GDPR v hotelnictví a cestovním ruchu

JUDr. Iva Kuckirová

Holiday Inn Brno, 16. 5. 2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

OCHRANA OSOBNÍCH ÚDAJŮ VE SVĚTLE GDPR

advokátní kancelář Křížka Kuckirová Legal
www.kklegal.cz

videa a další materiály včetně vzorů najdete na
www.skoleni.brnenskypravnik.cz

GDPR: NAŘÍZENÍ GDPR A ZÁKLADNÍ ZÁSADY

Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

čl. 1 – 3, 5, 94 – 99 GDPR

LEKCE Č. 1

Přehled vývoje české a evropské legislativy

ČESKÁ LEGISLATIVA:

- **1981** – Úmluva Rady Evropy č. 108
- **1992** – zákon č. 256/1992 Sb., o ochraně osobních údajů v inf. systémech
- **2000** – zákon č. 101/2000 Sb., o ochraně osobních údajů

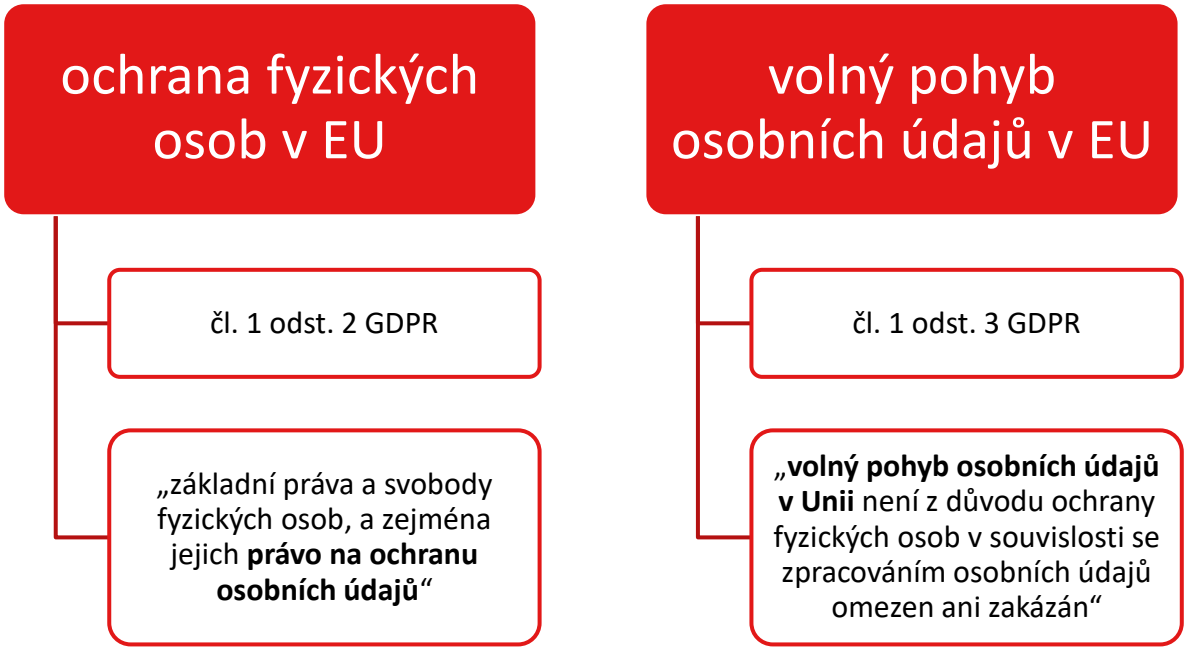
EVROPSKÁ LEGISLATIVA:

- **1981** – Úmluva Rady Evropy č. 108
- **1995** – směrnice Evropského parlamentu a rady č. 95/46/ES
- 1997 (**1999**) – Amsterodamská smlouva
- 2016 (**2018**) – nařízení Evropského parlamentu a Rady (EU) č. 2016/679 (GDPR)

Reforma evropského práva

- v současnosti je schváleno nařízení **General Data Protection Regulation** (GDPR) = nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- obecné nařízení o ochraně osobních údajů (GDPR) je součástí **balíčku opatření EU pro reformu ochrany údajů** společně se směrnicí o ochraně osobních údajů orgány činnými v trestním řízení.
- obecné nařízení o ochraně osobních údajů se použije od **25. května 2018**
- již nejde o směrnici jako v minulosti (směrnice Evropského parlamentu a rady č. 95/46/ES), ale tentokrát jde o **přímo aplikovatelné nařízení**
- EU deklaruje, že nařízení „umožňuje občanům Evropské unie **lépe kontrolovat své osobní údaje**; také modernizuje a sjednocuje předpisy **umožňující podnikům snížit administrativní zátěž** a mít **prospěch z větší důvěry spotřebitelů**“
- nepochybně bude muset být novelizována i česká právní úprava

Právem chráněné hodnoty



Důvody přijetí

bod 9 recitálu

Ačkoliv cíle a zásady směrnice 95/46/ES nadále platí, nezabránilo to roztříštěnosti v provádění ochrany údajů v celé Unii, právní nejistotě ani rozšířenému pocitu veřejnosti, že v souvislosti s ochranou fyzických osob existují značná rizika, zejména pokud jde o činnosti prováděné online. ***Rozdíly v úrovni ochrany práv a svobod fyzických osob, zejména práva na ochranu osobních údajů, v souvislosti se zpracováním osobních údajů v členských státech mohou bránit volnému pohybu osobních údajů v rámci Unie.*** *Tyto rozdíly proto mohou být překážkou pro výkon hospodářských činností na úrovni Unie, mohou narušovat hospodářskou soutěž a bránit orgánům veřejné moci ve výkonu povinností, které jim ukládají právní předpisy Unie. Tato rozdílná úroveň ochrany je způsobena rozdíly v provádění a uplatňování směrnice 95/46/ES.*

Důvody přijetí

bod 10 recitálu

*S cílem **zajistit soudržnou a vysokou úroveň ochrany fyzických osob a odstranit překážky bránící pohybu osobních údajů v rámci Unie** by měla být úroveň ochrany práv a svobod fyzických osob v souvislosti se zpracováním těchto údajů **rovnocenná ve všech členských státech.** V celé Unii je třeba zajistit soudržné a jednotné uplatňování pravidel ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů.*

[…]

***Toto nařízení rovněž poskytuje členským státům určitý prostor ke stanovení vlastních pravidel, včetně pravidel pro zpracování zvláštních kategorií osobních údajů („citlivé osobní údaje“)**. V tomto rozsahu nařízení nevylučuje, aby právo členského státu stanovilo okolnosti konkrétních situací, při nichž dochází ke zpracování, včetně přesnějšího určení podmínek, za nichž je zpracování osobních údajů zákonné.*

Důvody přijetí

bod 13 recitálu

[…] *Řádné fungování vnitřního trhu vyžaduje, aby* ***volný pohyb osobních údajů v Unii nebyl z důvodů souvisejících s ochranou fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán****. Aby byla zohledněna specifická situace mikropodniků a malých a středních podniků, obsahuje toto nařízení* ***odchylku pro organizace s méně než 250 zaměstnanci týkající se uchovávání údajů****. Kromě toho jsou orgány a instituce Unie, členské státy a jejich dozorové úřady podporovány v tom, aby specifické potřeby mikropodniků a malých a středních podniků zohledňovaly při uplatňování tohoto nařízení. Pojem mikropodniky a malé a střední podniky by měl vycházet z článku 2 přílohy doporučení Komise 2003/361/ES 5.*

Práva občanů

Obecné nařízení o ochraně osobních údajů posiluje stávající práva a přiznává nová práva:

- **snadnější přístup k údajům** – včetně poskytnutí více informací o tom, jak jsou údaje zpracovány, a zajištění toho, aby informace byly dostupné jasným a srozumitelným způsobem,
- **nové právo na přenositelnost údajů** – usnadňující přenos osobních údajů mezi poskytovateli služeb,
- **právo být zapomenut** – když si osoba nepřeje, aby její údaje byly dále zpracovávány, a není podložený důvod k jejich uchovávání, budou údaje smazány,
- **právo dozvědět se, že jejich osobní údaje byly napadeny** – společnosti a organizace budou mít povinnost bezodkladně informovat osoby o závažném porušení zabezpečení osobních údajů; všechny takové případy budou muset být ohlášeny příslušnému dozorovému orgánu.

Pravidla pro podniky

- **jednotný soubor předpisů platných v celé EU** – dle EU jednotné právní předpisy odhadem ročně ušetří 2,3 miliardy EUR
- veřejné orgány a podniky, které zpracovávají osobní údaje ve velkém měřítku, jmenují **pověřence pro ochranu osobních údajů**, který bude zodpovídat za ochranu osobních údajů
- **jediné kontaktní místo** – podniky jednají s jediným dozorovým úřadem (v zemi EU, kde mají hlavní sídlo)
- **předpisy EU pro společnosti mimo EU** – společnosti, které nejsou usazené v EU, musí dodržovat stejné předpisy, když nabízejí své služby nebo zboží v EU nebo když monitorují chování osob v EU
- **předpisy podporující inovace** – jistota, že záruky na ochranu osobních údajů jsou nedílnou součástí produktů a služeb od první fáze jejich vývoje (záměrná a standardní ochrana osobních údajů)

Pravidla pro podniky

- technologie podporující ochranu soukromí – **pseudonymizace** (když jsou identifikační pole v záznamech osobních údajů nahrazena jedním nebo více identifikačními kódy) a **šifrování** (kdy jsou údaje kódovány takovým způsobem, že je mohou přečíst jenom oprávněné strany)
- **odstranění oznamovací povinnosti** – nové předpisy na ochranu osobních údajů odstraní většinu oznamovacích povinností a nákladů s nimi spojených; jedním z cílů nařízení o ochraně údajů je odstranit překážky volnému pohybu osobních údajů v EU
- **posouzení vlivu** – podniky budou muset provádět posouzení vlivu, pokud zpracování údajů povede k vysokému riziku pro práva a svobody osob
- **uchovávání údajů** – malé a střední podniky nemusí uchovávat záznamy o zpracování údajů, pokud není pravidelné nebo nepředstavuje zvýšené riziko pro práva a svobody osob, jejichž údaje jsou zpracovávány

Význam formy nařízení z hlediska aplikace

- nově jde o **nařízení** dle čl. 288 Smlouvy o fungování EU, nikoli směrnici
- právní akt ve formě nařízení má **aplikační přednost před českou právní úpravou** (rozsudky SDEU ve věcech Van Gend en Loos, Costa vs. ENEL, Simmenthal, nález ÚS sp. zn. Pl. ÚS 50/2004)
- vlastní národní právní úpravou **není možné zpřísnit podmínky stanovené nařízením**, pokud to GDPR výslovně neumožňuje (např. čl. 23 GDPR, čl. 85 až 91 GDPR):
  - **možnost omezit základní zásady, pokud je omezení nezbytné v demokratické společnosti z veřejného zájmu** (čl. 23 GDPR)
  - zvláštní situace (svoboda projevu a právo na informace, zaměstnávání, …)

DŮLEŽITÉ

Věcná působnost

VĚCNÁ PŮSOBNOST:

- **zcela nebo částečně automatizované zpracování osobních údajů** – dikce je záměrně technologicky neutrální, vztahuje se na všechny způsoby zpracování, kde část neprovádí fyzicky člověk
- **manuální zpracování osobních údajů za podmínky zpracování v evidenci (kartotéce)** – ochrana v momentě, kdy jsou systematicky uspořádány podle kritérií

- tato úprava se neliší od směrnice
- manuální zpracování kopií dokumentů obsahujících osobní údaje, které nejsou rozřazeny či evidovány podle klíče nepodléhá nařízení, ale vztáhne se na ně ochrana dle občanského zákoníku, ochrana obchodního tajemství, bankovního tajemství či povinnost mlčenlivosti
- odlišná definice od současného § 3 odst. 4 zákona o ochraně osobních údajů

DŮLEŽITÉ

Evidence

- **jakýkoli strukturovaný soubor osobních údajů** (čl. 4 odst. 6 GDPR)
- může jít o soubor centralizovaný, decentralizovaný, rozdělený podle funkčního či zeměpisného hlediska
- definice se oproti směrnici nemění, český zákon ji nezná
- jedná se o spisové kartotéky, např. lékařské kartotéky v listinné podobě

Výjimky z věcné působnosti

VÝJIMKY Z VĚCNÉ PŮSOBNOSTI

- **výkon činností, které nespadají do oblasti působnosti práva EU** – zpracování údajů v souvislosti se zajišťováním národní bezpečnosti
- **výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 SEU** (společná zahraniční a bezpečnostní politika EU) – činnost Eurojust a Europol
- **výlučně osobní či domácí činnosti** – bez jakékoli souvislosti s profesní nebo obchodní činností, např. vedení osobního adresáře, využívání kontaktů Google, sociální sítě, restriktivní výklad (C-101/01, Lidquist; zveřejnění byť i jediného údaje na osobním webu či profilu sociální sítě již je zpracováním), kamerování (s pořízením záznamu) veřejného prostoru pro osobní potřebu také není možné
- **prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení** – právní úprava je ve zvláštní směrnici č. 2016/680

DŮLEŽITÉ

Odpovědnost poskytovatelů služeb informační společnosti

- GDPR se nijak nedotýká uplatňování směrnice č. 2000/31/ES, zejména pokud jde o pravidla týkající se odpovědnosti poskytovatelů zprostředkovatelských služeb uvedená v článcích 12 až 15 uvedené směrnice
- česká právní úprava – **zákon č. 480/2004 Sb., o některých službách informační společnosti** a o změně některých zákonů (zákon o některých službách informační společnosti)
- např. **služba Youtube** dodržuje stanovená pravidla, tudíž ve vztahu k ní je vyloučena jakákoli odpovědnost (trestněprávní, civilní, správněprávní) za obsah videí vložených jednotlivými uživateli

Vztah k ostatním evropským předpisům

- **směrnice 95/46/ES** – směrnice 95/46/ES se zrušuje a veškeré odkazy na ni se budou považovat za odkazy na GDPR; veškeré odkazy na pracovní skupinu WP29 se budou považovat za odkazy na **Sbor** – to má význam např. ve vztahu k nařízení eIDAS a směrnici PSD2
- **směrnice 2002/58/ES (směrnice e-Privacy)** – GDPR zachovává v platnosti e-Privacy a neukládá v souvislosti s e-Privacy žádné nové povinnosti (pokud se subjekt aplikuje e-Privacy i GDPR, pak se úprava GDPR použije jen v rozsahu, kde směrnice e-Privacy mlčí)
- **budoucí e-Privacy nařízení (nařízení PECR)** – očekává se kolem roku 2020, nicméně v plánu je, že nařízení e-Privacy bude lex specialis ke GDPR
- **dříve uzavřené mezinárodní dohody členských států** – zůstávají v platnosti; v praxi se bude jednat zejména o Úmluvu Rady Evropy č. 108

Místní působnost

VYMEZENÍ MÍSTNÍ PŘÍSLUŠNOSTI:

- **zpracování související s provozovnou v EU** – není rozhodné, kde ke zpracování dojde, postačí souvislost s provozovnou
- **extrateritoriální působnost GDPR** – zpracování souvisí s (a) nabídkou služeb a zboží subjektům v EU, nebo (b) monitorováním jejich chování, pokud k němu dochází v EU
- **působnost na základě mezinárodního práva veřejného**

- značné změny oproti směrnici a zákonu o ochraně osobních údajů
- hovoří se o EU, ale půjde o **celé EHP** (EU + Island, Norsko, Lichtenštejnsko) – GDPR bude totiž inkorporováno do Dohody o Evropském hospodářském prostoru
- monitorováním se rozumí rovněž **monitorování prostřednictvím tzv. sledovacích cookies** (ty lze také považovat za osobní údaj) – bližší informace ve směrnici e-Privacy

Časová působnost

- GDPR vstupuje v platnost dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie, tj. 24. května 2016
- GDPR vstupuje v účinnosti **25. května 2018**

VYHODNOCOVÁNÍ PRÁVNÍ ÚPRAVY V BUDOUCNU:

- do 25. května 2020 a poté každé další čtyři roky předloží Komise Evropskému parlamentu a Radě **zprávu o hodnocení GPDR**
- v případě potřeby předloží Komise **návrhy na změny GDPR** s přihlédnutím k vývoji informačních technologií

