

OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR)

Úvod do implementace v obcích



Brno

2. 2. 2018

Oldřich Kužílek

Progr

1. Mýty, strachy, poplašné zprávy
2. Základní definice, pojmy
3. Praktická implementace v úřadu - analýza souladu
4. 8 základních zásad ON a ochrany osobních údajů
5. Zákonnost - Právní tituly pro zpracování OÚ
6. Průlet „Kontrolním záznamem“
7. Ostatní zásady (informace, práva subjektů, omezení, minimalizace, přesnost, bezpečnost)
8. Pověřenec pro ochranu osobních údajů, kodexy, osvědčení
9. Speciality, diskuse

GePaRD?

25. května 2018
MOBILISACE!
Bombardovací svazy
Úřadu zaútočily!

Zpracování osobních údajů

- jakákoliv operace nebo soubor operací
- pomocí či bez pomoci automatizovaných postupů – ty musejí být **obsaženy v evidenci** nebo do ní mají být zařazeny – ON 2/1)
 - „evidence“ = *strukturovaný soubor OÚ přístupných podle zvláštních kritérií. Systematicky uspořádány podle určených kritérií.*
 - *spisové kartotéky, lékařské kartotéky s OÚ v listinné podobě.*

Příklady:

- 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

co **NENÍ** zpracování osobních údajů

- manuální zpracování fyzických kopií dokumentů obsahujících osobní údaje, které nejsou nijak rozřazeny či evidovány podle klíče či indexu.
- pořízení a použití jednotlivých **fotografií** / časově omezeného obrazového záznamu (schůze, kulturní, společenské, sportovní akce), **aniž** se vytváří **evidence**, **nejsou** kromě běžné identifikace jménem a příjmením **systematicky přiřazovány další osobní údaje**,
- I na ně - ochrana osobnosti dle občanského zákoníku, popř. ochrana dle dalších předpisů (např. ochrana bankovního tajemství, ochrana obchodního tajemství, smluvní povinnost mlčenlivosti apod.).



Školní web - žádný problém

(nepodléhá ON, pouze občanský zákoník)

Vůbec nejde o **ZPRACOVÁNÍ** osobních údajů.

O **zpracování** by se jednalo, pokud by fotografie byly v označeny nejen **jménem** a **příjmením**, ale dále by k nim byly **přidány další údaje** (např. věk, bydliště) anebo by byly setříděny do **evidence** podle příjmení, existoval by **rejstřík** umožňující vyhledat fotografie podle příjmení apod.

Doporučení: 1) u takového typu fotografií ze školních akcí uvádět jen **křestní** jméno nebo nic.

2) **Informovat** rodiče (ne souhlas), že se průběžně pořizují a na web umísťují fotografie ze života školy, zejména skupinové, bez bližší identifikace.



SPOLEČNÁ PLAVBA

2.A

ÚVOD

O NÁS

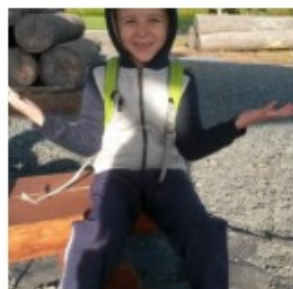
PLÁNOVANÉ TŘÍDNÍ AKCE

**FOTA - EKOCENTRUM
PRALES**

FOTA - ZOO

FOTA - PEKLO

soutěží, pantomimy, zapojení vlastních smyslů, dozvěděli plno zajímavostí o životě rostlin a zvířat v lese, jeho proměnách během čtyř ročních období, o práci lesníků i myslivců. Celá akce proběhla ve velmi přátelském duchu za doprovodu organizátorek, které se nám snažily předat co nejvíce informací. Všem návštěvu ekocentra doporučujeme!)



co **NENÍ** zpracování osobních údajů

- ad hoc přístup k datům – servis, nastavení hardwaru, softwaru (→ ujednat povinnost data chránit → smlouva o ochraně důvěrných informací, tzv. NDA).



K čemu v organizaci směřujeme – hlavní kroky

- analýza současného stavu
 - Identifikace AGEND - účelů zpracování
 - Posouzení jejich zákonnosti
 - Vyhodnocení dalších požadavků ON (checklist, kontrolní seznam)
- nastavit správně získávání souhlasů
- zabezpečení získaných dat
 - Pokud cloud - smlouva o poskytování cloudových služeb: odpovědnost za bezpečnost a umístění dat a jejich zpřístupnění
- Informace pro subjekty údajů a jejich práva

A	B	C	D	E	F	G	H	I
záznamy o činnostech zpracování ÚŘAD xxx, IČ.	skupina otázek k implementaci ON	Pojmenování a popis agendy / parametr zpracování OsÚ	ustanovení ON	související ustanovení ON	forma odpovědi	Barva výplně buňky: žlutě- nutno vysvětlit, AGENDA X		
poř.č.	Filtr	S KÝM DPO PROVEDL KONTROLNÍ ZÁZNAM DATUM KONTROL. ZÁZNAMU			jméno, příjmení, funkce		AGENDA X	AGENDA X
1	1 - zákl. údaje o zpracování	Odpovědný odbor a Odbor, kde se zpracování provádí	X	X	text - název odboru			
2	1 - zákl. údaje o zpracování	odpovědná osoba - garant zpracování	X	X	pozice			
3	Záznam zpracování (povinné) + Info	Jsem správcem nebo zpracovatelem? Pokud zpracovatelem - pro jakého správce (uvést)	24, 28	30/2/a	S - správce / Z - zpracovatel + označení správce/ kombinace S+Z			
4	1 - zákl. údaje o zpracování	technický způsob zpracování OsÚ	4/1		text např. - listinně nebo elektronicky -> programové vybavení (software), v němž zpracování probíhá, typ souborů (textové, zvukové, fotografie, video, apod.)			
5	1 - zákl. údaje o zpracování	Technické vybavení (hardware, kartotéka), na němž zpracování probíhá	X	X	text			
6	1 - zákl. údaje o zpracování	čerpá zpracování údaje z jiných zdrojů ? (např. EO, ROB, katastr, registr dlužníků apod.)	14		ANO/NE			

Nové principy

- princip **odpovědnosti správce - pořádek**
 - odpovědnost správce za dodržení 8 zásad zpracování, které jsou uvedeny v článku 5 odst. 1 ON (podrobněji dále)
 - zároveň musí správce být schopen tento soulad **doložit** (**záznamy** o činnostech zpracování, případně v budoucnu osvědčení).
- přístup **založený na riziku**
 - Prakticky znamená, že **správce má SÁM posoudit rizika**
 - Např. dopad **přesnosti údajů** → nároky na aktualizaci OÚ.
 - ON rozlišuje „riziko“ a „vysoké riziko“ a „nízké riziko“.



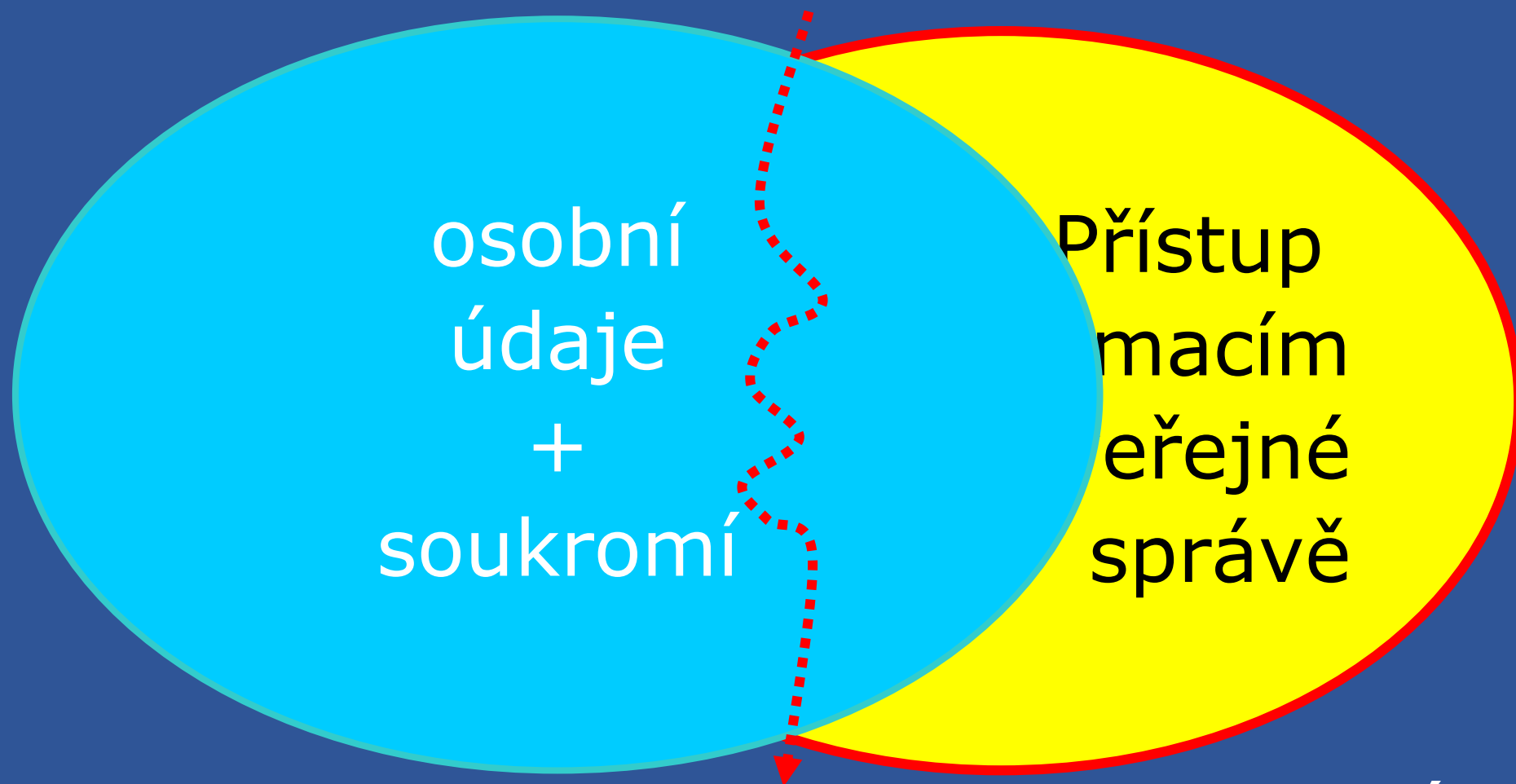
! POZOR !

