Ochrana osobních dat a legislativa, etika

PV080

Vašek Matyáš

Důležité právní úpravy (EU/CZ)

- Listina základních práv a svobod (zákon č. 2/1993 Sb.)
- Směrnice č. 95/46/EC Evropského parlamentu a Rady z roku 1995 o ochraně jednotlivců ve vztahu ke zpracování osobních dat a o volném pohybu těchto dat

- ***Zákon o ochraně osobních údajů (101/2000 Sb.)***

- ***General Data Protection Regulation (GDPR, 2016/679)***

- Doplňkové čtení – IS

Vývoj v Evropě – I.

- Rada Evropy (1950) – Konvence o ochraně lidských práv a základních svobod – dva články (8 a 10), zabývající se nakládáním s informacemi.
- První „informační zákony” ve Švédsku (1973), Spolkové republice Německo (1977) a Rakousku (1978).

Vývoj v Evropě – II.

- Rada Evropy (1981) – Úmluva na ochranu osob se zřetelem na automatizované zpracování osobních údajů (č. 108).
  - závaznost pravidel pro veřejný i soukromý sektor,
  - nutnost vzniku státního orgánu pro dozor nad jejich dodržováním,
  - podmínky pro získávání, aktualizaci a likvidaci informací,
  - zvláštní podmínky pro práci s tzv. „citlivými“ informacemi a
  - záruky pro občana ke kontrole svých osobních informací a způsobu nakládání s nimi.

Vývoj v Evropě – III.

- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 – *o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*
- Směrnice 2002/58/EC o soukromí a elektronických komunikacích

Vývoj v Evropě – IV.

- *Smlouva o Ústavě pro Evropu*
  - články II-67 a II-68 se věnují ochraně osobních údajů a soukromí – právo občana, zákon, nezávislý kontrolní orgán
- *Nařízení (EU) 2016/679 (GDPR – General Data Protection Regulation)*
  - zohlednění technologického vývoje, jednodušší zpracování dat napříč Evropou, výraznější pokuty, exekuce v rukou EK

Listina základních práv a svobod I.

- nedotknutelnost osoby a jejího soukromí;
- ochrana lidské důstojnosti, osobní cti, dobré pověsti a jména, soukromého a rodinného života;
- *ochrana před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.*

Listina základních práv a svobod II.

- Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

Ochrana osobnosti – Občanský zákoník

- Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy. (§11)

- §12: Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy

Zákoník práce, Obchodní a Trestní zák.

- Povinnosti vyjmenovaných („státních“) zaměstnanců ohledně *mlčenlivosti*
- Souvislost s neoprávněným průnikem do počítačových systémů
- Obchodní tajemství
- Nekalá soutěž
- …

CS/CZ Zákon o ochraně osobních dat v informačních systémech (256/1992)

- široká formulace pojmu osobní údaje, která nepřímo způsobila „znehodnocení” skutečně důležitých dat;
- široká formulace pojmu informační systém;
- nejasná sankční opatření;
- nespecifikované pojmy „osobnost”, „soukromí”;
- neexistence úřadu pro registraci systémů s osobními údaji, pro kontrolu dodržování zákona atd.

Osobní průzkum (1995?)

- Právo získat vyrozumění o informacích o osobě uchovávaných (§ 17, odst. l) – jednou ročně bezplatně.
- Dotázáno 44 firem a institucí (některé 2x – centrála a místní pobočka – např. VZP).

- Došlo jen 26 odpovědí!

Průzkum – 26 odpovědí (ze 44 dotazů)

- 6 řádně zpracovaných (armáda a VZP)
- 7 víceméně uspokojivých (zaměstnavatelé)
- 6 nejasných nebo nekvalifikovaných (banky a státní úřady)
- 7 lživých nebo zmatečných (státní policie)

Z průzkumu...

"...informace k Vaší osobě Vám poskytneme za podmínek, že ke své žádosti přiložíte příslušný správní poplatek..."

"...máte možnost zjistit na kterékoliv přepážce Střediska cenných papírů... např. zpoplatněnou informační službou...",

Z průzkumu...

