MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

GDPR – evoluce v ochraně osobních údajů

Karel Bačkovský, Petr Habarta, Jan Potměšil,
Ondřej Beňák, Kateřina Jamborová

OBP MVČR

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
- 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

Nařízení z pohledu právní formy

- Většina ustanovení platí přímo a „nepřekládá“ se do vnitrostátních zákonů → odchylky a rozdíly jen ve vymezených oblastech
- Nařízení vychází v Úředním věstníku EU, ne v naší Sbírce
- Cílem je zajistit jednotný právní režim v celé EU → ušetřit podnikům 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
- zákon může upřesnit zpracování ve veřejné sféře – proto se dále použijí české zákony, podle kterých úřady postupují

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

Struktura návrhu zákona

- Hlava I – základní ustanovení
  - Působnost zákona, subjekt údajů
- Hlava II – adaptace na GDPR
  - Výjimky z GDPR, vyjasnění některých pravidel GDPR
  - Zvláštní výjimky pro novinářské, umělecké, akademické účely
- Hlava III – transpozice Trestněprávní směrnice (neplatí ani pro obecní nebo městské policie)
- Hlava IV – pravidla pro zpravodajské služby aj.
- Hlava V – postavení ÚOOÚ
  - Přístup k informacím chráněným mlčenlivostí
- Hlava VI – přestupky a pokuty

Výjimky a vyjasnění GDPR

- Pokud má správce zákonem stanovenou povinnost, vykonává veřejnou moc nebo plní úkol ve veřejném zájmu:
  - je oprávněn kvůli tomu zpracovávat osobní údaje
  - může informace o zpracování poskytnout zveřejněním na internetu
- Správce zajišťující některé chráněné zájmy nemusí posuzovat slučitelnost účelů
- Povinnost jmenovat pověřence mají orgány veřejné moci a jim se blížící úzká skupina „veřejných subjektů“
- Subsidiární výjimky z práv subjektu údajů za kvůli zajištění některých chráněných zájmů kompenzovány 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

Pravomoci ÚOOÚ a pokuty

- Prolomení některých zákonem stanovených mlčenlivostí pro kontrolní činnost ÚOOÚ (nadále platí ochrana utajovaných informací)
- Kompenzováno mlčenlivostí zaměstnanců ÚOOÚ
- Omezení pokut pro veřejnou sféru na současných 10 mil. Kč
- Nové ustanovení, podle kterého ÚOOÚ ani nemusí zahájit řízení o přestupku např. z neznalosti, pokud je správce ochoten věc napravit

Co zákon neobsahuje

- 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

Co když zákon nebude 25. května?

- GDPR platí přímo, u většiny pravidel se to vůbec nepozná
- U některých povinností, kde zákon přináší výjimky, je možné je i nyní splnit alternativně (oznamování informací o zpracování oběžníky)
- Pro běžnou praxi obcí nepůjde o zásadní problémy

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

- Přístup založený na riziku – povinnosti mají odpovídat riziku
- *Standardní a záměrná ochrana osobních údajů*
- Příprava **záznamů o činnostech zpracování** (čl. 30) namísto ohlašování zpracování na ÚOOÚ nebo např. na webu
- **Hlášení porušení zabezpečení** osobních údajů (čl. 33 a 34)
- **Posouzení vlivu na ochranu** osobních údajů (čl. 35)
- **Konzultace** s ÚOOÚ (čl. 36)
- **Pověřenec** pro ochranu osobních údajů (čl. 37)
- *Více podmínek pro udělení souhlasu*
- *Věk pro on-line souhlas*
- *Akreditace certifikačních orgánů*
- *Kodexy chování*

Zpracovatel (čl. 28)

- Koncepčně stále platí, že správce je ten, kdo určuje účel a prostředky zpracování
- Zpracovatel provádí zpracování pro správce na základě smlouvy nebo zákona podle jeho pokynů
- Nutno zkontrolovat smlouvy se zpracovateli, zda vyhovují článku 28, kde jsou povinné náležitosti
- Rychlostní radary a pod. – nejde o automatizované rozhodování, protože rozhodnutí přijímá člověk, byť na základě automaticky připravených podkladů – neplatí proto omezení podle čl. 22 GDPR (smlouva se subjektem, výslovný souhlas, zákon)

Záznamy o činnostech zpracování (čl. 30)

- Nahrazuje oznamování nových zpracování
- Slouží k přehledu o zpracovávaných os. údajích pro správce i dozorový úřad
- Identifikace správce, účely zpracování, kategorie subjektů údajů a osobních údajů, kategorie příjemců, info o příp. předání do zahraničí, lhůty pro výmaz, obecně o bezpečnostních opatřeních
- Vede se písemně, lze i elektronicky
- Netýká se organizací do 250 osob, leda zpracování rizikové, soustavné nebo jde o citlivé údaje

Hlášení porušení zabezpečení (čl. 33,34)

- 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 (čl. 35)

- 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 (čl. 36)

- 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

Kamerové systémy

- Rozsáhlé systémy monitorující veřejné prostory se považují za vysoké riziko:
  - pokud budou spuštěny po 25. květnu 2018, musí se provést posouzení vlivu na ochranu soukromí (článek 35)
  - pokud z hodnocení dopadů vyjde vysoké riziko, které správce nedokáže kompenzovat, musí konzultovat ÚOOÚ (čl. 36)
- Snaha dozorových úřadů dále se kamerovým systémům ve veřejných prostorách pozorně věnovat – lze čekat, že „rozsáhlost“ a „míru rizika“ budou posuzovat spíš přísně.

Pověřenec pro ochranu os. údajů (čl. 37)

- 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

Kontakty:

- Odbor dozoru a kontroly veřejné správy MV (ODK): odbordk@mvcr.cz
- Odbor bezpečnostní politiky MV (OBP): obp@mvcr.cz
- Odbor legislativy a koordinace předpisů MV (OLG): ol@mvcr.cz
- **Ministerstvo vnitra ČR**: posta@mvcr.cz, www.mvcr.cz/gdpr
- **Úřad pro ochranu osobních údajů**: posta@uoou.cz, www.uoou.cz