Ochrana osobních údajů ve veřejné správě

NP302Zk, 29. 9. 2017

Jakub Míšek
jkb.misek@mail.muni.cz

Osnova přednášky

- Základní koncepty ochrany osobních údajů
- Povinnosti správce
- Práva subjektu údajů
- Přeshraniční působnost a předávání údajů do zahraničí
- Příklad: Osobní údaje v. PSI

Ochrana soukromí (osobnosti) v. Osobní údaje

- Rozsah působnosti
- Reaktivní v. preventivní princip
- Distributivní v. nedistributivní právo
- Soukromoprávní v. veřejnoprávní
- Žaloba v. podnět
- Občanské právo v. správní právo

Historie ochrany osobních údajů

- Pravidla ochrany soukromí a přeshraničních toků osobních údajů vydaná Organizací pro hospodářskou spolupráci a rozvoj (OECD) (1980)
- Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (tzv. „Úmluva 108“) (1981)
- Legislativní práce na směrnici 95/46/ES započaly v léta 1990

Ústavně právní úroveň

- Čl. 8 Evropské úmluvy o ochraně lidských práv (Právo na respektování rodinného a soukromého života)
  - Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.
  - Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.
- Listina základních práv a svobod
  - Čl. 7 (Ochrana osobnosti a obydlí
  - Čl. 10 (zejména odstavec 3: „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“)

Ústavně právní úroveň

- Listina základních práv Evropské unie
  - Čl. 8 – Ochrana osobních údajů

1. Každý má právo na ochranu osobních údajů, které se ho týkají.

2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.

3. Na dodržování těchto pravidel dohlíží nezávislý orgán.

Podústavní předpisy

- Směrnice 95/46/ES
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Nařízení EU 2016/679 – Obecné nařízení o ochraně osobních údajů (tzv. „GDPR“)

Základní koncepty – Osobní údaj

- § 4 písm. a) „*osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*“
- Přímá v. nepřímá identifikace
- Kontext!

Základní koncepty – Osobní údaj

Objektivní v. Subjektivní pojetí

- Objektivní pojetí
  - Pokud existuje objektivní možnost (byť teoretická a ilegální) identifikovat fyzickou osobu je to osobní údajů
- Subjektivní pojetí
  - Limitace nepřiměřenými náklady a nelegálností
- Příklad 1 – Rozhodnutí SDEU ve věci Breyer
- Příklad 2 – Anonymizace

Základní koncepty – Osobní údaj

- Příklad 1 - Rozhodnutí SDEU ve věci Breyer
  - Dynamická IP adresa je osobní údajů (navazuje na starší judikaturu SDEU)
  - Bod 46 rozhodnutí:

  O osobní údaj by se nejednalo v případě, že „ *identifikace subjektu údajů byla zakázána zákonem nebo … byla prakticky neproveditelná, například z důvodu skutečnosti, že by vyžadovala nepřiměřené úsilí z časového hlediska a z hlediska ekonomických a lidských zdrojů, takže riziko identifikace by se ve skutečnosti jevilo bezvýznamné“.*

Základní koncepty – Osobní údaj

- Příklad 2 – Anonymizace
  - AOL vyhledávač
    - Anonymizovaná data o vyhledávání zveřejněná 2006
  - Jedinečná kombinace pohlaví, datum narození a ZIP code – identifikace 87% obyvatel USA
  - Případ Netflix
    - Hodnocení kvality filmů uživateli
      - Hodnocení 6 „nezvyklých“ filmů – 84 % jedinečnost
      - Čas v rozsahu dvou týdnů
        - 6 libovolných filmů 99%
        - 2 libovolné filmy 68 %
    - Kombinace s dalšími zdroji (IMDb)

Citlivý osobní údaj

= zvláštní kategorie osobních údajů (GDPR, čl. 9)

„vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby“

Anonymizace v. Pseudonymizace

- Anonymizace – problém
  - Anonymita v. vypovídací hodnota
  - Anonymizační techniky
    - Odstranění přímých identifikátorů (jméno, identifikační čísla atd.)
    - Zobecnění (zmenšení granularity)
    - Agregace – statistika
    - Záměna dat
- Pseudonymizace
  - GDPR: *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě“*