Seznam základních zásad

GDPR stojí na těchto základních zásadách:

- **zásada zákonnosti, korektnosti a transparentnosti** – čl. 5 odst. 1 písm. a) GDPR
- **zásada účelového omezení** – čl. 5 odst. 1 písm. b) GDPR
- **zásada minimalizace údajů** – čl. 5 odst. 1 písm. c) GDPR
- **zásada přesnosti** – čl. 5 odst. 1 písm. d) GDPR
- **zásada omezení uložení** – čl. 5 odst. 1 písm. e) GDPR
- **zásada integrity a důvěrnosti** – čl. 5 odst. 1 písm. f) GDPR
- **zásada odpovědnosti** – čl. 5 odst. 2 GDPR

Základní zásady

- **zásada zákonnosti, korektnosti a transparentnosti** [čl. 5 odst. 1 písm. a) GDPR] – zpracování jen na základě právního titulu dle čl. 6 takovým způsobem, který by subjekty mohly legitimně očekávat; „být férový“
- **zásada účelového omezení** [čl. 5 odst. 1 písm. b) GDPR] – stěžejní zásada, účel je alfou a omegou zpracování; účel musí být určitý, výslovně vyjádřený a legitimní; pokud dojde ke změně účelu hovoříme o **dalším zpracování**, v takovém případě je nutné provést **posouzení slučitelnosti**
- **zásada minimalizace údajů** [čl. 5 odst. 1 písm. c) GDPR] – zpracovávat je nutné pouze ty údaje, které jsou ve vztahu k účelu relevantní; „nepotřebuji-li údaje, neshromažďuji je“

DŮLEŽITÉ

Základní zásady

- **zásada přesnosti** [čl. 5 odst. 1 písm. d) GDPR] – údaje musí přesné, musí odpovídat skutečnosti a být aktuální; přesnost neznamená nutně pravdivost, správce není odpovědný za to, že mu subjekt sdělil nepravdivé údaje
- **zásada omezení uložení** [čl. 5 odst. 1 písm. e) GDPR] – uchovávání údajů pouze po dobu, jež je nezbytná pro účel zpracování
- **zásada integrity a důvěrnosti** [čl. 5 odst. 1 písm. f) GDPR] – údaje musejí být zpracovány takovým způsobem, který zajistí jejich náležité zabezpečení; nově je bezpečnost klíčovou zásadou
- **zásada odpovědnosti** (čl. 5 odst. 2 GDPR) – správce musí být schopen soulad s GDPR vždy sám doložit, tzn. vést patřičné dokumentace, a odpovídá za porušení GDPR

DŮLEŽITÉ

GDPR:
OSOBNÍ ÚDAJ

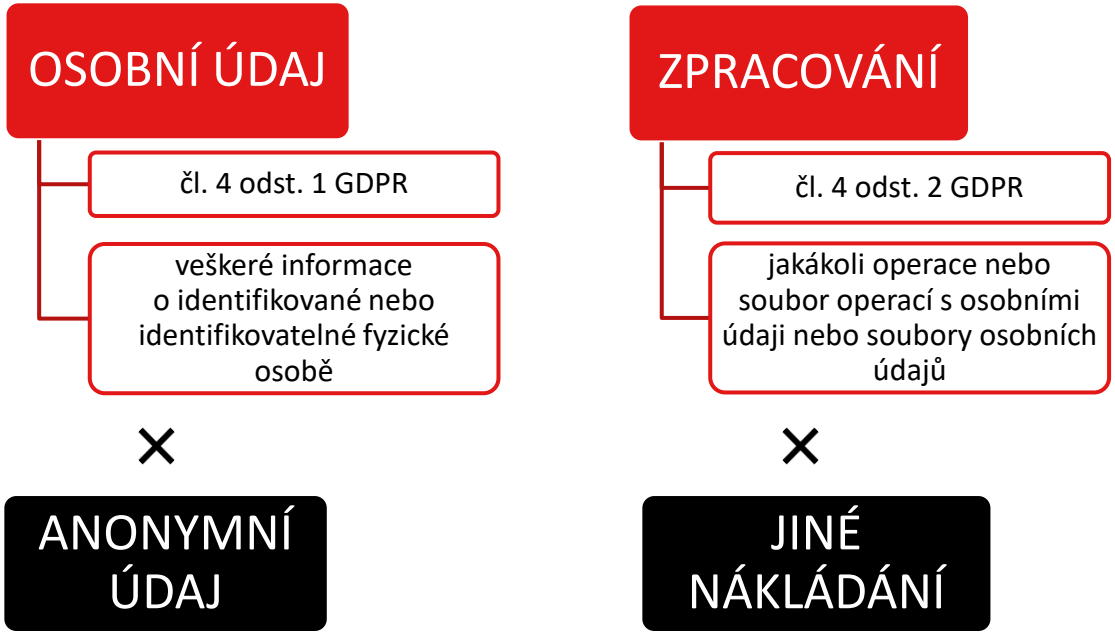
Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

čl. 4 GDPR

LEKCE Č. 2

Klíčové pojmy



Osobní údaj

- **definice osobního údaje v GDPR** byla přejata z mezinárodních dokumentů, konkrétně Úmluvy č. 108, směrnice č. 95/46/ES; **GDPR ji mírně rozšiřuje** (síťový identifikátor, genetické údaje)
- definice z Úmluvy č. 108 a směrnice byla přejata i českým zákonodárcem, který ji mírně doplnil
- zcela **klíčový pojem** v právu ochrany osobních údajů
- **VEŘEJNOPRÁVNÍ INSTITUT** – pokud informace týkající se fyzické osoby kvality osobního údaje v daném případě nedosahuje, pak není vyloučeno použití jiných odvětví – např. pokud daná osoba použití údaje, který není osobním ve smyslu zákona o ochraně osobních údajů, považuje za zásah do svého soukromí a osobního života, zákon o ochraně osobních údajů aplikovat sice nelze, ale v úvahu stále připadá **žaloba na ochranu osobnosti** nebo trestní postih (např. **trestný čin pomluvy**)
- je vhodné rozlišovat **přímé identifikátory osoby**, např. jméno či rodné číslo, od **ostatních osobních údajů**, které mají povahu osobních údajů právě až ve spojení s přímými identifikátory

KLÍČOVÝ POJEM

Přehled definic pojmu osobní údaj

zdroj definice	doslovené znění definice
čl. 2 písm. a) **Úmluvy č. 108**	každá informace týkající se identifikované nebo identifikovatelné fyzické osoby
čl. 2 písm. a) **směrnice EP a Rady č. 95/46/ES**	veškeré informace o identifikované nebo identifikovatelné osobě (dotčená osoba); identifikovatelnou osobou se rozumí osoba, která může být identifikovaná, přímo či nepřímo, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity
ustanovení § 4 písm. a) **zákona o ochraně osobních údajů**	jakákoliv informace týkající se určeného nebo určitelného subjektu údajů; Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu
čl. 4 odst. 1 **GDPR**	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, například jméno, identifikační číslo, **lokační údaje**, **síťový identifikátor** nebo na jeden či více zvláštních prvků fyzické, fyziologické, **genetické**, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby

Výklad pojmu osobní údaj

- **judikaturní rozšiřující (extenzivní) výklad** – SDEU vykládá tento pojem extenzivně – např. za osobní údaj se považuje i pohyblivá IP adresa, stejně k tomuto pojmu přistupuje i český Nejvyšší správní soud
- **výkladová metoda in dubio pro libertate** – pokud nevíme, zda lze údaj považovat za osobní, přikloníme se výkladu, že jde o osobní údaj
- za osobní údaj je nutno považovat jak objektivní, pravdivé, prokázané nebo ověřené skutečnosti, tak i **subjektivní a nepravdivá sdělení**, pokud jsou zpracovávána v rámci stejné databáze s ostatními údaji, a dále i **různá více či méně formální hodnocení a posudky**

DŮLEŽITÉ

Výklad pojmu osobní údaj

- **pojem je nutno vykládat vždy v konkrétním případě** – někdy je nutné k přímé či nepřímé identifikaci méně údajů, někdy více (záleží také na velikosti zasaženého území)
- **stanovisko WP29 ze dne 20. 6. 20017, WP136** – aby bylo možné konstatovat existenci vazby údaje a osoby (vazbu určitelnosti), je nutné zkoumat prvek obsahu, prvek účelu a prvek výsledku takové informace
- člověk nemusí být identifikovatelný jen podle daných osobních údajů, ale také pokud **je možné ho identifikovat pomocí těchto údajů v kombinaci s údaji, které jsou veřejně dostupné** (bod č. 26 GDPR; předpokládá se rozumnost, berou se v potaz všechny možné faktory, zejména náklady a čas takové identifikace)

Demonstrativní výčet osobních údajů

- **čísla, která nás mohou přímo nebo nepřímo identifikovat** - datum narození, rodné číslo, personální číslo přidělené zaměstnavatelem či číselné označení studenta, telefonní číslo, IP adresa či číslo bankovního účtu, …
- **prvky fyzické a fyziologické identity** - vzhled dané osoby, tvar jejího obličeje, hlavy i celého těla, výška, váha, barva vlasů a očí; informace o chování či reakcích dané osoby v určitých situacích, …
- **prvky ekonomické identity** - informace o majetku, pohledávkách i závazcích, o výši a zdroji příjmů, …
- **prvky kulturní identity** - zájmy, záliby a schopnosti jedince, …
- **prvky sociální identity** - rodinný stav, sociální původ, vzdělání, zaměstnání či jiné aktivity, místo narození, adresa zaměstnavatele, místo výkonu zaměstnání, údaje o příbuzných, osobách, s nimiž subjekt údajů žije ve společné domácnosti, o známých, sousedech a spolupracovnících, přátelích, …

Nově zařazené příklady osobních údajů

GDPR nově výslovně přidává de demonstrativního výčtu tyto údaje (judikatura je již před nařízením ovšem za osobní údaje považovala):

- **prvky genetické identity** – informace o genomu, DNA, dědičných onemocněních; GDPR je řadí do zvláštní kategorie osobních údajů (v českm právu se hovoří o citlivých osobních údajích)
- **lokační údaje** – informace týkající se místa pobytu a pohybu; podmnožinou jsou lokalizační údaje (§ 91 zákona o elektronických komunikacích)
- **síťový identifikátor** – bližší vysvětlení je v bodu 30 GDPR; jedná se o IP adresu, cookies, RFID (Radio Frequency Identification), IMEI (International Mobile Equipment Identity) – ačkoli se vztahují spíše k věci (mobilnímu telefonu, počítači, notebooku, …), lze je považovat za osobní údaje tehdy, pokud je daná věc (s vysokou mírou pravděpodobnosti) ve vlastnictví konkrétního člověka

Příklady některých osobních údajů

Příklady údajů, které se považují za osobní údaj, pokud na základě nich lze osobu identifikovat:

- **posouzení spolehlivosti dlužníka**
- **nákupní preference**
- **dynamická (pohyblivá) IP adresa** – pohyblivá IP adresa (C-213/15, Patrick Breyer proti SRN)
- **pohyb osoby** – GPS sledování
- **informace o spotřebě energií**
- **IMEI** – unikátní číslo mobilního telefonu
- **rodné číslo**

Dynamická IP adresa

- rozsudek SDEU ve věci **Patrick Breyer proti Bundesrepublik Deutchland**
- správce (poskytovatel mediální služby) měl informace o pohyblivé IP adrese subjektu údajů
- **pohyblivá adresa neumožňuje pomocí veřejně přístupných údajů identifikovat bod fyzického připojení počítače k síti**, z pohledu poskytovatele mediální služby by tedy mělo jít o anonymizovaný údaj
- SDEU ovšem konstatoval, že německé právo v některých případech dává mediálním agenturám možnost získat od poskytovatelů připojení k internetu dodatečnou sadu údajů, která ve spojení s dynamickou IP adresou umožní uživatele dostatečně přesně identifikovat
- **dynamická IP adresa byla v konkrétním případě považována za osobní údaj**

Telefonní číslo

„Plná identita fyzické osoby v současných podmínkách technologicky vyspělé společnosti, tj. za vysokého stupně rozvoje elektronických a jiných médií, která jsou většině populace snadno dostupná, ve své podstatě neznamená nic jiného než možnost tuto osobu určitým způsobem kontaktovat, aniž by bylo nutno znát místo jejího aktuálního pobytu. Proto se **výklad pojmu osobní údaj nemůže omezit striktně jen na znalost např. rodného čísla, adresy či pracoviště subjektu údajů**. Z tohoto pohledu **je za osobní údaj třeba považovat i číslo mobilního telefonu určité osoby, jakkoli může být takové číslo používáno příslušnou osobou jen dočasně**, a zároveň nijak nespecifikuje jeho fyzickou, psychickou, ekonomickou, kulturní nebo sociální identitu. **Prostřednictvím tohoto čísla je však možno daný subjekt v určitém časovém úseku přímo kontaktovat (**což se ostatně stalo i v posuzovaném případě), a tento subjekt je tak **dosažitelný** a jistým způsobem **určitelný**, **a to případně i bez znalosti jeho jména a dalších údajů**, které již vazbu na jeho fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu mají.“

(rozsudek Nejvyššího správního soudu ze dne 12. února 2009, sp. zn. 9 As 34/2008)

Rodné číslo

- rodné číslo považujeme za osobní údaj i bez znalosti dalších údajů; GDPR označuje rodné číslo jako **národní identifikační číslo** a nepovažuje jej za zvláštní kategorii osobních údajů; **nejde tedy o citlivý údaj**
- nakládání s rodnými čísly je předmětem samostatné úpravy v zákoně o evidenci obyvatel; definuje je § 13 a násl. **zákona č. 133/200 Sb., o evidenci obyvatel a rodných číslech**
- mohou jej používat pouze **orgány moci veřejné**, popř. **jiné osoby, pokud tak stanoví zvláštní zákon** (např. občanský soudní řád při podání žaloby); ostatní osoby pak jen se **souhlasem** (nejde ovšem o souhlas dle GDPR, ale o souhlas dle zákona o evidenci obyvatel; musí tedy být splněny náležitosti obou předpisů)

Úřední doklady

- doklad či jeho kopie samy o sobě nejsou osobními údaji, ale na každém dokladu je **soubor osobních údajů**, např. fotografie, jméno a příjmení, číslo dokladu ad.
- úřední doklady (občanské a řidičské průkazy, cestovní pasy …) jsou předmětem úpravy zvláštních zákonů
- **občanské průkazy** – je zakázáno pořizovat jakýmikoliv prostředky kopie občanského průkazu bez prokazatelného souhlasu občana, kterému byl občanský průkaz vydán, pokud zvláštní zákon nebo mezinárodní smlouva, kterou je Česká republika vázána, nestanoví jinak (§ 15a odst. 2 zákona č. 328/1999 Sb., o občanských průkazech)
- **cestovní pasy** – je zakázáno pořizovat jakýmikoliv prostředky kopie cestovního dokladu bez souhlasu občana, kterému byl cestovní doklad vydán, pokud zvláštní zákon nebo mezinárodní smlouva nestanoví jinak (§ 2 odst. 3 zákona č. 329/1999 Sb., o cestovních dokladech)
- v žádném z případů nejde ovšem o souhlas dle GDPR, ale o souhlas dle daného zvláštního zákona; musí tedy být splněny náležitosti obou předpisů
- **řidičské průkazy** – právní úprava v § 103 a násl. zákona č. 361/2000 Sb., o provozu na pozemních komunikacích, ani vyhláška č. 31/2001 Sb., o řidičských průkazech a o registru řidičů, nestanoví žádné zvláštní podmínky pro pořizování kopií (stanoví se pouze, že je veřejnou listinou a nesmí být ponecháván a přijímán jako zástava a odebírán při vstupu do objektů nebo na pozemky)

„Citlivé“ osobní údaje

ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ (čl. 9 GDPR)

- historicky se označují jako **citlivé údaje**
- osobní údaje, které vypovídají o **rasovém či etnickém původu**, **politických názorech**, **náboženském vyznání**, **filozofickém přesvědčení**, **členství v odborech**, **sexuálním životě** nebo **sexuální orientaci** fyzické osoby
- **genetické údaje**, **biometrické údaje** a **údaje o zdravotním stavu** – viz dále
- zpracování je obecně zakázáno, pokud není dána výjimka dle čl. 9 odst. 2 GDPR; vyžadují se vyšší bezpečnostní standardy, pověřenec pro ochranu osobní údaje, …