Uvnitř je extrémní
bordel !

Obecné nařízení

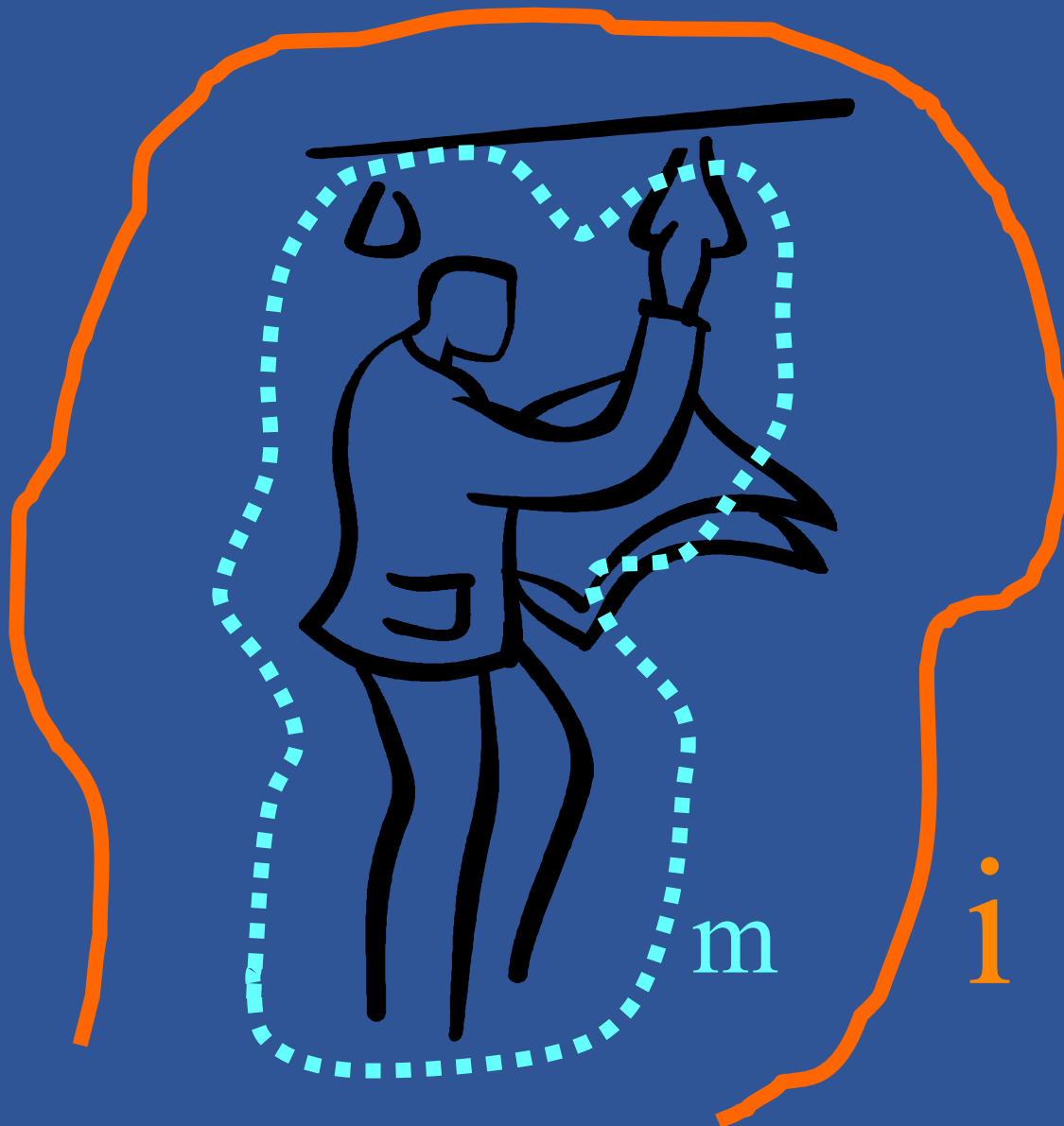


Vyvažování základních práv



přesná hranice přístupnosti OÚ

koncepce osobních údajů



osoba není
jen fyzické
tělo,

přesahuje:

vlastnictví

soukromí

osobní
údaje

Průzkum 2017

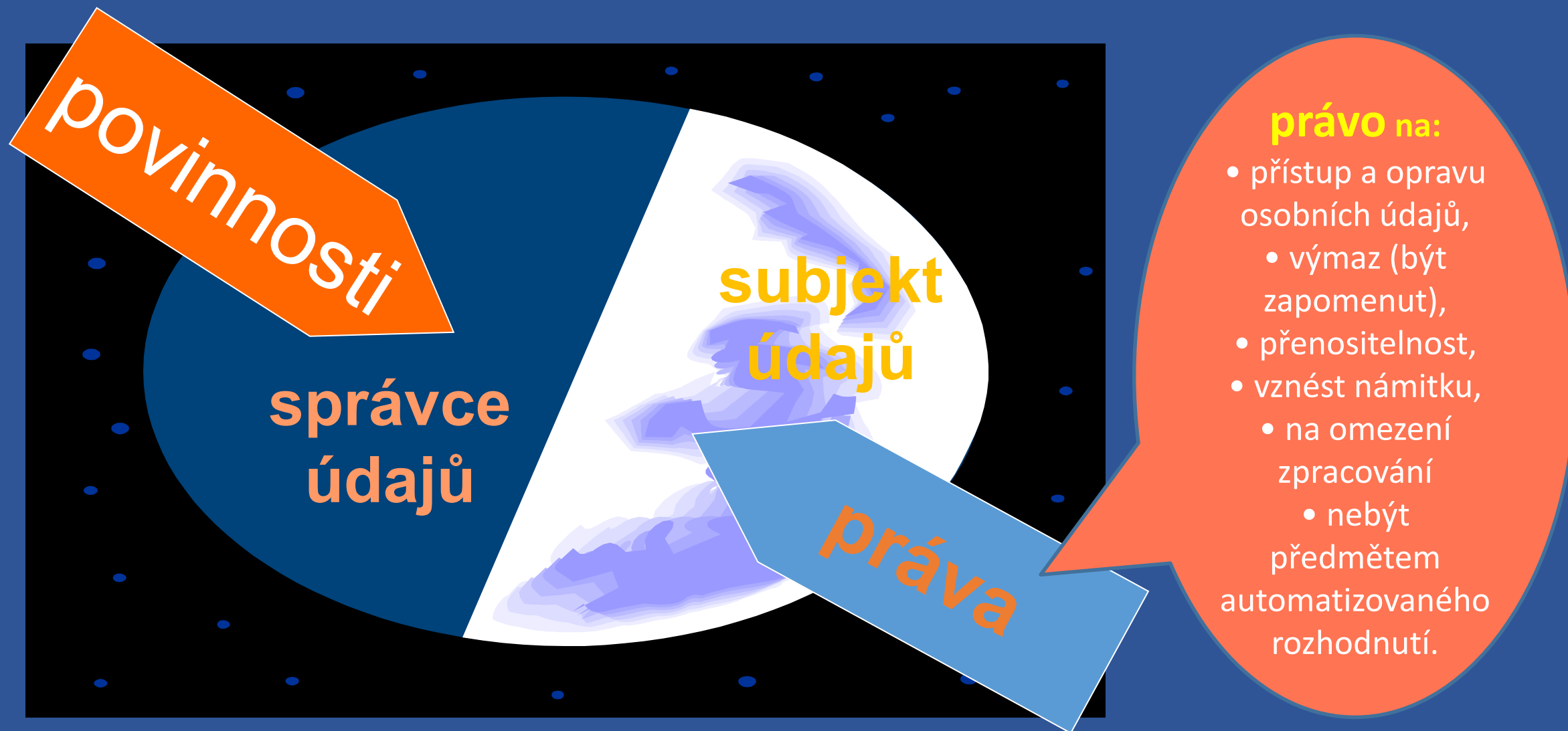
Citlivost jednotlivých údajů podle veřejnosti (%)

