

# ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ

---

7. 3. 2014

KISK FF MU

# EU a ochrana OÚ

- **Úmluva** o ochraně osob se zřetelem na **automatizované zpracování** osobních dat - pro ČR účinné od 1. 11. 2001
- **Dodatkový protokol** k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat – ČR od 1. 7. 2004
- **Směrnice** Evropského parlamentu a Rady:
  - 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se **zpracováním osobních údajů** a o volném pohybu těchto údajů
  - 2000/31/ES ze dne 8. června 2000, o určitých aspektech **služeb informační společnosti**, zejména **elektronického obchodního** styku v rámci vnitřního trhu
  - 2002/58/ES ze dne 12. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví **elektronických komunikací** – změněna dalšími směrnicemi
  - 2006/24/ES ze dne 15. března 2006, o **uchovávání údajů** vytvářených nebo zpracovávaných v souvislosti s poskytováním dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES
  - 2009/136/ES ze dne 25. listopadu 2009, kterou se **mění** předchozí směrnice
- Nařízení Komise (EU) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na **oznámení o narušení bezpečnosti osobních údajů** podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích
- **Rámcové rozhodnutí** Rady 2008/977/SVV ze dne 27. listopadu 2008, o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v **trestních věcech**
- **Doporučení** Komise 2009/387/ES ze dne 12. května 2009, o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě **rádiové frekvence**

# Mezinárodní úpravy v českém zákoně o ochraně OÚ

- Zákon se použije při zpracování OÚ na území ČR, i když správce jinde (třeba i mimo EU)
- Pokud správce na území EU, nutné zajistit respektování zákona členského státu
- Český zákon o ochraně OÚ stanovuje podmínky předání OÚ do jiných států – zvláště EU (obdobná úprava v předpisech) a třetí státy; výjimky v souhlasu subjektu, veřejných informacích apod.

# Zákon o ochraně OÚ v číslech

- Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech - zrušen zákonem č. 101/2000 Sb.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
  - Původní znění: platnost 25. 4. 2000, účinnost 1. 6. 2000, s výjimkou § 16, § 17 a § 35, ty účinné od 1. 12. 2000
  - 23 novelizací, poslední účinná od 1. 1. 2012

# Zákon o ochraně OÚ

- Snaha o naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí
- Stanovení práv a povinností při veškeré práci s OÚ (i mezinárodně, e- i tradičně...)
- Zpracování OÚ
  - Orgány státní správy a samosprávy,
  - Státními institucemi
  - Jinými orgány veřejné moci i FO/PO

# Na co se zákon nevztahuje

- Zpracování OÚ fyzickou osobou výlučně pro **osobní potřebu**
- **Nahodilé shromažďování** OÚ, pokud nejsou dále zpracovávány
- Zpracování OÚ **nezbytných pro plnění povinností** správce stanovených zvláštními **zákony** pro zajištění:
  - Bezpečnosti ČR
  - Předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů
  - Významného hospodářského zájmu ČR nebo EU
  - Výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci
  - ...

# Role osob v zákoně (§ 4)

- „d) **subjektem údajů fyzická osoba**, k níž se osobní údaje vztahují, (...)
- j) **správce** každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a **odpovídá** za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,
- k) **zpracovatelem** každý subjekt, který na základě zvláštního zákona nebo pověření správcem **zpracovává** osobní údaje podle tohoto zákona,“

# Údaje v zákoně (§ 4)

- „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,“



# Osobní údaj

- Nutná identifikace
- Přímá (jednoznačná), např. rodným číslem
- Nepřímá (souborem údajů), např. jméno + příjmení + datum narození
- Nepřímá i při napojení na cizí soubory, např. veřejné registry, IS VS...
- Stačí identifikace v konkrétním případě, ne v možném, např. často jméno + příjmení + adresa
- Údaje o PO chráněny jiným zákonem (občanský zákoník)
- Více viz ÚOOÚ k problémům z praxe 3/2012 (původně K problémům z praxe č. 1/2001, aktualizace květen 2010)

# Údaje v zákoně (§ 4)

- „b) **citlivým údajem osobní údaj** vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,
- l) **zveřejněným osobním údajem** osobní údaj **zpřístupněný** zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu,“

# Zpracování a shromažďování (§ 4)

- „e) **zpracováním** osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel **systematicky** provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,
- f) **shromažďováním** osobních údajů systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů **za účelem** jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější **zpracování**,“

# Povinnosti správce údajů

- Nutné myslet na soukromí subjektu údajů
- Stanovit účel, prostředky a způsob zpracování + jen s tím pracovat a jen v nezbytném rozsahu
- Shromažďovat OÚ pouze otevřeně (žádné záminky pro jiné účely či činnosti)
- Nesdružovat OÚ získané k rozdílným účelům
- Jen přesné OÚ, aktualizace hned po zjištění, jinak nutné znepřístupnění či označení
- Uchovávat OÚ pouze po nezbytnou dobu, pak nutná likvidace, výjimka jen pro státní statistické služby, účely vědecké a archivnictví a co nejdřív anonymizovat