OSOBNÍ ÚDAJE TÝKAJÍCÍ SE ROZSUDKŮ V TRESTNÍCH VĚCECH A TRESTNÝCH ČINŮ (čl. 10 GDPR)

- zpracování se může provádět pouze **pod dozorem orgánu veřejné moci**
- **souhrnný rejstřík trestů** může být veden pouze pod dozorem orgánu veřejné moci

Zvláštní kategorie osobních údajů

- **genetické údaje** – osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby
- **biometrické údaje** – osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje
- **údaje o zdravotním stavu** – osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu

Osobní, anonymní, anonymizované a pseudonymní údaje

- **osobní údaj** – veškeré informace, na základě kterých lze přímo či nepřímo identifikovat fyzickou osobu
- **anonymní údaj** – informace, na základě kterých nelze identifikovat žádnou fyzickou osobu, např. informace o počasí; nikdy nebyly a ani nebudou osobními údaji
- **anonymizovaný údaj** – údaj, který kdysi byl osobním údajem, ale přestal jím být, protože po určité úprava (anonymizaci) již není možné na základě něho osobu identifikovat; proces anonymizace musí být nezvratný (i s přihlédnutím k budoucímu stavu techniky, viz stanovisko WP29 ze dne 10. 4. 2014, WP 216)
- **pseudonymní údaje** – některé identifikátory jsou nahrazeny jinými či zakódovány, ale informace lze zpětně zjistit; považují se za osobní údaje

GDPR: ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

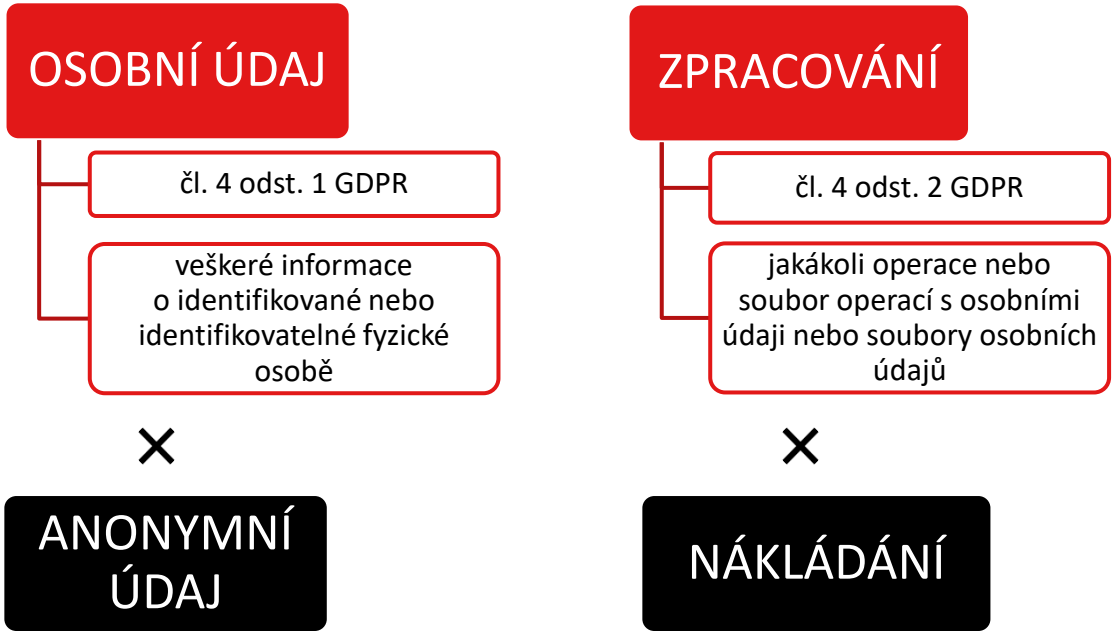
Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

čl. 4 a 11 GDPR

LEKCE Č. 3

Klíčové pojmy



Zpracování osobních údajů

- definice se oproti směrnici nezměnila, zároveň se neliší od českého zákona
- **nakládání s osobními údaji** – jakýkoli úkon či operace s osobními údaji, bez ohledu na účel a cíl
- **zpracování osobních údajů** – jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení

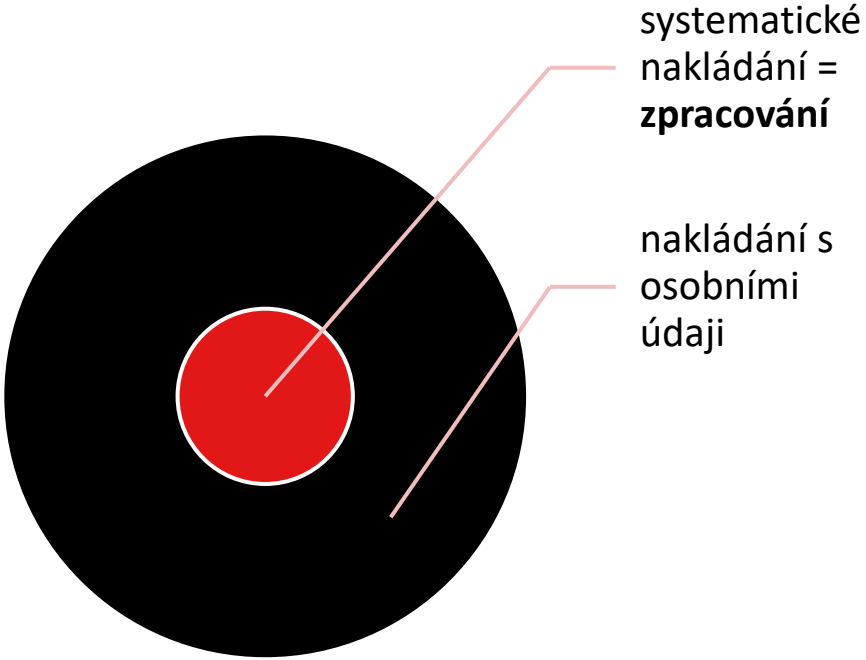
KLÍČOVÝ POJEM

Systematičnost zpracování

- k pojmu zpracování bylo vydáno **stanovisko ÚOOÚ č. 4/2013 k pojetí zpracování osobních údajů**
- je-li charakteristikou konkrétního nakládání **systematičnost**, jedná se o **zpracování** osobních údajů

K pravidelným znakům systematičnosti, nikoliv však definičním, patří:

- **opakovanost/hromadnost**
- **jednotící účel**



Výklad pojmu zpracování

- mezi zpracováním a jiným nakládáním s osobními údaji je tenká hranice, což je zvláště výrazné u uchování osobních údajů; některé znaky skutkové podstaty pomáhají v její správné kvalifikaci (systematičnost, hromadnost), avšak jejich absence neznamená, že se o zpracování osobních údajů nejedná
- **pojem „systematický“ v definici zpracování je v zásadě nadbytečný a jeho význam je okrajový**; lze se domnívat, že systematičnost je pozůstatkem předchozího zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech (stanovisko ÚOOÚ č. 4/2013 k pojetí zpracování osobních údajů)
- pojem „systematičnost“ se postupně výrazně zrelativizoval, někteří autoři se přiklánějí k názoru, že **zpracování je následkem či výsledkem účelného shromáždění údajů**
- **výkladová metoda in dubio pro libertate – „**Úřad proto bude v pochybnostech nakládání s osobními údaji spíše za jejich zpracování považovat, než nikoliv, aby se nedostal do rozporu s evropským právem“ (stanovisko ÚOOÚ č. 4/2013 k pojetí zpracování osobních údajů)

Extenzivní výklad pojmu zpracování

Německá kauza týkající se „lajků“ na Facebooku:

- internetová stránka Peek & Cloppenburg Fashion „chytila“ uživatelské údaje a poslala je na Facebook, ještě před tím, než zákazníci klikli na tlačítko „lajk“
- Obvodní soud v Düsseldorfu rozhodl, že takové přeposlání dat provozovatelem e-shopu bylo zpracováním, a to navíc protiprávním zpracováním
- Peek & Cloppenburg čelil pokutě až 250 000 eur (275 400 dolarů) a šestiměsíčnímu zatčení manažera

ZDROJ: http://www.reuters.com/article/us-facebook-like-germany-idUSKCN0WB1OI

KAUZA

Opakovanost/hromadnost zpracování

- **hromadnost/opakovanost** je typickým znakem, ale není nutným předpokladem zpracování

Zpracováním osobních údajů je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů:

- **operace** – **jednorázové zpracování**, např. pokud zaměstnavatel pro účel ochrany svých práv případě žaloby na bývalého zaměstnance vyhledá některé údaje ze své personální evidence, zkombinuje se s veřejně přístupnými údaji a předá je soudu,
- **soubor operací** – zde je již hromadnost znakem, např. vedení personální evidence pro účely plnění pracovněprávních smluv a povinností dle zákoníku práce a daňových předpisů.

Příklady jednorázových zpracování

Za **jednorázové zpracování osobních údajů** považujeme:

- uložení jednoho jediného e-mailu obsahujícího osobní údaje do speciální složky, je-li cílem umožnit další zpracování těchto údajů
- uložení pouze jediného životopisu, neboť na pracovní místo se přihlásil pouze jeden jediný uchazeč
- vytvoření formuláře na webu, který vyplní pouze jediný uživatel
- vedení spisu obsahujícího osobní údaje pouze jedné osoby či uchování jednotlivé smlouvy obsahující pouze osobní údaje dvou smluvních stran, je-li zpracování osobních údajů cílem nakládání s těmito dokumenty

Ve všech těchto případech sice nedošlo k hromadnému/opakovanému zpracování, nicméně byly vytvořeny **podmínky pro opakovanost** (vytvoření formuláře na webu), popř. **účelem bylo přímé nakládání s údaji** (uložené jedné smlouvy).

Účelnost zpracování

- **účelnost** je typickým znakem, ale není nutným předpokladem zpracování
- každé zpracování osobních údajů má být účelné, ale i neúčelné zpracování osobních údajů však zůstává zpracováním osobních údajů
- neúčelné je zpravidla **nahodilé shromáždění osobních údajů** nebo **nakládání s pouhými nosiči osobních údajů**

Nakládání s nosiči osobních údajů – pouhé nakládání s nosiči osobních údajů není zpracováním osobních údajů, protože zpracování není cílem takového nakládání s jejich nosiči, např.:

- nakládání s balíkem starých novin
- zametení kadeří vlasů v kadeřnictví
- provoz kamery bez záznamu
- skladování starých harddisků, o kterých správce skladu neví, že obsahují nedokonale smazané počítačové soubory s osobními údaji

Nahodilé shromáždění osobních údajů

- **nahodilé shromáždění osobních údajů**, pokud tyto údaje nejsou dále zpracovávány, **není zpracováním osobních údajů** – nesmí tedy dojít k dalšímu zpracování, např. zveřejnění
- za nahodilé nakládání s osobními údaji lze například považovat **práci s listinou**, která obsahuje relevantní osobní údaje; její uchování je tedy nezbytné, avšak vedle relevantních osobních údajů **obsahuje osobní údaje též nepotřebné a správcem cíleně neshromažďované**
- příkladem může být shromáždění nesouvisejících informací v profesním životopisu zaslané potencionálnímu zaměstnavateli – zveřejnění těchto údajů by však již zpracováním bylo, neboť údaje sice byly shromážděny nahodile, ale byly dále zpracovávány (zveřejněny)

Činnost médií

- problematické je, zda lze **činnost médií** (zveřejňování a šíření osobních údajů) považovat za zpracování osobních údajů
- dle části odborné veřejnosti a starších rozsudků Nejvyššího správní soudu novináři nezveřejňují informace systematicky ve smyslu zákona o ochraně osobních údajů, jedná se spíše o nahodilé či ojedinělé zveřejnění nezpracovaných osobních údajů – názor ovšem vychází ze staršího pojetí systematičnosti
- tento názor bude však nutné považovat s přijetím GDPR za překonaný, neboť čl. 85 dopadá na zpracování pro novinářské účely; činnost médií je tak nutné považovat rovněž za zpracování osobních údajů, byť za **zvláštní kategorii zpracování**, na kterou dopadají zvláštní pravidla (čl. 85 GDPR, bod 153 odůvodnění GDPR)

Rozlišovací kritérium – účel činnosti

Klíčem pro rozlišení, kdy se jedná o zpracování osobních údajů a kdy jde o jiné nakládání s osobními údaji, je **ÚČEL DANÉ ČINNOSTI**.

Je-li účelem **práce s daty**, byť i pasivní (tzn. jejich pouhé uchovávání) nebo poslední (anonymizace nebo likvidace), pak se o **zpracování osobních údajů** jedná. Zpracování je zejména výsledkem účelného shromáždění osobních údajů.

Naproti tomu pokud je přístup k datům pouhým nepravidelným a nahodilým důsledkem jiné činnosti o zpracování se nejedná a jde o **jiné nakládání s osobními údaji**.

DŮLEŽITÉ

Účely zpracování

Zpracování může být probíhat za různými účely; bez ohledu na tento účel jde vždy o zpracování:

- **zpracování za účelem vlastního cíle** – provádí správce; např. oslovování nových klientů, plnění smluv, ochrana majetku, …
- **zpracování při plnění zákonné povinnosti** – provádí typicky veřejnoprávní správci; např. plnění povinností ze zákona o registru smluv, výběr poplatků, …
- **poskytování uložiště dat** – jde rovněž o zpracování; typicky se jedná o cloudové služby a provádí jej zpravidla zpracovatel
- **zpracování pro domácí a osobní účely** – je nutné je rovněž považovat za zpracování (předchozí judikaturu je nutné považovat za překonanou), byť se ne něj nepoužije GDPR; např. uložení telefonního čísla do osobního mobilu, …

Druhy zpracování

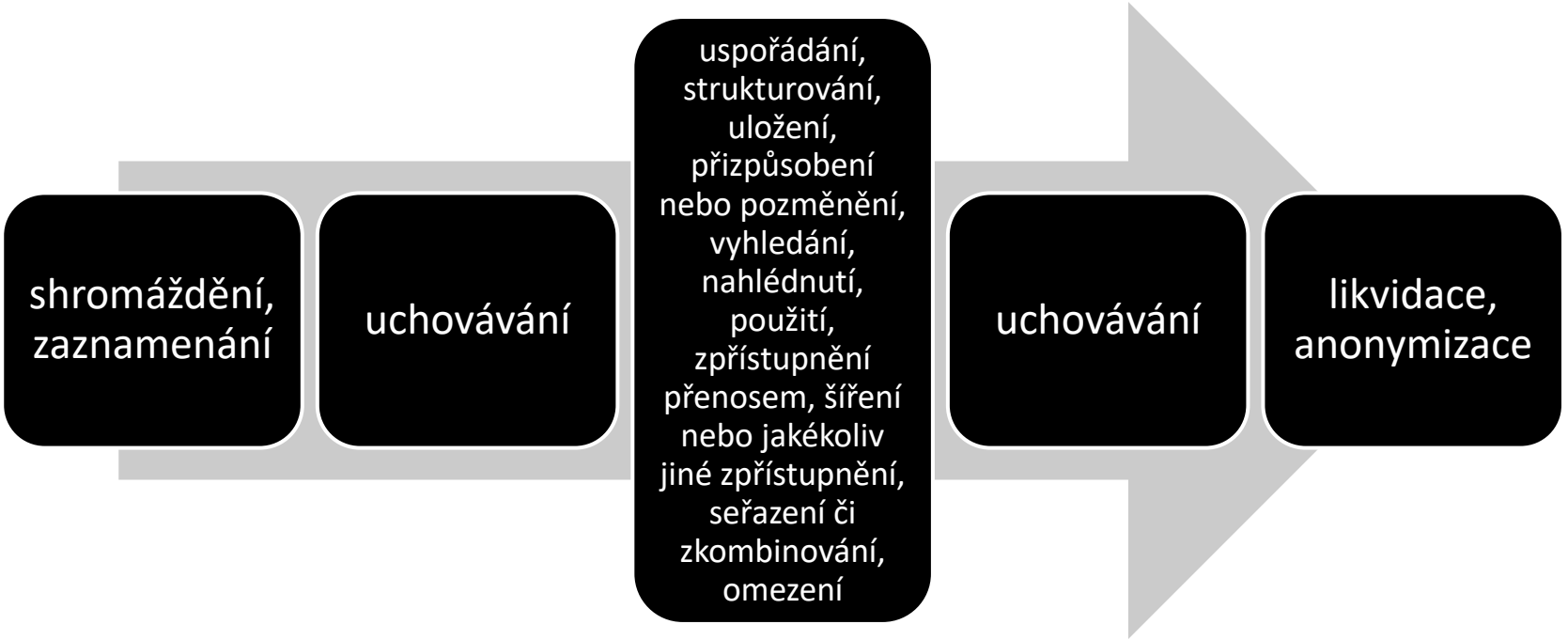
Z hlediska způsobu zpracování můžeme rozlišovat následující druhy zpracování:

- **automatizované zpracování** – technickými prostředky, zejména za použití výpočetní techniky, bez nutnosti lidské činnosti
- **částečně automatizované zpracování** – kombinace automatizovaného a manuálního zpracování
- **manuální zpracování v evidenci** – zpracování prováděné člověkem za použití psacích prostředků či počítače

Od automatizovaného zpracování je nutné odlišovat **automatizované rozhodování** o právech subjektů údajů dle čl. 22 GDPR, který v podstatě zavádí **právo lidí nebýt předmětem rozhodování robotů**.