- uvedu kdykoliv bez problémů
- uvedu za určitých okolností
- neuvedu za žádných okolností



ZDROJ: ČBA

Právní úprava – dvě strany mince



Definice - Osobní údaj

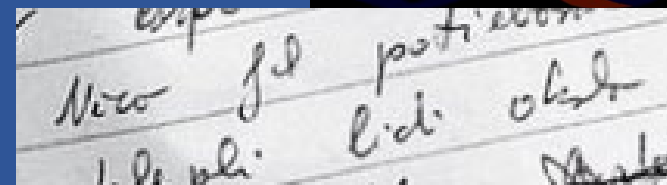
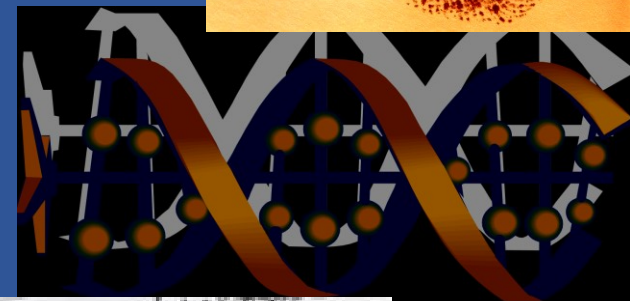
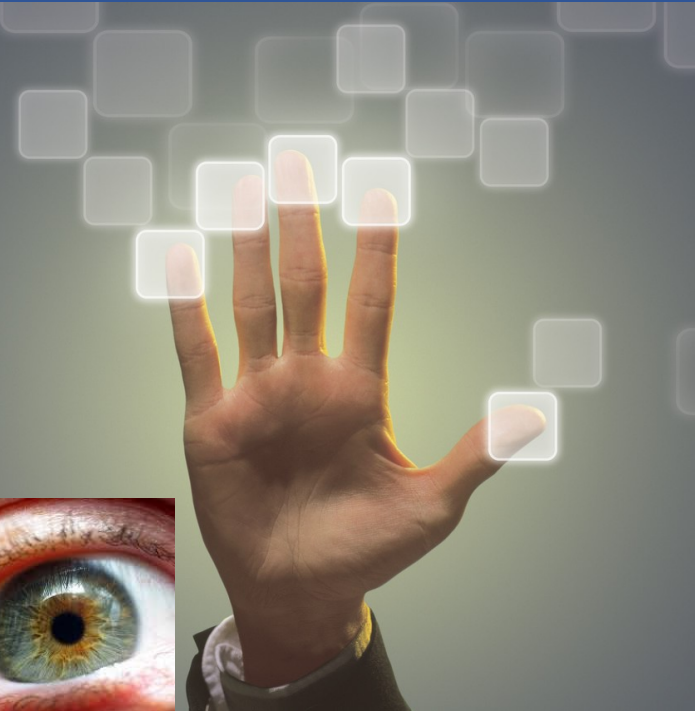


- Čl. 4 odst. 1 ON
- veškeré informace o identifikované nebo identifikovatelné fyzické osobě
- osoba je identifikovatelnou, když ji lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například
 - jméno,
 - identifikační číslo,
 - lokační údaje,
 - síťový identifikátor (např. IP adresa, i dynamická, cookies za urč. podmínek)
 - zvláštní prvky fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity
- možnost danou osobu (být nepřímo) identifikovat musí být rozumná, resp. rozumně předpokladatelná → Nikoli teoreticky existující možnost (mimořádné úsilí a náklady), ale jen reálně existující, byť ne zcela jednoduše dosažitelné možnosti a prostředky

Nemusím vědět, kdo za OÚ ve skutečnosti je

Formy osobních údajů

- Typické administrativní (jméno, adresa...)
- Dále **veškerá zobrazení vybraných charakteristik** subjektu údajů, zejména zachycení podoby („fotografie“) a biometrických charakteristik jako otisky prstů ruky, tvar ruky, vybraných částí obličeje, záznam hlasového projevu, *záznam dynamiky psaní na klávesnici* apod.
- Dle ON „biometrické“ – jen **pokud zpracovávání technickými prostředky** nebo systémy umožňujícími identifikaci člověka.



Formy / hranice osobních údajů



nejde o osobní
údaj – nelze
získat žádné
jedinečné
biometrické
údaje

Role při zpracování osobních údajů

listinně
zpracovatel



elektronicky

správce

U digitalizovaných agend je listinná forma (např. vstupní žádost, dotazník) logickou součástí zpracování, i když se zpracovává odděleně (papír zůstává ZDE, zatímco data tečou TAM)



Další důležité definice

- **„správce“** = osoba, orgán veřejné moci, agentura atd., který určuje účely a prostředky zpracování OÚ (*např. zákazník cloudových služeb*)
 - V případě zpracování stanoveného zákonem (*např. evidence cest. dokladů*)
→ správce = MV, vkládající obecní úřad = zpracovatel, vč. listinné formy žádostí).
 - ZOOU x ON – přímo v zákoně jako správce? → SPOLEČNÍ SPRÁVCI
- **„zpracovatel“** = kdo zpracovává osobní údaje pro správce (pověřen správcem - smlouvou nebo zvl. zákonem, s vlastní právní identitou) (*např. i poskytovatel uložistě, cloudových služeb, či jejich řada, pracoviště CzechPoint, MěÚ – evidence cest. dokladů*)
- **„příjemce“** = komu jsou OÚ zpřístupněny (včetně SÚ, správce, zpracovatele atd.) NE však inspekční, vyšetřovací orgány, např. ČŠI, ČOI, FÚ, ÚOHS, ERÚ, policie... „zvláštní šetření dle zákona“ – čl. 4/9 ON)

Další důležité definice

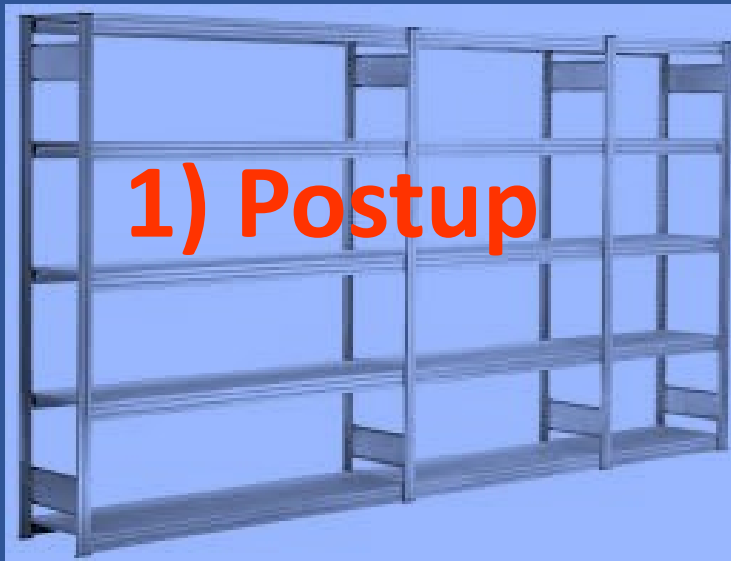
- **Citlivé osobní údaje - „zvláštní kategorie“** osobních údajů = vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci (*odpovídá dosavadním „citlivým údajům“ dle ZOOÚ*).
 - **Zpracování těchto údajů se obecně zakazuje**, pouze úzký okruh výjimek z tohoto zákazu
- **„údaje o trestných činech“** (vč. trestních rozsudků a souvisejících bezpečnostních opatření)
 - pod dozorem orgánu veřejné moci nebo oprávněné podle zákona (např. trestněprávní bezúhonnost, výpis z rejstříků trestů - zaměstnavatel při výběru uchazečů)

Další důležité definice

- **„omezení zpracování“** = označení uložených OÚ, aby bylo možné vyřadit je ze zpracování (ON 4/3)
- **„profilování“** = automatizované hodnocení osobních aspektů, zejména rozbor nebo odhad aspektů pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;
- **„automatizované individuální rozhodování“**
- **„pseudonymizace“** = OÚ nelze přiřadit k osobě bez dodatečných informací, které zároveň musejí být uchovávány odděleně a zabezpečeny před přiřazením

Analýza souladu

(splnění povinností - co vlastně budeme dělat)



Shrnutí postupu

- **osoba** zodpovědná za vstupní analýzu → starosta (tajemník?)
- kdo to bude dělat → Pověřenec SMS + starosta (tajemník?)
- U větších obcí **realizační tým** (+ vedoucí zaměstnanci, ICT, právník, bezpečnost.....)
- Proškolení ze **zásad GDPR** s důrazem na **konkrétní podmínky** organizace
- **Rozsah** vstupní analýzy (úřad, orgány města, zřizované organizace, Smart City atd...)
- **Harmonogram**, součinnost atd.

