

Ochrana osobních údajů

Jakub Míšek

Osnova přednášky

- Základní koncepty ochrany osobních údajů
- Povinnosti správce
- Práva subjektu údajů
- Přeshraniční působnost a předávání údajů do zahraničí



Ochrana soukromí (osobnosti) v. Osobní údaje

- Rozdílné cíle a účely úpravy
 - Ochrana osobních údajů dvojí účel: ochrana před zásahem a zároveň umožnění korektního zpracování
- Rozsah působnosti
- Reaktivní v. preventivní princip
- Distributivní v. nedistributivní právo
- Soukromoprávní v. veřejnoprávní (?)
- Občanské právo v. správní právo

Historie ochrany osobních údajů

- Evropská úmluva o ochraně lidských práv a základních svobod z roku 1950
- 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)
 - Revize, tzv. Úmluva 108+
- 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.“)

LZPS čl. 7

- (1) Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

Čl. 10 Listiny [Ochrana osobnosti]

- (1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.
- (2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.
- (3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Informační sebeurčení člověka

- Premisa – centricnost člověka jako základního zájmu práva
- 1983, Německo (Spolkový ústavní soud, kauza sčítání lidu)
- Původně odvozeno od ochrany soukromí a osobních údajů
 - Možnost určit si, co o mně bude známo
- Dnes integrální součástí:
 - Svoboda projevu
 - Ochrana soukromí + Ochrana osobních údajů
 - Právo na vzdělání
 - Právo na informace veřejného prostoru
- Nové technologie – není kvalitativní změna
 - Jen nové možnosti komunikace

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“)
- Zákon č. 110/2019 Sb., o zpracování osobních údajů

Základní teze systému ochrany osobních údajů

I. Prevenční princip

Základní teze systému ochrany osobních údajů

I. Prevenční princip



A. Široká aplikace

B. Limitace a vázanost účelem
zpracování

Základní teze systému ochrany osobních údajů

Obecné nařízení o ochraně osobních údajů



II. Princip odpovědnosti správce údajů



III. Regulace založená na riziku



Základní koncepty – Osobní údaj

- Čl. 4 odst. 1 *„osobními údaji (se rozumí) veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*
- 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 údaj
- Subjektivní pojetí
 - Limitace nepřiměřenými náklady a nelegálností

Základní koncepty – Osobní údaj

- Příklad 1 - Rozhodnutí SDEU ve věci Breyer
 - Dynamická IP adresa je osobní údaj (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“.

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 – 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“



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 Ryněš)

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**
- Společní správci
 - Nová rozhodovací praxe SDEU
 - C-210/16 - Wirtschaftsakademie Schleswig-Holstein (5. 6. 2018)
 - C-25/17 - Jehovan todistajat (10. 7. 2018)
 - C-40/17 - Fashion ID (29. 7. 2019)
- 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

Místní působnost

- Čl. 3, odst. 1:
 - *Toto nařízení se vztahuje na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii bez ohledu na to, zda zpracování probíhá v Unii či mimo ni.*
- Recitál 22:
 - *Provozovna předpokládá účinný a skutečný výkon činnosti prostřednictvím stálého zařízení. Právní forma této provozovny, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem.*
- Rozhodnutí SDEU ve věci Google Spain a Weltimmo
 - Provozovna = bankovní účet, webová prezentace a stálé právní zastoupení
- „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“

Základní zásady zpracování

- 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

Povinnosti správce

- Stanovit účel 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
- **Povinnosti vyplývající ze zásady odpovědnosti**

Úhelný kámen – Účel zpracování

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

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 (Čl. 6 odst. 1 GDPR)

- 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)
- Zpracování nezbytné pro plnění úkolu ve veřejném zájmu, nebo při výkonu veřejné moci, kterým je pověřen správce
- Nezbytnost zpracování pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby (test proporcionality)

Souhlas

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

Zpracování zvláštních kategorií osobních údajů (tzv. „citlivé údaje“)

- Čl. 9 Obecného nařízení
- 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
- ...

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

Posouzení vlivu zpracování

- 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

**HUMAN,
GIVE ME
PURRIVACY**



Práva subjektu údajů (Čl. 15-23)

- Právo být informován o zpracování osobních údajů
 - Čl. 13 (když pochází údaje přímo od subjektu)
 - Čl. 14 (když jsou údaje sesbírané jinde)
- Právo na přístup k údajům (čl. 15)
- Právo na opravu (čl. 16)
- Právo na výmaz („právo být zapomenut“) (čl. 17)
- Právo na omezení zpracování (čl. 18)
- Právo na přenositelnost údajů (čl. 20)
- Právo vznést námitku (čl. 21)
 - Když zpracování z důvodu: oprávněného zájmu NEBO plnění úkolu ve veřejném zájmu NEBO přímý marketing
- Právo na ochranu před automatizovaným individuálním rozhodováním, včetně profilování (čl. 22)

Právo na informace o zpracování osobních údajů

- Základní informace o zpracování:
 - Kdo, jak, proč (účel), proč (právní titul), jak dlouho, kde...
- Čl. 14 Odst. 5 – výjimky z informační povinnosti
 - Pokud subjekt již informaci má
 - Pokud se ukáže, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí
 - ...

Právo na přístup (Čl. 15)

- Základní informace o zpracování:
 - Kdo, jak, proč (účel), proč (právní titul), jak dlouho, kde...
- Odst. 3:
 - Správce poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

Právo na výmaz (Právo být zapomenut) Čl. 17

- Rozhodnutí Soudního dvora EU ve věci Google Spain
- Omezené množství případů, kdy se aplikuje
- Virální povaha práva
 - Pokud jsou data zveřejněná
- Výjimky, pokud je nezbytné pro výkon kolidujících práv (Odst. 3)
 - Příklad: Zpracování pro výkon práva na svobodu projevu a informace

Předávání údajů do zahraničí

- V rámci EU a EHS bez omezení
- Mimo EU a EHS:
 - Strany Úmluvy 108
 - GDPR - komplikované
 - Rozhodnutí Komise o adekvátní úrovni 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 Harbor 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

Soudní a správní ochrana

- Národní autorita – Úřad pro ochranu osobních údajů
- Evropský sbor ochrany osobních údajů
- Správní soudnictví
- Přímé nároky
 - Čl. 79 – obsahuje normu určující jurisdikci soudů
- Možnost zastupování subjektu údajů
 - Otevření možnosti hromadných žalob
- Právo na náhradu újmy
 - Např. zákonný regres správce vůči zpracovateli

Every time
you give
your
personal
information
away...



**a kitten
dies**

The Pr\|vacy Surgeon



Děkuji za pozornost.
Otázky?