DŮLEŽITÉ

Fáze zpracování osobních údajů



Shromáždění a uchovávání

Shromažďování osobních údajů

- systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování
- **první fáze zpracování** – shromáždění je vždy první operací, a proto je některými autory dokonce považována za **definiční znak samotného zpracování**

Uchovávání osobních údajů

- udržování údajů v takové podobě, která je umožňuje dále zpracovávat
- ačkoli jde o ryze **pasivní činnost**, kvůli jejímu účelu ji považujeme za zpracování

Práce s osobními údaji

Práce s osobními údaji – GDPR tyto činnosti pouze jmenuje, ale nestanoví pro ně přesná pravidla

- uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, seřazení či zkombinování

Zvláštní práce s osobními údaji – některé činnosti s osobními údaji GDPR blíže reguluje:

- **omezení zpracování osobních údajů** – označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu
- **profilování osobních údajů** – jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě
- **pseudonymizace osobních údajů** – zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně

Omezení zpracování

- **omezení zpracování osobních údajů** – označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu (čl. 4 odst. 3 GDPR, blíže bod 67 odůvodnění GDPR)
- zpravidla se jedná o **přesun údajů do jiného systému a znepřístupnění veřejnosti**, v původním systému je omezení vyznačeno – typické např. pro registr dlužníků
- **nejde nezbytně o blokování**, protože nemusí být nutně bráněno jakémukoli dalšímu zpracování
- k omezení musí dojít v případech uvedených v čl. 18 odst. 1 GDPR, např. pokud **subjekt údajů popírá přesnost** osobních údajů či **zpracování je protiprávní, ale subjekt údajů odmítá výmaz** osobních údajů a požaduje omezení jejich použití

Profilování

- **profilování osobních údajů** – jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu (čl. 4 odst. 4 GDPR)
- činnost sloužící k posouzení vlastností či preferencí osoby, tedy k odhadu budoucího chování daného jedince; získávání informací pro cílenou reklamu
- profilování **není zakázáno při dodržení podmínek dle čl. 22 odst. 2 GDPR**
- s profilováním souvisí **právo vznést námitku dle čl. 21 GDPR**

Pseudoanonymizace

- **pseudonymizace osobních údajů** – zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě (čl. 4 odst. 5 GDPR)
- svou povahu se jedná „šifrování“; stále se jedná o osobní údaje, ale jsou rozděleny na šifrované údaje a informace o šifře samotné
- pseudonymizace zvyšuje bezpečnost dat (body 26 a 28 odůvodnění GDPR) – jedná se o zároveň o **doporučené bezpečnostní opatření** (viz čl. 32 GDPR)
- rozdíl mezi pseudoanonymizací a anonymizací spočívá v **nevratnosti procesu anonymizace**
- pseudoanonymizace souvisí s dalším zpracováním [čl. 5 odst. 1 písm. b) GDPR], posuzováním vlivu (čl. 35 GDPR) a zpracováním pro účely archivace, výzkumu či statistiky (čl. 89 GDPR)

Zpřístupnění, zveřejnění a šíření

- **zpřístupnění osobních údajů** – zpřístupnění omezenému okruhu adresátů, byť může být i relativně velký, ale nejde o „širokou veřejnost“
- **zveřejnění osobních údajů** – zpřístupnění zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu
- **šíření osobních údajů** – rozšíření již zveřejněné informace, zpravidla formou sdělovacích prostředků či sociálních sítí

- **příjemce** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli (čl. 4 odst. 9 GDPR)
- orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu (např. policejní, daňové či celní orgány), se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování
- příjemce nemůže být zároveň správcem ani zpracovatelem – pojmy se navzájem vylučují

Likvidace a anonymizace

Poslední operace zpracování:

- **likvidace osobních údajů** – fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování, např. vrácení listiny subjektu údajů bez pořízení a uložení fotokopie
- **anonymizace osobních údajů** – dosažení stavu, kdy řada informací sice zůstane zachována, ale přestane být osobními údaji

V obou případech musí jít ex definitione o **poslední fázi zpracování**. Po likvidaci či anonymizaci přestávají být osobní údaje osobními; buď přestanou existovat, popř. jde o anonymizované údaje.

Zvláštní případy zpracování osobních údajů

GDPR upravuje některé případy zpracování odchylně. Jedná se o:

- zpracování osobních údajů, které **nevyžaduje identifikaci** – čl. 11 GDPR
- zpracování osobních údajů pro **novinářské účely** – čl. 85 GDPR
- zpracování osobních údajů pro **akademické a umělecké účely** – čl. 85 GDPR
- zpracování osobních údajů v **úředních dokumentech** – čl. 86 GDPR
- zpracování **národních identifikačních čísel** – čl. 87 GDPR
- zpracování **v souvislosti se zaměstnáním** – čl. 88 GDPR
- zpracování pro účely **archivace ve veřejném zájmu**, pro účely **vědeckého či historického výzkumu** nebo pro **statistické účely** – čl. 89 GDPR
- zpracování v souvislosti se **zákonnou povinností mlčenlivosti** – čl. 90 GDPR
- zpracování **církvemi a náboženskými sdruženími** – čl. 91 GDPR

Zpracování osobních údajů, které nevyžaduje identifikaci

- pokud účely, pro něž správce zpracovává osobní údaje, od správce nevyžadují nebo již nevyžadují identifikaci subjektu údajů, nemá správce povinnost uchovávat, získávat nebo zpracovávat dodatečné informace za účelem identifikace subjektu údajů výlučně kvůli dosažení souladu s GDPR (čl. 11 odst. 1 GDPR)
- zpracování, které nevyžaduje identifikaci, úzce souvisí s **nepřímou identifikací subjektů údajů** – správce údajů nezná přímé identifikátory, ale osoby jsou pro něj dosažitelné
- jedná se např. o **využívání IP adresy za účelem získávání informací o návštěvnosti a vzorcích chování uživatelů na webu** – ačkoli je IP adresa osobním údajem (je možná nepřímá identifikace), provozovatel webu není schopen zjistit, komu patří (není možná přímá identifikace) – to provozovateli ovšem brání vyhovět námitce proti zpracování, pokud subjekt sám neurčí, které IP adresy se ho týkají – ze čl. 11 plyne to, že provozovatel webu není povinen k IP adresám připojovat přímé identifikátory uživatelů webu pouze proto, aby mohl vyhovět žádostem svých uživatelů

DŮLEŽITÉ

Postup v případě nemožnosti identifikace

Pokud **subjekt údajů uplatní právo** dle čl. 15 GDPR (právo na přístup), čl. 16 GDPR (právo na opravu a výmaz), čl. 17 GDPR (právo na výmaz), čl. 18 GDPR (právo na omezení zpracování), čl. 19 GDPR (oznamovací povinnost při opravě, výmazu nebo omezení) nebo čl. 20 GDPR (právo na přenositelnost), má správce následující možnosti:

- **správce doloží, že není schopen identifikovat subjekt údajů**, informuje o tom subjekt údajů (bez zbytečného odkladu, nejpozději do 30 dnů) a žádostí samotnou se nebude zabývat
- **subjekt údajů poskytne dodatečné informace umožňující jeho identifikaci** – v takovém případě je nutné se žádostí o uplatnění práva zabývat (bez zbytečného odkladu, nejpozději do 30 dnů)

GDPR:
PRÁVNÍ TITUL KE ZPRACOVÁNÍ

Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

čl. 6 – 8 GDPR

LEKCE Č. 4

Právní titul

- **zásada zákonnosti** – zpracování je zákonné jen tehdy, je-li založeno na právním titulu
- **audit osobních údajů** – vyhodnocení, zda je každý osobní údaj zpracován na základě právní titul; první krok, který musí správce provést

- **zpracování zvláštní kategorie osobních údajů** – správce musí mít nejen právní titul, ale také zvláštní důvod pro zpracování dle čl. 9 odst. 2 GDPR
- **zpracování osobních údajů týkajících se rozsudku v trestních věcech a trestných činů** – správce musí mít nejen právní titul, ale také zvláštní důvod pro zpracování dle čl. 10 GDPR

Poznámka: informační povinnosti (čl. 13 a 14 GDPR) je nutné plnit i tehdy, jsou-li údaje zpracovány na základě jiného titulu než souhlasu – změna koncepce oproti § 5 zákona č. 101/2000 Sb., o ochraně osobních údajů

Právní titul a zvláštní důvody ke zpracování

zpracování osobních údajů

- právní titul (čl. 6 GDPR)

zpracování zvláštní kategorie osobních údajů

- právní titul (čl. 6 GDPR)
- zvláštní důvod pro zpracování dle čl. 9 odst. 2 GDPR

zpracování osobních údajů týkajících se rozsudku v trestních věcech a trestných činů

- právní titul (čl. 6 GDPR)
- zvláštní důvod pro zpracování dle čl. 10 GDPR

Právní titul a účel zpracování

PRÁVNÍ TITUL se vždy pojí s ÚČELEM ZPRACOVÁNÍ.

- **právní titul** je zákonným podkladem zpracování, který je vždy opřen o účel
- **účel** je alfou a omegou zpracování; „chybí-li účel, pak je zpracování nezákonné“; „nepotřebuju-li údaje, pak je nemám mít“
- právní tituly a účely na sebe mohou navazovat – po skončení původního zpracování, pak není nutné údaje smazat, pokud správci vznikne potřeba zpracovávat údaje pro jiný účel a pro tento účel bude mít právní titul – bude ovšem nutné provést **posouzení slučitelnosti původního a nového účelu** dle čl. 6 odst. 4 GDPR

DŮLEŽITÉ

Přehled právních titulů (dle čl. 6 GDPR)

souhlas	plnění smlouvy	plnění právní povinnosti
životně důležitý zájem	veřejný zájem	oprávněný zájem

Právní titul a účel zpracování - příklad

Provozovatel e-shopu může údaje „jméno a příjmení“ a „kontaktní adresa“ zpracovávat pro různé účely:

účel zpracování	právní titul
zaslání zboží a ověření provedení platby	plnění smlouvy
zasílání obchodních sdělení	oprávněný zájem
provoz zákaznické soutěže	souhlas se zpracováním

Pokud jeden z těchto účelů odpadne (zboží bylo dodáno, uplynula reklamační lhůta, smlouva byla splněna), nebude to znamenat, že musí provozovatel e-shopu údaje vymazat, jelikož je stále potřebuje pro zbylé účely a pro tyto má právní tituly. Musel ale splnit svou informační povinnost.

Změna koncepce zákonnosti zpracování

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

Vždy je nutné mít **souhlas**, ale zákon uvádí **výjimky**, kdy souhlas nutný není, např.:

- zpracování nezbytné pro **dodržení právní povinnosti** správce
- zpracování **nezbytné pro plnění smlouvy**
- ochrana **životně důležitých zájmů** subjektu údajů
- zpracování nezbytné pro **ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby**

GDPR

Vždy je nutné mít **právní titul**, a to bezvýjimečně; právní titulem se rozumí:

- **souhlas**
- **plnění smlouvy**
- **plnění právní povinnosti**
- **životně důležitý zájem**
- **veřejný zájem**
- **oprávněný zájem**

Nepochopení pojetí souhlasu v praxi

- kvůli nepřesné transpozici směrnice 95/46/ES do zákona č. 101/2000 Sb., o ochraně osobních údajů, byl souhlas chápán jako hlavní titul pro zpracování – česká praxe souhlas přeceňovala, **bylo „přesouhlasováno“**
- **stanovisko ÚOOÚ č. 3/2014 k nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti** – vyžaduji-li souhlas, kde plním zákonnou povinnost, špatně poučuji, protože vyvolávám dojem o odvolatelnosti souhlasu; neexistuje „neodvolatelný souhlas“

Souhlas je **zbytkovým právní titulem**, který vyžaduji až tehdy, není-li zpracováno možné na základě jiného právního titulu.

Nejobtížnější je posouzení kolize, zda mi svědčí oprávněný zájem, či nikoli a budu vyžadovat souhlas.

DŮLEŽITÉ

Zpřísnění souhlasu

- **výslovný souhlas** – není možné udělit souhlas konkludentním jednáním, které spočívá v opomenutí či pasivitě, např. nemůže jít o předvyplněné zaškrtávací tlačítko; z užívání webu také nelze dovodit souhlas s používáním cookies, …
- **jednoznačný souhlas** – pokud je souhlas získáván písemně, je nutné, aby byl viditelný a oddělený od zbylého textu; ideálně na samostatném listu; nesmí se nacházet ve všeobecných obchodních podmínkách
- **svobodný souhlas** – hlavní službu nelze podmiňovat poskytnutím souhlasu (hlavní službu vždy kryje titul plnění smlouvy); nevhodný pro zaměstnavatele a orgány moci veřejné
- **informovaný souhlas** – před poskytnutím souhlasu musí být subjekt poučen o účelu a způsobu zpracování
- **odvolatelný souhlas** – subjekt údajů může souhlas kdykoli odvolat
- **prokazatelný souhlas** – správce vždy musí být schopen prokázat udělení souhlasu
- **souhlas dítěte** – zpřísňují se a zpřesňují se požadavky na udělení souhlasu dítětem

DŮLEŽITÉ

Přehled právních titulů (dle významu)

plnění smlouvy	plnění právní povinnosti	životně důležitý zájem
veřejný zájem	oprávněný zájem	souhlas (zbytkový právní titul)

PLNĚNÍ SMLOUVY

Plnění smlouvy

- zpracování osobních údajů, které jsou **nezbytné pro plnění smlouvy** – pouze nezbytné, cokoli dalšího (zbytného; pro jiné účely, např. ryze marketingové) je nutné zpracovávat na základě jiného titulu
- v praxi jde o **velmi častý titul**
- účel není možné svévolně překročit (údaje např. po splnění smlouvy přeprodat třetí straně)
- doba zpracování – **po dobu uzavření a plnění smlouvy**; zpracování pro případ nesplnění závazku, např. vymáhání pohledávky, již nespadá pod tento právní titul (půjde zpravidla o výkon oprávněného zájmu)
- zaslání **výzvy ke splnění závazku** lze pod tento titul ještě podřadit

DŮLEŽITÉ

Plnění smlouvy – jádro závazku

- **zásada minimalizace údajů** – vždy je nutné identifikovat **esenciální jádro daného závazku** a zpracovávat osobní údaj pouze pro splnění tohoto jádra závazku, např. zpracování rodného čísla není nutné pro plnění pracovní smlouvy
- ve smlouvě **není možné stanovit, že zpracování bude probíhat za jinými (vedlejšími) účely** a spoléhat se na právní titul plnění smlouvy – v podstatě by šlo o souhlas vtělený do textu smlouvy, což je samo o sobě problematické, protože souhlas má být oddělený
- **text „strany souhlasí se zpracováním osobních údajů v souvislosti s touto smlouvu“** v závěrečných ustanovení nemá žádný právní význam

