhlasu*
- *Věk pro on-line souhlas*
- *Akreditace certifikačních orgánů*
- *Kodexy chování*

Hlášení porušení zabezpečení

- Pokud správce zjistí, že bylo narušeno zabezpečení osobních údajů, například **hackerským útokem**, nebo vloupáním, nebo ztrátou nosiče dat
- 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)

Posouzení vlivu na ochranu osobních údajů

- Platí pro zpracování zahájená **po 25. květnu 2018**
- Pokud je pravděpodobné, že zpracování povede k vysokému riziku pro subjekt údajů, musí se provést hodnocení dopadů, posoudit rizika a kompenzovat je
- Pokud ale bude již návrh právního předpisu, který zpracování upravuje, doplněn o analýzu rizik pro soukromí, nejsou nutná další hodnocení dopadů ani konzultace s ÚOOÚ

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

- Je povinný pro **orgány veřejné moci** a „veřejné subjekty“
 - Povinnost jmenovat pověřence je pro „veřejné subjekty“ zákonem omezena tak, aby **nešlo** o takovou šíři subjektů jako jsou „veřejné instituce“ podle zákona o svobodném přístupu k informacím (nespadnou tam příspěvkové organizace, obecní s.r.o. apod.)
- Dále je povinný pro správce, kteří
 - provádějí rozsáhlé monitorování (mobilní operátoři, banky), nebo
 - zpracovávají citlivé údaje ve velkém rozsahu (např. krajské nemocnice)
- Lze jmenovat jednoho pověřence pro více orgánů nebo subjektů (například pro **všechny základní školy** v regionu), záleží na rozsahu 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, ale nemusí to mít jako jedinou činnost

Co na veřejnou správu prakticky nedopadne

- Na veřejnou správu se v rozsahu, v jakém provádí zpracování při plnění právní povinnosti, úkolu ve veřejném zájmu nebo výkonu veřejné moci, nebude vztahovat téměř nebo zcela:
 - Právo na **výmaz nebo likvidaci** (článek 17) se uplatní až po předepsané skartační době
 - Právo na **přenositelnost** (článek 18) – většina zpracování je podle zákona nebo veřejného zájmu
 - Právo na **námitku** (článek 21) – jen ve výjimečných případech

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