# Povinnosti zpracovatele OÚ

- 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

# Souhlas subjektu údajů

- „Svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“ (§ 4)
- Souhlas musí být správce schopen prokázat po celou dobu zpracování
- Odvolání souhlasu, příp. zamítnutí zpracování nutné písemně

# Možné zpracování bez souhlasu - výjimky

- Dodržení právní povinnosti
- Ochrana života či práv subjektu
- Oprávněně zveřejněné OÚ dle předpisu
- Archivnictví dle zvláštního předpisu atd.

# Jméno + příjmení + adresa z veřejného seznamu

- Pro obchodní účely
- Bez přiřazení dalších údajů
- Jen do doby, než subjekt zamítne (pak nutné informovat správce, kterým údaje předal, o tomto zamítnutí)
- Předání možné, pokud další správce dodrží stejné podmínky a pokud není zamítnuto



# Pravidla zpracování údajů

- Před zahájením zpracování nutné informovat ÚOOÚ
- „Při zpracování osobních údajů správce a zpracovatel dbá, **aby subjekt údajů neutrpěl újmu** na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.“  
(§ 10)

# Informování subjektu

- Pro jaký účel zpracování
- K jakým OÚ je souhlas dáván
- Jakému správci
- Na jaké období
- Komu OÚ přístupné
- Zda je poskytnutí povinné či dobrovolné a co z (ne)poskytnutí vyplyne
  
- Zákon udává, při jakých typech zpracování informování na žádost a kdy z iniciativy zpracovatele

# Zpracování citlivých údajů

- Lze zpracovávat jen ze zákonem vymezených důvodů (obdobné, ale striktnější než běžné OÚ)
- Se souhlasem subjektu (opět nutné poučení)
- Umožněno pro ochranu zdraví či majetku subjektu či jiných osob, pokud nelze získat souhlas (nezpůsobilost, nezdělost...)
- Pro oprávněnou činnost sdružení, nadace či PO nevýdělečné povahy v souvislosti osobami ve vztahu k nim (nelze zpřístupňovat bez souhlasu)
- Pro zajištění sociálních služeb (pojištění, dávky...)
- Možné u OÚ zveřejněných subjektem
- + další výjimky jako u jiných OÚ (vztah k trestným činům, archivnictví...)

# Ochrana OÚ

- „(1) Správce a zpracovatel jsou povinni přijmout taková **opatření**, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, **neoprávněným** přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí **i po ukončení** zpracování osobních údajů.
- (2) Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená **technicko-organizační opatření** k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.“ (§ 13)
- § 15 povinnost mlčenlivosti o OÚ (i po skončení zpracování)
- Při problému subjekt může žádat nápravu správce, následně pomoc ÚOOÚ

# Úřad pro ochranu osobních údajů

- Zřízen zákonem 101/2000 Sb.
- Dozorový úřad pro ochranu OÚ vyplývající z mezinárodních smluv, které jsou součástí právního řádu
- § 28, odst. 1 „Úřad je **nezávislý** orgán. Ve své činnosti postupuje nezávisle a řídí se pouze zákony a jinými právními předpisy.“ (zákon 101/2000 Sb.)
- Financován ze samostatné kapitoly rozpočtu ČR

# Organizace ÚOOÚ

- Předseda
- Inspektoři
- Další zaměstnanci

# Předseda

- Plat, náhrada výdajů a naturální plnění jako prezident NKÚ
- Jmenuje a odvolává prezident na návrh Senátu
- 5 let, max. 2 období po sobě
- Občan ČR: způsobilý, bezúhonný („znalosti, zkušenosti a **morální** vlastnosti jsou předpokladem, že bude svoji funkci řádně zastávat“ – zákon 101/2000 Sb.), ukončené VŠ vzdělání
- Nesmí zastávat většinu funkcí ve státní správě a samosprávě, ani být člen politické strany či hnutí, ani vykonávat výdělečnou činnost, které by mohla ohrozit důvěru v jeho nestrannost

# Inspektoři

- Plat, náhrada výdajů a naturální plnění jako členové NKÚ
- Jmenuje a odvolává prezident na návrh Senátu
- 10 let, možné opakovaně
- Současně 7 inspektorů
- Provádí kontrolní činnost spolu s pověřenými zaměstnanci
- Stejně podmínky na osobu jako u předsedy (jako občana i další působnost)



# ÚOOÚ dnes (k 1. 3. 2013)

- 11. 8. 2010 jmenován RNDr. Igor Němec předsedou na druhé funkční období
- Inspektoři: MVDr. František Bartoš, RNDr. Kamila Bendová, CSc., Mgr. et Mgr. Božena Čajková, PhDr. Petr Krejčí, Mgr. Daniel Rován, PaedDr. Jana Rybínová, Ing. Josef Vacula
- Kontakt: osobně (sídlo v Praze), e-mailem, datovou schránkou, podatelna (fyzická i elektronická), diskuzní fórum na webu (probíhá [diskuze](#)?)