Analýza souladu – postup

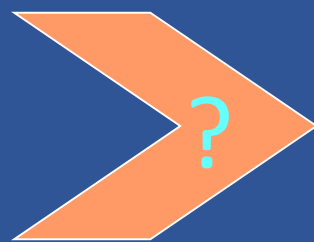
1. Pověřenec SMS → pošle formulář „Kontrolní záznam“
2. Starosta předběžně **vyplní**, komunikuje a pošle Pověřenci, navrhuje **řešení**
3. Pověřenec prověří, doplní, konzultuje, navrhuje **řešení**
4. Pověřenec dodá univerzální **podklady** (např. zveřejnění info na webu), navrhne úpravy interních **předpisů**, formulářů, smluv)
5. Starosta maximum **realizuje**
6. Návštěva Pověřence – kontrola dosaženého stavu, zanesení do „Kontrolního záznamu“

záznamy o činnostech zpracování ÚŘAD xxx, IČ.	skupina otázek k implementaci ON	Pojmenování a popis agendy / parametr zpracování OsÚ	ustanovení ON	Ag Barva výplně buňky: žlutě- nutno vyjasnit, oranžově- pronájem bytu ze sociálních důvodů - OSZP OSV	Vítání dětí
11	1 - zák. údaje o zpracování	volný popis, kdo všechno se reálně dostane do styku s OsÚ, vč. vlastních zaměstnanců	30/1, d)	dokumentace: zpracovávající referent, vedoucí odboru, pověřený člen a předsedkyně komise (KSBO), a u realizovaných žádostí referent agendy bytů na OSM a vedoucí OSM. Dále stručné shrnutí je přístupné členům KSBO a RMČ, ale též všem s přístupem do Lotus Notes. PROBLÉM	účetní, starosta, členové SPOZ pamětní kniha: volně na obecních akcích, např. rodáci
12	1a - Záznam zpracování (povinné) + Info	Kategorie příjemců údajů	30/1, d)	dokumentace: určení zaměstnanci, předsedkyně Komise pro sociálně bytové otázky. Stručné shrnutí: zaměstnanci, členové zastupitelstva, Komise pro sociálně bytové otázky. PROBLÉM	zaměstnanci, členové SPOZ pamětní kniha: volně na obecních akcích, např. rodáci
13	1a - Záznam zpracování (povinné) + Info	Doba uchování OsÚ	30/1, d)	Plný rozsah dokumentace: skartační hůta 5 let na OSV, podle trvání pronájmu na OSM. Shrnutí v LN: bez ... PROBLÉM	pamětní kniha: stále pracovní seznam: 1 měsíc po akci
14	1a - Záznam zpracování (povinné)	Obecný popis technických a organizačních bezpečnostních opatření (je-li to možné)	5/1/f) 30/1, g, 32/1	členové KSBO seznámeni s ochranou OÚ (101/2000 Sb.), obecné vymezení pracovní náplně. Není vyjasněný přenos na SNEO (obyčejný e-mail?) PROBLÉM	PC: pod heslem do SW Triada pod heslem, antivirus Avast free protipožární dveře, mříže,

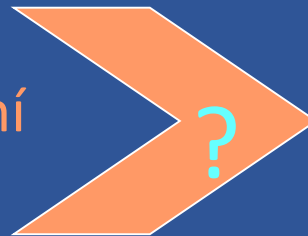
Odhalují se otazníky a problémy → uvedou se do záznamu

Analýza souladu - obsah

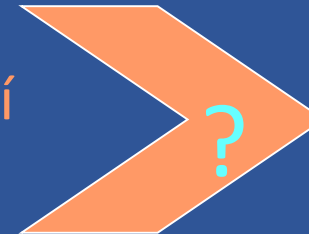
skutečnost (spisy,
evidence,
korespondence,
záznamy)



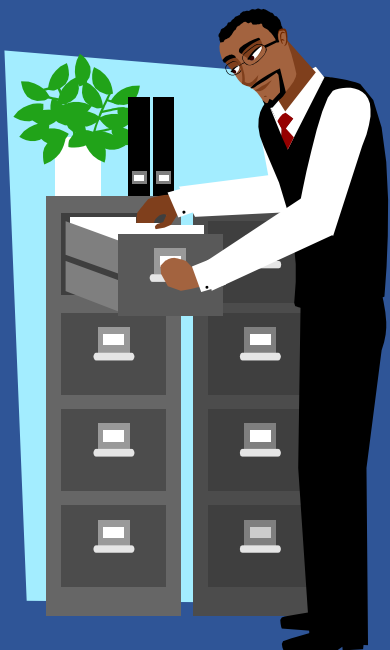
osobní
údaje



zpracování
oú

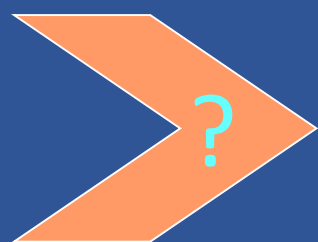


Základní
parametry
každého účelu
(agendy)

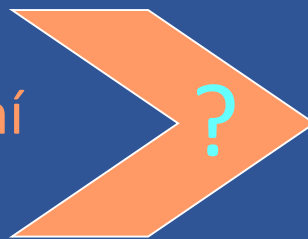


Analýza souladu

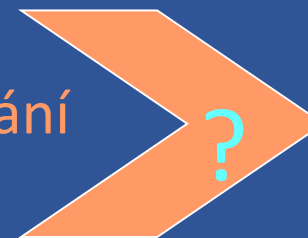
skutečnost (spisy,
evidence,
korespondence,
záznamy)



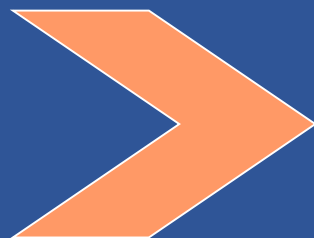
osobní
údaje



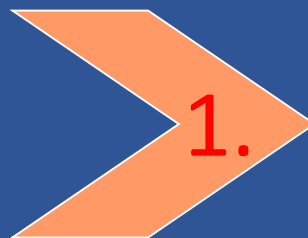
zpracování
OÚ



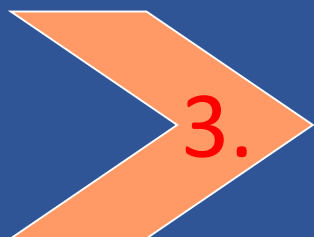
Základní
parametry
každého účelu
(agendy)



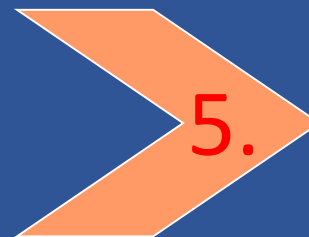
8 **zásad**
zpracování,
například:



zásada **zákonnosti**: právní titul pro
zpracování



zásada **omezení**
účelem: data jen ke
stanovenému účelu



zásada **přesnosti**:
aktualizace a kontrola
dat

8 základních zásad zpracování OÚ podle Obecného nařízení

Hlavní povinnost správce:

1. Zákonnost (jen na základě zákonného zmocnění)

Práva subjektu údajů (a tím povinnosti správce):

2. korektnost a transparentnost (informace, požadavky)

Další povinnosti správce (zpracovatele):

3. účelové omezení (určité, výslovně vyjádřené a legitimní účely)
4. minimalizace údajů (přiměřené, relevantní a omezené na nezbytný rozsah)
5. přesnost (přesné a v případě potřeby aktualizované)
6. omezení uložení (po dobu ne delší, než je nezbytné pro účely)
7. integrita a důvěrnost (náležité zabezpečení, hlášení incidentů)
8. odpovědnost správce (za to vše zodpovídá a musí to **umět doložit** – pod sankcí až 20 000 000 €) – např. pořizovat „záznamy zpracování“

Zákonnost

korektnost a
transparentnost

omezení
účelem

minimali
zace
údajů

přesnost

a) souhlas (orgány VS
ne)

b) pro splnění smlouvy

c) právní povinnost
(„tvrdé ustanovení“)

d) ochrana životně
důležitých zájmů

e) úkol ve veřejném
zájmu, výkon veřejné
moci („měkké
ustanovení“)

f) oprávněný zájem

1. informace o
zpracování
2. přístup ke svým OÚ
3. oprava nepřesných OÚ
4. výmaz („právo být
zapomenut“)
5. omezení zpracování
6. přenositelnost údajů
7. námitka
8. Ne automatizované
rozhodnutí

