ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ

KISK FF MU

Mezinárodní úpravy v českém zákoně o ochraně OÚ

- Vychází ze směrnic a úmluv EU
- Z. při zpracování OÚ na území ČR, i když správce jinde (i mimo EU)
- Aktuálně diskutované GDPR - *nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES*
- Dále úprava aktuální, i nová (nejpozději 25. 5. 2018, zákon?) a s důrazem na knihovny (viz Příručka pro knihovny)

Zákon o ochraně OÚ

- Právo každého na ochranu před neoprávněným zásahem do soukromí
- Práva a povinnosti při veškeré práci s OÚ, zpracování kýmkoli mimo:
  - Zpracování FO výlučně pro osobní potřebu
  - Nahodilé shromažďování, pokud nezpracovávány
  - Zpracování nezbytných pro povinnosti v zákoně

Pojmy v zákoně

- Subjekt údajů – správce – zpracovatel
- OÚ
  - Informace o určitelném SÚ (v konkrétním případě)
  - Přímá X nepřímá (souborem, vč. IS VS)
  - Citlivý = národnost, odsouzení, zdraví… + biometrický
  - Zveřejněný = dostupný hromadnými sdělovacími prostředky i jako součást veřejného seznamu
  - ZMĚNY:
    - OÚ i elektronická identifikace (e-mail, IP adresa…)
    - Citlivé údaje => zvláštní kategorie OÚ (+ genetické)
    - Přísnější ochrana OÚ dětí, např. až do 16 let u služeb informační společnosti
- Zpracování = jakákoli systematická práce s OÚ, od shromažďování po likvidaci
- Shromažďování = systematicky pro zpracování

Povinnosti správce

- Před zahájením zpracování **informovat ÚOOÚ**
- Myslet na **soukromí SÚ** a **informovat** ho o zpracování
- **Stanovit** účel, prostředky a způsob zpracování => jen s tím a jen v **nezbytném rozsahu**
- Shromažďovat OÚ pouze **otevřeně** (žádné záminky)
- **Nesdružovat** OÚ k rozdílným účelům
- Jen **přesné** OÚ, aktualizace hned po zjištění, jinak znepřístupnění či označení
- Jen nezbytnou dobu, pak **likvidace**, výjimka věda, statistika, archivnictví + co nejdřív **anonymizace**

Povinnosti správce - NOVĚ

- Zákonnost, korektnost a transparentnost (k SÚ)
- Účelové omezení – konkrétní, výslovně vyjádřené (+ archivace, věda a výzkum, statistika)
- Minimalizace údajů (k účelu)
- Přesnost (OÚ)
- Omezení uložení (umožnění identifikace jen po nezbytně dlouho pro účel + výjimky výše za předpokladu technicko-organizačních opatření)
- Integrita a důvěrnost (zabezpečení technické a organizační před neoprávněným zpracováním, náhodnou ztrátou, zničením nebo poškozením)
- Odpovědnost (schopnost doložení souladu), opatření na základě posouzení rizika konkrétní OÚ, zrušení oznamovací povinnosti

Povinnosti zpracovatele

- Obdobné jako správce
- Přesun činnosti na zpracovatele nutný písemně (rozsah, účel a doba trvání + záruky o technickém a organizačním zabezpečení)
- Při zjištění problémů u správce nutné oznámit, jinak sdílí podíl za škodu
- NOVĚ: výrazné zvýšení odpovědnosti zpracovatele (přiblížení správci)

Souhlas SÚ

- „Svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“ (§ 4)
- Správce schopen prokázat po celé zpracování
- Odvolání, příp. zamítnutí zpracování písemně
- Výjimky bez souhlasu
  - Dodržení právní povinnosti
  - Ochrana života či práv subjektu
  - Oprávněně zveřejněné OÚ dle předpisu

Zákonnost zpracování pro konkrétní účel - NOVĚ

- Min. 1 z dále uvedených podmínek a v odpovídajícím rozsahu
  - Plnění smlouvy (přihláška do knihovny)
  - Plnění právní povinnosti (evidence zaměstnanců)
  - Plnění úkolu ve veřejném zájmu nebo výkonu veřejné moci (právo veřejnost na informace o autorech)
  - Oprávněný zájem (nutný balanční test, např. číslo identifikačního průkazu nebo kamerový systém pro ochranu majetku)
  - Ochrana životně důležitých zájmů SÚ nebo jiné FO
  - Souhlas pro konkrétní účel (nepodmíněný, odvolatelný; evidování bývalých zaměstnanců/žadatelů o zaměstnání)

Ochrana OÚ

- **Nutná** proti neoprávněnému i nahodilému zpracování (přístupu/změně/přenosu…) či jinému zneužití OÚ + **mlčenlivost**, a to i po ukončení
- „…povinen zpracovat a dokumentovat přijatá a provedená **technicko-organizační opatření** k zajištění ochrany…“ (§ 13, odst. 2)
- Opět výjimka v zodpovědnosti při vynaloženém úsilí pro zabránění problému
- Při problému subjekt může žádat nápravu správce, následně pomoc ÚOOÚ
- NOVĚ: opatření pro soulad se změnami, nutná dokumentace