# Činnosti

- **Dohlíží** na dodržování povinností při zpracování OÚ
- Vede registr zpracování OÚ (veřejný s dálkovým přístupem)
- Přijímá **podněty a stížnosti** na porušení povinností při zpracování OÚ a informuje o jejich vyřízení
- Zpracovává a zveřejňuje výroční zprávu o činnosti, hl. informace o provedených kontrolách a stavu oblasti zpracování OÚ v ČR
- Vykonává další působnosti dané zákonem,
- Projednává správní delikty a uděluje **pokuty**,
- Poskytuje **konzultace** v oblasti ochrany OÚ,
- Zajišťuje plnění požadavků **mezinárodních** smluv,
- Spolupracuje s obdobnými úřady jiných států

# Oznamovací povinnost

- Před zahájením zpracování nutné informovat ÚOOÚ
- Registrované informace:
  - Identifikace správce (FO i PO)
  - Účel zpracování
  - Kategorie subjektů a OÚ
  - Způsob a místo zpracování OÚ
  - Příjemce a předpokládaná předání do jiných států
  - Opatření k ochraně OÚ
- Při splnění všech podmínek zápis do registru a vydání osvědčení, jinak výzva k doplnění, po lhůtě na oznamovatele pohlíženo, jako by neoznámil

# Bez nutnosti oznamovat

- OÚ z legálně **veřejných** datových souborů
- Zpracování správci ukládá **zvláštní zákon** pro uplatnění zvláštních práv a povinností (k tomu nutné zpřístupnit i dálkovým přístupem informace v jiných případech registrované úřadem)
- Nutné pro politické, filosofické, náboženské nebo odborové cíle **sdužení**, ale OÚ jen o subjektech v opakujícím se kontaktu se sdužením a bez souhlasu nezveřejněno

# Konec zpracování dle ÚOOÚ

- Při důvodné obavě z porušení zákona při zpracování OÚ zahájí ÚOOÚ z vlastního podnětu řízení
- Pokud problém nenalezen, jen zápis
- Když nalezen, zrušení povolení dalšího zpracování + úprava registru
- Po pominutí účelu zpracování ÚOOÚ sám nebo správce podnětem zruší registraci
- Po ukončení činnosti správce nutné ÚOOÚ informovat o naložení s osobními údaji určenými v registru

# IS ORG

- Na základě z. č. 111/2009 Sb., o základních registrech, v platném znění má ÚOOÚ vytvořit IS ORG (část základních registrů)
- ORG = převodník identifikátorů FO, v registrech nahradí rodné číslo
- Všechny identifikátory jen v ORG, ale nic jiného => ÚOOÚ nebude moci přiřadit konkrétním FO
- Vzhledem k roli a významu klíčové zabezpečení
- Cílem předcházet krádežím identity
- Aktuální harmonogram:
  - 1. etapa – BASE - 9. 2. 2011 – 30. 9. 2011
  - 2. etapa – ADVANCED - 1. 10. 2011 – 16. 1. 2012
  - 3. etapa – FULL - 17. 1. 2012 – 30. 6. 2012

# Kontrolní činnost

- Prováděna na základě kontrolního plánu (projednán a schválen na rok) nebo podnětů a stížností
- Kontrolující oprávnění:
  - Vstupovat do pracovních prostor kontrolovaných správců, zpracovatelů a dalších kvůli kontrole zpracování
  - Požadovat předložení dokladů a dokumentů pro kontrolu a připravovat vlastní dokumentaci
  - Seznamovat se s utajovanými informacemi a informacemi chráněnými povinností mlčenlivosti (za dodržení zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti)
  - Zajišťovat v odůvodněných důvodech doklady

# Kontrolní činnost (2)

- Povinnosti kontrolujících:
  - Kontrolují jen ti, u nichž nelze pochybovat o nepodjatosti
  - Kontrolovanému se prokázat, oznámit zahájení kontroly, chránit zájmy kontrolovaných a převzaté doklady, neprodleně vrátit dokumenty kontrolovanému (jak jen je to možné), poříditi protokol, dodržovat povinnost mlčenlivosti o kontrole a souvislostech
- Nutná spolupráce kontrolovaných, jinak (i opakovaně) pokuta do 25 000 Kč
- Pro prohřešky kontrolujícím stanoven termín a způsob nápravy, v případě rozhodnutí o likvidaci OÚ nutné do jejího provedení údaje blokovat
- [Výsledky na stránkách](#): za každý rok případy, jejich shrnutí a výsledek se zdůvodněním



# Dozor formou kontroly

- Z. o ochraně OÚ odkazuje na zákon č. 552/1991 Sb., o státní kontrole:
  - Výjimky z kontroly (soudy, ozbrojené sbory apod.)
  - Uvedeno obecnější znění pravidel jako v 101/2000 Sb.