PLNĚNÍ PRÁVNÍ POVINNOSTI

Plnění právní povinnosti

- zpracování osobních údajů z **titulu plnění právní povinnosti** – správce nepotřebuje souhlas, pokud osobní údaje zpracovávat musí, např. povinnost předávat informace, vč. rodného čísla, zdravotní pojišťovně podle § 10 zákona o veřejném zdravotním pojištění
- v praxi jde vedle plnění smlouvy rovněž o **velmi častý titul**
- **není možné jít nad rámec zákona** – banka má právní povinnost identifikovat a verifikovat svého klienta podle AML zákona (§ 7 až 15 stanoví okruh údajů a postup), nicméně pokud banka (pro zvýšení bezpečnosti) začne používat otisky prstů (jde nad rámec zákona), pak bude muset najít jiný právní titul dle čl. 6 odst. 1 GDPR a navíc splnit povinnost dle čl. 9 odst. 2 GDPR (jde o biometrický údaj)

DŮLEŽITÉ

Právní základ povinnosti

Právní základ povinnosti musí spočívat v **povinnosti**, nikoli oprávnění, **stanovené právem EU nebo právem členského státu**, přitom v České republice platí, že **povinnosti je možno ukládat pouze na základě zákona** (čl. 4 odst. 1 Listiny základních práv a svobod):

- právní základ musí být v **zákoně**; konkretizace právní povinnosti může být i v podzákonném právním předpise (nařízení vlády, vyhláška ministerstva, …, nikoli však např. metodický pokyn)
- povinnost musí být **zvláštním právním předpisem** určena natolik **určitě**, aby z ní bylo možné poznat, jaká zpracování na jejím základě budou probíhat
- **právo na informace** dle čl. 13 a 14 GDPR zahrnuje také sdělení, které ustanovení kterého zvláštního zákona danou povinnost stanoví

Právní základ povinnosti

Jako právní základ pro zpracování na základě plnění právní povinnosti tedy nepřipadají:

- **mimoprávní povinnosti** – nelze se také odvolávat na plnění mimoprávních povinností, např. povinností vyplývajících z technických norem ISO, popř. povinností vyplývajících z pravidel dotačních programů
- **povinnosti vyplývající z práva třetích zemí** – nelze se odkazovat na cizí právo, např. na povinnost vytvořit v rámci organizace systém pro ochranu whistleblowerů, neboť tato povinnost vyplývá z práva USA (Sarbanes-Oxley Act z roku 2002)
- **zákonné licence (oprávnění)** – např. § 312 zákoníku práce (vedení osobního spisu zaměstnance)

Zákonné oprávnění

§ 312 odst. 1 zákoníku práce

*Zaměstnavatel **je oprávněn** vést osobní spis zaměstnance. Osobní spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu uvedeném v § 3.*

- § 13 odst. 1 zákoníku práce formuluje **zákonné oprávnění**, nikoli zákonnou možnost
- pokud je již spis veden, má zaměstnance právo do něj nahlížet (viz 13 odst. 3 zákoníku práce)
- vedení spisu zaměstnance tak není právní povinností, a proto pro něj **nelze použít právní titul plnění právní povinnost**, je nutné najít jiný právní titul – v tomto případě půjde o oprávněný zájem
- stanovení zákonného oprávnění nám ovšem pomáhá označit daný zájem za **oprávněný zájem**, a proto v těchto případech zpravidla **není nutné vyžadovat souhlas**

Trvání právní povinnosti

- zpracování je možné **po dobu trvání právní povinnosti**, poté je nutné najít jiný právní titul nebo zpracování ukončit (údaje zlikvidovat, popř. provést další zpracování spočívající v anonymizaci)
- důležité je hlídat zejména zákonné **archivační lhůty**, poté je zpravidla nutné dokumenty skartovat

NĚKTERÉ ARCHIVAČNÍ LHŮTY:

- účetní jednotky (podle § 1 odst. 2 zákona o účetnictví) jsou povinny uchovávat **účetní závěrky** a **výroční zprávy** po dobu 10 let a **účetní doklady, účetní knihy, odpisové plány, inventurní soupisy, účtový rozvrh a účetní záznamy, kterými dokládají vedení účetnictví**, po dobu 5 let počínajících koncem účetního období, kterého se týkají
- zaměstnavatel je povinen uchovávat **stejnopisy evidenčních listů** po dobu 3 kalendářních roků po roce, kterého se týkají, a **mzdové listy** po dobu 30 kalendářních roků následujících po roce, kterého se týkají, dále **doklady o druhu, vzniku a skončení pracovního vztahu, záznamy o pracovních úrazech a o nemocech z povolání a záznamy o evidenci pracovní doby včetně doby pracovního volna bez náhrady příjmu** po dobu 5 let a **vnitřní předpis, kterým zaměstnavatel stanovuje výhodněji práva z pracovněprávních vztahů,** po dobu 10 let ode dne ukončení doby jeho platnosti

Odchylky v národní úpravě

V případě právního titulu plnění právní povinnosti (a rovněž při zpracování ve veřejném zájmu) mohou členské státy stanovit formou legislativního opatření (v České republice půjde o plánovaný **adaptační zákon**) **konkrétnější požadavky na zpracování osobních údajů ve zvláštních situacích**:

- zpracování osobních údajů pro **novinářské účely** – čl. 85 GDPR
- zpracování osobních údajů pro **akademické a umělecké účely** – čl. 85 GDPR
- zpracování osobních údajů v **úředních dokumentech** – čl. 86 GDPR
- zpracování **národních identifikačních čísel** – čl. 87 GDPR
- zpracování **v souvislosti se zaměstnáním** – čl. 88 GDPR
- zpracování pro účely **archivace ve veřejném zájmu**, pro účely **vědeckého či historického výzkumu** nebo pro **statistické účely** – čl. 89 GDPR

ŽIVOTNĚ DŮLEŽITÝ ZÁJEM

Životně důležitý zájem

- **životně důležitý zájem** – **zájem na ochraně života nebo zdraví**, např. informace o pacientovi, který je přijímán v bezvědomí po autonehodě, či **veřejný důležitý životní zájem**, tj. humanitární účely, včetně monitorování epidemií a jejich šíření, nebo zpracování v naléhavých humanitárních situacích, zejména v případech přírodních a člověkem způsobených katastrof (viz bod 46 odůvodnění GDPR)
- zpracování osobních údajů na základě životně důležitého zájmu jiné fyzické osoby by mělo v zásadě proběhnout pouze tehdy, pokud vně nemůže být založeno na **jiném právním základě**
- nově nemusí jít o **zájem subjektu údajů**, ale rovněž o **zájem třetí osoby**, např. můžu zpracovat osobní údaje příbuzného (subjekt údajů) pro ochranu života a zdraví člena rodiny (třetí osoba)
- oproti zákonu č. 101/2000 Sb., **odpadá podmínka dodatečného získání souhlasu**
- v praxi jde o **méně častý právní titul**, neboť jej často překryje právní titul plnění právní povinnosti (zdravotnické předpisy, např. zákon o poskytování zdravotní péče)

VEŘEJNÝ ZÁJEM

Veřejný zájem

- **veřejný zájem** – úkol ve veřejném zájmu nebo výkon veřejné moci
- svědčí **orgánu moci veřejné** (úřady, obce, kraje, …) nebo **soukromému subjektu, na který byl přenesen výkon veřejné moci** (stanice STK, lesní stráž, …)
- **právo na informace** dle čl. 13 a 14 GDPR zahrnuje také sdělení, v čem veřejný zájem spočívá

Orgány veřejné moci zpravidla využívají **dva právní tituly**:

- **plnění právní povinnosti** – v případě, kdy právní základ (zmocnění ve zvláštním zákoně) je dostatečně určitý; orgán moci výkonné nemá na výběr, zda bude údaje zpracovávat (bez správního uvážení, bez možnosti diskrece)
- **veřejný zájem** – v případě, kdy je právní základ neurčitý, orgánu veřejné moci je dán určitý úkol ve veřejném zájmu, ale je na orgánu, jak jej bude naplňovat, je dána možnost správního uvážená, široká míra diskrece

DŮLEŽITÉ

Odchylky v národní úpravě

V případě zpracování ve veřejném zájmu mohou členské státy (stejně jako u plnění právní povinnosti) stanovit formou legislativního opatření (v České republice půjde o plánovaný **adaptační zákon**) **konkrétnější požadavky na zpracování osobních údajů ve zvláštních situacích**:

- zpracování osobních údajů pro **novinářské účely** – čl. 85 GDPR
- zpracování osobních údajů pro **akademické a umělecké účely** – čl. 85 GDPR
- zpracování osobních údajů v **úředních dokumentech** – čl. 86 GDPR
- zpracování **národních identifikačních čísel** – čl. 87 GDPR
- zpracování **v souvislosti se zaměstnáním** – čl. 88 GDPR
- zpracování pro účely **archivace ve veřejném zájmu**, pro účely **vědeckého či historického výzkumu** nebo pro **statistické účely** – čl. 89 GDPR

Práva spojená s veřejným zájmem

V případě tohoto titulu je nutné počítat s dalšími povinnosti spojenými s právem vznést námitku:

- **poučení o právu vznést námitku (čl. 21 odst. 4 GDPR)** – subjekt údajů musí být výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů
- **právo vznést námitku dle čl. 21 odst. 1 GDPR** – správce musí provést test proporcionality pro daný individuální případ, který se totiž může odlišovat od provedeného testu oprávněnosti

DŮLEŽITÉ

OPRÁVNĚNÝ ZÁJEM

Oprávněný zájem

- jde o **nejflexibilnější právní titul** – „je možno pod skrýt téměř cokoli“, a proto bude v praxi **velmi častý** a zároveň **nejproblematičtější**
- zákon č. 101/2000 Sb. stanovil, že muselo jít o právem chráněný zájem, např. ochrana vlastnického práva, nicméně tato podmínka odpadá
- jde o **oprávněný zájem správce údajů či třetí strany**, nikoli subjektu údajů
- oprávněný zájem **nesmí využívat orgány moci veřejné** při plnění svých úkolů ve veřejném zájmu, nicméně mohou jej využívat tam, kde vystupují v soukromoprávním postavení, např. ochrana majetku kamerovým systémem
- před každým zpracováním je nutné **posoudit oprávněnost daného zájmu**, tj. provést tzv. **test oprávněnosti**

DŮLEŽITÉ

Příklady oprávněných zájmů

Oprávněný zájem může spočívat v mnohém:

- **ochrana majetku** – např. provoz kamerového systému
- **kontrola pracovních výkonů zaměstnanců** – např. zavedení docházkového systému
- **kontrola efektivity práce** – např. umístnění GPS do pracovních vozů
- **vymáhání pohledávek a jiných práv** – např. zavedení černé listiny dlužníků
- **marketingové zájmy** – např. zasílání obchodních sdělení
- **generování podnikatelského zisku** – např. provoz internetového vyhledávače či provoz registru dlužníků
- **kulturní život v obci** – např. vydávání ročenky z fotkami s kulturních akcí

Test oprávněnosti

Před každým zpracováním je nutné **posoudit oprávněnost daného zájmu**, tj. provést tzv. **test oprávněnosti**, který spočívá ve **třech krocích**:

- Je stanovený zájem oprávněný? Splňuje požadované kvality?
- Je zamýšlené zpracování skutečně nezbytné?
- Nepřevažují nad tímto zájmem práva a svobody subjektu údajů?

Test může skončit dvěma výsledky:

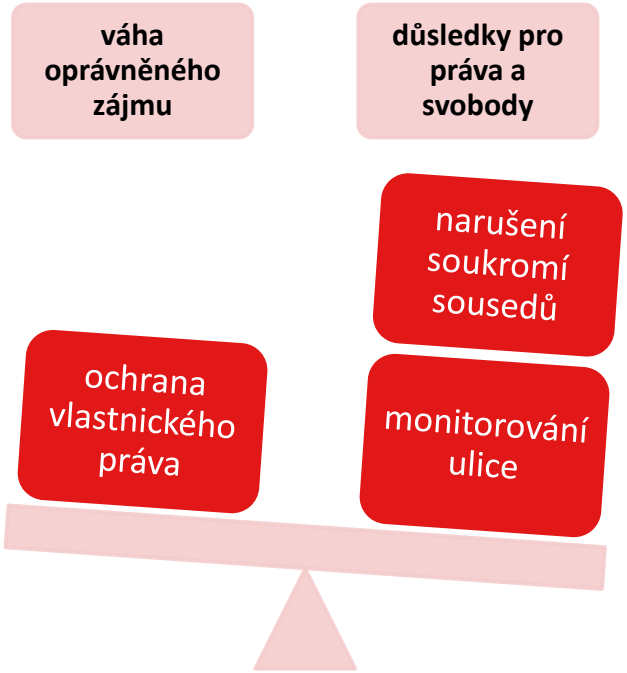
- **pokud oprávněný zájem převáží nad právy a svobodami subjektu údajů**, pak je zpracování osobních údajů pro daný účel možné,
- **pokud práva a svobody subjektu údajů převáží nad oprávněným zájmem**, pak je zpracování osobních údajů na základě tohoto titulu nemožné; je však možné si vyžádat souhlas.

DŮLEŽITÉ

Test oprávněnosti

V testu oprávněnosti je nutné porovnávat

- **váha oprávněného zájmu** – rozlišujeme různé kategorie zájmů od těch chráněných zákonem až po ty ryze subjektivní
- **důsledky pro práva a svobody subjektu údajů** – ty mohou pozitivní i negativní



Posouzení váhy oprávněného zájmu

Můžeme rozlišovat **různé úrovně oprávněných zájmů**:

- **právem chráněné zájmy** - můžeme dále rozlišovat (a) **oprávněný zájem na výkonu základních lidských práv** – svoboda projevu, právo na informace, svoboda podnikaní, vlastnické právo a (a) **zákonné licence** či **zákonné oprávnění** (pokud zákon stanoví určitou možnost, pak lze předpokládat, že tento zájem je právem chráněný zájem a jako takový je oprávněný),
- **veřejné zájmy a zájmy širší komunity** – dobročinné činnosti, např. odhalování korupce ve veřejné sféře, činnost podnikatelů zaměřená na předcházení podvodů, např. registr dlužníků,
- **ostatní oprávněné zájmy** – subjektivní zájmy správce, nejde o právem chráněné zájmy; např. marketingové zájmy.

Můžeme si pomoci také sta**noviskem WP29 ke konceptu oprávněného zájmu dle čl. 7 směrnice 95/46/ES** ze dne 9. 4. 2014 (str. 23 až 24).

Důsledky zpracování pro práva a svobody subjektu údajů

Je třeba zohlednit veškeré možné důsledky zpracování:

- **pozitivní důsledky** – pozitivní důsledky pro samotný subjekt (ochrana jeho vlastních zájmů) a pozitivní důsledky pro společnost (šíření informací, odhalování korupce a trestné činnosti), …
- **negativní důsledky** – možnost vzniku majetkové škody, možnost zvýšení rizika krádeže (čísla bankovních účtů, informace o majetku, …), ztráta schopnosti získat úvěr, možnost vzniku nemajetkové újmy např. zveřejněním informací (diskriminace, dehonestace, zesměšnění), …

Míra rizika záleží na **citlivosti údajů**, což nezáleží pouze na tom, zda jde o zvláštní kategorii osobních údajů dle čl. 9 GDPR. Pojem citlivosti je nutné chápat v tomto kontextu šířeji.