"Informace, jež jste poskytl... Jednalo se pouze o údaje, které jsou předmětem osobního dotazníku... V informačním systému, jehož jsme provozovatelem, nejsou informace o Vaší osobě vedeny."

Z průzkumu...

"...jedná se pouze o údaje Vámi osobně vypsané žádosti o vydání cestovního pasu, kterou jste sám podepsal a jistě je Vám známo, které údaje jste do žádosti uvedl."

Z průzkumu...

"V této souvislosti sděluji, že k řádnému vypracování odpovědi považuji za nezbytné, abyste podal zprávu o charakteru informací..., které jste poskytl subjektům resortu..."

Zákon o ochraně osobních údajů (101/2000 Sb.)

- Nabyl účinnosti obecně 1. 6. 2000.
- Účinnost vybraných ustanovení posunuta až na 1. 12. 2000 (ustanovení v souvislosti s oznamovací povinností a registrací zpracování osobních údajů u Úřadu pro ochranu osobních údajů), resp. k 1. 6. 2001.
- Plná účinnost od 1. 1. 2003
- Řada změn (zejm. e-podpis, návaznost na další zákony)
- Nahrazen GDPR v květnu 2018 a novým „adaptačním“ zákonem (někdy ☺)

O čem je tento zákon (101)?

- Zákon upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů a stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států.

- Zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby, pokud tento zákon nebo zvláštní zákon nestanoví jinak.

Pozor!!!

- Zákon se vztahuje na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.
- Zákon se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.
- Zákon se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány, nebo pokud nejsou pro podnikání (jiné než nezávislé povolání).

Osobní údaj (101)

- Jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů.
- Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu.
- O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků.

Náhrada škody, pokuty (101)

- V otázkách neupravených tímto zákonem se použije obecná úprava odpovědnosti za škodu (Občanský zák., Obchodní zák.).

- Zaměstanci až do 50’000 Kč za porušení mlčenlivosti.
- Pokuta za neposkytnutí součinnosti 25’000 Kč.
- Správce/zpracovatel až do 10’000’000 Kč.

Úprava evropské legislativy – GDPR

- Směrnice/direktiva (pro národní legislativu) nahrazena – *Nařízení Evropského parlamentu a Rady (EU) 2016/679 (a souvis. 680, 681).* General Data Protection Regulation (*GDPR*):
  - I data obyvatel EU uložená mimo EU
  - Národní bezpečnost a výkon práva vyňaty z působnosti
  - Evropská komise vydávající prováděcí předpisy
  - Formalizováno právo „být zapomenut“ ☺
  - Cookies budou obvykle brány jako osobní údaje
  - Povinná analýza rizik v určitých situacích
  - Pokuta až 4 % celosvětového obratu firmy
  - Pověřenec ochrany osobních údajů – úřady a jiné orgány, které rozhodují o právech občanů
  - Povinnost ohlášení průniku úřadu a při dopadu na subjekty i jim
- Platnost od května 2018

Osobní údaj (GDPR)

- 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

Osobní údaje II

- zpracovávány korektně a zákonným a transparentním způsobem;
- shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný;
- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány

Zpracování

- jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je 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

Další zaváděné klíčové pojmy

- Omezení zpracování
- Profilování
- Pseudonymizace
- Evidence
- Genetické údaje
- Biometrické údaje

GDPR v IT

- Zpracovateli nejsou osoby, které se při provádění svých služeb, pouze nahodile dostávají do styku s osobními údaji.
- Subjekt údajů = člověk, o jehož údaje se jedná.
- Správce = kdo operace s osobními údaji provádí buď z vlastního rozhodnutí, nebo proto, že je to jeho zákonnou povinností.
- Zpracovatel = správcem pověřen prací s osobními údaji, ty zpracovává pouze na základě pokynů správce.
  - Zpracovatel nesmí zapojit do zpracování žádného dalšího zpracovatele bez předchozího písemného povolení správce.