Úřad pro ochranu osobních údajů

- Nezávislý orgán, financován ze samostatné kapitoly rozpočtu ČR (podobně jako NKÚ)
- Dozorový úřad pro OÚ (+ nevyžádané zprávy)
- Organizace:
  - Předseda a inspektoři (7): jmenuje a odvolává prezident na návrh senátu, nutné VŠ vzdělání, bezúhonnost a způsobilost a žádné funkce ve státní správě a samosprávě nebo politice
  - Další zaměstnanci (sekce dozorových činností, informatiky a základních identifikátorů, bezpečnostní ředitel a další)
- NOVĚ: dozorový orgán bude, ale práce nastavena v zákoně, obecně stále poradenství, kontroly, mezinárodní spolupráce

Činnosti

- **Dohlíží** na dodržování povinností při zpracování OÚ
- Vede registr zpracování OÚ
- Přijímá **podněty a stížnosti** k zpracování a informuje o výsledku
- Výroční zpráva o činnosti
- Další působnosti dané zákonem
- Projednává správní delikty a **pokuty**
- **Konzultace** v oblasti OÚ
- Zajišťuje plnění požadavků **mezinárodních** smluv
- Spolupracuje s obdobnými úřady jiných států

Oznamovací povinnost

- Před zahájením zpracování nutné informovat ÚOOÚ
- Registrované informace: o správci a zpracování (účel, typy subjektů a OÚ, způsob a ochrana)
- Při splnění všech podmínek zápis do registru a vydání osvědčení, jinak výzva k doplnění, po lhůtě na oznamovatele pohlíženo, jako by neoznámil
- Bez nutnosti oznámení:
  - OÚ z legálně veřejných datových souborů
  - Zpracování dle zvláštního zákona
  - Nutné pro politické, … cíle sdružení, ale jen o SÚ v opakujícím se kontaktu a bez souhlasu nezveřejněno
- NOVĚ: povinnost zrušena

Konec zpracování dle ÚOOÚ

- Při důvodné obavě z porušení z. při zpracování zahájí z vlastního podnětu řízení
- Pokud problém nenalezen, jen zápis
- Když nalezen, zrušení povolení dalšího zpracování + úprava registru
- Po pominutí účelu zpracování ÚOOÚ sám nebo podnětem správce zruší registraci
- Po ukončení činnosti správce nutné ÚOOÚ informovat o naložení s OÚ
- NOVĚ: bez registru nutné po vypršení nezbytné doby anonymizace, skartace

Kontrolní činnost

- Dle základě kontrolního plánu (schválen na rok) nebo podnětů a stížností
- Nutné se prokázat
- Kontrolující oprávněni: „oprávněn seznamovat se se všemi informacemi v rozsahu nezbytném pro dosažení účelu kontroly, včetně citlivých údajů“
- Při zjištění nedostatku uloženo opatření k odstranění + lhůta; pokud opraveno, lze upustit od uložení pokuty
- Výsledky na stránkách: shrnutí a zdůvodnění

Informační činnost

- Nevyžádaná obchodní sdělení a elektronická komunikace (telekomunikace a její regulace) zvlášť, vč. právních předpisů
- Kategorie Zahraničí: zajímavé konkrétní problémy a jejich řešení v zahraničí, např. K novým zásadám ochrany osobních údajů společnosti Google
- Právní předpisy a judikatura, vč. souvisejících předpisů, další osvětové materiály
- Zvláštní snaha cílit na děti a dospívající, hl. zábavou, příklady situací, soutěžemi (Soutěž "Moje soukromí! Nekoukat, nešťourat!" podporuje i SKIP)
- Výsledky činnosti ÚOOÚ

Nejčastější problémy (Výroční zpráva 2011)

- „zneužívání (…) k jiným než deklarovaným účelům,
- zpřístupňování (…) neoprávněným osobám,
- nepřijetí adekvátních technicko-organizačních opatření (…),
- překračování principů proporcionality mezi chráněným zájmem (…) a zasahováním do soukromí fyzických osob,
- neplnění informační a oznamovací povinnosti.“

Příklady neopatrnosti

- Odesílání e-mailu množství osob v poli příjemce (ne skrytý)
- Zasílání OÚ nešifrovaně (možný omyl v adrese)
- Špatně začerněno
- V tiskárně neskartovány chybné výtisky s OÚ
- Traverzováním webu (i omylem) přístup k informacím o jiném klientovi
- Veřejně vystaveny faktury vč. OÚ zákazníků

Další zdroje k tématu

- Občanský zákoník, §§ 12-13 ochrana soukromí, osobnosti apod.
- Trestní zákoník, § 180 Neoprávněné nakládání s osobními údaji
- Iuridicum Remedium + Big Brother Awards

Otázky

- Musí zákon 101/2000 Sb. dodržovat při zpracování OÚ:
  - Autobazar?
  - Já ve svém osobním adresáři?
  - Městský úřad?
  - Policie ČR?
  - Policie, když je v ohrožení bezpečnost EU?
  - Živnostenský úřad?
- Jaký je vztah mezi osobními a citlivými údaji? A mezi shromažďováním a zpracováním OÚ?
- Kdo je zodpovědný za prozrazení zpracovávaných OÚ dle zákona?
- Jaké instituci se zodpovídá ÚOOÚ?

