

Obecné nařízení č.2016/679 o ochraně osobních údajů (GDPR)

Nový právní rámec ochrany osobních údajů v evropském prostoru

Příprava pověřence pro ochranu OÚ

Obecné nařízení GDPR a národní legislativa

**NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679
ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti
se zpracováním osobních údajů a o volném pohybu těchto
údajů a o zrušení směrnice 95/46/ES**

- *účinnost od 25.5.2018*

=====

ZÁKON č. 101/2000 Sb., o ochraně osobních údajů

ZÁKON o zpracování osobních údajů – tzv. adaptační zákon

- *ve schvalovacím řízení*

ZÁKON č. 181/2014 Sb., o kybernetické bezpečnosti

VYHLÁŠKA č. 316/2014 Sb., o kybernetické bezpečnosti

Obecné nařízení GDPR a národní legislativa

Další dokumenty vydávané k obecnému nařízení GDPR

Pracovní skupina WP29 - nezávislý evropský poradní orgán na ochranu dat a soukromí

- vydává **pokyny, vodítka a doporučení** která mají poskytnout určitý výklad k některým ustanovením obecného nařízení GDPR

Úřad na ochranu osobních údajů (ÚOOÚ)

- na svých www stránkách zveřejňuje vlastní stanoviska a pokyny k obecnému nařízení GDPR
- zveřejňuje materiály WP29

Ministerstva, oborové svazy a profesní sdružení

- vydávají metodické materiály k implementaci GDPR
vč. komentářů a právních stanovisek, vzory dokumentace

Obecné nařízení GDPR

Historie ochrany OÚ – pozadí vzniku GDPR

- 1950 – Evropská úmluva o ochraně lidských práv a zákl. svobod
- 1981 – Úmluva o ochraně osob se zřetelem na autom. zprac. os. dat
- 1993 – Ústava české republiky a listina zákl. práv a svobod
- 1995 – Směrnice EU o ochraně osobních údajů (95/46 ES)
- 2000 – Princip bezpečného přístavu – zneplatněn 2015 (USA x EU)
- 2000 – Zákon č. 101/2000 Sb., o ochraně osobních údajů



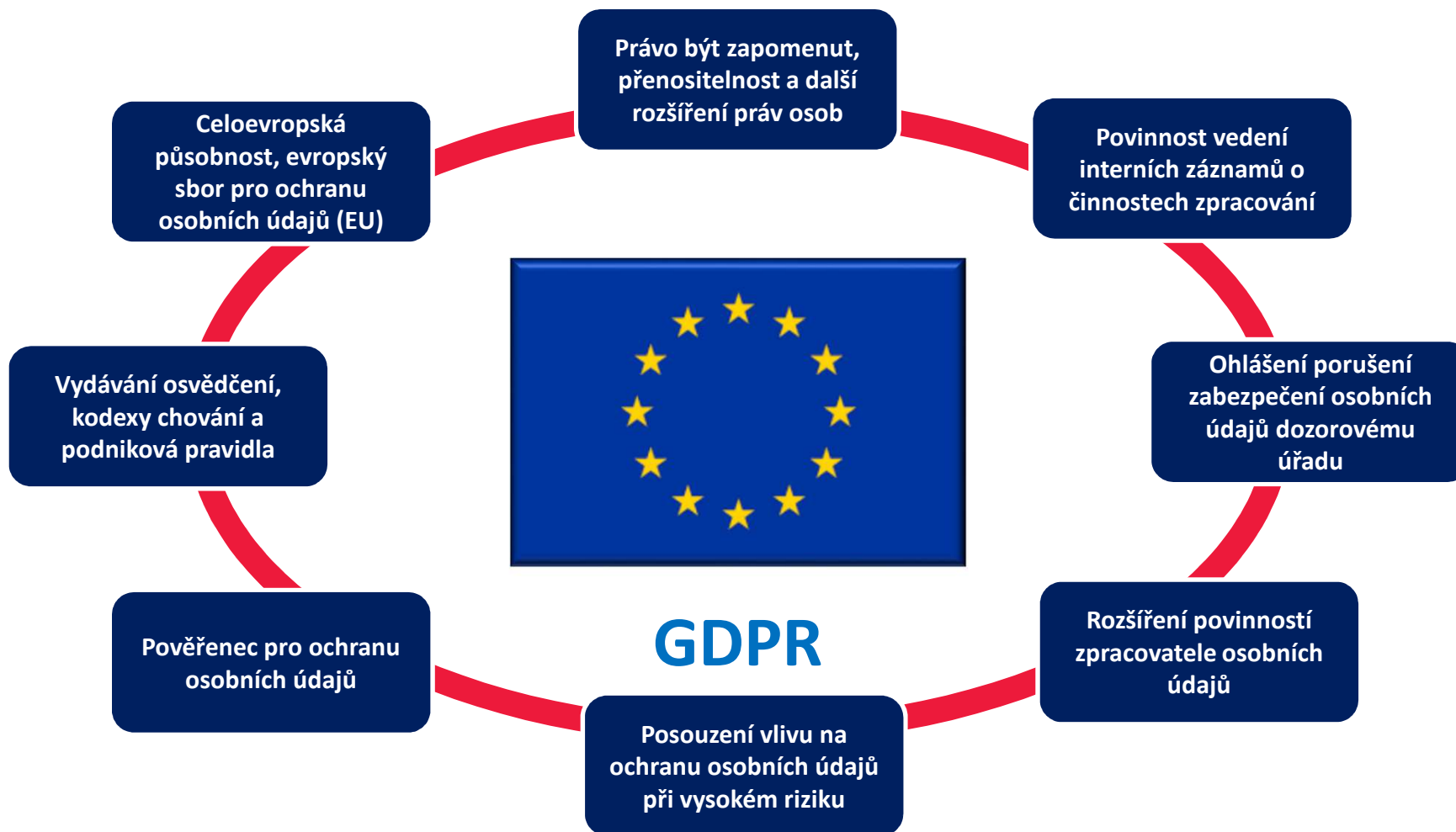
Postupné zpřísňování národních legislativ na ochranu osobních údajů

- 2002 – Směrnice EU 2002/58/ES (ePrivacy)
- 2016 – Nařízení EU 2016/679 (GDPR), Nařízení EU 2016/680 (tr. činy)
- 2017 – *Nařízení o soukromí a elektronických komunikacích (PECR)*

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)
Pověřenec pro ochranu OÚ

Základní změny a dopad nařízení
Věcná a místní působnost

Změny v ochraně osobních údajů



Na koho GDPR dopadá

Nařízení dopadá na kohokoliv (i mimo EU), kdo shromažďuje či zpracovává osobní údaje občanů – subjektů údajů členských zemí EU. Nařízení v mnoha ohledech stírá rozdíl mezi správcem a zpracovatelem

Veřejný sektor

- výkon veřejné moci
- veřejný zájem
- ostatní činnosti

Soukromý sektor

- nabídka zboží a služeb
- monitoring chování FO
- ostatní činnosti

Výjimky z působnosti Nařízení:

- zpracování OÚ nespadá do působnosti práva EU (zpravodajské služby)
- zpracování při výkonu činností společné zahr. a bezp. politiky EU
- zpracování za účelem prevence, vyšetřování, odhalování a stíhání TČ
- zpracování provádí FO výhradně pro své osobní a domácí potřeby

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)
Pověřenec pro ochranu OÚ

Pojmy a definice

Obecné nařízení – pojmy a definice

Definice (čl.4 Nařízení)

Subjekt údajů - pouze fyzická osoba, již se osobní údaje týkají. Údaje vztahující se k právnické osobě nejsou osobními údaji. Subjektem údajů ale pravděpodobně bude i FO podnikající – záleží na charakteru údajů - zda spadají do soukromého života nebo se týkají profesní činnosti

Osobní údaje - jakékoli informace, které se týkají určené nebo přímo či nepřímo určitelné žijící fyzické osoby

Zpracování OÚ - operace, nebo soustava operací, kterou systematicky provádí správce či zpracovatel za určitým účelem či cílem, a to bez ohledu na způsob nebo prostředky zpracování

Obecné nařízení – pojmy a definice

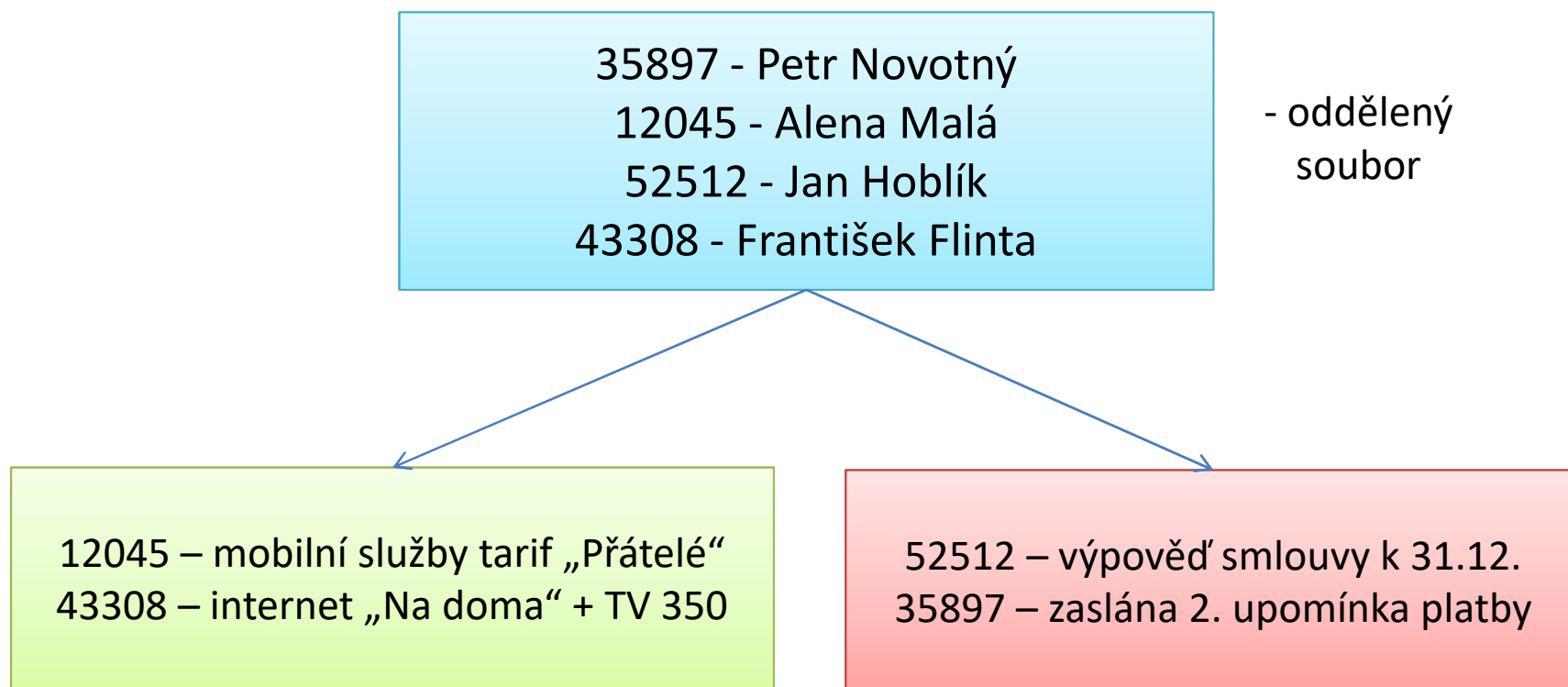
Profilování - automatizované zpracování dat, jehož výsledkem je profil osoby - její chování, ekonomická situace, zdravotní stav, osobní preference, zájmy, spolehlivost atd. s cílem s významnou mírou pravděpodobnosti předpovídat chování či jednání konkrétního člověka

Pseudonymizace - nahrazení identifikačních údajů osob (např. jména a příjmení) nějakým bezvýznamovým identifikátorem - pseudonymem (např. číslem). Soubor, který páruje pseudonymy s konkrétními osobami, je od souboru s osobními daty oddělen.

Je třeba ji odlišit od **anonymizace** – znemožnění zpětné identifikace konkrétní osoby. Anonymizované údaje již nejsou osobními údaji a nespádají do působnosti Nařízení

Obecné nařízení – pojmy a definice

Příklad pseudonymizace – „skrytí identity“



!!! Nezaměňovat pseudonymizaci s anonymizací !!!