Využity texty ÚOOÚ

GDPR – pohled správce I

- Zpracování údajů, ať je nařízeno zákonem, prováděno z vůle správce nebo po dohodě či se souhlasem dotčených osob, musí být legitimní a nesmí být v rozporu s právními předpisy či morálkou.
- Každé zpracování údajů musí být založeno na některém ze základních důvodů (právních titulů pro zpracování), nejčastěji se jedná o smluvní plnění, výkon právních povinností či plnění zákonného oprávnění, výkon veřejné moci nebo zpracování na základě souhlasu dotčené osoby.
- Každý, kdo shromažduje, dále zpracovává a uchovává osobní údaje, musí jasně vymezit (stanovit a být schopen vysvětlit) sledovaný záměr - účel zpracování údajů.

Využity texty ÚOOÚ

GDPR – pohled správce II

- Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být **vždy přiměřené účelu zpracování**.
- Pokud detaily zpracování stanoví veřejnoprávní předpis, nelze se od nich většinou odchýlit. Každé zpracování ve veřejném sektoru musí mít **jasný zákonný podklad**, takové zpracování nelze nahradit souhlasem se zpracováním údajů.
- Správce i zpracovatel osobních údajů musí osobní údaje **patřičně zabezpečit** a chránit organizačními a technickými opatřeními – v míře odpovídající rizikovosti zpracování.
- Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno **férově, korektně a transparentně**. Informace o zpracování poskytované subjektu údajů musí být **zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci**.

Využity texty ÚOOÚ

GDPR – pohled správce III

- Zpracování **nesmí nadměrně zasahovat do soukromí**. Správci mohou volit různé přiměřené prostředky zpracování, v případě moderních technologií jsou však povinni zvážit nová rizika i dopady do soukromí jednotlivců. Zejména musí uvážit důvodnost a oprávněnost každého sdílení či zveřejnění negativních či jinak citlivých údajů.
- Po naplnění účelu zpracování je dána povinnost osobní údaje **zlikvidovat**. Delší dobu uchování mohou stanovit zákonná pravidla pro archivaci nebo zvláštní využívání údajů (státní statistická služba, nemocenské a důchodové pojištění apod.).
- Předávat osobní údaje mimo Evropskou unii lze jen za splnění dodatečných pravidel nebo za určitých okolností, jako je např. plnění smlouvy se subjektem údajů.

Využity texty ÚOOÚ

Případ Schrems

- Předávání údajů do zahraničí (adekvátní ochrana nebo stanovené výjimky)
- Safe Harbour – “samocertifikace” firem v USA
  - Úroveň není stejná, konstatoval i Evropský parl.
  - Rakušan Max Schrems napadl v Irsku úroveň ochrany pro FB (data pro velkou část světa, vč. EU)
- 6. 10. 2015 – národní úřady mohou přešetřovat adekvátnost systému Safe Harbour
  - Safe Harbour jako takový nebyl zrušen
  - Nejistota ohledně předávání
  - Chaos – obavy z rozpadu rozhodovací praxe

EU-US Privacy Shield

- Dohoda mezi EU a US
- Program pro zajištění ochrany ekvivalentní ochranou dle GDPR

- https://www.privacyshield.gov/welcome

Etika, profesionalita a práce s informacemi

Počítačová etika

- *Etika* – systém morálních principů a pravidel chování.
- *Počítačová etika* –aplikace systémů morálních hodnot a pravidel chování na práci s počítači.

- Užitečné články (dále také využity):
  - A. Hönigová – článek seriálu Bezpečnost pro všechny, soukromí pro každého – ComputerWorld 1997
  - Libor Miloš – bak. práce FI (2000)
- Pravidla a principy – linky v IS

Počítačová etika

- Cílem je identifikovat otázky a formulovat odpovědi na otázky k morálnímu podkladu činů a zodpovědnosti jedince (v oblasti IT).

- Změny v technologiích => změny ve společnosti.

Motivace chování (Don Parker)

1. Úroveň zákona a předpisů (strach z trestu, vynucení).

2. Úroveň konvencí (profesní kódy, dobrovolné atestace ap.).

3. Úroveň morální (zvyky okolí, zkušenosti).

Lze morálce naučit?

- Když někomu něco dělám, vadilo by mi, kdyby (mně nebo osobě blízké) to dělal někdo jiný?