Základní
zásady:
porušení
podléhá **vyšší
sankci**

omezení
uložení

integrita a
důvěrnost

odpovědnost
správce

1. Zákonnost

(právní tituly zpracování – hlavní povinnost správce)

Zákonnost obecně

Každé zpracování OÚ musí být založeno výhradně na alespoň jednom z těchto právních titulů v čl. 6/1 ON:

- a) udělil **souhlas**
- b) nezbytné pro splnění **smlouvy**
- c) nezbytné pro splnění **právní povinnosti správce** („*tvrdé ustanovení*“)
- d) nezbytné pro ochranu **životně důležitých zájmů subjektu údajů** nebo jiné fyzické osoby
- e) nezbytné pro splnění **úkolu** prováděného **ve veřejném zájmu** nebo **při výkonu veřejné moci**, kterým je pověřen správce
- f) nezbytné pro účely **oprávněných zájmů** příslušného **správce** či třetí strany (omezeno testem proporcionality, zejm. u dětí)

e) + f) „měkká ustanovení“ → námitka





Souhlas 1

Čl. 4/11

Čl. 7/1

(42)

- svobodný, konkrétní, informovaný, odlišitelný a jednoznačný projev vůle
 - Svobodný = SÚ má skutečnou nebo svobodnou volbu a může souhlas odmítnout nebo odvolat, aniž by byl poškozen.
 - Není svobodný - když mezi SÚ a správcem existuje jasná nerovnováha, zejména pokud je správce orgánem veřejné moci,
 - Není svobodný - je-li plnění smlouvy (vč. služby) závislé na souhlasu, i když to není nezbytné
 - Konkrétní – jasně uvedeno k jakému účelu
 - Informovaný - znát alespoň totožnost správce a účely zpracování
 - Odlišitelný – zřetelně oddělený od jiného textu, informací
 - Jednoznačný – nedávat možnost dvojího výkladu



Souhlas 2

Čl. 7/1

- Musí být vyjádřen **prohlášením** nebo „zjevným **potvrzením**“ (*nutná aktivita SÚ!*)
 - (vyplněním e-mailové adresy se přihlašujete k odběru obchodních sdělení a zpracování svých osobních údajů k tomuto účelu) → z okolností zcela zřejmé, že vyplněním e-mailu souhlasí se zpracováním OÚ)
- Cookies (pokud jde o zprac. OÚ) – **nelze pouhým užíváním** webové stránky bez aktivního vyjádření souhlasu.
- Musí být stejně jednoduše odvolatelný, jako jeho udělení
- U zvláštních kategorií OÚ (citlivé OÚ) musí být **VÝSLOVNÝ** (nemůže být udělen konkludentně – např. pouze tím, že osoba údaje sdělila).
→ je třeba, aby subjekt údajů **explicitně prohlásil**, že souhlasí se zpracováním svých **citlivých** údajů k vymezenému účelu.



Souhlas 3

Čl. 4/1
+ 7/1

- Správce musí po celou dobu zpracování být schopen jej **doložit**. Tzn. že pokud jej ztratí → přerušit zpracování a získat znovu, jinak **ukončit**. Doložení – i ve formě **příznaku v databázi** → její důvěryhodnost - pomocí vytvoření hash otisku dokumentu
- Souhlas osoby **pod 13 let pro služby inf. společnosti** (dle nového ZZOÚ) – potvrzen zákonným zástupcem + přiměřeně jej ověřit
- Souhlas = nestabilní (možnost odvolat → právo na výmaz, čl. 17 ON)
 - problematická forma → **nepoužívat**
- Souhlasy získané dříve – pokud **nejsou v souladu s ON** → **neplatné** (→ prověrka souhlasů, informovat o přechodu na jiný titul)

Právní tituly pro zákonnost ve veř. správě

hlavní případy

Čl. 6/1

c)

- splnění **právní povinnosti správce** – na základě výslovného zmocnění v zákoně. Např. zákon o registru smluv → povinnost zveřejnit smlouvu včetně metadat.
- splnění **úkolů ve veřejném zájmu** nebo **při výkonu veřejné moci**, kterým je pověřen správce

e)

→ ne-výslovné, volnější uložení úkolu v zákoně. Nejde o konkrétní právní povinnost. Např. zák. o obcích: „*pečuje ... o vytváření podmínek pro rozvoj sociální péče a pro uspokojování potřeb svých občanů, ... především o uspokojování potřeby bydlení,*“ → lze dovodit oprávnění pro agendu přidělování sociálních bytů



Znova: Rozdíl právních titulů VS

- **6/1/C) právní povinnost** = **přímo** vyplývá **ze zákona**, upřesněna může být i v podzákoně předpisu („právní základ“). *(např. povinnost zaměstnavatele předávat osobní údaje zdravotní pojišťovně dle § 10 zákona o veřejném zdravotním pojištění). Nejde o „oprávnění“ (správce nemá na výběr)*
- **6/1/e) Úkol ve veřejném zájmu nebo výkon veřejné moci** = právní základ dává určitý **úkol** ve veřejném zájmu (**oprávnění**). Správce si může zvolit, jakým způsobem úkol splní, zda k tomu zpracuje OÚ. *(např. profesní komora je oprávněna vést disciplinární řízení se svými členy – pro řízení může zpracovávat relevantní osobní údaje.)*

Právní tituly pro zákonnost ve veř. správě méně obvyklé případy

Čl. 6/1

a)

- **Souhlas** – lze použít jen v případě činností mimo vlastní výkon veřejné správy, v soukromoprávní oblasti, např. pokud obec nabízí připojení wifi.

b)

- Podobně právní titul pro **plnění smlouvy** (např. *antisprejový program*).
- pro účely **oprávněných zájmů** příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.



f)

OVM – jen v soukromoprávní oblasti (např. kamerový systém ochrany majetku, nakládání s majetkem - neuplatňuje veřejnou moc)

- *Poznámka: pokud OVM dosud zpracovával při plnění úkolu dle § 5/2/e ZOOÚ (nezbytné pro ochranu práv a právem chráněných zájmů), musí s GDPR přejít na čl. 6/1/e, výjimečně /f !)*

Právní tituly pro zákonnost ve veř. správě méně obvyklé případy – oprávněný zájem

Čl. 6/1/f

vždy před zahájením zpracování komplexně posoudit:

- (1) jestli je stanovený **zájem oprávněný** (tedy jestli splňuje požadované kvality),
- (2) jestli je zamýšlené **zpracování** skutečně **nezbytné**
- (3) jestli nad zájmem nepřevažují zájmy nebo základní práva a svobody SÚ (balanční test).

Dosud byl oprávněný zájem jen na právním základě.

Nově: podle Nařízení lze **subjektivně stanovený oprávněný zájem**.

Oprávněný zájem - typicky např. vymáhání právních nároků, předcházení podvodům, IT bezpečnost...u soukr. osob: výkon svobody projevu a práva na informace.

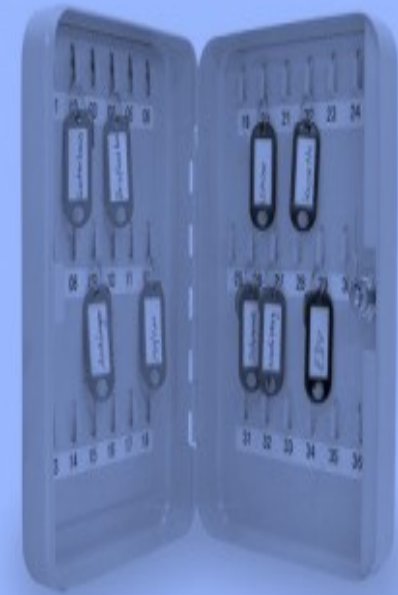


Právní tituly pro zákonnost – citlivé údaje

Čl. 9

Zvláštní kategorie údajů – obecně se zpracování zakazuje. Pouze výjimky:

- a) výslovný souhlas (+ zjevně zveřejněné subjektem údajů)
- b) nezbytné v oblasti **pracovního práva, sociálního zabezpečení a sociální ochrany**
- c) nutné pro ochranu **životně důležitých zájmů** subjektu údajů nebo jiné fyzické osoby pokud subjekt není schopen dát souhlas
- d) nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle
- e) OÚ zjevně zveřejněné subjektem údajů
- f) nezbytné pro určení, výkon nebo obhajobu **právních nároků** nebo pro výkon pravomocí **soudu**