Obecné nařízení – pojmy a definice

Správce - fyzická nebo právnická osoba, orgán veřejné moci nebo jiný subjekt, který sám nebo společně určuje účely a prostředky zpracování OÚ

Zpracovatel - fyzická nebo právnická osoba, orgán veřejné moci nebo jiný subjekt, který zpracovává OÚ pro správce

Příjemce - fyzická nebo právnická osoba, orgán veřejné moci nebo jiný subjekt, kterému jsou OÚ poskytnuty

Souhlas subjektu údajů – jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým dává subjekt údajů prohlášením či jiným zjevným potvrzením souhlas se zpracováním svých OÚ

Porušení zabezpečení OÚ (bezpečnostní incident) – situace, která vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění OÚ

Obecné nařízení – pojmy a definice

Genetické údaje – zděděné nebo získané genetické znaky, poskytující jedinečné informace o fyzické osobě

Biometrické údaje – technicky zpracované fyzické a fyziologické znaky nebo znaky chování fyzické osoby, umožňující nebo potvrzující identifikaci (zobrazení obličeje, očního obrazu, daktyloskopické údaje)

Údaje o zdravotním stavu – OÚ o tělesném nebo duševním zdraví fyzické osoby, vč. informací o poskytnuté zdrav. péči (nikoli pouze schopen x neschopen)

Dozorový úřad – nezávislý dozorový orgán veřejné moci

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)
Pověřenec pro ochranu OÚ

Osobní údaje
Zásady a zákonnost zpracování

Osobní údaje

Životní proces ochrany OÚ

Zákonnost při shromažďování a zpracování OÚ



Ochrana OÚ při zpracování a sdílení



Ochrana OÚ při jejich přenosu



Ochrana OÚ při jejich zálohování



Bezpečná likvidace OÚ

Osobní údaje

Čl. 4, odst. 1 Nařízení

„Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“

- je to tedy jakákoli informace, která se týká určené nebo přímo či nepřímo určitelné fyzické osoby
- informaci lze označit za osobní údaj pouze v případě, že se týká žijící osoby

Obecné osobní údaje

Nejčastější obecné osobní údaje

- jméno, adresa, trvalé bydliště, doručovací adresa, pohlaví, věk, datum narození, rodné číslo, místo narození, osobní stav
- fotografie, video a audio záznam, tel. číslo, e-mailová adresa
- různé identifikační údaje vydané státem: IČ, DIČ, číslo OP...
- vzdělání, kulturní profil
- příjem ze zaměstnání (mzda, plat), příjem z důchodu
- osobní údaje dětí nebo manžela/manželky

Sítové identifikátory

- IP adresa, cookies, RFID identifikátory, logovací soubory

Lokační údaje

- informace, týkající se místa pobytu nebo pohybu osoby (GPS)

Zvláštní osobní údaje

Nejčastější zvláštní osobní údaje

- rasový a etnický původ, zdravotní stav, sexuální orientace, trestní delikty, pravomocná odsouzení, náboženské vyznání, členství v odborech

Genetické údaje

- DNA + RNA (čtení genetického kódu), krevní skupina, Rh faktor krve

Biometrické údaje

- otisk prstu, snímek obličeje, snímek oční duhovky, snímek sítnice, charakteristika písma, podpis, charakteristika hlasu (zabarvení), mapa žil na hřbetu ruky

Zpracování osobních údajů

Zpracování osobních údajů je jakýkoli úkon nebo soubor úkonů, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky

- jedná se zejména o shromažďování, zaznamenání, uspořádání, strukturování, vyhledávání, nahlédnutí, ukládání na nosiče, zpřístupňování, úprava nebo pozměňování, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování, výmaz či zničení

Nejedná se ovšem o jakékoli nakládání s osobním údajem, ale o sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky

Zásady zpracování OÚ – čl.5

Zásada zákonnosti – zpracování pouze na základě právního titulu

Zásada přesnosti – zpracovávané OÚ musí být přesné a aktualizované.
Nepřesné údaje je třeba opravit nebo vymazat

Zásada omezení účelem – povinnost uchovávat OÚ pouze po dobu, nezbytnou pro účely zpracování.

Minimalizace a omezení uložení – zpracování pouze nezbytných OÚ a povinnost anonymizovat či vymazat nepotřebných OÚ

Zásada integrity a důvěrnosti – přijetí vhodných technických a organizačních opatření – ochrana OÚ před neoprávněným či protiprávním zpracováním, ztrátou, zničením nebo poškozením (čl.32 Nařízení)

Zásada odpovědnosti – povinnost správce zajistit soulad zpracovávání OÚ s Nařízením a schopnost tento soulad prokázat

Zákonnost zpracování OÚ

Čl. 6 Nařízení

Správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a pouze v odpovídajícím rozsahu

Splnění právní povinnosti	Splnění smlouvy
Veřejný zájem, výkon veřejné moci	Ochrana životně důležitých zájmů SÚ nebo jiné FO
Souhlas SÚ	Oprávněný zájem správce nebo třetí strany

Zákonnost zpracování OÚ

Zpracování zvláštních kategorií OÚ (čl.9 Nařízení)

Výslovný souhlas	Plnění povinností dle pracovního práva
Životně důležité zájmy	Zdravotní a soc. péče
Zjevně zveřejněné údaje	Výkon nebo obhajoba právních nároků
Významný veřejný zájem	Veřejný zájem při ochraně veřejného zdraví či archivaci

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)
Pověřenec pro ochranu OÚ

Právní základ zpracování OÚ

Zpracování osobních údajů

Kdo je kdo

Správce = osoba určující účel a způsob zpracování OÚ

Základní odpovědnost za údaje

Řada nových povinností

Zpracovatel = zpracovává osobní údaje jménem správce

Sdílená odpovědnost a sdílené povinnosti

Možnost řetězení zpracovatelů

Zpracování osobních údajů na základě smlouvy

Subjekt údajů (SÚ) = fyzická osoba, které se OÚ týká

Právní základ zpracování OÚ

Plnění právní povinnosti

Pokud pro správce vyplývá z právního předpisu čl. státu nebo EU, povinnost zpracovávat určité OÚ, pak je na takové zpracování aplikovatelný právní titul plnění právní povinnosti bez nutnosti souhlasu SÚ se zpracováním jeho OÚ

Právní povinnost musí být právním předpisem stanovena jistě a určitě k minimalizaci možnosti vlastního uvážení správce, jak povinnost splní

Př.: zaměstnavatel má dle §10 zákona o veřejném zdravotním pojištění povinnost předávat osobní údaje zaměstnance zdravotní pojišťovně. Takové zpracování tedy bude možné i bez souhlasu SÚ z důvodu splnění právní povinnosti

Plnění právní povinnosti

Zvláštní právní předpisy, které zaměstnavateli ukládají povinnost zpracovávat osobní údaje ke stanoveným účelům:

- *zákon č. 262/2006 Sb., zákoník práce*
- *zákon č. 187/2006 Sb., o nemocenském pojištění*
- *zákon č. 48/1997 Sb., o veřejném zdravotním pojištění*
- *zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení*
- *zákon č. 586/1992 Sb., o daních z příjmů*
- *zákon č. 565/1990 Sb., o místních poplatcích*
- *zákon č. 277/2009 Sb., zákon o pojišťovnictví*
- *zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu*

Právní základ (titul) zpracování OÚ

Plnění smlouvy

1. Pokud je zpracování nezbytné pro plnění smluvního závazku
2. Pokud se jedná o zpracování OÚ, které směřuje k uzavření smlouvy (i když v konci nemusí být uzavřena)

Nesmí být překročen účel, ke kterému se zpracování vztahuje, musí být pouze v nezbytném rozsahu pro splnění závazku

Př.: prodejce zpracovává osobní údaje zákazníků na základě právního titulu – smlouvy o poskytování služeb nebo kupní smlouvy. Chce začít využívat osobní údaje zákazníků k účelům přímého marketingu prostřednictvím reklamní agentury. K tomu ovšem bude potřebovat jiný právní titul – souhlas.

Právní základ zpracování OÚ

Veřejný zájem nebo výkon veřejné moci

- primárně náleží pro zpracování OÚ orgány veřejné moci
- mohou využívat i subjekty soukromého práva, pověřené výkonem určitých úkolů státní moci (soukr. školy, komory, revize,...)
- správce – možnost si v některých případech zvolit, jakým způsobem úkol ve veřejném zájmu splní (rozdíl s právní povinností)

Tento právní titul v Zákoně č. 101/2000 Sb. zcela chyběl.

Orgány veřejné moci budou v naprosté většině případů zpracovávat OÚ na základě právního titulu plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci nebo jako doposud – na základě právního titulu plnění právní povinnosti

Právní základ zpracování OÚ

Vybrané zákonné agendy veřejné moci

Archivnictví	Veřejný pořádek, vnitřní a vnější bezpečnost
Poskytování informací veřejnou správou	Územní samospráva
Správní a daňové řízení	Pracovněprávní vztahy, zaměstnanost
Doprava	Rodná čísla
Elektronická veřejná správa (e-government)	Místní poplatky
Elektronické komunikace	Sociální zabezpečení
Evidence obyvatel, matriky, registry	Veřejné rejstříky a evidence
Kamerové systémy	Školství
Regulace provozování sázkových her	Statistická zjišťování
Předávání OÚ do zahraničí	Volby

Právní základ (titul) zpracování OÚ

Souhlas se zpracováním OÚ (čl.7 Nařízení)

V současné právní úpravě (ZOOÚ) se jedná o dominantní titul

V Nařízení je možnost využívání jen doplňkově, pokud správce nebude mít možnost využití jiného právního titulu, ale jeho získání současně podléhá podstatně přísnějším pravidlům

Souhlas je právním jednáním, jímž subjekt údajů vyjadřuje souhlas k tomu, aby správce zpracovával jeho osobní údaje

Právní základ (titul) zpracování OÚ

Souhlas se zpracováním OÚ

**Souhlas musí být:
*svobodný, konkrétní, informovaný, a jednoznačný***

Svobodný – SÚ musí mít možnost volby bez rizika klamání, zastrašování, nátlaku či jiných negativních důsledků

Konkrétní – souhlas musí být udělen pro konkrétní účely zpracování, nelze jej udělit obecným prohlášením

Informovaný – subjekt musí být před jeho udělením informován o všech skutečnostech zpracování (čl.12 – 13 Nařízení)

Jednoznačný – udělení souhlasu by mělo být nezpochybnitelné (prohlášení nebo jiné zjevné potvrzení) ?? konkludence ??

Právní základ (titul) zpracování OÚ

Souhlas se zpracováním OÚ

Doporučení k prohlášení o souhlasu:

- *oddělitelnost obsahu od ostatních skutečností v dokumentu*
- *srozumitelné znění a jednoduchý jazyk*
- *správce by se měl vyvarovat právníckému jazyku a nesrozumitelným formulacím*
- *využití vhodných metod v textu (otázka – odpověď)*
- *vyločit jeho umístění v obchodních podmínkách*
- *neměl by být umístován do adhezních (formulářových) smluv*
- *vyločit podmíněný souhlas, preferovat „členěný“ souhlas*

Z důvodu vyloučení pochybností se doporučuje

písemná forma souhlasu

Právní základ (titul) zpracování OÚ

Prokázání udělení souhlasu

Správce by měl být vždy schopen doložit udělení souhlasu se současným splněním všech na něj kladených požadavků

Ze záznamu o udělení souhlasu by mělo být patrné:

- a) kdo souhlas udělil*
- b) kdy jej udělil*
- c) o čem všem byl SÚ před udělením souhlasu informován*
- d) jak byl souhlas udělen (v případě že písemně – kopie)*
- e) údaj o tom, zda byl souhlas odvolán*

Právní základ (titul) zpracování OÚ

Odvolání souhlasu:

- pro SÚ musí být odvolání souhlasu stejně jednoduché, jako jeho udělení, **o možnosti odvolat souhlas musí být SÚ informován**
- správce musí vždy ověřit identitu toho, kdo souhlas odvolává
- pro správce povinnost OÚ vymazat či anonymizovat s výjimkou údajů, které správce zpracovává odděleně na základě více právních titulů
- pokud nebude žádný právní titul, musí správce vyhledat a smazat veškeré OÚ, vč. např. dřívější e-mailové komunikace se SÚ

Právní základ zpracování OÚ

Životně důležitý zájem

Tento právní titul pro zpracování je možné použít v případě nutnosti předejití újmy na životě SÚ nebo jiné osoby

- použití pouze pokud není možné využít jiného právního titulu
- **nově lze využít i pro případ ohrožení životního zájmu jiné FO**
- podle současné úpravy (Zák.č.101/2000 Sb.) musí správce zajistit dodatečně souhlas od SÚ, nově podle Nařízení již dodatečný souhlas SÚ nebude nutný

Př.: nemocnice přijímá do péče zraněnou osobu v bezvědomí a potřebuje zjistit její totožnost z důvodu zjištění, zda netrpí alergií na určité léky. Musí prohledat jeho osobní věci a najít průkaz k získání potřebných údajů

Právní základ zpracování OÚ

Oprávněný zájem správce nebo třetí strany

Výsledkem posouzení zda se jedná o oprávněný zájem
by mělo být určení, jestli:

1. stanovený oprávněný zájem splňuje požadované kvality
2. zamýšlené zpracování je skutečně nezbytné
3. nad takovým oprávněným zájmem nepřevažují zájmy nebo zákl. práva na svobody subjektů údajů

Zájem je oprávněný tehdy, je-li:

1. v souladu s právním řádem
2. dostatečně vyspecifikován k **provedení balančního testu**
3. zájem správce na zpracování reálný a současný

Vždy je třeba posoudit, zda je zpracování přiměřené a nezbytné

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)
Pověřenec pro ochranu OÚ

Informační povinnost

Výkon informační povinnosti

Zásada transparentnosti (čl.5 Nařízení)

- správce je povinen **automaticky informovat SÚ o zpracování OÚ, které se jej týkají**, přičemž je povinen splnit informační povinnost **nejpozději současně s jejich samotným získáním**
- poskytování informací se bude uskutečňovat písemně, nebo jinými vhodnými prostředky (např. elektronicky) a to bezplatně

Za okamžik získání OÚ je dle komentáře k Nařízení nutno považovat okamžik, kdy SÚ svoje osobní údaje poskytuje správci (např. vyplňuje formulář). Informace dle informační povinnosti správce tedy musejí být uvedeny přímo na formuláři pro sběr údajů, nelze je zasílat až následně

Práva SÚ – právo na informace

Transparentnost a postupy (čl.12 Nařízení)

Odst.1 „Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem veškeré informace uvedené v čl. 13 a 14 a učinil veškerá sdělení podle čl. 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně“.