# Informační činnost

- Právní předpisy a judikatura – základní právní informace k tématu, české i evropské; oblasti zpracování OÚ (vztah k jiným předpisům, než základním pro ÚOOÚ)
- Nevyžádaná obchodní sdělení a elektronická komunikace (telekomunikace a její regulace) zvláště, vč. právních předpisů
- Kategorie Zahraničí – mezinárodní organizace a zahraniční zákony + informace ze světa (zajímavé konkrétní problémy a jejich řešení v zahraničí; např. [K novým zásadám ochrany osobních údajů společnosti Google](#))

## Informační činnost (2)

- Média – zajímavé články z českých i zahraničních médií
- Publikace – materiály (nejen vytvořené ÚOOÚ) různých typů (od letáků, přes výroční zprávy, anotace knih)
- Zvláštní snaha cílit na děti a dospívající, hl. zábavou, příklady situací, soutěžemi (Soutěž "Moje soukromí! Nekoukat, nešťourat!" podporuje i SKIP)

# Publikování výsledků činnosti – Názory Úřadu

- Na aktuální témata: nejzajímavější, vč. rad pro postižené
- Stanoviska: delší objasnění obecnějšího problému, základní problematické oblasti, např. zpracování osobních údajů zemřelých osob
- Často kladené otázky: nepřehledné, ale konkrétní a týkající se mnoha osob
- Z rozhodovací činnosti Úřadu: výsledky reálných problémů
- Tiskové zprávy a konference: hl. tiskové zprávy k tématům, ke kterým má ÚOOÚ negativní vztah, a dementi

# Výroční zpráva 2013

Dotazy a konzultace	Dotazy z ČR	2994 (↑↑)
	Konzultace státní správě a samosprávě	321
	Konzultace PO a podnikajícím FO	830 (↑)
	Konzultace FO	1863 (↑↑)
Stížnosti a podněty	Dle z. o ochraně OÚ	1475 (↑), z toho 139 (↓) předaných ke kontrole
	Nevyžádaná obchodní sdělení	7428 (↓), vyřešeno 5436 (↑↑)
Kontroly		Zahájených 180 (↑)
Registrace	Oznámení	6570 (↑)
Předání	Žádosti do zahraničí	25, z toho 20 povoleno (↑)
	Informací dle 106/1999	79 (↑), z toho 10 odmítnuto

# Sledování kamerami (výroční zpráva 2011)

- Z 375 podání 90 % sledování zaměstnanců na pracovišti, provozu kamerových systémů v bytových a soukromých domech => „většina občanů je víceméně smířena s kamerami např. na letišti, v metru, bance, ale je značně citlivá k zásahům do svého soukromí zejména na pracovišti a v bydlišti“ (Výroční zpráva za rok 2011)
- Platí stejné podmínky jako u jiných údajů, např. osobní potřeba (ochrana majetku)
- Nejčastější problémy s kamerami (doloženy konkrétními případy):
  - „zneužívání shromážděných záběrů k jiným než deklarovaným účelům,
  - zpřístupňování či zveřejňování kamerových záběrů neoprávněným osobám,
  - nepřijetí adekvátních technicko-organizačních opatření minimalizujících rizika neoprávněného přístupu ke kamerovým záznamům,
  - překračování principů proporcionality mezi chráněným zájmem (účelem) 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 (vysoká možnost omylu v adrese)
- Špatně začerněno (šlo odstranit)
- V tiskárně tisknouce dokumenty s OÚ neskartovány chybné výtisky
- Traverzováním webu (i omylem) přístup k informacím o jiném klientovi
- Veřejně vystaveny faktury vč. OÚ zákazníků

# Sankce

- Za přešupek FO pokuta 100 000 – 5 000 000 Kč
- Správní delikt PO nebo podnikající FO 1-10 mil. Kč
- Možnost postihu zaniká po 1 roce od znalosti správního orgánu bez zahájení jednání, nejpozději ale po 3 letech od problému
- „Právníká osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.“



## Další zdroje k tématu

- Občanský zákoník, §§ 11-13 ochrana soukromí, osobnosti apod.
- Trestní zákoník, § 180 Neoprávněné nakládání s osobními údaji – zneužití či umožnění zneužití OÚ, ke kterým měli přístup díky svému povolání, zaměstnání nebo funkci, umožňuje postih i při nedbalosti
- Iuridicum Remedium + [Big Brother Awards](#)