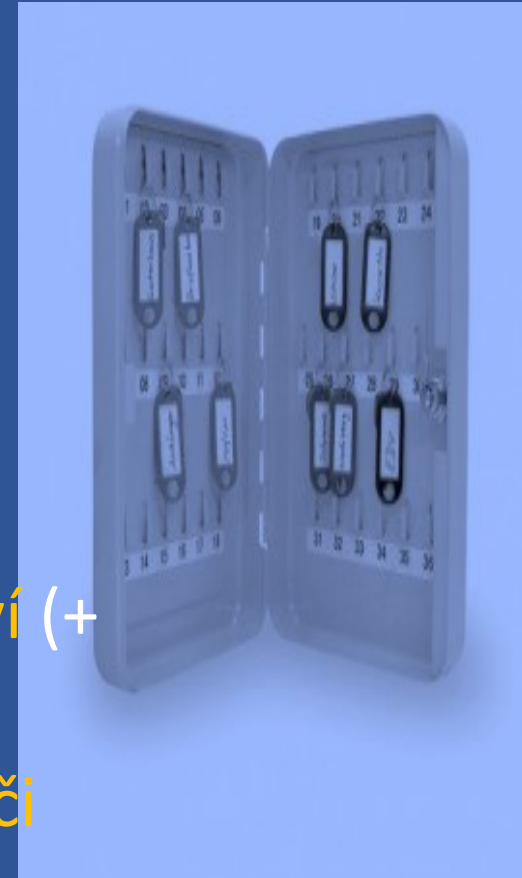


Právní tituly pro zákonnost – citlivé údaje

Čl. 9

Zvláštní kategorie údajů – další výjimky jen na základě zákona:

- g) nezbytné z důvodu **významného veřejného zájmu**
- h) nezbytné pro účely **preventivního nebo pracovního lékařství**, posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče
- i) nezbytné z důvodů veřejného zájmu v oblasti **veřejného zdraví** (+ nutná mlčenlivost)
- j) pro účely **archivace** ve veřejném zájmu, pro účely **vědeckého či historického výzkumu** nebo pro **statistické** účely



Kontrolní záznam - průlet



záznamy o činnostech zpracování ÚŘAD xxx, i.č.	skupina otázek k implementaci ON	Pojmenování a popis agendy / parametr zpracování OsÚ	ustanovení ON	související ustanovení ON	forma odpovědi	Agenda žádostí o pronájem bytu ze sociálních důvodů - OSZP OSV	Vítání dětí
37	3 - zákonno st zpracová ní	pokud jde o "citlivé os. údaje", konkrétní právní základ	9		X/ ANO - příslušné ustanovení zvláštního zákona	ANO - § 16/3 zák. o Praze - samostatná působnost	ne
38	3 - zákonno st zpracová ní	pokud jde o "citlivé os. údaje", splňují pr. tituly b/g/h/i/j požadavky čl. 9 ?	9		X/ANO/NE	ANO (mlčenlivost dle ZOOÚ je v pracovních náplních)	X
39	3 - zákonno st zpracová ní	je technicky nebo organizačně určen okruh pracovníků, kteří opravdu potřebují přístup k OsÚ v této agendě?	5/1/f		ANO / NE	kompletní dokumentace: plyne z pracovních náplní, obecná shrnutí v Lotus Notes - NE (PROBLÉM)	ano
40	3 - zákonno st zpracová ní	Mají přístup v pracovní náplni?	5/1/f		ANO / NE	ANO (v některé pracovní náplni je výslovně sociální bydlení)	ano
41	3 - zákonno st zpracová ní	Mají mlčenlivost?	5/1/f		ANO / NE	ANO	ano
42	3 - zákonno st zpracová ní	Je přístup jiných pracovníků k údajům v IT systému blokován? (nemají přístupová práva)	5/1/f		ANO / NE	kompletní dokumentace: ANO obecné shrnutí v Lotus Notes: NE (PROBLÉM)	ano
43	3 - zákonno st zpracová ní	mohou údaje editovat jen k tomu oprávněné osoby?	5/1/f	32	ANO / NE	???	ano

Barva výplně buňky: žlutě - nutno vyjasnit, oranžově - je problém, nutno řešit

2. Korektnost a transparentnost

(komunikace se subjektem údajů – jeho **práva**,
otevřenost ve věcech zpracování **a férovost** jednání)



Korektnost a transparentnost

(komunikace se subjektem údajů - SOUHRN)

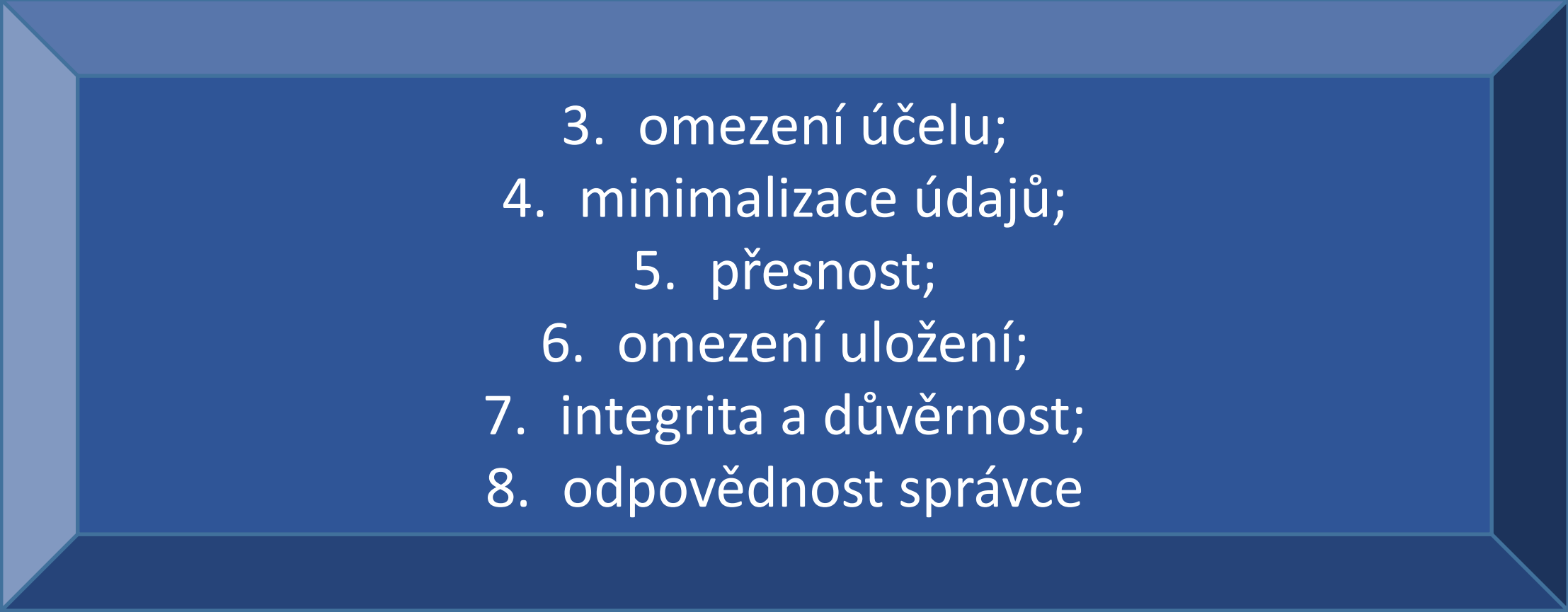
Právo subjektu údajů na:

- informace o prováděném zpracování a souvisejících právech (čl. 13 a 14)
- přístup ke svým OÚ (čl. 15)
- opravu nepřesných OÚ (čl. 16)
- výmaz („právo být zapomenut“) (čl. 17)
- omezení zpracování (čl. 18)
- přenositelnost údajů (čl. 20)
- vznést námitku (čl. 21)
- nebýt předmětem rozhodnutí z výhradně automatizovaného zpracování (čl. 22)

} + Oznamovací
povinnost
příjemcům

Další povinnosti správce

(a zpracovatele)

- 
- 3. omezení účelu;
 - 4. minimalizace údajů;
 - 5. přesnost;
 - 6. omezení uložení;
 - 7. integrita a důvěrnost;
 - 8. odpovědnost správce

3. Omezení účelem 1

Čl. 5/1/b

- **KLÍČOVÁ ZÁSADA** zpracování osobních údajů
- vymezením účelu - správce určí, z jakého důvodu osobní údaje zpracovává → dál je může zpracovávat pouze k tomuto účelu
- zakazuje se - až na výjimky - zpracovávat osobní údaje za jinými účely, než za kterými byly shromážděny.
- **Účel** stanovit (vyjádřit) dostatečně určitě, aby bylo jasné, jaká zpracování budou probíhat, (příklad: *pronájem bytů sociálně potřebným osobám na zákl. usn. RMČ č. 1691/12*)
- vyvarovat se obecných frází, nezaměňovat z právními tituly (např. „splnění právní povinnosti“)



3. Omezení účelem 2

Čl. 5/1/b

- Uvádí se v záznamech o činnostech zpracování (Kontrolní seznam, checklist)
- Výjimky: tzv. „jiný účel zpracování“ přípustné pouze:
 - archivace ve veřejném zájmu, vědecký či historický výzkum nebo statistické účely
 - souhlas
 - Povoleno zákonem pro důležitý veřejný cíl (dle čl. 23/1 ON)
 - „posouzení slučitelnosti“ dle čl. 6/4 ON (zdokumentovat, uchovat k prokázání souladu)
 - *+ nutno SÚ informovat o zahájení dalšího zpracování*



4. Minimalizace údajů

Čl. 5/1/c

- správce smí k danému **účelu** zpracovávat pouze osobní údaje, které jsou pro **dosažení účelu** nezbytné, a to pouze v nutném rozsahu.
- Je součástí „Záměrné a standardní ochrany osobních údajů“
→ volba prostředků (softwarových aplikací, HW prostředků) i zpracování - zajistit minimalizaci údajů.
- Např. **rodné číslo** se někdy používá jako jedinečný identifikátor. Není však relevantní, přiměřené, nezbytné. Jako jedinečný identifikátor lze využít jakékoliv jiné přidělené číslo (např. pořadové).