Obecně platí, že SÚ si de facto vybírá, jak s ním správce má při výkonu práv komunikovat

Výkon informační povinnosti

Obsah informační povinnosti (čl.13 Nařízení)

Kontaktní údaje – totožnost a kontaktní údaje správce, případně jeho zástupce a pověřence ochrany OÚ

Účel a právní základ zpracování – důvody a cíle shromažďování OÚ a právní základ pro zpracování

Oprávněné zájmy – správce je povinen SÚ o takovém zájmu informovat se současným poučením o právu vznést námitku (výslovně, zřetelně a **odděleně od ostatních informací**)

Příjemce OÚ – informace, které zpracovatele správce využívá ke zpracování OÚ, nebo kterým jiným správcům OÚ předává

Předání do zahraničí – SÚ musí obdržet informaci o tom, že správce hodlá předat jeho OÚ do země mimo EU

Výkon informační povinnosti

Další informace poskytované správcem

Doba uložení OÚ – pokud nelze předem určit, tak např. vztáhnout k právnímu důvodu („*po dobu trvání pracovního poměru*“)

Práva SÚ – odvolat souhlas se zpracováním, požadovat přístup ke svým OÚ, právo na opravu nebo výmaz OÚ, omezení zpracování, právo na přenositelnost OÚ, právo podat stížnost u dozorového úřadu

Důvod poskytnutí OÚ – zda je důvod založen zákonem, smlouvou, výkonem veřejné moci apod. Info, zda je SÚ povinen tyto poskytnout a případný důsledek jejich neposkytnutí

Práva SÚ – transparentní informace

Plnění informační povinnosti správce

Vrstva č.1 – krátké oznámení: uvedeny klíčové údaje – identita správce, k čemu správce OÚ potřebuje, kdo, jak a proč bude OÚ zpracovávat

ODKAZ NA DALŠÍ VRSTVU

Vrstva č.2 – stručné oznámení: již podrobnější informace – kontaktní údaje správce nebo jeho zástupce, kontaktní údaje pověřence OOÚ, účely a právní základ zpracování, doba uložení OÚ u správce, sdělení o právu SÚ k přístupu ke svým OÚ, informace o možnosti omezení zpracování OÚ, informace o právu odvolat souhlas se zpracováním, existence práva podat stížnost **ODKAZ NA DALŠÍ VRSTVU**

Vrstva č.3 – plné oznámení: všechny informace dle čl.13 a 14 Nařízení. Text obchodních podmínek. Lze již užít odbornější jazyk pro přesnost sdělení

Výkon informační povinnosti

Vyřizování žádostí subjektů údajů

Identifikace SÚ

- u každé žádosti musí správce **ověřit totožnost žadatele** a určit, zda se skutečně jedná o daný SÚ aby nebyla zneužita jeho práva jinými osobami
- doporučuje se, aby správce již při shromažďování OÚ určil **identifikátory**, se kterými se budou SÚ prokazovat (doklad totožnosti, e-mail, zaručený elektronický podpis, PIN apod.)

Míra ověření totožnosti by měla odpovídat výši rizika újmy, která by mohla SÚ hrozit při vyřízení žádosti pro jinou osobu

Výkon informační povinnosti

Identifikace subjektů údajů

- pokud **správce** po obdržení žádosti zjistí, že **nemá dostatek identifikačních údajů** k tomu, aby mohl žadatele **bezpečně ztotožnit**, měl by je dle čl. 12, odst. 6 Nařízení vyzvat, aby svoji totožnost doložil **dalšími identifikátory**, které bude moci správce propojit s informacemi, které již má k dispozici
- pokud ani poté **nebude moci SÚ bezpečně identifikovat**, informuje o tom žadatele a **výkon práva neumožní**. Po dalším následném doplnění a bezpečné identifikaci však bude muset správce žadateli výkon jeho práv umožnit

Výkon informační povinnosti

Vyřizování žádostí subjektů údajů

- správce musí žádost zpracovat, posoudit a odpovědět na ni bez zbytečného odkladu, nejpozději do 1 měsíce od obdržení

Prodloužení termínu vyřízení žádosti

- **max. o 2 měsíce**, povinnost o tom informovat žadatele s uvedením důvodů (složitost vyřízení žádosti, časové důvody..)
- po prodloužení již nebude moci správce žádost odmítnout

Odmítnutí žádosti

- pokud žádost nesplňuje předpoklady pro její vyřízení, správce o tomto musí informovat žadatele **do 1 měsíce od přijetí**
- odmítnout lze také žádost, která je nedůvodná nebo nepřiměřená

!!! Nelze v případě žádosti SÚ o poskytnutí jeho OÚ !!!

Výkon informační povinnosti

Vyřizování žádostí subjektů údajů

Po obdržení žádosti tedy správce musí nejpozději do 1 měsíce udělat alespoň jeden z následujících kroků:

- a) *žádosti vyhovět, provést opatření a informovat o nich SÚ*
- b) *odmítnout ji a informovat do 1 měsíce žadatele o důvodech odmítnutí a poučit jej o možnostech dalšího postupu*
- c) *lhůtu o 2 měsíce prodloužit a informovat žadatele o důvodech prodloužení (po tomto prodloužení již musí správce žádosti vyhovět)*

Veškeré činnosti při vyřizování žádosti provádí správce bezplatně, s výjimkou nedůvodné či nepřiměřené žádosti

Výkon informační povinnosti

Další informace poskytované správcem

Automatizované zpracování – info, zda bude docházet k automatizovanému zpracování nebo profilování a o použitých postupech - **není nutno v případech dle čl.22, odst.2 Nařízení**

Př.: banka u žadatele o úvěr provádí automatizované zpracování jeho OÚ a současně profilování z důvodu stanovení jeho bonity. Banka bude muset tyto informace poskytnout žadateli současně se získáváním jeho OÚ

Informace o novém účelu zpracování OÚ (čl.6, odst.4 Nařízení)

*Př.: správce dosud shromažďoval OÚ pouze za účelem plnění smluv. Má záměr začít profilovat zákazníky za účelem poskytování slev. O tomto bude muset nejdřív informovat zákazníky a u nového zpracování posoudit slučitelnost podle čl. 6, odst. 4 Nařízení (**test slučitelnosti**)*

Výkon informační povinnosti

Nový účel zpracování – další zpracování

Další zpracování lze provádět pouze ve čtyřech případech:

- a) udělen souhlas SÚ s dalším zpracováním**
- b) jedná se o zpracování pro účely archivace ve veřejném zájmu, účely historického výzkumu nebo pro statistické účely**
- c) je povoleno právem EU nebo čl. státu a slouží k zajištění důležitých veřejných cílů dle čl.23, odst.1 Nařízení**
- d) nový účel zpracování slučitelný s původním (nutno provést test slučitelnosti dle čl.6, odst.4 Nařízení)**

Výkon informační povinnosti

Výjimky z povinnosti poskytnout informaci

- **pokud SÚ již disponuje informacemi o které žádá, nemusí je správce opětovně poskytovat (musí být ale schopen prokázat splnění dřívější informační povinnosti)**

Př.: správce uzavírá se SÚ dodatek ke stávající smlouvě, kterým se mění předmět smlouvy, ale nemění se účel zpracování. V takovém případě již správce nemá informační povinnost, neboť SÚ již informacemi disponuje

!!! Nelze ovšem SÚ odmítnout informace z důvodu, že jsou již obsaženy v právním předpisu. Nelze tak neinformovat SÚ o jeho právech pouze proto, že jsou uvedena v textu Nařízení !!!

Výkon informační povinnosti

Osobní údaje nebyly získány od SÚ (čl. 14 Nařízení)

Informační povinnost jako podle čl. 13 Nařízení rozšířená o:

- informaci o **kategorii dotčených OÚ** (které OÚ byly získány)
- informaci o **zdroji**, ze kterého OÚ pocházejí
- informaci o **právu vznést námitku proti zpracování** (v okamžiku první komunikace se SÚ) v případě, že je zpracování nezbytné při výkonu veřejné moci nebo ve veřejném zájmu

Informační povinnost správce

Osobní údaje nebyly získány od SÚ (čl. 14 Nařízení)

Lhůty pro informační povinnost:

- **v přiměřené lhůtě** po získání OÚ, **max. 1 měsíc**
- při první komunikaci se SÚ (nabídka služeb e-mailem...)
- v případě, že správce hodlá poskytnout OÚ jinému správci, např. zpracovateli, při prvním zpřístupnění OÚ takovému příjemci

Výjimky z informační povinnosti:

- pokud by poskytnutí informací bylo nemožné nebo by vyžadovalo nepřiměřené úsilí
- **pokud by se tím výrazně ztížilo dosažení cílů zpracování**
- OÚ mají zůstat důvěrné a osoby, které s nimi přicházejí do styku mají povinnost mlčenlivosti (advokáti, lékaři, auditoři)

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)
Pověřenec pro ochranu OÚ

Práva subjektů údajů

Práva subjektů údajů

Právo na přístup k OÚ	Právo na opravu OÚ
Právo na výmaz („být zapomenut“)	Právo na přenositelnost OÚ (portabilitu)
Právo na omezení zpracování OÚ	Právo vznést námitku

Práva SÚ – právo na přístup k OÚ

Toto právo je již zakotveno v dřívějších předpisech EU 95/46 EU, transpozice je provedena v rámci § 12 Zák. o ochraně os. údajů

SÚ má dle čl. 15 Nařízení v případě, že jeho OÚ jsou správcem zpracovávány, právo získat přístup k těmto informacím:

- kategorie dotčených OÚ a účel jejich zpracování
- příjemci, kterým OÚ byly nebo budou zpřístupněny
- plánovaná doba, po kterou budou OÚ uloženy
- existence práva na opravu (čl.16), výmaz (čl.17), omezení zpracování (čl.18), právo vznést námitku proti zpracování OÚ (čl.21)
- existence práva podat stížnost u dozorového úřadu (čl. 77)
- informace o zdroji OÚ , pokud nejsou získány od SÚ
- že dochází k automatizovanému rozhodování vč. profilování

Právo SÚ na jednu bezplatnou kopii OÚ, zpracovávaných správcem.

Práva SÚ – právo na přístup k OÚ

Ochrana práv třetích osob

„Správce poskytne SÚ kopii zpracovávaných osobních údajů“.

(čl. 15, odst.3 Nařízení)

„Právem získat kopii uvedenou v odstavci 3 nesmějí být nepříznivě dotčena práva a svobody jiných osob“.

(čl. 15, odst.4 Nařízení)

Mohou nastávat komplikace u správce:

- např. při **předávání kopií kamerových záznamů** – bude zřejmě docházet k omezení rozsahu poskytnutých údajů
- při **žádosti o výpis z účtu volání** – informace nejen o čase a délce hovorů, ale také o tlf číslech, na které žadatel volal

Práva SÚ – oprava a výmaz

Právo na opravu a doplnění OÚ (čl. 16 Nařízení)

*„Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají.
„...subjekt údajů má právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení“.*

Zásada přesnosti OÚ – správce má zpracovávat přesné a aktuální údaje a nepřesné údaje buď vymazal nebo opravil

Než správce přesnost údajů ověří, je jejich **zpracování omezeno** a po jejich opravě či ověření musí SÚ informovat, že ve zpracování OÚ bude pokračovat (čl. 18 Nařízení)

V praxi může docházet k doplnění OÚ využitím zabezpečeného elektronického formuláře nebo dodatečným prohlášením SÚ

Práva SÚ – oprava a výmaz

Právo na výmaz – „být zapomenut“ (čl. 17 Nařízení)

„Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden důvodů dle čl. 17, odst. 1, písm. a) – f)

Právo na výmaz („právo být zapomenut“) dává SÚ za splnění určitých podmínek právo požadovat po správci, aby zlikvidoval jeho osobní údaje a dále je neuchovával (*informovat jiné správce*)

Práva SÚ – oprava a výmaz

Podmínky pro uplatnění práva na výmaz (čl. 17, odst.1)

- a) správce již OÚ nepotřebuje k účelu pro který je shromáždil nebo zpracovává (zásada omezení uložení dle čl. 5, odst.1 Nařízení)
- b) SÚ odvolá souhlas, na jehož základě správce údaje zpracovává a neexistuje jiný právní důvod pro zpracování – čl. 6, odst.1
- c) SÚ vznesse námitku proti zpracování dle čl. 21, odst.1 (veřejný zájem, veřejná moc, oprávněné zájmy správce) a na základě balančním testu převáží zájem SÚ nad zájmem správce pro další zpracování těchto OÚ, nebo SÚ vznesse námitku proti zpracování dle čl. 21, odst.1 (přímý marketing)
- d) OÚ byly zpracovány protiprávně
- e) na správce doléhá právní povinnost (EU, čl. stát), která mu ukládá OÚ vymazat
- f) jedná se o OÚ dětí a není dán rodičovský souhlas se shromážděním a dalším zpracováním dle čl. 8 Nařízení

Práva SÚ – oprava a výmaz

Výjimky z práva na výmaz

- a) OÚ je nutné zpracovávat pro **výkon práva na svobodu projevu a informace** (žurnalistika, veřejné rejstříky)
- b) **plnění právní povinnosti** (banky, účetní záznamy..) nebo úkolu ve veřejném zájmu nebo při výkonu veřejné moci správcem
- c) **veřejný zájem v oblasti veřejného zdraví** dle čl. 9, odst.2, písm. h) a i)
- d) **veřejný zájem z důvodu archivace pro statistické účely a pro účely vědeckého či historického výzkumu**
- e) OÚ je nutné zpracovávat pro **určení, výkon nebo obhajobu právních nároků** – pokud nelze jinak (zásada nezbytnosti)

Práva SÚ – omezení zpracování

Právo na omezení zpracování (čl. 18 Nařízení)

Právo SÚ požádat správce, aby omezil zpracování jeho OÚ, pokud jsou splněny podmínky dle čl. 18, odst.1 Nařízení