Základní koncepty – Zpracování osobních údajů

- jakákoliv operace nebo soubor operací s osobními údaji
- shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení
- Zpracování pro osobní potřebu (rozhodnutí SDEU ve věci Ryneš)

Základní koncepty – Správce a zpracovatel osobních údajů

- fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými **určuje účely a prostředky zpracování osobních údajů**
- Správce může pověřit zpracovatele
  - Definice: „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce*“
  - Smlouva
  - Oprávnění v rozsahu pověření

Povinnosti správce

- Stanovit **<u>účel</u>** zpracování
- Stanovit prostředky a způsob zpracování
- Zpracovávat pouze přesné osobní údaje
- Shromažďovat údaje pouze za stanoveným účelem a v rozsahu nezbytném pro jeho naplnění
- Shromažďovat údaje otevřeně
- Nesdružovat údaje získané za jinými účely
- Informovat subjekt o zpracování
- (GDPR) Povinnosti vyplývající ze zásady odpovědnosti

Úhelný kámen – Účel zpracování

Vůči deklarovanému účelu zpracování se poměřuje jeho zákonnost a plnění povinností správce

Základní zásady (GDPR)

- Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem
- Zásada limitace účelem
- Zásada minimalizace údajů (nezbytný rozsah)
- Zásada přesnosti
- Zásada omezení uložení (souvisí s minimalizací; právo být zapomenut)
- Zásada integrity a důvěrnosti
- Zásada odpovědnosti

Princip odpovědnosti (GDPR)

- Správce má povinnost být schopen kdykoli prokázat, že splňuje zákonné požadavky – nezbytné vedení dokumentace o zpracování
- Záměrná a standardní ochrana osobních údajů (Data protection by design and default)
- Společní správci (čl. 26 GDPR) – nutnost vzájemného ujednání o povinnostech
- Zabezpečení zpracování a hlášení bezpečnostních incidentů

Zákonnost zpracování – právní tituly

- Souhlas se zpracováním
- **Zpracování nezbytné pro dodržení právní povinnosti správce**
- Zpracování nezbytné pro plnění smlouvy
- Ochrana životně důležitých zájmů subjektu údajů (souhlas bez zbytečného odkladu)
- Oprávněně zveřejněné osobní údaje
- Nezbytnost pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby (test proporcionality)
- Údaje veřejně činných osob, funkcionářů nebo zaměstnanců veřejné správy vypovídající o veřejné nebo úřední činnosti
- Zpracování pro účely archivnictví podle zvláštního zákona (499/2004 Sb.)

Souhlas

- Většinou není potřeba
- Požadavky:
  - Svobodný
  - Určitý
  - Vědomý a informovaný
  - Explicitní

Zpracování citlivých osobní údajů

- Souhlas
- plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany
- ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
- zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle (jen na členy organizace)
- údaje zjevně zveřejněné subjektem údajů
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí
- významný veřejný zájem
- …

GDPR novinka - Pověřenec pro ochranu osobních údajů

- Povinně:
  - zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí
    - Metodické doporučení MV k pověřencům v obcích
  - hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů
  - hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů
  - V dalších případech pokud to uvede zákon
- Může být víc správců na jednoho pověřence

GDPR novinka – Posouzení vlivu zpracování

- Nejasná povinnost – raději to dělejte (princip odpovědnosti)
  - Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů
- Povinně:
  - Profilování
  - Rozsáhlé zpracování citlivých osobních údajů
  - Rozsáhlé monitorování veřejně přístupných prostor

Práva subjektu údajů (95/46/ES + 101/2000 Sb.)

- Přístup k údajům (§ 12)
  - Sdělení o
    - Účelu zpracování
    - Kategoriích osobních údajů
    - Povaze automatizovaného zpracování
    - Příjemci, případně kategoriích příjemců
- Právo na námitku (§ 21)
  - Pokud se subjekt domnívá, že je zpracováváno nezákonně nebo v rozporu s ochranou jeho soukromého a osobního života
    - Vysvětlení
    - Odstranění nezákonného stavu
    - Případ Google Spain a „právo být zapomenut“

Práva subjektu údajů (GDPR)