Výklad ÚOOÚ pro knihovny (stanovisko č. 2/2002)

- Má přednost knihovní zákon nebo z. o ochraně OÚ?
- => KZ k ZOOÚ zákonem zvláštním, ale práce s OÚ v něm není, proto na to aplikace ZOOÚ
- Je nutný souhlas zákazníka ke zpracování jeho OÚ?
- => bez souhlasu možnost pro ochranu práv správce a pro plnění smlouvy (např. o výpůjčce, MVS, rešerše…), ale jen po dobu trvání tohoto X údaje o zákaznících trvalé (i když nepůjčeno nic), proto nutný souhlas
- Musí knihovna smazat OÚ zákazníka, který o to požádal, když ještě nemá zaplaceno zpozdné za vrácené knihy?
- => ne, zpracovávat lze i bez souhlasu po dobu trvání smlouvy nebo pro ochranu zájmů a práv správce, tj. i výpůjčka do vyrovnání závazků

Výklad ÚOOÚ pro knihovny (stanovisko č. 2/2002) (2)

- Může knihovna zpracovávat OÚ i po odvolání souhlasu a vyrovnání závazků pro případné řešení poškození knihy oznámené následujícím vypůjčitelem?
- => ne, závada by musela být zjištěna hned při vrácení, jinak irelevantní
- Může knihovna chtít od zákazníka všechny údaje potřebné ke všem jí nabízeným službám, i když zákazník se jejich využití zřekne?
- => nesmí a registrační formulář by tomu měl být přizpůsoben, aby byly požadovány jen nezbytné údaje, dále nesmí být zjištěné doplňováno adresně zjišťovanými dalšími informacemi, ať už je subjektivní zdůvodnění jakékoli, možné jen anketní
- Je v ZOOÚ důvod, proč je v NTK možný statut zákazníka i návštěvníka?
- => ano, VKIS nelze na poskytnutí OÚ vázat (+ Listina základních práv a svobod), ale je třeba informovat o omezeních (např. jen prezenční, ne absenční výpůjčky)

Otázky z praxe – Je v pořádku postup knihovny?

- Při registraci čtenářů vyžaduje identifikaci průkazem totožnosti
- Při registraci se zaznamená číslo průkazu totožnosti
- + jméno, příjmení, datum narození, e-mail FO, adresa trvalého pobytu, číslo karty, druh a číslo dokladu pro ověření údajů, údaje o přestupcích a zákazech čtenáře
- Pro identifikaci PO požadují doklad o zřízení a přidělení IČ
- Zaznamenávají čtenářskou historii v profilu čtenáře
- Záznam po dobu registrace a do vyrovnání závazků (+ 5 let dle směrnice o skartačním řádu)
- Monitoring práce uživatelů s technikou knihovny
- Monitoring všech v knihovně kamerami

Budoucí změny – GDPR (General Data Protection Regulation)

- Nařízení EU (státy musí převzít)
- Schváleno v dubnu 2016, platné od 25. 5. 2018
- Do té doby nutný zákon + změny v IS a nakládání s OÚ u všech správců
- Více než 50 bodů pro úpravu
- Řešení OÚ v EU nebo o občanech EU
- Nadále dozor ÚOOÚ (pod EDPB – Evropský sbor pro ochranu osobních údajů)
- Podrobnosti na GDPR prakticky

Klíčové změny v GDPR

- Výrazné zvýšení sankcí
- Prokazatelné doložení ochrany OÚ správcem i zpracovatelem => administrace
- Rozšíření definice OÚ – i technické údaje (e-mail, IP adresa, cookie…), telefonní číslo, identifikátory vydané státem
- Mezi citlivými údaji nově OÚ dětí a genetické údaje
- Opravdu jen data nezbytná k účelu
- Více zodpovědnosti zpracovatelů (ne vše na správci)
- Oznamovací povinnosti při narušení bezpečnosti OÚ nejpozději do 72 hodin od zjištění narušení
- Institut pověřence pro OÚ
- Analýza rizikovosti OÚ ve zpracování

Klíčové změny v GDPR – práva subjektů údajů

- více informováni
- možnost námitky proti zpracování => bez prokazatelných důvodů dál nemožné zpracovávat
- přenositelnost OÚ k jinému správci při automatizovaném zpracování (SÚ dostane strukturovaný, strojově čitelný formát)
- přístup k OÚ pro SÚ, ideálně přímo a online
- právo na výmaz + právo být zapomenut (pokud není právní důvod dalšího zpracování)

GDPR a knihovny

- AKS posuzované každý individuálně (rizika), zajištění dat vhodné smluvně ošetřit s dodavatelem
- Možné sdílení identit mezi knihovnami se souhlasem SÚ
- Není potřeba pověřence pro ochranu OÚ
- Souhlas zákonného zástupce až do 16 let pro služby informační společnosti
- Požadavek pro všechny IS – protokol https (šifrování)
- Zvýšení dokumentace, vč. smluv se zpracovateli