- právo na blokaci OÚ již existuje v současné právní úpravě, oproti právu na omezení zpracování dle čl. 18 Nařízení má však mnohem menší možnost uplatnění
- **oproti současné právní úpravě (Zák. č. 101/2000 Sb.) se možnost SÚ požádat správce o omezení zpracování jeho OÚ rozšiřuje**

Práva SÚ – omezení zpracování

Podmínky pro omezení zpracování

- a) **SÚ popírá přesnost OÚ** - zpracování lze omezit na dobu potřebnou k tomu, aby správce mohl přesnost OÚ ověřit
- b) **zpracování je protiprávní a SÚ odmítá výmaz OÚ** a žádá místo toho o omezení jejich použití
- c) **správce již OÚ nepotřebuje** pro účely zpracování, ale **SÚ je požaduje pro uplatnění svých právních nároků**
- d) **SÚ vznesl námitku proti zpracování podle čl. 21, odst.1 Nařízení** dokud nebude ověřeno zda oprávněné důvody správce převažují nad oprávněnými důvody SÚ

Práva SÚ – omezení zpracování

Činnost správce po obdržení žádosti

Správce musí nejprve posoudit, zda je naplněna alespoň jedna z podmínek dle čl. 18, odst.1 Nařízení. Do 1 měsíce musí správce SÚ informovat o výsledku posouzení

Pokud je splněna některá z podmínek, provede správce označení dotčených OÚ, které lze provést např. jako:

- **dočasný přesun OÚ** do jiného systému
- **znenávštěvnění** vybraných OÚ ostatním uživatelům
- **dočasné odstranění** zveřejněných OÚ z **internetových stránek**
- při automatizovaném zpracování zajistit vhodnými technickými prostředky, aby se již na OÚ nevztahovaly žádné další operace

Práva SÚ – omezení zpracování

Další zpracování označených OÚ

Správce nesmí označené OÚ dále zpracovávat s výjimkou:

- a) udělení souhlasu SÚ, který o omezení zpracování požádal
- b) uplatnění (určení, výkonu nebo obhajoby) **právních nároků**
- c) **ochrany práv jiné fyzické nebo právnické osoby**
- d) **důležitého veřejného zájmu EU nebo čl. státu**

Př.: b) správce připravuje žalobu na bývalého zaměstnance na náhradu způsobené škody. Správce již dříve obdržel žádost o omezení zpracování jeho OÚ. Správce tyto OÚ označil, nicméně je může dále zpracovat pro potřeby uplatnění právního nároku

Práva SÚ – omezení zpracování

Pokud pominou důvody pro omezení zpracování, správce omezení neprodleně zruší. O zrušení musí správce SÚ předem informovat

Zrušení omezení zpracování:

- a) dle čl.18, odst.1,písm a) - **správce provede opravu OÚ a dále může pokračovat ve zpracovávání opravených OÚ**
- b) dle čl.18, odst.1,písm b) - **SÚ správce požádá o výmaz nebo zrušení omezení zpracování**
- c) dle čl.18, odst.1,písm c) – SÚ požádá o zrušení omezení, správce bude muset OÚ vymazat dle zásady omezení uložení
- d) dle čl.18, odst.1,písm d) – správce rozhodne o námitce proti zpracování, buď jí vyhoví nebo odmítne

Oznamovací povinnost ohledně opravy, výmazu nebo omezení zpracování

Dle čl. 19 nařízení má správce **povinnost oznamovat opravy, výmazy a omezení zpracování** dle čl. 16, 17 a 18 Nařízení **všem příjemcům, jimž dotčené OÚ kdykoli předtím poskytnul** (dnes již v § 21, odst.5 ZOOÚ)

Rozšíření je pouze o povinnost informovat SÚ o identitě příjemců, pokud o to požádá – výjimka u některých orgánů veřejné moci

Př.: poskytovateli internetových služeb je doručena žádost uživatele (SÚ) o provedení opravy jeho některých OÚ (chyba v ČP u adresy).
Poskytovatel – SÚ opravu provede, ale bude o tomto muset informovat jiného správce – provozovatele registru, zřízeného např. podle zákona, kterému dříve poskytnul adresu SÚ o jím provedené opravě.
Provozovatel registru bude muset nepřesné OÚ rovněž opravit

Právo na přenositelnost OÚ

Právo na přenositelnost – portabilitu je v oblasti ochrany osobních údajů zcela novým pojmem. Vztahuje se pouze na zpracování prováděná „automatizovanými prostředky“, tedy nikoli manuálně – např. vedení fyzické kartotéky

Dle čl. 20 Nařízení má SÚ právo na to, aby jeden správce jeho OÚ přímo předal jinému správci dle instrukce SÚ

- musí být technicky proveditelné
- nesmí zasahovat do práv třetích osob
- bude se nejvíce uplatňovat u poskytovatelů internetových a dalších telekomunikačních služeb

Právo na přenositelnost OÚ

Právo na přenositelnost lze uplatnit dvěma způsoby:

- a) právem SÚ **získat** (zejména „stáhnout“) **od správce své OÚ** ve strukturovaném, běžně používaném a strojově čitelném formátu
- b) právem na **přímé poskytnutí OÚ** správcem **jinému správci**

Lze jej uplatnit pouze u automatizovaného zpracování OÚ (za použití výpočetní techniky), které je zároveň prováděno na základě:

- a) souhlasu SÚ podle čl.6, odst.1, písm.a) nebo čl.9, odst.2, písm.a)
Nařízení
- b) plnění smlouvy, jejíž stranou je SÚ podle čl.6, odst.1, písm.b)
Nařízení

Právo na přenositelnost OÚ

Vztah práva na přenositelnost OÚ a práva na výmaz OÚ

Právo na přenositelnost OÚ v sobě implicitně neobsahuje právo na výmaz, ale současně jej nijak neomezuje

- pokud si SÚ přeje, aby původní správce po předání OÚ vymazal, musí tak učinit zvlášť

Právo na přenositelnost OÚ automaticky nezasahuje do smluvních a jiných obdobných vztahů mezi původním správcem a SÚ

- uplatnění práva na přenositelnost OÚ tedy nezpůsobuje zánik ani změnu smluvního vztahu s původním správcem

Právo vznést námitku

Podle čl. 21 Nařízení má SÚ právo vznést 3 druhy námitek
proti zpracování jeho OÚ:

- a) proti zpracování, které je prováděno na základě právního titulu oprávněného zájmu a plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci
- b) proti zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely

U obou uvedených případů je potřeba provést test proporcionality

- c) proti zpracování pro účely přímého marketingu vč. profilování, pokud se tohoto přímého marketingu týká

Jde o námitku absolutní, správce musí ukončit zpracování OÚ

Práva subjektů vs. základy zpracování

Právní důvod	Informování jsou-li údaje získány od subjektu údajů	Informování jsou-li údaje získány z jiného zdroje	Právo na přístup	Právo na opravu (řetězení)	Právo na výmaz (řetězení)	Právo na omezení zpracování (řetězení)	Právo na přenositelnost (smlouva, souhlas a automatizované zpracování)	Právo vznést námitku	Právo nebýt podroben automatizovanému rozhodování
Právní povinnost	Ano	Ne, je-li výslovně stanoveno předpisem spolu se zárukami	Ano	Ano	Ne (do skartační lhůty)	Ano	Ne	Ne	Ne, pokud není povoleno právním předpisem stanovícím záruky
Životně důležitý zájem	Ne	Ne, je-li výslovně stanoveno předpisem spolu se zárukami	Ano	Ano	Ne (do skartační lhůty)	Ano	Ne	Ne	Ne, pokud není povoleno právním předpisem stanovícím záruky
Udělený souhlas	Ano, upozornit na možnost odvolání souhlasu	Ano	Ano	Ano	Ano	Ano	Ano	Ne (ale může odvolat souhlas)	Ne, pokud je souhlas výslovný
Plnění smlouvy	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ano
Veřejný zájem	Ano	Jako právní povinnost. Ne, pokud by popřelo smysl zpracování	Ano	Ano	Ne (do skartační lhůty)	Ano	Ne	Ano	Ne, pokud není povoleno právním předpisem stanovícím záruky
Oprávněný zájem	Ano	Ano. Ne, pokud by popřelo smysl zpracování	Ano	Ano	Ano. Ne, pokud jde o ochranu právních nároků	Ano	Ne	Ano	Ano

Obecné nařízení č.2016/679

o ochraně osobních údajů

(GDPR)

Pověřenec pro ochranu OÚ

Správce a zpracovatel

osobních údajů

Správce

Problematika správců je řešena v čl. 24 - 27 Nařízení

Čl. 24, odst.1 Nařízení

„S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována“

Nařízení je ve vztahu k ochraně OÚ založeno na dvou hlavních principech:

- princip odpovědnosti správce a
- přístup správce a zpracovatele založený na riziku

Odpovědnost správce

Správce má odpovědnost za:

- dodržování zásad zpracování,
- za dodržování povinností upravených Nařízením,
- za zabezpečení údajů.

Klíčovou složkou odpovědnosti správce je :

- přijímání a zavádění technických a organizačních opatření pro zajištění souladu s Nařízením (čl.25, čl.32 Nařízením)**
- schopnost soulad s Nařízením prokázat**

Technická opatření – tzv. **záměrná ochrana OÚ**

Organizační opatření – tzv. **standardní ochrana**

Odpovědnost správce

Významné povinnosti správce

- aplikace záměrné a standardní ochrany osobních údajů
- jmenování pověřence pro ochranu osobních údajů (netýká se všech správců)
- posuzování vlivu na ochranu osobních údajů a provádění předchozí konzultace
- ohlašování případů porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a oznamování případy porušení zabezpečení osobních údajů subjektu osobních údajů (fyzickým osobám, jež se údaje týkají)
- vedení záznamů o zpracování (netýká se všech správců)

Odpovědnost správce

Druhy rizika pro práva a svobody fyzických osob

Riziko – obecné měřítko pro zavádění technických a organizačních opatření. Jeho posouzením je komplexní analýza ke zjištění možné újmy pro SÚ

Vysoké riziko – aktivuje povinnost správce provést posouzení vlivu na ochranu OÚ dle čl. 35 Nařízení. Může vznikat při zavádění nových technologií nebo jiných operací zpracování OÚ

Nízké riziko – aktivuje některé výjimky z povinností správce, může jej zprostit povinnosti ohlašování bezpečnostních incidentů dozorovému úřadu

Odpovědnost správce

Identifikace hrozeb spojených se zpracováním

Možné hrozby při zpracovávání OÚ nebo samotnou činností správce:

- excesivní shromažďování OÚ (porušení zásady minimalizace OÚ)
- uchovávání OÚ po dobu delší než nezbytně nutnou
- narušení integrity nebo důvěrnosti OÚ

Míra pravděpodobnosti vzniku újmy může záviset především na:

- počtu osob zapojených do zpracování
- zapojení třetích stran do zpracování
- slabá místa v procesech zpracování a ve správě OÚ

Odpovědnost správce

Zhodnocení závažnosti potenciální újmy a přijetí vhodných opatření k zajištění souladu s Nařízením

Mezi faktory určující závažnost újmy mohou patřit:

- citlivost OÚ (kromě zvl. kategorie OÚ také např. platební údaje)
- objem zpracovaných OÚ
- zranitelnost dotčených FO (dítě, senior...)
- možný dopad zpracování na významné události v životě FO
- možný dopad na ekonomickou nebo sociální situaci FO

Př.: *provozovatel nebankovního registru dlužníků vyhodnotil možné riziko újmy pro zveřejněné FO při nepřesnosti poskytnutých údajů jako vysoké. Proto přijal smluvní opatření s jednotlivými poskytovateli údajů a údaje průběžně ověřuje a aktualizuje*

Odpovědnost správce

Opatření k doložení souladu s Nařízením

Vedle přijetí opatření k zajištění souladu je správce povinen takový soulad také prokázat. V praxi bude nejefektivnějším nástrojem k prokázání souladu přiměřená dokumentace plnění jednotlivých povinností

Dokumentace by měla být komplexnější:

- v závislosti na vyšší rizikovosti zpracování
- v závislosti na velikosti organizace
- v závislosti na množství osob, zainteresovaných na zpracovávání
- v návaznosti na déletrvající zpracování OÚ, u nichž se mohou měnit odpovědné osoby

Směrnice

Koncepce ochrany OÚ - směrnice

Pokud je to s ohledem na rozsah zpracování přiměřené, měl by správce ve formě interního předpisu zavést interní koncepci zásad ochrany a zpracování OÚ a zveřejnit vhodná opatření, kterými by se měli řídit zaměstnanci při zpracovávání OÚ

Směrnice by měla obsahovat konkrétní pokyny pro zaměstnance, jak mají vzhledem ke specifikům dané organizace v praxi provádět zásady a povinnosti při zpracovávání OÚ v souladu s Nařízením