Práva spojená s oprávněným zájmem

V případě tohoto titulu je nutné počítat s dalšími povinnosti spojenými s právem vznést námitku:

- **poučení o právu vznést námitku (čl. 21 odst. 4 GDPR)** – subjekt údajů musí být výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů
- **právo vznést námitku dle čl. 21 odst. 1 GDPR** – správce musí provést test proporcionality pro daný individuální případ, který se totiž může odlišovat od provedeného testu oprávněnosti
- **právo vznést námitku dle čl. 21 odst. 2 GDPR** – v případě oprávněného zájmu spočívajícím v přímém marketingu je nutné této námitce ihned vyhovět

DŮLEŽITÉ

SOUHLAS

Souhlas

Souhlas – jakýkoli **svobodný, konkrétní, informovaný a jednoznačný projev vůle**, kterým subjekt údajů dává **prohlášením či jiným zjevným potvrzením své svolení** ke zpracování svých osobních údajů (čl. 4 odst. 11 GDPR):

- **svobodný projev vůle** – ničím nepodmíněný členěný souhlas, který není učiněn pod tíhou jakékoli negativní hrozby, mezi rovnými stranami (není vhodné pro orgány moci veřejné a zaměstnavatele)
- **konkrétní projev vůle** – učiněný pro konkrétní účel
- **informovaný projev vůle** – před jeho poskytnutím musel být subjekt poučen podle čl. 12 GDPR v rozsahu dle čl. 13 GDPR
- **jednoznačný projev vůle** – souhlas učiněný prohlášením nebo jiným zjevným potvrzením, musí jít o komisivní právní jednání (aktivní jednání)

Svobodný souhlas

- souhlas nesmí být udělen pod nátlakem, zastrašováním či klamáním
- **souhlas zaměstnance je vždy spojen s rizikem, a proto na něj ve většině případů hledíme jako na nesvobodný**, např. souhlas se sledováním aktivity na počítači – viz stanovisko WP29 č. 15/2011 k definici souhlasu (s. 13)
- **pro orgány moci veřejné není souhlas nikdy vhodný** (bod 43 odůvodnění GDPR) – stát by měl využívat jiné právní tituly
- **nepodmíněný souhlas** – uzavření určité smlouvy či poskytnutí určité služby nesmí být podmíněno udělením souhlasu (čl. 7 odst. 4 GDPR) – např. banka sdělí zájemci o úvěr, že musí poskytnout souhlas pro marketingové účely, jde o zakázanou **praktiku „take it or leave it“**
- **hromadný souhlas je také považován za nesvobodný**, protože subjekt musí dát souhlas ke všem operacím, ačkoli by rád povolil jen některé operace zpracování – mělo by se jednat o tzv. **členěný souhlas** (**granular consent**) – viz stanovisko WP29 č. 2/2013 k aplikacím na chytrých zařízeních (s. 15)

Svobodný souhlas

bod 43 recitálu

S cílem zajistit, aby byl souhlas svobodný, by vyjádření souhlasu nemělo představovat platný právní důvod pro zpracování osobních údajů ***ve zvláštním případě, kdy mezi subjektem údajů a správcem existuje jasná nerovnováha, zejména pokud je správce orgánem veřejné moci, a je tedy nepravděpodobné, že za všech okolností této konkrétní situace byl souhlas udělen svobodně****. Lze předpokládat, že souhlas* ***není svobodný, není-li možné vyjádřit samostatný souhlas s jednotlivými operacemi zpracování osobních údajů****, i když je to v daném případě vhodné, nebo je-li plnění smlouvy, včetně poskytnutí služby učiněno závislým na souhlasu, i když to není pro toto plnění nezbytné.*

Konkrétní souhlas

- souhlas udělený pro **konkrétní účel**
- účel musí být navíc **legitimní**; není možné souhlas s čímkoli

PŘÍKLADY PŘÍLIŠ OBECNÝCH SOUHLASŮ:

- „souhlasím se zpracováním těchto údajů“
- „souhlasím se zpracováním těchto údajů pro všechny účely“
- „souhlasím se zpracováním těchto údajů pro všechny legitimní účely“
- „souhlasím se zpracováním těchto údajů pro marketingové účely“ – stále příliš obecné (viz stanovisko WP29 č. 15/2011 k definici souhlasu, s. 17)

Informovaný souhlas

- před poskytnutím souhlasu musel být subjekt poučen podle čl. 12 GDPR v rozsahu dle čl. 13 GDPR
- poučení musí být učiněno **stručným, transparentním, srozumitelným a snadno přístupným způsobem** za použití jasných a jednoduchých jazykových prostředků

Minimální rozsah poučení:

- totožnost a kontaktní údaje správce, případného zástupce a případného pověřence pro ochranu osobních údajů;
- účely zpracování, pro které jsou osobní údaje určeny, a informace o tom, zde jde o zpracování na základě souhlasu
- poučení o právu kdykoli odvolat souhlas a o tom, že odvolání souhlasu nemá zpětné účinky a nedopadá na zpracování, které již proběhlo
- případní příjemce nebo kategorie příjemců osobních údajů a případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci

Jednoznačný souhlas

- souhlas může být stále učiněn v **písemné, ústní či konkludentní formě**
- souhlas musí být učiněn **komisivním právním jednáním** (aktivitou), nikoli omisivním právním jednání (pasivitou, mlčením)
- prohlášení o souhlasu by mělo vyhovovat podmínkám **směrnice č. 93/13/EHS o nepřiměřených podmínkách ve spotřebitelských smlouvách** – srozumitelné a snadno přístupné znění; např. souhlas není zahrnut v obchodních podmínkách
- např. vyplnění e-mailu do kolonky vedle textu „přihlaste se k zasílání novinek o našich produktech“ lze dovodit, že byl dán platný souhlas, byť konkludentním jednáním (poskytnutím e-mailové adresy), byť slovo „souhlas“ ani „osobní údaj“ nikde nebylo zmíněno
- **prokázání uděleného souhlasu** – správce musí být po celou dobu zpracování prokázat udělení souhlasu

Jednoznačný souhlas

PŘÍKLADY PLATNÉHO SOUHLASU:

- podepsání souhlasu v listinné podobě (ideálně na samostatné listině)
- zaškrtnutí políčka na webu
- kliknutí na souhlasné tlačítko
- výběr „ano/ne“ v dotazníku
- vyjádření vůle v e-mailu

PŘÍKLADY NEPLATNÉHO SOUHLASU:

- souhlas udělený mlčením
- předem zaškrtnuté políčko na webu
- zahrnutí souhlasné formulace do obchodních podmínek

Prokázání uděleného souhlasu

Správce musí prokázat:

- **kdo souhlas udělil** – jméno subjektu nebo jiný identifikátor (uživatelské jméno, IP adresa)
- **kdy byl souhlas udělen** – kopie datovaného dokumentu, elektronický záznam obsahující časovou známku
- **o čem byl subjekt před poskytnutím souhlasu informován** – ideálně kopie prohlášení o souhlasu vč. podmínek ochrany osobních údajů s vlastnoručně napsaným textem „byl jsem poučen a poučením rozumím“
- **jak byl souhlas udělen** – kopie listinného prohlášení, elektronický záznam (pomocí logů či příznaků v databázi)
- **údaj o tom, zda byl souhlas odvolán**

Prokázání uděleného souhlasu v elektronické komunikaci

- otázkou zůstává, nakolik je v elektronické komunikace možné udělení souhlasu vůbec prokázat – málokdo totiž využívá takové technologie, které jsou schopny **přesné identifikace subjektu údajů**
- prostředky elektronické identity upravuje **nařízení eIDAS** – nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- jedním z cílů nařízení eIDAS je odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci, které se v členských státech používají k autentizaci, alespoň pro účely veřejných služeb
- nařízení vytvořilo **standardy pro elektronické podpisy, kvalifikované digitální certifikáty, elektronické pečeti, časová razítka a další způsoby ověření autentizačních mechanismů**

Regulované aspekty elektronických transakcí dle eIDAS

Nařízení vytváří právní prostředí pro následující důležité aspekty elektronických transakcí:

- **zaručený elektronický podpis** - elektronický podpis se považuje za zaručený, pokud splňuje požadavky směrnice, tj. poskytuje jedinečné identifikační údaje, které ho spojují s podepisující osobou. Podepisující osoba má výlučnou kontrolu nad údaji použitými pro vytvoření elektronického podpisu a musí být schopna rozpoznat případnou změnu dat provedenou po podpisu.
- **Certifikát pro elektronický podpis** - elektronický doklad potvrzuje totožnost uživatele a spojuje data, která potvrzují platnost elektronického podpisu s danou osobou. Zaručené elektronické podpisy mohou být technicky realizovány v návaznosti na normu XAdES, PAdES nebo CAdES pro digitální podpisy, které byly specifikovány organizací ETSI.
- **Uznávaný elektronický podpis** - zaručený elektronický podpis, který využívá digitální certifikát a byl zašifrován pomocí zařízení pro tvorbu bezpečnostního podpisu.
- **Kvalifikovaný digitální certifikát pro elektronický podpis** - potvrzení o pravosti uznávaného elektronického podpisu, které bylo vydáno kvalifikovaným poskytovatelem důvěryhodných služeb.
- **Důvěryhodná služba** - elektronická služba, která vytváří, potvrzuje a ověřuje elektronické podpisy, časová razítka, pečetě a certifikáty. Důvěryhodná služba nadto může ověřovat webové stránky a uchovávat vytvořené elektronické podpisy, certifikáty a pečeti. Službu zajišťuje certifikační autorita.

Prokázání uděleného souhlasu v elektronické komunikaci

Autoři komentářové literatury se přiklánějí k názoru, že **prozatím není nutné souhlas prokazovat prostředky, které vyžaduje eIDAS**. Postačí pouhé uložení kopie e-mailu, což se ovšem v budoucnu zřejmě ukáže nedostatečné a je třeba se připravit na změnu právní praxe, která nejspíše přijde.

Odvolání souhlasu

- **souhlas je nestabilní** – proto by neměl být ústředním titulem pro zpracování osobních údajů
- po odvolání souhlasu odpadá právní titul ke zpracování a subjektu ihned vzniká **právo na výmaz** (čl. 17 GDPR) – některé údaje však správce může zpracovávat dále na základě jiných právní titulů (typicky e-mail na základě oprávněného zájmu spočívajícím v marketingu)
- osobní údaje je nutné **zcela zlikvidovat** – vymazat v archivech, zničit všechny kopie, odstranit je ve veškeré komunikaci, na všech cloudech, ve všech zálohách, …
- odvolání souhlasu musí být **stejně snadné jako jeho poskytnutí** – před odvoláním souhlasu je ovšem nutné subjekt **identifikovat** (viz identifikace při uplatňování práv)
- **odvolání souhlasu nemá zpětné účinky** a nedopadá na zpracování, které již proběhlo – nebude tak nutné mazat údajů u příjemců, kterým již byly poskytnuty v souladu s uděleným souhlasem

Platnost „starých“ souhlasů

- správci se budou moci na souhlasy získané před účinností GDPR spoléhat jen tehdy, splňují-li přísnější podmínky nově nastavené dle GDPR
- audit osobních údajů by tedy měl zahrnovat tzv. **prověrku souhlasů**
- souhlas je vždy nutné zkoumat z **časového a kontextuálního hlediska** – souhlas „Chci dostávat módní tipy pro léto 2018“ byl udělen skutečně jen pro léto 2018, na podzim již nebude platný; zaslání životopisu je účinné pouze po dobu, dokud se výrazně nezmění sociální poměry (cca 6 měsíců)

Souhlas vs. oprávněný zájem

	VÝHODY	NEVYHÝODY
souhlas	možné zpracovávat prakticky cokoli	přísné podmínky snadná odvolatelnost nutnost prokázat jej
oprávněný zájem	zákonnost zpracování až do sdělení námitky, poté rozhoduji opět sám	potřeba definovat zájem test oprávněnosti

Souhlas dítěte

- v případě souhlasu v souvislosti s **nabídkou služeb informační společnosti přímo dítěti**, je zpracování osobních údajů dítěte zákonné, je-li dítě ve věku nejméně 16 let
- je-li **dítě mladší 16 let**, je takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti
- správce musí vyvinout **přiměřené úsilí s ohledem na dostupnou technologii**, aby ověřil, že byl souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti
- členské státy se od této právní úpravy mohou odchýlit – **Česká republika navrhuje snížení věku na 13 let**

Právní jednání dítěte

- GDPR se nijak nedotýká občanskoprávní úpravy jednání dítěte - čl. 9 odst. 1, 2 GDPR není dotčeno obecné smluvní právo členských států, například pravidla týkající se platnosti, uzavírání nebo účinků smlouvy vzhledem k dítěti
- vždy je tedy nutné zohledňovat **rozumovou a mravní vyspělost dítěte** jako kritérium při posuzování svéprávnosti dítěte (§ 31 občanského zákoníku)

Další zpracování

- **zásada účelového omezení** – stěžejní zásada, účel je alfou a omegou zpracování; zpracování je možné pouze pro předem stanovené určité, výslovně vyjádřené a legitimní účely
- **prolomení zásady účelového omezení** – výjimkou ze zásady účelového omezení je tzv. **další zpracování**, tj. zpracování za jiným účelem než byl původní účel

Další zpracování je možné ve čtyřech případech:

- na základě **výslovného souhlasu** k dalšímu zpracování
- zpracování pro účely **archivace ve veřejném zájmu**, pro účely **historického výzkumu** či pro **statistické účely** v souladu s čl. 89 odst. 1 GDPR
- **zpracování, které je povoleno právem EU nebo členského státu** (dle čl. 23 odst. 1 GDPR)
- v případě provedení **posouzení slučitelnosti**, kdy nový účel navazuje na původní (čl. 6 odst. 4 GDPR) – typickým příkladem je anonymizace

DŮLEŽITÉ

Posouzení slučitelnosti

Správce musí zohlednit, zda je **zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny**, což zahrnuje posoudit:

- **vazbu mezi účely** – nový účel by měl logicky navazovat na původní účel (uchovávání údajů ze smluv, zpracovaných na základě titulu plnění smlouvy, po splnění smlouvy pro případné budoucí soudní spory z těchto smluv, což je zpracování na základě oprávněného zájmu)
- **vztah mezi subjekty údajů a správcem** – zkoumáme zejména legitimní očekávání; tedy to, co mohou subjekty údajů od správce legitimně očekávat,
- **povahu osobních údajů** – zejména zda jsou citlivé osobní údaje čl. 9 nebo 10 GDPR či citlivé osobní údaje ve smyslu materiálním (lokalizační údaje, údaje finanční situaci, …)
- **možné důsledky zamýšleného dalšího zpracování** pro subjekty údajů – pokud pro ně má mát pouze pozitivní důsledky, je další zpracování zpravidla možné (např. prodejce aut zjistí vážnou vadu a dojde ke zkontaktování vlastníků pomocí veřejného registru vozidel)
- **existenci vhodných záruk –** zejména šifrování nebo pseudonymizaci

Právo na informace v souvislosti s dalším zpracováním

Při dalším zpracování je nutné myslet na následující práva:

- **právo na informace dle čl. 13 odst. 3 GDPR** – další zpracování, pokud byly údaje získány od subjektu údajů a nyní se mění účel
- **právo na informace dle čl. 14 odst. 4 GDPR** – další zpracování za situace, kdy údaje nebyly získány od subjektu údajů
- sdělení musí naplňovat **formální požadavky dle čl. 12 odst. 1 GDPR**

GDPR: **PRÁVA SUBJEKTŮ ÚDAJŮ**

Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

Čl. 12 – 22 GDPR

LEKCE Č. 5

Subjekt údajů

- **subjekt údajů** – fyzická osoba, k níž se osobní údaje vztahují
- za subjekt údajů **nepovažujeme právnické osoby ani zvířata**, naopak fyzické osoby podnikající za subjekt údajů obecně považujeme

Právo ochrany osobních údajů je provedením **základního lidského práva na soukromí**, a proto svědčí pouze živým bytostem.

Subjektu údajů svědčí **katalog základních práv** v souvislosti se zpracováním jeho osobních údajů.