- Když nějaký čin zvažuji, co se tak zeptat těch, na které to bude mít dopad?

Pohledy

- Pohled vlastníka: já rozhoduji o využití
- Pohled uživatele: používám cizí majetek
- Hacking: informace patří všem
  - Případně i zařízení na jejich zpracování. (!?)

Informace vs. věc

- Kopírování triviální.
- Originál stejný jako kopie.

- Kopírování (obvykle) netriviální.
- Originál (obvykle) lze zjistit.

Posilující trend

- Rozhodují algoritmy
  - Resp. jejich tvůrci a dodavatelé vstupů
  - Je potřeba dopady sledovat, příp. napravovat
- ACM: Zajistit, aby veřejné dobro bylo hlavním bodem zájmu při veškeré práci informatiků.
- ACM Statement on Algorithmic Transparency and Accountability
  - Link v IS

Etické a profesní kodexy

- **ACM – Code of Ethics and Professional Conduct**

- IEEE-CS/ACM – Software Engineering Code of Ethics

ACM: GENERAL ETHICAL PRINCIPLES

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

1.2 Avoid harm.

1.3 Be honest and trustworthy.

1.4 Be fair and take action not to discriminate.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

1.6 Respect privacy.

1.7 Honor confidentiality.

ACM: PROFESSIONAL RESPONSIBILITIES

2.1 Strive to achieve high quality in both the processes and products of professional work.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

2.3 Know and respect existing rules pertaining to professional work.

2.4 Accept and provide appropriate professional review.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

ACM: PROFESSIONAL RESPONSIBILITIES II

2.6 Perform work only in areas of competence.

2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.

2.8 Access computing and communication resources only when authorized or when compelled by the public good.

2.9 Design and implement systems that are robustly and usably secure.

ACM: PROFESSIONAL LEADERSHIP PRINCIPLES

3.1 Ensure that the public good is the central concern during all professional computing work.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.

3.3 Manage personnel and resources to enhance the quality of working life.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.

ACM: PROFESSIONAL LEADERSHIP PRINCIPLES II

3.5 Create opportunities for members of the organization or group to grow as professionals.

3.6 Use care when modifying or retiring systems.

3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

Pravidla užívání IS MU

- Používání IS v souladu s akademickým, vzdělávacím a výzkumným posláním
  - porušení pravidel – komerční činnost nesouvisející s činností školy, politická, náboženská nebo rasová agitace
- Vlastní uživatelské jméno. Nepracovat pod cizí identitou.
- Ochrana soukromých dat (hrubé porušení pravidel!).
- Dobrá volba a ochrana hesla, nezjišťovat hesla jiných.
- Důvěrnost soukromých informací.
- Spam
- Používání vulgárních a silně emotivních výrazů v otevřené komunikaci zakázáno.
- ...

Diskuze – pornografie na internetu

- Primární zodpovědnost za děti mají rodiče.
- Odborníci a stát mají rodiče poučit o problémech.
- Provideři by neměli *přímo* poskytovat pornografii nezletilým.
- Provideři by ale neměli omezovat svobodu těm, kdo již jsou za své činy zodpovědni.

Diskuze – selhání počítače a škoda

- Informace na počítači uchované/upracovávané

vs

- Poškození počítače jako takového (HW i SW)

- Je v některých případech správné způsobit škodu na počítači?
- Ve kterých?

Diskuze – nepovolené kopie SW

- Software někdo vytvořil a chce být odměněn

vs

  - Potřeba jej vyzkoušet před zakoupením
  - Jiný důvod ověření funkčnosti
  - Důvodné podezření z nesprávného postupu tvůrce
  - …

Diskuze – hacking

- Svobodný přístup k informacím

vs

- Práva vlastníka informací
- Způsobení škod vlastníkovi i třetím osobám

Diskuze – svoboda slova a prezentace nápadů/myšlenek

- Svoboda projevu

vs

- Způsobení škod jinému

...

Motto (Saji Baba)

- Věda bez lidskosti je marná a nebezpečná.
- Výchova bez charakteru je marná a nebezpečná.
- Ekonomie bez morálky je marná a nebezpečná.