Odpovědnost správce

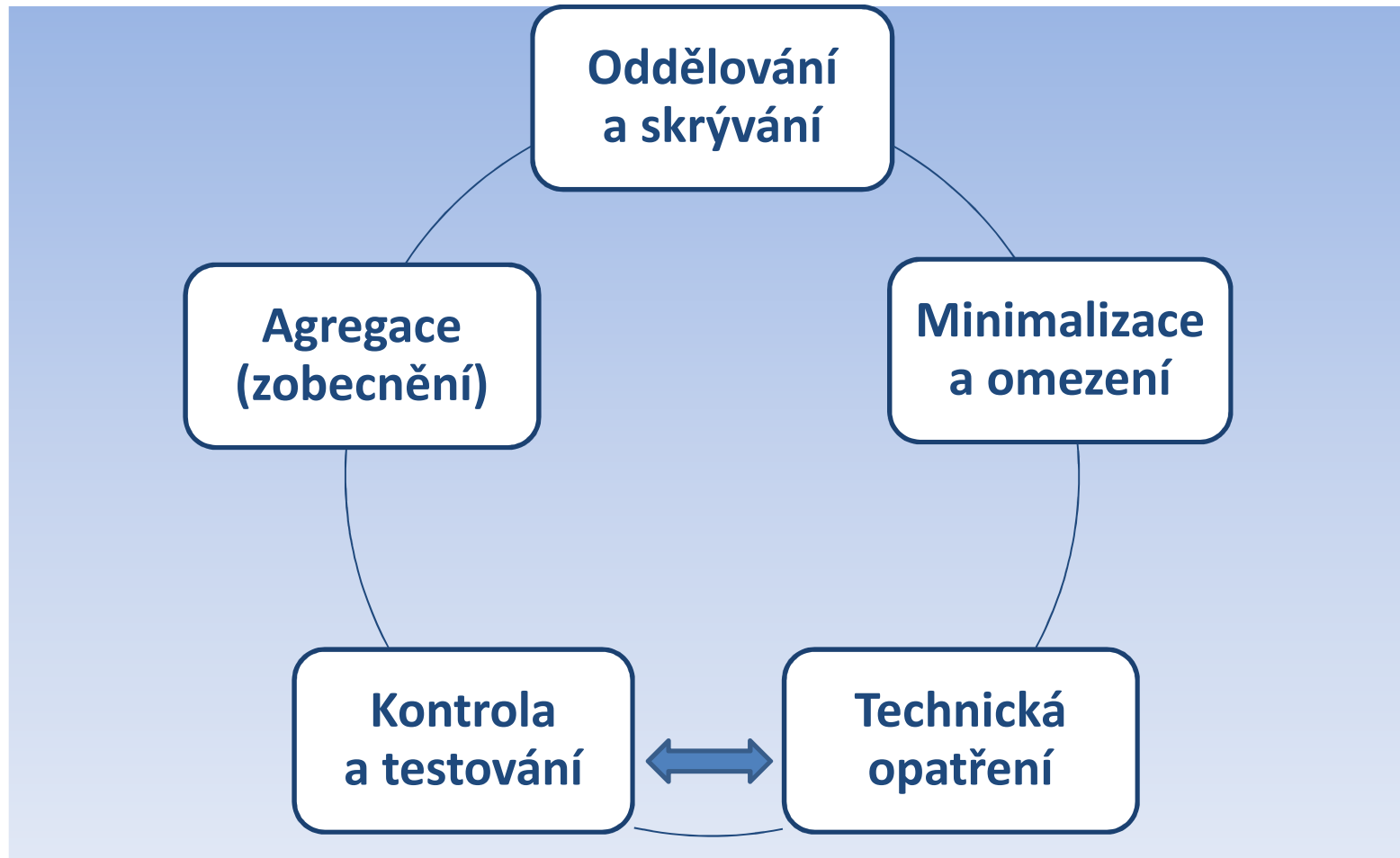
Záměrná a standardní ochrana OÚ (čl.25 Nařízení)

Záměrná ochrana OÚ je jednou z nejvýznamnějších složek principu odpovědnosti. Již v době určení prostředků zpracování musí správce přijmout určitá technická opatření k zajištění plnění zásad ochrany OÚ

- **správci by měli využívat takové aplikace, služby a techniky, které umožní plnit povinnosti při zajišťování souladu s Nařízením a snadný zásah v případě hrozícího bezpečnostního incidentu**
- aplikace a počítačové programy by měly být schopny zpracovávat nezbytné minimum OÚ a následně umožňovat vylepšování bezpečnostních prvků v průběhu dalšího zpracování OÚ

Odpovědnost správce

Záměrná ochrana OÚ vychází ze strategií záměrné ochrany soukromí



Odpovědnost správce

Z požadavků na standardní ochranu OÚ vyplývá pro správce povinnost přijmout vhodná organizační a bezpečnostní opatření k zajištění zpracovávání jen OÚ nezbytně nutných – zásada minimalizace zpracování OÚ

Bezpečnostní (technická) a organizační (standardní) opatření správce v rámci ochrany OÚ by měla být taková, aby:

- ihned při zahájení zpracování zajistila **co nejrychlejší pseudonymizaci OÚ** a tyto byly **přístupné pouze nezbytně nutnému počtu osob**
- zajistila transparentnost ohledně funkcí a přístupu ke zpracování OÚ
- OÚ byly **zpracovávány pouze v nezbytně nutném rozsahu** a byly uchovávány pouze po dobu nezbytně nutnou
- umožnila SÚ přístup k informacím o zpracování jejich OÚ a monitoring

Společní správci

Dle čl. 4, odst. 7 je správcem ten subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování OÚ

- čl. 26 Nařízení upravuje situace, kdy se na zpracování OÚ podílí více subjektů, kteří určují účely a prostředky zpracování
- v takovém případě se z nich stávají **společní správci a musejí mezi sebou uzavřít smlouvu**, kterou upraví vzájemné vztahy tak, aby byla zajištěna ochrana práv a svobod SÚ

Př.: společnost využívá služeb personální agentury k výběru nových pracovníků a k tomu předává agentuře životopisy uchazečů do společné databáze. Agentura je porovnává s vlastní databází uchazečů a vybírá nejvhodnější kandidáty. Tím sama určuje účel a prostředky zpracování, čímž se se společností stává společným správcem

Zpracovatel

Problematika zpracovatelů je řešena v čl. 28 - 29 Nařízení

Správce může pověřit prováděním zpracování OÚ zpracovatele. Zpracovatelem je FO nebo PO, orgán veřejné moci nebo jiný subjekt, který zpracovává OÚ pro správce. Správce může také určit, že se na zpracování OÚ bude podílet více zpracovatelů

- zpracovatel může OÚ zpracovávat **pouze na základě smlouvy se správcem** (smlouva o zpracování OÚ) nebo jiného právního aktu
- **pouze správce může určovat**, jaké OÚ a jakými prostředky bude zpracovatel nebo zpracovatelé OÚ zpracovávat
- správce je povinen pověřit zpracováním pouze zpracovatele, který poskytuje dostatečné záruky ochrany práv subjektů OÚ
- **povinnost správce prokázat, že k předání OÚ došlo až po zavedení vhodných opatření k ochraně OÚ na straně zpracovatele**

Zpracovatel

Zpracovatel je z pohledu ochrany OÚ v podřízeném postavení vůči správci. Pokud překročí pokyny správce a sám určí účel a prostředky zpracování, dostává se do postavení správce s plnou odpovědností za případné porušení Nařízení !!!

Základní povinnosti zpracovatele

- zavést vhodná **technická a organizační opatření** k ochraně OÚ
- **zpracovávat OÚ pouze na základě pokynů správce**
- vést záznamy o zpracování (pokud mu taková povinnost vznikne)
- jmenovat pověřence pro ochranu OÚ, jsou-li splněny podmínky podle čl. 37 Nařízení
- spolupracovat s dozorovým úřadem
- **hlásit porušení zabezpečení OÚ (bezpečnostní incidenty)**

Interní zpracovatelé

Zpracování z pověření správce nebo zpracovatele

- **vedoucí zaměstnanci**, provádějící zpracování OÚ v rámci výkonu své pracovní činnosti
- mají **obecnou odpovědnost** za vykonávané činnosti
- musí být **vyškoleni pro oblast ochrany osobních údajů** vč. jejich podřízených
- musí jim být poskytnuta **metodická podpora** ze strany správce
 - pro oblast zpracování
 - pro oblast ochrany OÚ
 - v oblasti metodiky a dokumentace
- musí mít **možnost kontaktu a konzultací s pověřencem (DPO)**

Externí zpracovatelé

Činnosti zpracovatelů jednotlivých zpracování

- **provádějí zpracování** dle účelu, rozsahu, kategorií... **(dle smlouvy)**
- **se souhlasem správce zajišťují další zpracovatele** a připravují k tomu potřebné smlouvy o zpracování OÚ
- v rámci své působnosti **zajišťují bezpečnost zpracování OÚ** vč. proškolení dalších zpracovatelů

Dále poskytují potřebnou informační součinnost:

- při identifikaci rizik pro práva a svobody SÚ a ochranu OÚ
- pro posouzení vlivu na ochranu OÚ
- při vedení záznamů o činnostech zpracování
- pro předávání informací mimo EU

Zpracovatelská smlouva

Písemně nebo v elektronické podobě

Doporučené náležitosti zpracovatelské smlouvy :

- **předmět a doba trvání zpracování** (vymezit naprosto konkrétně)
- **povaha a účel zpracování** (např. „*vedení mzdové agendy*“)
- **typ a kategorie OÚ** (např. údaje o zdravotním stavu...)
- pokyny správce ke způsobu a formě zpracování OÚ
- **ujednání o mlčenlivosti** (zavázání pracovníků zpracovatele)
- určení konkrétních opatření k zabezpečení zpracování OÚ
- **podmínky řetězení zpracovatelů** (pouze se souhlasem správce)
- **povinnost součinnosti** zpracovatele ve vztahu ke správci a DÚ
- **povinnosti zpracovatele v případě ukončení smlouvy (výmaz OÚ)**

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)

Pověřenec pro ochranu OÚ

Vedení dokumentace

Zabezpečení zpracování

Porušení zabezpečení

Vedení dokumentace dle Nařízení

Nařízení stanovuje povinnost správce a zpracovatele (organizace) uchovávat záznamy k prokázání shody zpracování OÚ s Nařízením a v případě potřeby dozorovému orgánu soulad zdokumentovat

- **dokumentace** by měla být dostatečně určitá, srozumitelná a schopná vyjádřit soulad s Nařízením
- **komplexnost** dokumentace by měla růst s **velikostí organizace** a dále s **rostoucí rizikovostí** zpracování
- nemusí mít pouze listinnou podobu, lze i v elektronické podobě
- měla by být **aktualizovaná v čase**

Vedení dokumentace dle Nařízení

Dokumentace vedená správcem

- identifikace jednotlivých zpracování
- dokumentace k posuzování rizik pro práva a svobody SÚ
- dokumentace k prokázání plnění jednotlivých zásad zpracování
- dokumentace k prokázání právního základu zpracování (čl.6)
- dokumentace k vyřizování žádostí k uplatnění práv SÚ
- záznamy o činnostech zpracování (čl.30)
- smlouvy o zpracování osobních údajů (čl.28)
- dokumentace k případům porušení zabezpečení OÚ (čl.33)

Vedení dokumentace dle Nařízení

Dokumentace vedená zpracovatelem

- identifikace jednotlivých zpracování
- záznamy o činnostech zpracování (čl.30)
- smlouvy o zpracování osobních údajů (čl.28)
- **písemný souhlas správce se zapojením dalšího zpracovatele**
- dokumentace k zavedení vhodných technických a organ. Opatření
- pokyny udělené podřízeným pracovníkům
- dokumentace k prokázání plnění jednotlivých zásad zpracování
- dokumentace k případům porušení zabezpečení OÚ (čl.33)

Záznamy o činnostech zpracování

Čl.30, odst.1 Nařízení

„Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá“

Čl.30, odst.2 Nařízení

„Každý zpracovatel a jeho případný zástupce vede záznamy o všech kategoriích činností zpracování prováděných pro správce...“

Povinnosti vést záznamy o činnostech zpracování nepodléhají podniky nebo organizace s méně než 250 zaměstnanci, ledaže prováděné zpracování pravděpodobně představuje riziko pro práva a svobody SÚ, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech

Záznamy o činnostech zpracování

WP29 vykládá slovo „pravidelný“ jednou nebo kombinací více následujících charakteristik:

- průběžný nebo v pravidelných intervalech a po určitou dobu se opakující
- stále se opakující nebo opakovaný ve stanovených časech
- neustále nebo pravidelně se vyskytující

WP29 vykládá slovo „systematický“ jednou nebo kombinací více následujících charakteristik:

- vyskytující se podle určitého systému
- přednastavený, organizovaný nebo metodický
- uskutečňující se jako součást obecného plánu pro sběr dat
- vykonávaný jako součást strategie

Záznamy o činnostech zpracování

Příklady činností, které mohou zakládat pravidelné a systematické monitorování subjektů údajů:

- provozování telekomunikační sítě, poskytování telekomunikačních služeb
- cílená internetová reklama
- profilování a bodování pro účely posouzení rizik
- sledování polohy (GPS, WiFi)
- **kamerové systémy**
- na těle nositelná monitorovací zařízení (zdravotní data...)
- propojená zařízení (chytré měřiče, inteligentní domy...)

Záznamy o činnostech zpracování

Záznamy správce obsahují:

- jméno - název a kontaktní údaje správce/právnícké osoby
- jméno a kontaktní údaje pověřence pro ochranu OÚ (DPO)
- důvody – účely zpracování OÚ
- popis kategorií SÚ a OÚ
- kategorie příjemců, kterým byly nebo budou OÚ zpřístupněny
- informace o předání OÚ do třetí země či mezinárodní organizace

Doporučeno:

- plánované lhůty pro výmaz jednotlivých kategorií údajů
- popis technických a organizačních bezpečnostních opatření uplatňovaných při zpracování

Záznamy o činnostech zpracování

Záznamy zpracovatele obsahují:

- jméno a kontaktní údaje zpracovatele nebo zpracovatelů a všech správců, se kterými zpracovatel jedná
- jméno a kontaktní údaje pověřence pro ochranu OÚ (DPO)
- kategorie zpracování pro každého správce
- informace o předání OÚ do třetí země či mezinárodní organizace

Doporučeno:

- obecný popis technických a organizačních bezpečnostních opatření uplatňovaných při zpracování

Zabezpečení zpracování OÚ

Povinnost zabezpečení OÚ nepodléhá podle Nařízení výraznějším změnám ve vztahu ke stávající právní úpravě (Zák. č. 101/2000 Sb.)