- Nově formulovaná, staré principy
- Právo na přístup (čl. 15) – jako ve směrnici, ale navíc:
  - plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby
  - informaci o existenci práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování a nebo vznést námitku proti tomuto zpracování
  - informaci o existenci práva podat stížnost u dozorového úřadu
  - veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů
  - poskytnutí kopie zpracovávaných osobních údajů

Práva subjektu údajů (GDPR)

- Právo na výmaz („právo být zapomenut“) a právo na omezení zpracování
  - taxativní vymezení v čl. 17 a 18
- Právo na přenositelnost údajů (čl. 20)
  - Týká se údajů poskytnutých subjektem
- Právo vznést námitku proti zpracování
  - Když je právní titul:
    - zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce
    - zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany
- Přímé nároky

Teritoriální působnost

- Směrnice 95/46/ES:
  - Užití národního práva:
    - zpracování je prováděno v rámci činností provozovny správce na území členského státu; pokud je stejný správce usazen na území několika členských států, musí přijmout opatření nezbytná pro dodržování povinností stanovených použitelným vnitrostátním právem každou ze svých provozoven
    - Rozhodnutí SDEU ve věci Google Spain a Weltimmo
      - Provozovna = bankovní účet, webová prezentace a stálé právní zastoupení
- GDPR:
  - „One stop shop“
  - Hlavní provozovna = místo, kde se nachází jeho ústřední správa v Unii

GDPR – přeshraniční působnost

- Již aktuální případ – Rozhodnutí Google Spain a CNIL
- Čl. 3 odst. 2
  - *Toto nařízení se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí:*
    - *a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba; nebo*
    - *b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie.*
- Problémy:
  - Vymáhání práva
  - „Všechno nebo nic“

Předávání údajů do zahraničí

- V rámci EU a EHS bez omezení
- Mimo EU a EHS:
  - Strany Úmluvy 108
    - Doposud možné předávání; od GDPR spíš ne
  - Rozhodnutí Komise o adekvátní úrovně ochrany
  - Předávání při existenci potřebných opatření pro zajištění úrovně ochrany
    - právně závazný a vymahatelný nástroj mezi orgány veřejné moci nebo veřejnými subjekty
    - závazná podniková pravidla
    - standardní smluvní doložky
    - schválený kodex chování
  - Souhlas subjektu údajů

Předávání údajů do zahraničí – Rozhodnutí komise o adekvátní úrovni ochrany

- Adekvátní neznamená totožná
- Safe Harbour a Privacy Shield
  - Rozhodnutí SDEU ve věci Schrems
- Další:
  - Andora
  - Argentina
  - Kanada
  - Švýcarsko
  - Faerské ostrovy
  - Guernsey
  - Izrael
  - Ostrova Man
  - Jersey
  - Nový Zéland
  - Uruguay

Předávání údajů do zahraničí

- Problém – umístění dat
  - Cloud
  - Transfer
- Vhodnější regulace – skrze usazení správců a zpracovatelů

Praktický příklad: Vztah OÚ a PSI

- 2 typy správců údajů
  - Poskytovatel informací (orgán veřejné správy)
    - Plní své úkoly dané zákonem
    - Právní titul: plnění zákonné povinnosti
  - 3. osoba, která data přijímá a pracuje s nimi dál (tvůrce aplikací)
    - Určuje si účel
    - Potřebuje vhodný právní titul (nejčastěji zpracování za účelem ochrany práv a oprávněného zájmu správce, dle §5 odst. 2 písm. e))
    - Od GDPR není možnost zpracování oprávněně zveřejněných údajů

Praktický příklad: Vztah OÚ a PSI

- Poskytování informací - obecně z. č. 106/1999 Sb.
  - Aplikuje se, pokud zvláštní zákon neupravuje jinak
  - Typové dělení:
    - Na žádost
    - Zveřejněním
      - Povinné
      - Dobrovolné (§ 5 odst. 7 z. č. 106/1999 Sb.)
  - Požadavky na poskytování zveřejněním
    - § 4b odst. 1: otevřený a pokud možno strojově čitelný formát, metadata a otevřené formální normy
    - § 4b odst. 2: kvalifikované poskytování zveřejněním - jako otevřená data
      - Nařízení vlády č. 425/2016 Sb.

Závěrem

Kdo měl režim ochrany osobních údajů v pořádku nyní, nemusí se GDPR bát.

Děkuji za pozornost.

Otázky?