KLÍČOVÝ POJEM

Právnické osoby a podnikatelé

- **bod 14 odůvodnění GDPR** – ochrana poskytovaná GDPR by se měla týkat zpracování osobních údajů fyzických osob bez ohledu na jejich státní příslušnost nebo bydliště; GDPR se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně **názvu**, **právní formy** a **kontaktních údajů právnické osoby**
- e-mail **prijmeni@firma.cz** je však již údajem fyzické osoby, protože dle něj je fyzická osoba přímo dohledatelná; adresa **info@firma.cz** však již ochrany nepožívá
- **podnikající fyzické osoby** – dle nálezu ÚS sp. zn. Pl. ÚS 38/92 jim ochrana není poskytována, ale tento nález je nutné považovat za překonaný s ohledem na úvodní body GDPR, což odpovídá stanovisku ÚOOÚ č. 3/2011 i rozsudku ESLP ve věci Amann proti Švýcarsku; podnikající fyzické osoby tedy také požívají ochrany

Zesnulé a dosud nenarozené osoby

- **bod 27 odůvodnění GDPR** – GDPR se nevztahuje na osobní údaje **zesnulých osob**; členské státy mohou stanovit pravidla týkající se zpracování osobních údajů zesnulých osob
- ochrana **dosud nenarozených lidí** je v kompetenci národních států (stanovisko WP29 č. 4/2007, WP136, s. 23) – v ČR dle ustanovení § 25 obč. zák. nenarozené dítě ochrany požívá, narodí-li se živé
- údaj o zesnulém ovšem může být zároveň údajem o živé osobě (např. údaj o chorobě, jež se dědí; údaj o pozůstalých na smutečním oznámení)
- soukromoprávní úprava je zcela odlišná – **postmortální ochrana osobnosti**

Katalog práv dle GDPR

- **práva spojená s procesem** – právo na vyřízení žádostí dle předem stanovených pravidel a zásad slušnosti (čl. 12 GDPR)
- **právo být informován** – právo na informace o zpracování, opravných prostředích, poučení o dalších právech (čl. 13, 14 GDPR)
- **právo na přístup k údajům** – právo na sdělení osobních údajů, které se mě týkají (čl. 15 GDPR)
- **právo na opravu** – oprava nepřesných údajů a doplnění chybějících údajů (čl. 16 GDPR)
- **právo na výmaz** – tzv. právo být zapomenut (čl. 17 GDPR)
- **právo na omezení zpracování** – možnost subjektu, aby po určitou dobu probíhalo zpracování omezeným způsobem (čl. 18, 19 GDPR)
- **právo na přenositelnost** – právo na portabilitu je zcela novým institutem (čl. 20 GDPR)
- **právo vznést námitku** – možnost ukončit zpracování v určitých případech (čl. 21 GDPR)
- **právo nebýt předmětem pouhého automatizovaného rozhodování** – zavádí se povinnost, aby o právech subjektů údajů v poslední stupni rozhodovali žijící lidé, nikoli stroje (čl. 22 GDPR)

DŮLEŽITÉ

Stručná kategorizace práv dle GDPR

Jednotlivá práva můžeme rozdělit do následujících oblastí:

- **informace a přístup k osobním údajům** – práva spojená s procesem, informace a právo na sdělení osobních údajů, které se mě týkají (čl. 12 – 15 GDPR)
- **oprava, výmaz a omezení zpracování** – oprava nepřesných údajů, doplnění chybějících údajů, právo být zapomenut a právo dočasně pozastavit zpracování (čl. 16 – 19 GDPR)
- **přenositelnost osobních údajů** – právo na portabilitu je zcela novým institutem (čl. 20 GDPR)
- **námitka proti zpracování** – možnost ukončit zpracování v určitých případech (čl. 21 GDPR)
- **automatizované rozhodování a profilování** – zavádí se povinnost, aby o právech subjektů údajů v poslední stupni rozhodovali žijící lidé, nikoli stroje (čl. 22 GDPR)

INFORMACE A PŘÍSTUP K OSOBNÍM ÚDAJŮM

Transparentnost a postupy

- **forma komunikace** – čl. 12 odst. 1 GDPR, stručný, transparentní, srozumitelný a snadno přístupný způsob získat **informace dle čl. 13 až 22 a 34 GDPR**
- **podmínky ochrany osobních údajů** (privacy policy, zásady ochrany osobních údajů, pravidla ochrany osobních údajů) – dokument, který je zpravidla na webu, kde správce uvádí všechny informace, které musí sdělovat (správce musí důkaz o tom, že tuto povinnost splnil; viz čl. 24 odst. 1 GDPR)
- **zavedení standardizovaných ikon** – zatím nejsou zavedeny
- **výkon práv subjektů** – ideálně všemi kanály (poštou, formulářem, e-mailem, osobně na pobočce, …); ústní forma jen tehdy, prokáže-li se subjekt svou identitu; správce by měl stanovit pravidla identifikace osob (dle míry rizika)
- **bezplatný výkon práv** – informace se poskytují zásadně bezplatně; výjimku stanoví čl. 15 odst. 3 GDPR (poplatek by měl vyměřen předem) a čl. 12 odst. 5 (nepřiměřené nebo zjevně nedůvodné žádosti; tzv. obstrukční žádosti)

Jak mají vypadat podmínky ochrany osobních údajů?

- **využívání hypertextových odkazů** – rozklikávací nabídky
- **psaní jednoduchým jazykem** – „vy máte toto právo, my máme tuto povinnost“
- **metoda otázek a odpovědí** – „K čemu potřebujeme tyto údaje? Abychom mohli zajistit síťovou bezpečnost, potřebujeme znát vaši IP adresu.“
- **vizualizace a infografiky**
- **zásada nezbytnosti** – informování až v momentu, kdy je to nezbytné; při podpisu smlouvy o účtu není nutné řešit zpracování údajů souvisejících služeb, např. při žádosti o úvěr, popř. při prvním přihlášení do elektronického bankovnictví
- **vrstvené podmínky ochrany** – krátké oznámení (1. vrstva), stručné oznámení (2. vrstva), plné oznámení (3. vrstva, může být více přesná a technická)

Průběh vyřizování žádostí subjektů

- **lhůta „bez zbytečného odkladu“** – primárně jde o lhůtu „bez zbytečného odkladu“, maximálně 1 měsíc; výjimečně (z důvodu množství žádostí od konkrétního žadatele) ji lze prodloužit o dva měsíce
- **informace o odmítnutí žádosti** musí být vždy poskytnuta do 1 měsíce – není možné ji prodloužit
- při **odmítnutí žádosti** musí být subjekt informován o **možnosti podat stížnost k Úřadu pro ochranu osobních údajů** (dle čl. 77 GDPR) a **možnosti soudního přezkumu** (čl. 79 GDPR)

SPRÁVCE TEDY MÁ V ZÁSADĚ POUZE TŘI MOŽNOSTI (DO JEDNOHO MĚSÍCE):

- **žádosti vyhovět**, provést nutná opatření a subjekt o nich informovat
- **žádost odmítnout**, poučit subjekt údajů o důvodech odmítnutí a možnosti opravných prostředků
- **prodloužit lhůtu o dva měsíce** s tím, že žádosti již bude muset být vyhověno

DŮLEŽITÉ

Zjevně nedůvodné nebo nepřiměřené žádosti

- ochrana před **obstrukčními žádostmi** (zjevně nedůvodné nebo nepřiměřené žádosti)
- zjevnou nedůvodnost nebo nepřiměřenost žádosti **dokládá správce**
- v praxi se jedná zejména o stále se **opakující žádosti**

V PŘÍPADĚ OBSTRUKČNÍ ŽÁDOSTI MŮŽE SPRÁVCE:

- **uložit přiměřený poplatek zohledňující administrativní náklady** spojené s poskytnutím požadovaných informací
- **žádost odmítnout**

Identifikace subjektu údajů

- při uplatňování práv je vždy nutné **subjekt nejprve identifikovat**
- **požadovaná důvěryhodnost ověření totožnosti** by měla odpovídat **míru rizika** (čl. 24 odst. 1 GDPR) – u potvrzení správnosti údajů je vždy riziko nižší než u sdělení údajů
- je vhodné, aby správce již při sběru údajů určil **identifikátory, jejichž doložení bude při výkonu práv požadovat** (toto by se mělo objevit též v zásadách osobních údajů), např. konkrétní e-mailová adresa, ze které může být žádost zaslána, popř. další ověřovací procesy (kontrolní otázky, hesla, …)
- **přísnější podmínky** – předložení dokladu totožnosti či zaručeného, uznávaného nebo kvalifikovaného elektronického podpisu
- **nedostatečná identifikace** – správce informuje subjekt a vyžádá si další údaje (čl. 11 odst. 2 GDPR, čl. 12 odst. 6 GDPR)

Různé druhy identifikace subjektu údajů

IDENTIFIKACE DLE GDPR

- čl. 11, 12 odst. 6 GPDR – postačí údaje dle míry rizika

IDENTIFIKACE DLE ZÁKONA PROTI PRANÍ ŠPINAVÝCH PENĚZ

- ustanovení § 5 zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu – daleko **přísnější požadavky**
- u **fyzické osoby** vyžaduje všechna jména a příjmení, rodné číslo, a nebylo-li přiděleno, datum narození, dále místo narození, pohlaví, trvalý nebo jiný pobyt a státní občanství; jde-li o podnikající fyzickou osobu, též její obchodní firma, odlišující dodatek nebo další označení, místo podnikání a identifikační číslo osoby
- vyžaduje se po **bankách**, **advokátech**, **notářích**, ale třeba i dle § 31 odst. 4 zákona o živnostenském podnikání (**nákup použitého zboží** nebo **zboží bez dokladu**, **nabytí kulturních památek nebo předmětů kulturní hodnoty**, přijímání tohoto zboží do zástavy nebo zprostředkování jeho nákupu či přijetí do zástavy)

Informace a přístup k osobním údajům

- **informace poskytované v případě, že osobní údaje jsou získány od subjektů údajů** – čl. 13 GDPR
- **informace poskytované v případě, že osobní údaje nebyly získány od subjektů údajů** – čl. 14 GDPR
- **přístup k osobním údajům** – čl. 15 GDPR

Nelze neinformovat subjekt jen z toho důvodu, že povinnost zpracovávat informace je stanovena zákonem [čl. 14 odst. 5 písm. a) a c) GDPR].

Právo na informace u původního správce

- **právo na informace dle čl. 13 GDPR** – informace poskytované v případě, že osobní údaje jsou získány od subjektů údajů, a to jakoukoli formou (ústně, písemně, přes formulář, elektronicky, v průběhu lékařské prohlídky, …); hovoříme o tzv. **původním (prvotním) správci**
- informace se poskytují písemně nebo ústně, ale jejich poskytnutí musí správce vždy prokázat
- ke splnění povinnosti musí dojít **nejpozději při poskytování informací** (např. při vyplňování formuláře, nikoli při jeho přijetí správcem, byl-li např. odeslán poštou)
- informační povinnost je **vždy nutné splnit na daném formuláři**, např. na prezenční listině, či **při daném jednání předáním informací písemně**
- z důvodu právní jistoty je vhodné tuto povinnost plnit i v zásadách ochrany osobních údajů

Obsah informační povinnosti původního správce

- **kontaktní údaje** – totožnost a kontaktní údaje správce, jeho případného zástupce a případného pověřence pro ochranu osobních údajů
- **účel a právní základ zpracování** – právní základem se rozumí právní titul dle čl. 6 GDPR a případně zvláštní důvod pro zpracování dle čl. 9 GDPR
- **oprávněný zájem** – pouze v případě, že je zpracování založeno na oprávněném zájmu dle čl. 6 odst. 1 písm. f) GDPR; v tomto případě je rovněž nutné **poučit o právu vznést námitku** dle čl. 21 odst. 4 GDPR, a to odděleně od ostatních informací
- **příjemci osobních údajů** – pokud se předpokládá poskytnutí příjemci, nikoli zpracovateli, pak je nutné sdělit daného příjemce či jeho kategorii, např. orgány činné v trestním řízení, banky, obchodní partneři
- **předávání do zahraničí** – úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně (v případě USA se jedná o EU – U.S. Privacy Shield) nebo odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny

Rozšířená informační povinnost původního správce

Je-li to nezbytné pro zajištění **spravedlivého a transparentního zpracování** (zejména při automatizovaném zpracování, v případě dětí či slabší smluvní strany) a v **případě dalšího zpracování** je nutné doplnit také následující informace:

- **doba zpracování** – doba, po kterou budou osobní údaje uloženy, popř. kritéria použitá pro její stanovení
- **poučení o právech** – poučení o právu na přístup, opravu, výmaz, omezení zpracování, právu vznést námitku, právu na přenositelnost údajů a **právu podat stížnost k Úřadu pro ochranu osobních údajů**
- **poučení o odvolatelnosti souhlasu** – pokud je zpracování založeno na čl. 6 odst. 1 písm. a) GDPR nebo čl. 9 odst. 2 písm. a) GPDR
- **důvod poskytnutí** – zda má subjekt údajů povinnost osobní údaje poskytnout a proč (zpracování je zákonným či smluvním požadavkem) a informace o možných důsledcích při neposkytnutí údajů
- **skutečnost, že dochází k automatizovanému rozhodování, včetně profilování** – nutné také uvést informace týkající se použitého postupu, významu a předpokládaných důsledků zpracování

Výjimky z informační povinnost původního správce

Původní správce nemusí informace poskytovat v tomto jediném případě:

- **subjekt údajů již uvedené informace má**

Nelze tedy neinformovat subjekt jen z toho důvodu, že povinnost zpracovávat informace je stanovena zákonem [čl. 14 odst. 5 písm. a) a c) GDPR]. Taková výjimka (navíc v omezeném rozsahu) je stanovena jen pro nepůvodní správce.

Právo na informace u nepůvodního správce

- **právo na informace dle čl. 14 GDPR** – informace poskytované v případě, že osobní údaje nebyly získány od subjektů údajů, tj. došlo-li k jejich získání např. nákupe, z veřejně dostupných zdrojů nebo při vyšetřování škodní události; hovoří o tzv. **nepůvodním správci**
- informace se poskytují písemně nebo ústně, ale jejich poskytnutí musí správce vždy prokázat; z důvodu právní jistoty je vhodné tuto povinnost plnit i v zásadách ochrany osobních údajů

LHŮTA PRO POSKYTNUTÍ INFORMACÍ:

- **osobní údaje určené pro komunikaci** (např. nákup e-mailů) – nejpozději při první komunikaci
- **osobní údaje určené pro příjemce** – nejpozději při předání příjemci
- **ostatní osobní údaje** – v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce

Obsah informační povinnosti nepůvodního správce

- **obsah základní informační povinnosti je stejný jako při získání údajů od subjektu údajů** (kontaktní údaje, účel a právní základ zpracování, oprávněný zájem a poučení o právu vznést námitku, příjemci osobních údajů, předávání do zahraničí)
- v případě rozšířené informační povinnosti je nutné uvést stejné informace jako u původního správce a navíc **informaci o zdroji údajů**
- v případě, kdy se změní účel u původního a nepůvodního správce, jde o tzv. **další zpracování** – vždy se pak poskytují rozšířené informace dle čl. 14 odst. 1, 2 GDPR

Výjimky z informační povinnost nepůvodního správce

Nepůvodní správce nemusí informace poskytovat v těchto případech:

- **subjekt údajů již uvedené informace má**
- **poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí** (zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely)
- **získávání nebo zpřístupnění je výslovně stanoveno právem Unie nebo členského státu, které se na správce vztahuje** a v němž jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektu údajů
- osobní údaje musí zůstat důvěrné s ohledem na **povinnost zachovávat služební tajemství** nebo s ohledem na **zákonnou povinnost mlčenlivosti** (advokáti, lékaři)

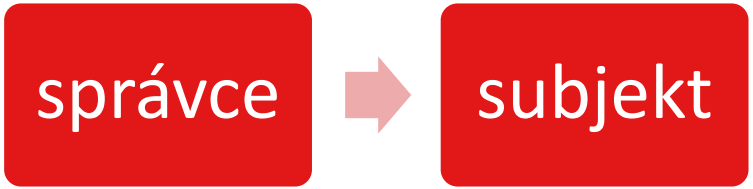
Obsah informační povinnosti při dalším zpracování

V případě **dalšího zpracování**, tedy při změně účelu, je nutné vždy sdělit následující informace:

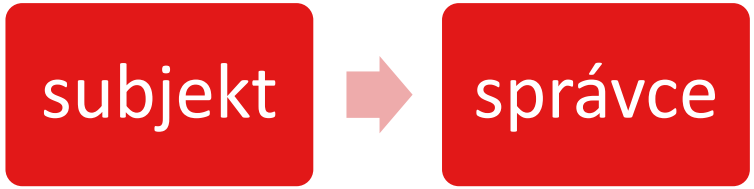
- **informace poskytované v případě, že osobní údaje byly původně získány od subjektů údajů** – nutné sdělit základní informace dle čl. 13 odst. 1 GDPR i rozšířené informace dle čl. 13 odst. 2 GDPR a rovněž informace o novém účelu
- **informace poskytované v případě, že osobní údaje nebyly původně získány od subjektů údajů** – nutné sdělit základní informace dle čl. 14 odst. 1 GDPR i rozšířené informace dle čl. 14 odst. 2 GDPR a rovněž informace o novém účelu