Dle Čl.32, odst 2 Nařízení je nutné zohlednit násl. rizika:

- „Porušení důvěrnosti“ – neoprávněné nebo náhodné poskytnutí nebo zpřístupnění osobních údajů
- „Porušení dostupnosti“ – náhodná nebo neoprávněná ztráta přístupu (trvalá, dočasná) nebo zničení osobních údajů
- „Porušení integrity“ – v případě neoprávněného nebo náhodného pozměnění osobních údajů

*Nově Nařízení zavádí povinnost ohlašovat porušení zabezpečení OÚ
DÚ v některých případech také SÚ, jejichž OÚ jsou ohroženy*

Zabezpečení zpracování OÚ

Úprava přístupu fyzických osob k OÚ

Správce a zpracovatel musí přijmout taková opatření k zabezpečení OÚ a jejich zpracování, aby k nim měly přístup a zpracovávaly je pouze oprávněné osoby a jejich zpracování současně prováděly pouze podle pokynů správce

V praxi bude tento požadavek znamenat, že správce a zpracovatel bude muset své zaměstnance nebo třetí strany, které budou mít přístup k OÚ a jejich zpracování, zavázat v pracovní smlouvě (nebo dohodě o provedení práce) jednoznačnými pokyny jak s OÚ nakládat a jednoznačně zakázat nakládat s nimi v rozporu s udělenými pokyny

Porušení zabezpečení OÚ

Porušení zabezpečení, které vede k náhodnému nebo protiprávnímu (záměrnému) zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných OÚ

- může k němu dojít činnostmi zvenčí (kybernetické útoky....) nebo činnostmi zevnitř organizace (neoprávněné zpřístupnění OÚ jak úmyslně, tak z nedbalosti (!!! §180 tr. zák. – neopráv. nakl. s OÚ)

Čl.33, odst.1 Nařízení

***„Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob*“**

Porušení zabezpečení OÚ

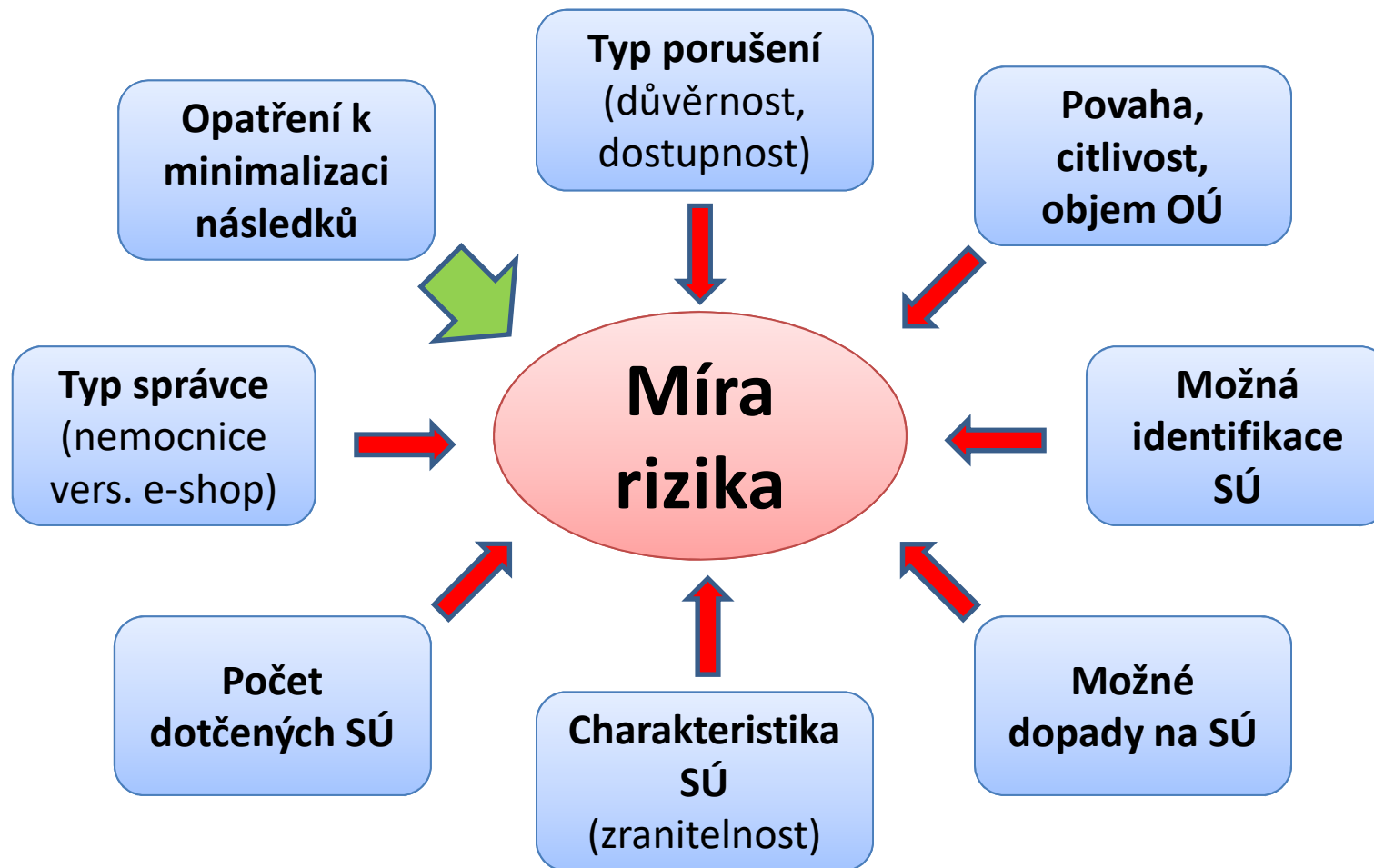
Posouzení ohlášení porušení zabezpečení

- a) vyhodnocení, zda se skutečně jedná o porušení zabezpečení
- b) posouzení rizika pro SÚ, zda je natolik nízké, že nevznikne povinnost porušení ohlašovat DÚ, nebo je naopak natolik vysoké, že zakládá povinnost oznámit porušení také SÚ
- c) posouzení, zda zavedená bezpečnostní opatření jsou taková, že budou činit OÚ nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup (např. šifrování)

Př. vysokého rizika: *ztráta kontroly nad OÚ, omezení práv SÚ, krádež nebo zneužití identity, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti, významné hospodářské a společenské znevýhodnění apod.*

Porušení zabezpečení OÚ

Možné faktory při posuzování rizika porušení



Porušení zabezpečení OÚ

Lhůta pro ohlášení porušení zabezpečení

Pokud správci vznikne povinnost porušení zabezpečení oznámit DÚ, musí tak učinit bez zbytečného odkladu, pokud možno do 72 hodin od okamžiku, kdy se o porušení dozvěděl

- běh lhůty by neměla spouštět jakákoli informace o možném porušení zabezpečení
- **relevantní** by měla být **informace od osoby**, u které je rozumné předpokládat **schopnost vyhodnocení skutečností** jako možné porušení zabezpečení OÚ
- správce může DÚ **předávat informace postupně** podle toho, jak je v rámci porušení zabezpečení **zjišťuje a dokumentuje**
- pokud správce **nezvládne 72 hod. lhůtu** pro oznámení, musí DÚ **oznámit důvody, proč** ve lhůtě nebylo oznámení učiněno

Porušení zabezpečení OÚ

Obsah ohlášení DÚ o porušení zabezpečení

Nařízení stanoví minimální obsahové náležitosti ohlášení porušení zabezpečení OÚ

- a) **popis, o jaké porušení zabezpečení se v daném případě jedná**, (neoprávněný přístup nebo předání OÚ, náhodné poškození nebo zničení OÚ, ...) a popsat okolnosti a průběh porušení
- b) **jméno a kontaktní údaje pověřence** pro ochranu OÚ
- c) **popis pravděpodobných důsledků** porušení zabezpečení OÚ
- d) **popis opatření**, která SÚ přijal nebo přijme, aby vyřešil porušení nebo zmírnil jeho nepříznivé dopady především pro SÚ – **tato část je klíčová**, umožní DÚ posoudit, zda správce na porušení správně zareagoval a není tedy nutné vůči němu uplatnit pravomoci DÚ

Porušení zabezpečení OÚ

Ohlašování porušení zabezpečení zpracovatelem

Na zpracovatele se nevztahuje povinnost ohlašovat porušení zabezpečení OÚ dozorovému úřadu ani SÚ. Jakmile ovšem porušení zjistí, je povinen jej bez zbytečného odkladu oznámit správci. Nařízení přímo nestanovuje náležitosti ohlášení správci ze strany zpracovatele

Na správci leží odpovědnost za splnění ohlašovací povinnosti vůči DÚ a SÚ - zpracovatelská smlouva by měla obsahovat konkrétní ujednání o ohlašovací povinnosti zpracovatele vůči správci a o minimálním rozsahu poskytovaných informací o porušení

Porušení zabezpečení OÚ

Oznamování porušení zabezpečení subjektům údajů

Čl.34, odst.1 Nařízení

„Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů“

Př.: e-shop umožňuje zákazníkům platby platební kartou. Údaje o platebních kartách jsou ukládány na zabezpečený server. Správce zjistí kontrolou tohoto serveru intervencí třetí osobou, která si pořídila kopie těchto údajů. Správce musí tento incident oznámit DÚ s uvedením, že může dojít k hmotné újmě dotčených SÚ. Protože se jedná o vysoké riziko pro práva a svobody fyzických osob, musí o tomto informovat i samotné SÚ

Porušení zabezpečení OÚ

Forma a obsah oznámení porušení zabezpečení SÚ

Na formu a obsah oznámení o porušení zabezpečení subjektům údajů je třeba aplikovat formální požadavky dle čl.12 Nařízení. Mělo by být učiněno „stručným, transparentním, srozumitelným a snadno přístupným způsobem“.

Oznámení musí minimálně obsahovat:

- a) kontaktní údaje na pověřence pro ochranu OÚ
- b) srozumitelné vysvětlení, jaké důsledky může pro SÚ porušení zabezpečení mít (fyzická, hmotná či nehmotná újma)
- c) srozumitelný popis, jaká opatření správce přijal nebo přijme s cílem napravit porušení zabezpečení a ke zmírnění možných nepříznivých dopadů na SÚ

Porušení zabezpečení OÚ

Výjimky z oznamovací povinnosti subjektům údajů

- 1. v případech, kdy přijatá technická opatření zajišťují, že dotčené OÚ jsou nesrozumitelné pro kohokoli, kdo nemá oprávnění k přístupu k nim – šifrování*
- 2. pokud správce po zjištění porušení zabezpečení přijme taková opatření, že se neprojeví vysoké riziko pro práva a svobody SÚ*
- 3. pokud by oznámení znamenalo pro správce vynaložení nepřiměřeného úsilí – např. nemá možnost s přiměřeným úsilím získat kontaktní údaje na SÚ*

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)
Pověřenec pro ochranu OÚ

Pověřenec pro ochranu OÚ
Posouzení vlivu na ochranu OÚ

Pověřenec pro ochranu OÚ

Dle čl.37 Nařízení bude muset část správců a zpracovatelů jmenovat pověřence pro ochranu OÚ (DPO – Data Protection Officer). Pověřenec bude muset fungovat jako samostatný poradní orgán, který se nemusí řídit obchodními či jinými zájmy správce nebo zpracovatele

Postavení pověřence v organizaci správce nebo zpracovatele:

- má mít **specifické** a v mnohých ohledech **nezávislé postavení**
- **nesmí se dostat do střetu zájmů**, v rámci jeho činnosti mu nesmějí být správcem ukládány žádné úkoly či pokyny
- **musí se vymezit proti postupu správce v rozporu s Nařízením** a ostatní legislativou na ochranu OÚ
- slouží jako **kontaktní místo pro dozorový úřad a SÚ**

Pověřenec pro ochranu OÚ

Jmenovat pověřence je povinné v následujících případech:

- 1. Zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů v rámci svých pravomocí*
- 2. Hlavní činnosti správce spočívají v operacích zpracování, které vyžadují pravidelné a systematické monitorování SÚ*
- 3. Hlavní činnosti správce spočívají v rozsáhlém zpracování zvláštních kategorií OÚ dle čl.9 a OÚ týkajících se rozsudků v trestních věcech dle čl.10 Nařízení*

Přestože se na **správce či zpracovatele** povinnost dle čl.37, odst.1 Nařízení nebude vztahovat, **může pověřence jmenovat dobrovolně. V takovém případě** se na správce budou ve vztahu k pověřenci vztahovat veškeré **povinnosti a požadavky** Nařízení, **jako kdyby jeho jmenování bylo povinné**

Pověřenec pro ochranu OÚ

Pokud není jasné zda pověřence jmenovat, pak je doporučeno vzít při určování rozsáhlosti zpracování v úvahu následující faktory:

- počet dotčených subjektů údajů – vyjádřený buď konkrétním číslem, nebo podílem na relevantní populaci
- objem dat a (nebo) rozsah různých datových položek
- počet osob zapojených do zpracování
- předávání OÚ třetím subjektům (zpracovatelům)
- doba trvání nebo nepřetržitost zpracování
- územní rozsah zpracování

Pověřenec pro ochranu OÚ

ad1 Orgány veřejné moci a veřejné subjekty

- *státní orgány, např. ministerstva, různé správní úřady apod.*
- *orgány samosprávy, a to jak územní, tak profesní (komory)*
- *veřejnoprávní korporace – přenesený výkon státní moci (školy ...)*

ad2 Hlavní činnost

- *činnost, jež je primární aktivitou správce, kvůli které byl zřízen,*
- *činnost, která je jeho hlavním cílem*
- *sekundární činnosti – jsou od hlavní činnosti jasně oddělitelné*

ad3 Rozsáhlé zpracování zvl. kategorií OÚ a údajů o TČ

- *vybraná zdravotnická zařízení, náborové agentury*
- *veřejné rejstříky (trestů, přestupků), státní zastupitelství...*