5. Přesnost

Čl. 5/1/d

Čl. 16

- Na žádost SÚ – správce má povinnost OÚ opravit
- A dále sám aktualizuje a ověřuje
- Míra ověřování a aktualizace se řídí rizikem újmy:
 - Údaj o dlužníkovi → riziko značné újmy → nutno prověřovat
 - Údaj z evidence docházky → riziko značné újmy → nutno prověřovat
 - Údaj o soukromé e-mailové adrese pro příležitostná sdělení → malé riziko



Zda pravidelně
probíhá ověřování

6. Omezení uložení

Čl. 5/1/e

- uchovávat osobní údaje pouze po dobu, jež je nezbytná pro účel,
- O době informovat SÚ
- Doba může být stanovena relativně – např. 2 měsíce po ukončení řízení. Nemůže však být neurčitá.
- Po této době – výmaz nebo anonymizace
- Některý údaj může zůstat, pokud spadá také pod jiný účel
- Anonymizace – není jednoduchá, často není dokonalá



Zda je stanoveno a dodržuje se

7. Integrita a důvěrnost 1

Čl. 5/1/f

Čl. 32

- zabezpečení před neoprávněným zpracováním a zároveň před náhodnou ztrátou, zničením nebo poškozením.
- S přihlédnutím:
 - ke stavu techniky, nákladům
 - povaze, rozsahu, kontextu a účelům zpracování
 - různě pravděpodobným a různě závažným rizikům pro práva a svobody SÚ
- Příklady:
 - pseudonymizace a šifrování
 - zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti
 - schopnost obnovy dostupnosti v případě incidentů;
 - pravidelné testování, posuzování a hodnocení



7. Integrita a důvěrnost 2

Čl. 5/1/f

Čl. 32

Bezpečnost osobních údajů

- Co vlastně chráníme?
 1. Technická forma nosičů: listinně (spisy, složky), elektronické dokumenty, databáze. Data na PC, NB, sdílených discích v emailech atd. Zálohy – strukturovaná i nestrukturovaná data
 2. Životní cyklus OÚ: zdroj údajů → účel aplikace → co vše se s údaji děje → kdo k nim přistupuje (exporty, kopie, zpracovatel, externí administrátor) → vynášejí se tech. prostředky s údaji (notebook, flash disky) ? → doba uchování → zálohování → kdo jsou příjemci.
 3. Je někde v řetězci „díra“? Tj. jsou všude nastavena nějaká pravidla? Plní se?

7. Integrita a důvěrnost 3

Čl. 5/1/f

Čl. 33

Incident:

- Správce – ohlásit **do 72 hodin** (*od vědomosti relevantního zaměstnance, ale lze i postupně dle vývoje, čl. 33/4*)
 - Výjimka: je **nepravděpodobné**, že by mělo za následek riziko pro práva a svobody SÚ.
- Zpracovatel – ohlásit správci bez zbytečného odkladu (ihned)

Hlášení:

- popis **povahy případu** (asi včetně míry rizika), a dále pokud je to možné:
 - Kategorie OÚ, jejich počet
 - přibližný počet dotčených SÚ
 - přibližné množství dotčených záznamů OÚ;



7. Integrita a důvěrnost 4

Čl. 5/1/f

Čl. 33

Obvyklé nedostatky:

- U větších informačních systémů - absence systematického hodnocení auditních záznamů
- nedostatečně aplikovaná a prosazovaná pravidla pro používání hesel,
- nedostatečná dokumentace opatření na ochranu OÚ,
- Zdokumentovat zejména:
 - přidělování a odebírání uživatelských oprávnění,
 - povinnosti uživatelů,
- nedostatečné zálohování dat - zálohovaná data zůstávají na pevných discích zálohovaného serveru nebo na externím datovém nosiči uloženém a připojeném trvale k serveru,
- nedostatečná nebo žádná pravidla pro likvidaci dat a evidenci datových médií a práci s nimi,
- neprovádí se kontrola dodržování bezpečnostních pravidel,
- externí správce IT odnáší zálohy mimo prostory správce – „v dobré víře“

8. odpovědnost správce 1

Čl. 5/2

Čl. 24 - 25

- správce odpovídá za dodržení všech povinností
 1. zavede vhodná technická a organizační opatření
 2. musí být schopen dodržení souladu doložit **(NOVÉ!)**
 - *reaktivní* → *proaktivní*
 - Vede **ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ**
 - uchovávat důkazy ohledně všech opatření (posouzení, dokumentace systémů zpracování, popisy bezpečnostních opatření, důkazy o udělených souhlasech se zpracováním, o splnění informační povinnosti).



8. odpovědnost správce 2

Čl. 24 - 25

- Záměrná ochrana = vhodná technická a organizační opatření
 - při **určení prostředků** pro zpracování
 - v době zpracování
 - na základě posouzení závažnosti rizik pro práva a svobody subjektů údajů.
 - Příklad – program pro zápis dětí do MŠ a ZŠ - vyloučit křížový přístup ředitelů
- Standardní ochrana = vhodná organizační a **bezpečnostní** opatření
 - k zajištění aby standardně zpracovány jen osobní údaje nezbytně nutné.
 - = konkrétní opatření k minimalizaci a omezení uložení



Úkoly pověřence



- Monitorování souladu s ON a dalšími předpisy EU a zákony, včetně rozdělení rolí a odpovědnosti
- Odborná příprava pracovníků (školení)
- Poskytování poradenství pracovníkům správce i zpracovatele,
- Kontaktní bod pro **subjekty údajů** i pro **dozorový úřad**
- spolupráce s dozorovým úřadem a kontaktní místo pro něj

Čl. 39

Zastupování pověřence

- Krátkodobě – zástup jako jiný zaměstnanec
- Dlouhodobě - ustanovit „náhradního“ pověřence

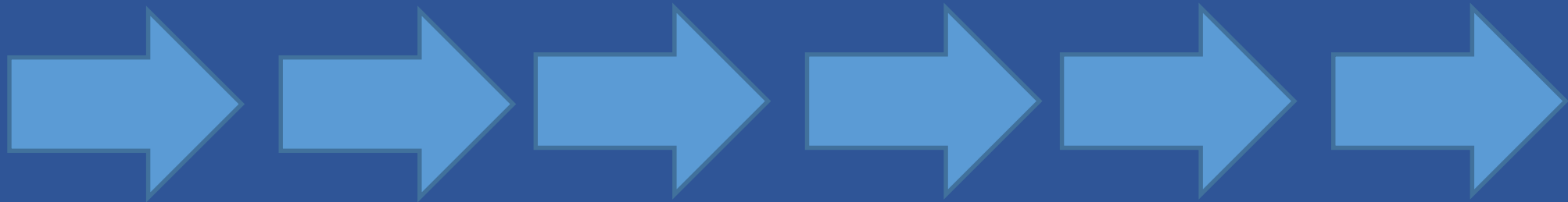
role pověřence v organizaci, kvalifikace



- Pomocník a konzultant v systému ochrany osobních údajů
- Nenese osobní odpovědnost za nedodržování Nařízení
- Úkoly vykonává nezávislým způsobem
- Měl by být přímo podřízen vedení organizace, účast na jednání (např. rada obce, pokud jde o **určení účelu zpracování** OÚ)
- Odborník s dostatečnými vědomostmi v oblasti práva a praxí v oblasti ochrany osobních údajů
- Odpovídající znalost informačních technologií a bezpečnosti
- Zásadní – dobrá znalost organizace a její působnosti
- Etické předpoklady, Mlčenlivost
- Není sankcionovatelný ani od Úřadu pro ochranu OÚ

Čl. 39

Kroky správce k zajištění souladu s ON



Přehled postupu správce (též zpracovatele)