Pověřenec pro ochranu OÚ

Kvalifikace pověřence

Úroveň odbornosti a profesionální kvality:

- úroveň odbornosti by měla odpovídat citlivosti zpracovávaných OÚ, složitosti zpracování a úrovni technických prostředků zpracování
- dostatečné znalosti evropských a národních předpisů v oblasti ochrany OÚ
- znalost procesů zpracování správce, přehled o informačních systémech a zabezpečovacích opatření správce

Schopnost vykonávat úkoly pověřence

- dostatečné povědomí o IT, bezpečnosti, právu a lidských zdrojích
- určitý standard morální a etické integrity

Pověřenec pro ochranu OÚ

Dosažitelnost a komunikace s pověřencem

- pověřenec by měl být **skutečně fyzicky dostupný**
- správce a zpracovatel jsou **povinni zveřejnit kontaktní údaje pověřence a sdělit je také dozorovému úřadu**
- **zavedení takových komunikačních prostředků**, aby je mohli **zaměstnanci správce či zpracovatele a ostatní osoby snadno kontaktovat** s případnými dotazy ohledně zpracování OÚ (např. webový formulář)
- **zajištění důvěrnosti** komunikace s pověřencem
- **bezpečné komunikační prostředky** musí být **bez monitorovacích technologií**

Pověřenec pro ochranu OÚ

Úkoly pověřence (čl.39 Nařízení)

Poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle Nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany OÚ

- pověřenec by měl mít **velmi dobrou znalost Nařízení a ostatních právních předpisů v oblasti ochrany OÚ** a měl by je umět také správně vysvětlit a aplikovat v praxi
- měl by **zavést** takové **komunikační prostředky**, aby jej mohli **zaměstnanci správce či zpracovatele snadno kontaktovat** s případnými dotazy a konzultacemi ohledně zpracování OÚ

Pověřenec pro ochranu OÚ

Úkoly pověřence (čl.39 Nařízení)

Poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle čl.35 Nařízení

Správce by měl požádat pověřence o stanovisko:

- zda je potřeba provádět posouzení a pokud ano, jakou metodiku případně zvolit, zda jej lze provést interně nebo zadat externě
- jaká opatření přijmout k zmírnění rizik ohrožení práv a svobod SÚ
- zda bylo posouzení provedeno správně a jak je následně aplikováno

Pověřenec pro ochranu OÚ

Informační a poradenská činnost pověřence

- **Informovat a radit organizaci**, jejím relevantním partnerům a dodavatelům v ochraně osobních údajů a souladu s nařízením GDPR a zákony o ochraně osobních údajů [členských států]
- **Informovat a radit zaměstnancům** v jejich povinnostech při dodržování GDPR a zákonů členských států při nakládání s osobními údaji
- Interně **zajistit přidělení odpovědností** tak, aby došlo k podpoření trvalého souladu s nařízením GDPR a příslušnými právními normami ČR
- **Zajistit možnost školení a budování povědomí** tak, aby zaměstnanci, kteří se zabývají operacemi zpracování týkajícími se osobních údajů, byli seznámeni s povinnostmi a požadavky plynoucími z nařízení GDPR a souvisejících zákonů

Pověřenec pro ochranu OÚ

Úkoly pověřence (čl.39 Nařízení)

Monitorování souladu s Nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany OÚ, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů

- shromažďování informací o procesech zpracování OÚ
- analýza procesů zpracování a ověřování jejich souladu s Nařízením
- poskytovat informace, rady a doporučení správci a zpracovateli ohledně zpracování OÚ a dodržování souladu zpracování s Nařízením

Pověřenec pro ochranu OÚ

Dohledová činnost pověřence

- Monitoring **identifikace jednotlivých** zpracování osobních údajů
- Monitoring **provádění zpracování na základě zákonného důvodu** podle čl. 6 GDPR či dalších ustanovení GDPR a jiných právních předpisů
- Kontrola **souladu účelů zpracování** osobních údajů
- Kontrola **základních zásad zpracování osobních údajů** ve smyslu čl. 5 GDPR a dbá o to, aby každé zpracování osobních
- Kontrola **balančních testů při použití oprávněného zájmu**

Pověřenec pro ochranu OÚ

Dohledová činnost pověřence

- **Zdokumentovat a udržovat přehledy operací zpracování** na základě informací od organizačních útvarů organizace, zodpovědných za zpracování osobních údajů, a to včetně vedení jejich registru (evidence)
- **Spolupracovat při vytvoření systému ochrany osobních údajů** a pravidelně (1x – 2x ročně) jej hodnotit
- **Prosazovat přístup založený na riziku** –stanovovat priority pro zajištění ochrany zpracování osobních údajů s vysokým rizikem pro práva a svobody subjektů údajů

Pověřenec pro ochranu OÚ

Dohledová činnost pověřence

- Průběžně **sledovat ochranu** záznamů zpracování;
- **Zjišťovat**, do jaké míry jsou osobní údaje **shromažďovány, uchovávány** a (nebo) **používány** v organizaci a **zda jsou řádně kontrolovány a chráněny** před ztrátou důvěrnosti, integrity nebo dostupnosti
- Revidovat a zhodnotit **spolehlivost, přiměřenost a uplatňování bezpečnostních a dalších zásad pro ochranu** osobních údajů
- **Identifikovat a otestovat zásady** a případně **navrhnout další postupy a pravidla**, které mohou být zavedeny **k zachování důvěrnosti, integrity a dostupnosti** osobních údajů.

Pověřenec pro ochranu OÚ

Dohledová činnost pověřence

- **Upozornit** management organizace na případné skutečnosti, které jsou považovány za **potenciální rizikové faktory pro řádné zabezpečení osobních údajů** v rámci organizace
- DPO by měl mít **oprávnění k přístupu ke všem systémům organizace, které se týkají shromažďování, zpracování a uchování osobních údajů za účelem posouzení užívání a zabezpečení osobních údajů**
- **DPO má právo očekávat spolupráci všech zaměstnanců** při plnění těchto povinností, včetně přístupu k systémům a záznamům. **V případě, že nedojde ke spolupráci, podá zprávu vrcholnému vedení organizace**

Pověřenec pro ochranu OÚ

Úkoly pověřence (čl.39 Nařízení)

Spolupráce s dozorovým úřadem a působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle čl.36 Nařízení a případně vedení konzultací v jakékoli jiné věci

- **pověřenec je povinen poskytnout DÚ v případě potřeby veškerou součinnost**
- **pověřenec bude s DÚ komunikovat** např. ve věci předchozí konzultace, v případě kontrol a auditů a dále **vždy, kdy DÚ bude uplatňovat své pravomoci vůči správci či zpracovateli**
- pověřenec bude mít **povinnost sdělit DÚ své kontaktní údaje**

Pověřenec pro ochranu OÚ

Spolupráce a komunikace pověřence s ÚOOÚ

- **Zajistit soulad** společnosti s cíli **GDPR** a dalšími příslušnými právními předpisy
- **Nastavení obhajitelných lhůt** pro uchovávání osobních údajů
- **Povolování nebo schvalování** konkrétních pracovních **postupů**, které umožňují přístup k údajům
- **Návrh způsobu anonymizace** uchovaných dat
- Postup při pseudonymizaci dat
- Následné **sledování všech** těchto **procesů**
- **Komunikace s úřadem v případě porušení zabezpečení OÚ**

Pověřenec pro ochranu OÚ

Pravidelná měsíční agenda DPO (5 – 10 MD)

- **Vedení registru (evidence) zpracování**
- **Identifikace nových zpracování včetně spolupráce při určení právní titulů pro zpracování**
- **Školení nových zaměstnanců**
- **Běžná poradenská činnost** zaměstnancům a vedení organizace
- **Zajištění právního souladu (monitoring právních předpisů)**
- **Spolupráce s klienty** a zajištění kontaktu s **dozorovým úřadem**
- **Posuzování souhlasů, informací a zpracovatelských smluv**
- **Kontrolní činnost**

Pověřenec pro ochranu OÚ

Jmenování interního nebo externího pověřence?

Čl.37, odst.6 Nařízení dává správcům a zpracovatelům možnost místo svého zaměstnance pověřit výkonem funkce pověřence externí osobu (smlouva o poskytování služeb, o pracovní činnosti..)

Jmenování interního pověřence

- **především velcí správci a zpracovatelé** s velkým množstvím interních procesů a informačních systémů
- **výhody** – znalost prostředí, snadnější komunikace
- **nevýhody** – prevence střetu zájmů, zvl. ochrana proti ukončení pracovního poměru, limitace pro případnou náhradu škody způsobené zaměstnancem

Pověřenec pro ochranu OÚ

Jmenování interního nebo externího pověřence?

Jmenování externího pověřence

- spíše **střední a malé podniky** (nižší finanční náročnost)
- **výhody** – předcházení střetu zájmů, jednodušší změna pověřence, tým lidí okolo pověřence s různou odborností (IT, právník....)
- **nevýhody** – nemusí disponovat dostatečně detailními informacemi o organizaci správce nebo pověřence

Správce a zpracovatel má povinnost zveřejnit kontaktní údaje pověřence. Údaje by měly zahrnovat poštovní adresu, tel. číslo, e-mailovou adresu příp. zřídit kontaktní webový formulář

Pověřenec pro ochranu OÚ

Postavení pověřence

Čl.38, odst.1 Nařízení

„Správce a zpracovatel zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů“

- **včasné zapojení** především z důvodu zásady záměrné ochrany OÚ
- je nanejvýš vhodné, aby pověřenec byl přítomen všem procesům zpracování OÚ již od co nejrannějšího stádia
- pověřenec by měl **již od počátku** správci či zpracovateli dávat **stanoviska k zamýšlenému rizikovému zpracování OÚ** či k dostatečnosti zamýšlených technických a organizačních opatření

Pověřenec pro ochranu OÚ

Správce či zpracovatel by měli zejména zajistit:

- *oprávnění k přístupu ke všem systémům organizace, které se týkají shromažďování, zpracování a uchování osobních údajů za účelem posouzení užívání a zabezpečení osobních údajů*
- *konzultaci pověřence v případě porušení zabezpečení*
- *stanovisko v případě provádění posouzení vlivu na ochranu OÚ*
- *dostatečné finanční a hmotné zdroje (prostory a vybavení)*
- *snadnou dosažitelnost zaměstnanců, kteří zpracovávají OÚ pro pověřence*
- *zveřejnění kontaktních údajů na pověřence uvnitř organizace*
- *podporu jiných oddělení (právní, IT, personální...) v rámci organizace*
- *podporu pověřenci v oblasti dalšího vzdělávání*

Pověřenec pro ochranu OÚ

Součinnost správce a zpracovatele s pověřencem

- DPO musí mít **aktivní podporu vedení organizace**
- DPO by se měl **účastnit všech jednání vyššího a středního managementu s dopadem na zpracování osobních údajů** (minimálně těch s vysokým rizikem)
- **Bezpečnostní orgány, orgány ICT a další relevantní zaměstnanci musí průběžně poskytovat pověřenci všechny relevantní informace o postupech týkajících se zpracování OÚ a o přijatých opatřeních k ochraně OÚ**

Pověřenec pro ochranu OÚ

Ochrana postavení pověřence

Pověřenec nesmí být v rámci výkonu své funkce nijak úkolován ani instruován ze strany správce či zpracovatele (např. jak řešit stížnosti apod.). Soulad s Nařízením není odpovědností pověřence a nadále zůstává povinností a odpovědností správce nebo zpracovatele

- pokud je **pověřenec zaměstnancem** správce či zpracovatele, přiznává mu Nařízení **zvýšenou ochranu před jeho zaměstnavatelem** v souvislosti s plněním úkolů DPO
- to ovšem neznamená, že se na takového pověřence nebude vztahovat obecná úprava pracovního práva

Pověřenec pro ochranu OÚ

Ochrana postavení pověřence

Článek 38, odst. 3 stanoví, že pověřenec *„není správcem nebo zpracovatelem propuštěn ani sankcionován v souvislosti s plněním svých úkolů“*

- **tresty nebo jiné postihy**, které jsou uloženy **jako následek výkonu povinností pověřence** jsou podle Nařízení **zakázány**
- pověřenec může být legitimně **propuštěn z důvodů jiných, než v souvislosti s výkonem jeho povinností** (trestní nebo neetické jednání)

Pověřenec pro ochranu OÚ

Zabránění střetu zájmů

Pověřenec se nikdy nesmí dostat do pozice, kdy by určoval nebo schvaloval účely nebo prostředky zpracování. Kontroloval by vlastní činnost a tím se dostával do střetu zájmů

Pro vyloučení střetu zájmů je doporučeno:

- **určit pozice neslučitelné s výkonem funkce pověřence** (člen statutárního orgánu, personalista, interní právník, správce IT...)
- interním předpisem **identifikovat, co je střetem zájmů** a proč je zakázán a přijmout pravidla k jeho zamezení
- přijmout dostatečné **kontrolní mechanismy pro detekci hrozícího střetu zájmů** (neslučitelnost některých pozic s výkonem funkce)

!! Pozor na zastupování v soudních řízeních týkajících se OÚ !!

Pověřenec pro ochranu OÚ

Povinnost mlčenlivosti pověřence

Čl.38, odst.5 Nařízení

„Pověřenec pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností, v souladu s právem Unie nebo členského státu“

- je třeba vycházet z obecně zavedeného chápání tohoto pojmu (v návrhu adaptačního zákona řeší § 42)
- povinnost mlčenlivosti bude zahrnovat zákaz jednání, kterým by se neoprávněná osoba mohla seznámit s informacemi, ke kterým má pověřenec přístup v rámci výkonu své funkce
- pozor na trestněprávní odpovědnost pověřence (§180 tr. zákoníku)

Posouzení vlivu na ochranu OÚ

Čl. 35 a 36 Nařízení

Pro správce usazené na území ČR přináší Nařízení nově povinnost provádět v určitých případech tzv. posouzení vlivu na ochranu OÚ. Pokud správce v rámci posouzení dojde k závěru, že u zamýšleného zpracování OÚ nelze vhodnými opatřeními riziko zmírnit, předá dokumentaci k zamýšlenému zpracování dozorovému úřadu, aby vše posoudil v rámci předchozí konzultace

Posouzení vlivu na ochranu OÚ je nutné zejména v případech:

- a) **automatizovaného zpracování OÚ vč. profilování s právními účinky** nebo jiným rozsáhlým dopadem na FO
- b) **rozsáhlého zpracování zvl. kategorií OÚ** nebo OÚ týkajících se rozsudků v trestních věcech (čl.9, odst.1 a čl.10 Nařízení)
- c) **rozsáhlého systematického monitorování veřejných prostorů**

Posouzení vlivu na ochranu OÚ

Operace zpracování OÚ obsahující faktory s vysokým rizikem

- **profilování a jiný scoring SÚ vč. automatizovaného rozhodování** s právními nebo obdobně významnými účinky
- **systematické monitorování SÚ**
- **zpracování citlivých údajů** (vč. např. údajů o platebních kartách..)
- **zpracování OÚ ve velkém rozsahu** (nemocnice, banky, MHD...)
- **kombinování OÚ z různých datasetů** (datových sad)
- **zpracování OÚ týkajících se zvláště zranitelných osob** (děti, senioři, osoby se zdravotním hendikepem...)
- **zavádění nových technologií** nebo organizačních řešení

Posouzení vlivu na ochranu OÚ

V Nařízení není pojem „posouzení vlivu na ochranu osobních údajů“ přímo definován, ale čl. 35, odst. 7 stanovuje, jaké náležitosti musí přinejmenším splňovat:

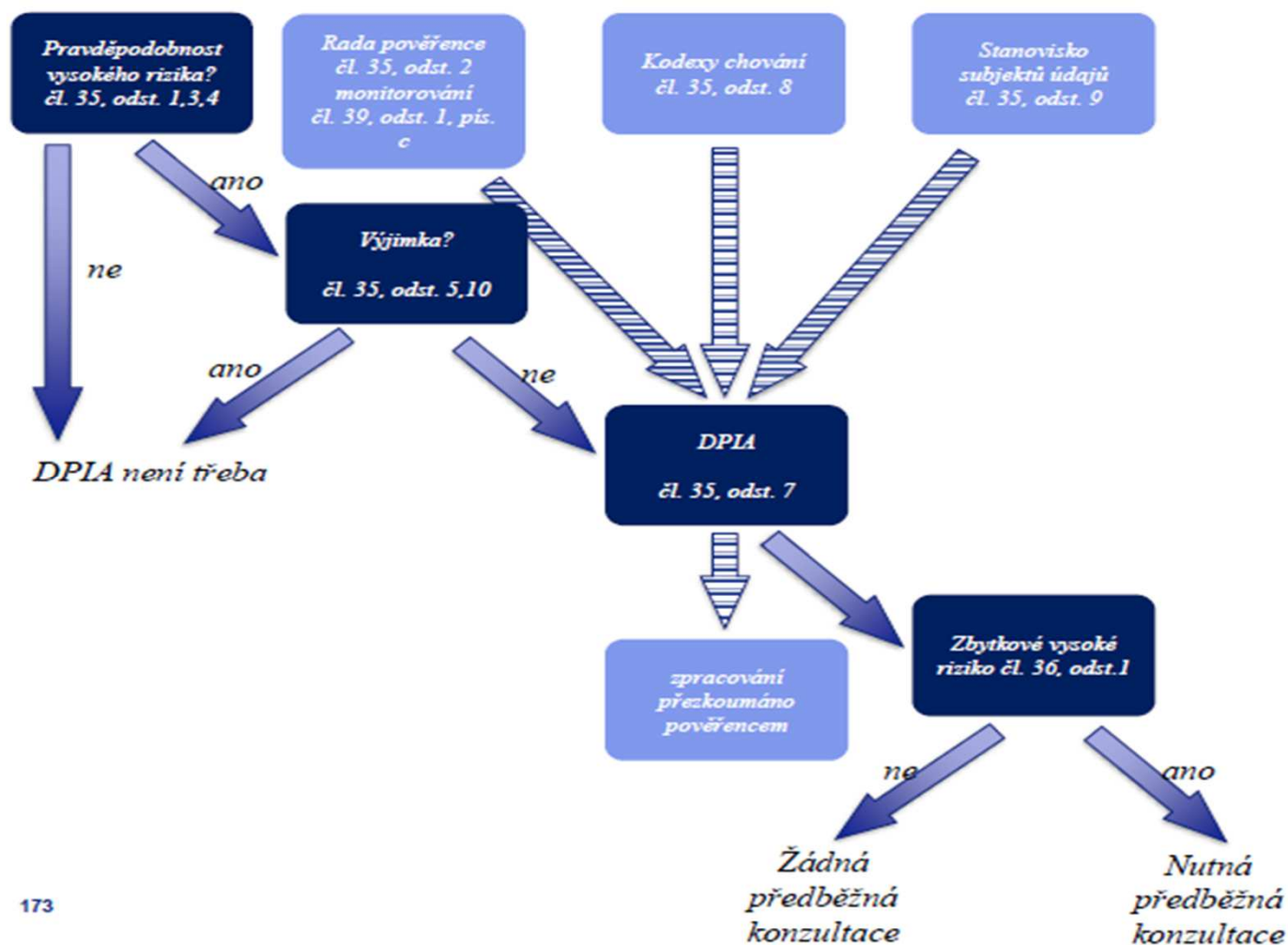
- a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce*
- b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů*
- c) posouzení rizik pro práva a svobody subjektů údajů*
- d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany OÚ a k doložení souladu s Nařízením, s přihlédnutím k právům a oprávněným zájmům SÚ a dalších dotčených osob*

Posouzení rizik

Posouzení rizik pro práva a svobody osob:	
/Uvést, zda je u tohoto zpracování přítomen některý z níže uvedených rizikových faktorů/	
<ul style="list-style-type: none"> Automatizované, systematické vyhodnocování osobních aspektů týkající se fyzických osob včetně profilování s následným rozhodováním s právním nebo obdobně významným účinkem 	
<ul style="list-style-type: none"> Rozsáhlé systematické monitorování veřejně přístupných prostorů 	
<ul style="list-style-type: none"> Zpracování OÚ zvláštní kategorie 	
<ul style="list-style-type: none"> Zpracování je rozsáhlé 	
<ul style="list-style-type: none"> Soubory dat, které byly porovnány nebo zkombinovány 	
<ul style="list-style-type: none"> Zahrnutí údajů týkající se zranitelných subjektů údajů 	
<ul style="list-style-type: none"> Inovativní používání nebo uplatňování technologických nebo organizačních řešení (např. biometrika) 	
<ul style="list-style-type: none"> Přesun dat přes hranice mimo Evropskou unii 	
<ul style="list-style-type: none"> Pokud samotné zpracování zabraňuje subjektům údajů vykonávat právo nebo využívat službu nebo smlouvu 	
Jedná se o zpracování s vysokým rizikem pro práva a svobody osob:	Ano/Ne

Posouzení vlivu na ochranu OÚ

Schéma posouzení vlivu na ochranu OÚ (DPIA)



Kodexy a osvědčení

Kodexy chování - čl.40 – 41 Nařízení

Pro potřeby mikropodniků, malých a středních podniků je možné, aby jejich zájmová a profesí sdružení v rámci odvětví vydávala kodexy chování, jejichž cílem bude s ohledem na specifika daného odvětví upřesnění dodržování povinnosti dle Nařízení s prvky samoregulace

Monitorování dodržování kodexu chování

- akreditovaným subjektem bude Český institut pro akreditaci o.p.s.
- ČIA bude oprávněn kontrolovat dodržování kodexů a bude mít pravomoc pozastavit účast správce nebo zpracovatele na dodržování kodexu příp. jej zcela vyloučit, pokud kodex nedodržuje

Kodexy a osvědčení

Vydávání osvědčení - čl.42 – 43 Nařízení

Získání osvědčení ve formě známky nebo pečetě je dalším prvkem, který má správci a zpracovatelům pomoci při prokazování souladu s Nařízením a ověřování jejich věrohodnosti ze strany SÚ

Vydávání osvědčení

- subjektem pro vydávání osvědčení může být dozorový úřad nebo „vnitrostátní akreditační orgán“, v tomto případě ČIA
- osvědčení bude vydáváno na dobu 3 let s možností prodloužení na další období v případě plnění podmínek vydání osvědčení
- může přinést výhody správci (předávání OÚ) i zpracovatelům (zjednodušení procesu jejich výběru správcem)

Obecné nařízení č.2016/679
o ochraně osobních údajů
(GDPR)
Pověřenec pro ochranu OÚ

Dozorové úřady
Právní ochrana

Dozorové úřady

Problematiku dozorových úřadů řeší čl.51 – 59 Nařízení

Dozorovým úřadem v ČR je Úřad na ochranu osobních údajů (ÚOOÚ), a to pro veškeré zpracování OÚ s výjimkou zpracování zpravodajskými službami. V evropském kontextu má ÚOOÚ poměrně silné postavení s tomu odpovídajícími kompetencemi

- všechny členské státy, na které dopadá Nařízení, jsou povinny do 25.5.2018 informovat Evropskou komisi o vnitrostátní úpravě výkonu dozoru nad uplatňováním Nařízení
- správce, zpracovatel a **nově i SÚ** mají právo na soudní ochranu před DÚ (správní soudnictví)

Právní ochrana

Právo podat stížnost u dozorového úřadu (čl.77 Nařízení)

Nařízení navazuje na dosavadní úpravu podle §29 ZOOÚ ohledně podávání podnětů a stížností na porušení povinností stanovených ZOOÚ a zpřesňuje, že podáním takové stížnosti je právem SÚ

Stížnost může být vyřízena:

- **napomenutím** správce či zpracovatele,
- **dočasným či trvalým omezením** zpracování OÚ nebo
- **pokutou**

Dozorový úřad je **povinen informovat do 3 měsíců SÚ**
o průběhu vyřizování jeho stížnosti

Právní ochrana

Právo na soudní ochranu proti DÚ (čl.78 Nařízení)

Každý má právo napadnout závazné rozhodnutí dozorového úřadu, které se jej týká. Řízení se zahajuje u soudu, v jehož obvodu se nachází dozorový úřad. Žalobou je možno se bránit proti právně závaznému rozhodnutí dozorového úřadu

- postup při uplatnění soudní ochrany proti rozhodnutí dozorového úřadu se řídí příslušnými předpisy správního práva
- správce, zpracovatel a nově také SÚ musí nejprve vyčerpat všechny řádné opravné prostředky v řízení před správním orgánem
- v řízení před ÚOOÚ je takovým opravným prostředkem rozklad

Újma a sankce

Sankce podle GDPR

Správní

Peněžitá pokuta až do 20 mil. EUR
nebo do 4 % ročního obratu

- Národní legislativa může stanovit další správní sankce
- Národní legislativa může zmocnit neziskovou organizaci k podávání stížností i bez zmocnění dotčeným subjektem údajů

Civilní

Náhrada škody

+

Náhrada
nemajetkové
újmy

- Možnost žalovat u soudů v zemi bydliště subjektu údajů
- Možnost subjektu údajů nechat se zastoupit neziskovou organizací zaměřenou na ochranu osobních údajů
- Společná a nerozdílná odpovědnost správce a zpracovatele

Újma a sankce

Právo na náhradu újmy (čl.82 Nařízení)

V logické návaznosti na právo na účinnou soudní ochranu SÚ vůči správci či zpracovateli přiznává Nařízení SÚ právo na náhradu hmotné či nehmotné újmy, způsobené zpracováním, porušujícím Nařízení

- Nařízení zpřesňuje stávající úpravu dle §21 ve spojení s §8 ZOOÚ
- **odpovědnost správce je širší než odpovědnost zpracovatele** - ten odpovídá za újmu pouze ve dvou případech:
 - a) při **porušení povinností, které mu přímo ukládá Nařízení**
 - b) kdy **jedná nad rámec zákonných pokynů správce** nebo v **rozporu s nimi** (např. zapojí dalšího zpracovatele)

Újma a sankce

Sankce (čl.84 Nařízení)

Jiné sankce se uplatňují tam, kde nelze přistoupit k uložení správní pokuty. Sankce se budou týkat např. případů, kdy se zaměstnanec správce nebo zpracovatele dopustí přestupku povinnosti mlčenlivosti. Stejného přestupku se mohou dopustit např. znalci, svědci v řízeních nebo členové stutárních orgánů

- **porušení ochrany OÚ může mít i trestněprávní následky** možným spácháním trestného činu neoprávněného nakládání s osobními údaji podle **§180 trestního zákoníku** s trestní sazbou až 8 let nepodmíněně
- přichází v úvahu také **trestní odpovědnost právnických osob**

Platnost a účinnost Nařízení

Mějte prosím v patrnosti, že:

Nařízení vstoupilo v platnost 20 dní po jeho vyhlášení v Úředním věstníku EU, tedy 24. května 2016.

Nařízení nabývá použitelnosti – účinnosti dne 25. května 2018.

Nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech EU

© Mgr. Hynek Veselý, 2018