1. Záznamy o jednotlivých **účelech** zpracování
 - Najít všechna zpracování OÚ
 - K nim založit základní **záznamy** podle čl. 30 ON
 - Doplnit k nim **další položky** pro prokázání souladu – „Kontrolní seznam“
2. Vyhodnocení nedostatků – rozdílová (GAP) analýza – červené praporky
3. Rozhodnutí o formě nápravy
 - Stanovení priorit – podle nejvyšších rizik
 - Náprava právních titulů (zejm. zbavit se souhlasů)
 - Analýza životního cyklu OÚ – případná změna, jak zpracovávat
 - Změny v rozsahu údajů, v době uložení
 - Výmaz, anonymizace, vrácení zbytečných dokumentů (např. lékař. zpráva)
 - zajištění informovanosti a uplatňování práv SÚ
4. vztahy se zpracovateli
 - Kde jsou potřební?
 - Revize smluv se zpracovateli



Vyhodnocení (příklad)

agenda	Problém 1	Návrh opatření	Problém 2	Návrh opatření
Organizace zápisu do 1. r. ZŠ	nadbytečné RČ	Neshromažďovat RČ, Shromážděné vymazat	Ukládají se zbytečně dlouho	Po přijetí na ZŠ záznamy mazat, Dosavadní vymazat
Agenda žádostí o pronájem bytu ze sociálních důvodů	stručné shrnutí je přístupné všem s přístupem do Lotus Notes.	Zavést přístupová práva	Kopíruje se OP	Pro kopírování zavést masku pro nezbytné údaje z OP
Poplatek ze psů	SÚ nejsou při získání údajů (formulář) informovány o právním základu, příjemcích, době uložení, právo na přístup, opravu, výmaz a námitku, stížnost u UOOU	Doplnit formulář o toto poučení		

Speciality, diskuse



Smlouvy se zpracovateli

Obsahuje smlouva s veškeré potřebné náležitosti, zejména stanoví:

- Předmět, dobu trvání, povahu a účel zpracování, typy OÚ a kategorie SÚ
- Zajištění mlčenlivosti zaměstnanců
- Garance bezpečnosti údajů v minimálně stejném rozsahu jako u správce
- Potřebnou součinnost při výkonu práv SÚ, zejm. závaznou dobu reakce na požadavky, ohlášení incidentu
- Umožnění auditu, kontroly, inspekce
- Zákaz pověření dalšího zpracovatele bez předchozího souhlasu správce
- Zajištění procesu ohlašovací povinnosti správci při bezpečnostním incidentu

Poskytování informací dle Infozákona

- Nedochází ke změně oproti současnosti
- Právo na informace představuje „oprávněný zájem“ (§ 5/2/e ZOOU – rozsudek NSS 1 As 78/2014)
- Právo na informace je v ON zakotveno výslovně: (4), (65), (153), Článek 17, Článek 85, Článek 86. Zcela respektuje domácí úpravu přístupu k osobním údajům v rámci práva na informace a dává mu přednost před ON.

Sledování na pracovišti

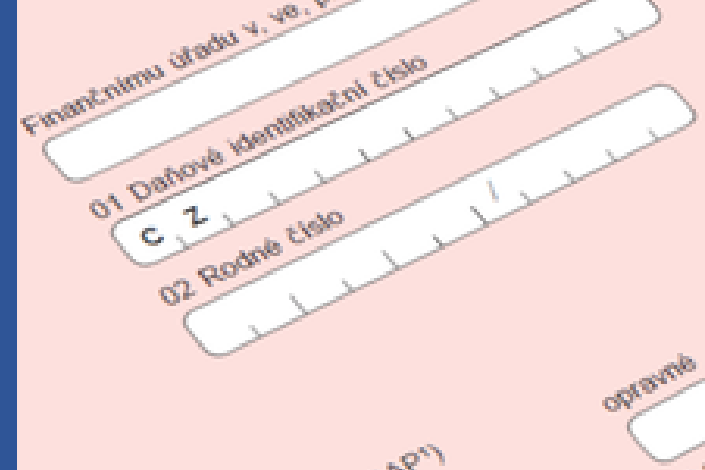
Právo zaměstnance na **soukromí** a **ochranu OÚ**

- Zákoník práce (§ 316), GDPR
- Zákaz narušování soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele (otevřené nebo skryté sledování, odposlech a záznam telefonických hovorů, kontrola elektronické pošty, kontrola listovních zásilek adresovaných zaměstnanci)
- Výjimka – **závažný důvod spočívající ve zvláštní povaze** činnosti zaměstnavatele
- Povinnost přímo informovat zaměstnance o rozsahu a způsobech provádění kontroly, o jmenování pověřence.



Rodná čísla 1

Uvádět jen tam, kde to výslovně vyžaduje zákon



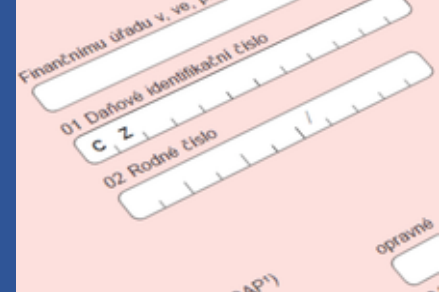
§ 13c odst. 1 písm. a) zákona o evidenci obyvatel

Rodná čísla lze využívat jen:

- a) V činnosti vyplývající ze **zákonem** stanovené působnosti **ministerstev, správních úřadů**, orgánů pověřených výkonem státní správy, soudů, notářů (jen pro evidenci závětí),
- b) stanoví-li tak **zvláštní zákon** (tzn. zvláštní právní předpis - výslovně identifikovat v právním vztahu rodným číslem, např. o veřejném zdravotním pojištění)

Kladné vyřízení žádosti se nesmí podmínit poskytnutím rodného čísla (pokud to není stanoveno právním předpisem) → šlo by o protiprávní postup.

Rodná čísla 2

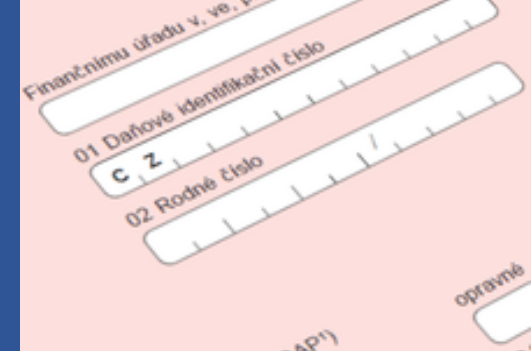


- RČ je i jakákoliv **kombinace čísel** vyjadřující den, měsíc, rok narození a třímístnou nebo čtyřmístnou koncovku rodného čísla
- RČ nelze (mimo správní úřady k zákonem stanovené působnosti) využít pro právní titul „pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci“ (čl. 6/2/e ON), ani „pro účely oprávněných zájmů příslušného správce či třetí strany (6/2/f ON)
- Skutečnost, že v některé veřejně dostupné evidenci i na internetu jsou RČ, neznamená, že je lze užít pro identifikaci osob (není výslovný zákonný podklad).

Příklady:

- RČ nelze požadovat a zpracovávat, i když by to zjednodušilo určitou evidenci (např. v evidenci zápisů do 1. tříd ZŠ by to vyloučilo duplicity).
- V pracovně-právních vztazích RČ jen tam, kde to stanoví zákon – nelze pak užívat pro další dokumenty. Ne do pracovní smlouvy.

Rodná čísla 3



pracovní smlouva podle § 33 až 39 zákoníku práce:

- Může sloužit jako prostředek shromažďování rodných čísel pro využívání zaměstnavatelem na základě:
 - § 10 zákona č. 48/1997 Sb., o veřejném zdravotním pojištění,
 - § 25 zákona č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění,
 - § 46 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení.

Pokud nositel RČ s uvedením ve smlouvě nesouhlasí → sdělí RČ jiným způsobem.

Bezúhonnost (rejstřík trestů)

- Ve vztahu k pracovnímu poměru lze žádat jen tam, kde to stanoví zákon: např. o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních, služební zákon, o sociálních službách, o nelékařských zdravotnických povoláních atd.
- Lze též žádat „je-li k tomu dán věcný důvod spočívající v povaze práce“ (§ 316 odst. 4 ZP)

Občanské průkazy

- zakázáno pořizovat kopie občanského průkazu (§ 15a odst. 2 zák. o OP)
- Výjimka – stanoveno zvláštním zákonem
- Zákaz zpracovávat strojově čitelné údaje (i na čipu)
- Správce musí zajistit, že kopírováním OP se neshromáždí nadbytečné údaje → kopírovací maska s výřezy jen na potřebné údaje



Závěr: 5 pravidel



1. Mapovat – jaké OÚ máme?, Kde jsou? Atd.
2. Spravovat – rozhodnout o způsobech využití a přístupu k OÚ
3. Chránit – zavést bezpečnostní kontroly k předcházení, detekování a řešení hrozeb a incidentů
4. Dokumentovat – vytvářet a uchovávat potřebnou dokumentaci, vyřizovat žádosti a upozornění na rizika
5. Likvidovat

kuzilek@otevrete.cz

Poradna pro právo na informace / OÚ:

<http://poradna.otevrenaspolecnost.cz/pravo-na-informace>