Právo na informace vs. právo na přístup

PRÁVO NA INFORMACE



PRÁVO NA PŘÍSTUP



Právo na přístup

- subjekt má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, **jsou či nejsou zpracovávány**, a pokud je tomu tak, má prá**vo získat přístup k těmto osobním údajům**
- správce je povinen zpřístupnit osobní údaje ve lhůtě dle čl. 12 GDPR (**30 dnů**)
- Ideální řešení spočívá v **přímém vzdáleném přístupu v zabezpečeném systému** (bod 63 odůvodnění GDPR) – nejde o právní povinnost
- **pokud správce zpracovává mnoho údajů, může po subjektu údajů požadovat, aby sdělil, které údaje požaduje** – právní na přístup však nemůže být omezeno, pokud subjekt svou žádost blíže nespecifikuje – poté se jí vyhoví v plném rozsahu

Poskytované informace v případě přístupu k osobním údajům

Při uplatnění práva na přístup má subjekt údajů právo na sdělení těchto dalších údajů:

- **účel zpracování** a **kategorie osobních údajů**
- **doba zpracování** – doba, po kterou budou osobní údaje uloženy, popř. kritéria použitá pro její stanovení
- **poučení o právech** – poučení o právu na opravu, výmaz, omezení zpracování, právu vznést námitku a **právu podat stížnost k Úřadu pro ochranu osobních údajů**
- **informace o zdroji osobních údajů** – v případě nepůvodního správce
- **skutečnost, že dochází k automatizovanému rozhodování, včetně profilování** – nutné také uvést informace týkající se použitého postupu, významu a předpokládaných důsledků zpracování
- **předávání do třetích zemí** – informace o vhodných zárukách podle čl. 46 GDPR, které se vztahují na předání

Kopie osobních údajů

- subjekt údajů má **právo na kopii zpracovávaných osobních údajů, které se ho týkají** – pojem má být vykládat **extenzivně**, např. informace od telefonního operátora o všech hovorech, jejich délce, začátku a konci a číslu, na které volal
- **forma kopie** – jestliže je žádost podána elektronicky, poskytnou se informace v elektronické formě, pokud subjekt údajů výslovně nepožádá o jiný způsob
- **(technický) formát kopie** – kopie musí být v „běžně užívaném formátu“, nemusí jít nutně o „strukturovaný a strojově čitelný formát“ (viz právo na portabilitu)
- **bezplatnost** – první kopie se poskytuje zdarma, za další kopie (na žádost subjektu údajů) může správce účtovat přiměřený poplatek na základě administrativních nákladů
- **ochrana práv třetích osob** – právem získat kopii nesmějí být nepříznivě dotčena práva a svobody jiných osob (ochrana obchodního tajemství, duševní vlastnictví, snímky jiných osob ze záznamů z kamer, … - viz bod 63 odůvodnění GDPR)

OPRAVA, VÝMAZ A OMEZENÍ ZPRACOVÁNÍ

Právo na opravu

Právo na opravu zahrnuje dvě dílčí práva:

- **právo na opravu nepřesných osobních údajů** – projev zásady přesnosti; do doby než správce přesnost ověří, tj. zpravidla do 30 dnů, musí být zpracovaní omezeno (o ukončení omezení je nutné subjekt informovat)
- **právo na doplnění neúplných osobních údajů** – s přihlédnutím k účelům zpracování má subjekt údajů právo na poskytnutí dodatečných osobních údajů, které bude muset správce začít zpracovávat

Právo na výmaz

- právo být zapomenut (právo na výmaz) se vyvinulo soudním výkladem v květnu 2014, kdy SDEU vydal přelomové rozhodnutí ve věci C 131/12 **Google Spain SL, Google Inc. proti Agencia Espoñola de Protección de Datos (AEPD), Mario Costeja González**
- v návaznosti na tuto kauzu Google zavedl specializovaný webový formulář, pomocí kterého mohou subjekty žádat o právo na výmaz
- SDEU stanovil zároveň **limity tohoto práva ve vztahu k veřejným rejstříkům** – veřejný zájem je zde natolik silný, že se zde toto právo vůbec neuplatní
- toto právo se **neuplatňuje nutně na žádost subjektu údajů**, ale tato povinnost platí „sama od sebe“ – správce musí sám údaje **pravidelně mazat**

Podmínky uplatnění práva na výmaz

- osobní údaje **již nejsou potřebné pro účely, pro které byly shromážděny**
- subjekt údajů **odvolá souhlas**, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) GDPR zpracovány, a neexistuje žádný další právní důvod pro zpracování – souhlas není možné následně měnit na oprávněný zájem (zákaz obcházení zákona)
- subjekt údajů vznese **námitky proti zpracování podle čl. 21 odst. 1 GDPR a neexistují žádné převažující oprávněné důvody** – právo na soukromí převáží nad oprávněným zájem
- subjekt údajů vznese **námitky proti zpracování podle čl. 21 odst. 2 GDPR** – oprávněný zájem, který spočívá v přímém marketingu
- osobní údaje byly **zpracovány protiprávně**, tj. neexistuje žádný právní titul
- osobní údaje musí být vymazány ke **splnění právní povinnosti stanovené v právu Unie nebo členského státu**, které se na správce vztahuje
- osobní údaje byly **shromážděny v souvislosti s nabídkou služeb informační společnosti dítěti** podle čl. 8 odst. 1 GDPR – právo na výmaz platí i poté, co subjekt údajů věk dítěte již překročil

Výjimky z uplatnění práva na výmaz

Právo na výmaz **není absolutním právem**. V těchto situacích se neuplatní:

- **výkon práva na svobodu projevu a práva na informace** – široké uplatnění této výjimky se najde v žurnalistice (viz čl. 85 GDPR)
- **splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu**, které se na správce vztahuje
- **splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci**, kterým je správce pověřen
- **veřejný zájem v oblasti veřejného zdraví** v souladu s čl. 9 odst. 2 písm. h) a i) GDPR a čl. 9 odst. 3 GDPR
- **archivace ve veřejném zájmu**, **vědecký či historický výzkum**, **statistické účely** (v souladu s čl. 89 odst. 1 GDPR)
- **určení, výkon nebo obhajoba právních nároků**

Provedení výmazu

- **výmaz musí být učiněn formou likvidace a dalšího nezpracovávání**, anonymizaci považujeme naopak za další zpracování, které je ovšem – pokud je provedeno správně – vždy přístupné na základě oprávněného zájmu (je tedy možné také **anonymizovat**)
- subjekt údajů **nesmí být při výmazu podroben efektu Barbry Streisandové** (sociální fenomén, při němž pokus o skrytí či odebrání nějaké informace vede naopak k jejímu mnohem většímu rozšíření, obvykle na Internetu)
- jestliže správce osobní údaje **již zveřejnil**, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby **informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace**

Omezení zpracování

- **právo na omezení zpracování dle čl. 18 GDPR** se podobá staršímu právu na blokování
- omezením zpracování se rozumí **označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu** (čl. 4 odst. 3 GDPR)

Pokud bylo zpracování omezeno, připadá v úvahu pouze jejich **uložení**, pokud nejde o některý z těchto případů:

- zpracování se **souhlasem subjektu údajů**
- zpracování z důvodu **určení, výkonu nebo obhajoby právních nároků**
- zpracování z důvodu **ochrany práv jiné fyzické nebo právnické osoby**
- zpracování z důvodu **důležitého veřejného zájmu Unie nebo některého členského státu**

Důvody omezení zpracování

Správce musí omezení provést v těchto případech:

- subjekt údajů vznesl **námitku proti zpracování podle čl. 21 odst. 1 GDPR**, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů [čl. 18 odst. 1 písm. d) GDPR]
- **popření přesnosti osobních údajů** po dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit [čl. 18 odst. 1 písm. a) GDPR] – v praxi velmi častý případ u registrů dlužníků
- **správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků** [čl. 18 odst. 1 písm. c) GDPR]
- **zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů** a žádá místo toho o omezení jejich použití [čl. 18 odst. 1 písm. b) GDPR]

Způsoby omezení zpracování

PŘÍKLADY ZPŮSOBŮ OMEZENÍ (bod 67 odůvodnění GDPR)**:**

- dočasný přesun vybraných údajů do jiného systému zpracování
- znepřístupnění vybraných osobních údajů uživatelům
- dočasné odstranění zveřejněných údajů z internetových stránek

- v **systémech automatizovaného zpracování** by omezení zpracování mělo být v zásadě zajištěno technickými prostředky tak, aby se na osobní údaje již nevztahovaly žádné další operace zpracování a aby nemohly být změněny
- skutečnost, že zpracování osobních údajů je omezeno, by měla být **v systému jasně vyznačena**

Zrušení omezení zpracování

Subjekt údajů, který dosáhl omezení zpracování, musí být správcem **předem upozorněn na to, že omezení zpracování bude zrušeno**. To nastane v těchto případech:

- správce **provede opravu údajů, či odmítne opravu provést**
- správce **rozhodne o námitce proti zpracování dle čl. 21 odst. 1 GDPR**, tj. vyhoví jí, popř. ji zamítne
- na **žádost subjektu údajů, pokud bylo omezení prováděno na jeho příkaz** [dle čl. 18 odst. 1 písm. b) a c) GDPR]

Oznamovací povinnost vůči příjemcům

- správce **oznamuje jednotlivým příjemcům**, jimž byly osobní údaje zpřístupněny, **veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování** provedené v souladu s čl. 16, čl. 17 odst. 1 a čl. 18 GDPR, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí
- **příjemci** mají rovněž **povinnost údaje opravit, nikoli však již omezit či smazat** (tato otázka je ovšem zatím v praxi sporná)
- **povinnost sdělení totožnosti příjemců** – správce informuje subjekt údajů o příjemcích, kterým byly sděleny opravy, výmazy nebo omezení zpracování, pokud to subjekt údajů požaduje (pouze na žádost, do 30 dnů)
- **daňové, celní a některé další státní orgány** (orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, viz čl. 4 odst. 9 in fine GDPR) **se za příjemce nepovažují**

PŘENOSITELNOST OSOBNÍCH ÚDAJŮ

Právo na portabilitu

- **právo na přenositelnost (právo na portabilitu)** je skutečnou novinkou v právu ochrany osobních údajů; jde trochu o revoluci
- právo na přenositelnost má rozšířit možnosti převádění osobních údajů mezi správci (často mezi konkurencí) tím, že **usnadní přesouvání, kopírování a předávání osobních údajů**
- toto právo má **rozšířit soupeření mezi poskytovateli internetových služeb a služeb e-commerce** (veškeré obchodní transakce realizované za pomoci internetu a dalších elektronických prostředků)
- omezí se situace, kdy subjekt nezačne používat jinou službu jen z toho důvodu, že se mu nechce do ní převádět své osobní údaje, např. události v kalendáři či kontakty v mobilu

Podmínky výkonu práva na portabilitu

Subjekt má právo na portabilitu při současném splnění těchto podmínek:

- zpracování se provádí **automatizovaně**
- zpracování je založeno na **souhlasu** [čl. 6 odst. 1 písm. a) GDPR, čl. 9 odst. 2 písm. a) GDPR] nebo na základě titulu **plnění smlouvy** [čl. 6 odst. 1 písm. b) GDPR]
- jde o **osobní údaje, které subjekt správci sám poskytl** – jde tedy o původního správce – pojem je nutné vykládat široce (nepůjde jen o vyplněné formuláře, ale i o „nasbírané“ údaje, např. lokační údaje, počet přehrání určité skladby, srdeční tep zaznamenaný na náramku, …), nepůjde však o údaje již určitým tvůrčím algoritmem zpracované správcem (vyhodnocení kredibility, např. úvěruschopnosti, výběr nejvhodnější partnera na základě údaje na seznamce, hudební vkus a doporučované skladby)

Realizace práva na portabilitu

Právo na portabilitu lze realizovat dvěma způsoby:

- **právo získat údaje ve strukturovaném, běžně používaném a strojově čitelném formátu** a následně je sám předat jinému správci, aniž by tomu původní správce bránil
- **právo na přímé předání mezi správci** – právo to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné

Uplatnění práva na přenositelnost nemá vliv na ostatní práva. Přenesené osobní údaje tedy nemusí být smazány. Právo na přenositelnost v sobě tedy **implicitně neobsahuje právo na výmaz**. Nemá ani vliv na smluvní vztahy. Přenos údajů v sobě **nezahrnuje kompletní převod smluvního vztahu k novému poskytovateli služby**.

Strukturovaný, běžně používaný a strojově čitelný formát

- **strukturovaný, běžně používaný a strojově čitelný formát** – nikdy nepůjde o formát, který je spojen s vysokými náklady, obzvlášť za situace, kdy existuje levnější nebo bezplatná alternativa
- jde o **soubory** (otevřené, chráněné vlastnickým právem, formálně normalizované, či nikoli)
- právo na přenositelnost **by nemělo zakládat povinnost správců zavést nebo zachovávat technicky kompatibilní systémy zpracování** (bod 68 odůvodnění GDPR)

Ochrana práv třetích osob při přenosu osobních údajů

„V mnoha případech budou správci údajů zpracovávat informace obsahující osobní údaje několika subjektů údajů. Správci údajů by v těchto případech neměli přijímat příliš restriktivní výklad věty „osobní údaje, které se týkají subjektu údajů“. **Například telefonní hovory, interpersonální přenos zpráv nebo záznamy VoIP mohou zahrnovat (v historii účtu uživatele) údaje o třetích stranách zapojených do příchozích a odchozích hovorů.** Ačkoliv záznamy tedy budou obsahovat osobní údaje týkající se několika osob, uživatelé by měli být schopni tyto záznamy v návaznosti na žádost o přenositelnost údajů získat, jelikož tyto záznamy se (rovněž) týkají subjektu údajů. **Jsou-li však tyto záznamy následně předány novému správci údajů, tento nový správce údajů by je neměl zpracovávat pro žádný účel, kterým by byla nepříznivě dotčena práva a svobody třetích stran.**“

(stanovisko pracovní skupiny WP29 ze dne 13. 12. 2016 k právu na přenositelnost)

NÁMITKA PROTI ZPRACOVÁNÍ

Právo vznést námitku

GDPR rozlišuje čtyři druhy tzv. námitek proti zpracování:

- **námitka proti zpracování na základě oprávněného zájmu** dle čl. 6 odst. 1 písm. f) GDPR, včetně profilování založeného na oprávněném zájmu
- **námitka proti zpracování na základě veřejného zájmu** dle čl. 6 odst. 1 písm. e) GPDR, včetně profilování založeného na veřejném zájmu
- **námitka proti zpracování pro účely přímého marketingu** – jde rovněž o zpracování na základě oprávněného zájmu dle čl. 6 odst. 1 písm. f) GDPR, kdy tímto zájmem je přímý marketing
- **námitka proti zpracovávání pro účely vědeckého či historického výzkumu nebo pro statistické účely** podle čl. 89 odst. 1 GDPR

V případě zpracování na základě životně důležitého zájmu GDPR námitku nepřipouští, což je z ústavněprávního hlediska obhajitelné.

Forma námitka

- obecně pro formu námitky platí čl. 12 GDPR, tzn. námitku je možné uplatnit **různými způsoby, které snadno dostupné** – s uplatněním námitky tedy nesmí být spojeny vysoké náklady, není možné ji zpoplatnit
- v souvislosti s využíváním **služeb informační společnosti**, a aniž je dotčena směrnice 2002/58/ES, může subjekt údajů **uplatnit své právo vznést námitku automatizovanými prostředky pomocí technických specifikací** – jedná se např. o tlačítko „Nahlásit“ na Facebooku
- za námitku je možné také např. považovat **automatické způsoby vyjádření opt-outu**, jako např. u standardu Do-Not-Track od organizace W3C, který je dnes součástí většiny prohlížečů (nastavení zákazu cookies) – tento názor je zatím v praxi sporný

Rozhodnutí o námitce

Po podání námitky a před rozhodnutí je nutné **zpracování omezit** a následně do 30 dnů rozhodnout:

- **námitka proti zpracování na základě oprávněného nebo veřejného zájmu** – před rozhodnutím je nutné provést tzv. **test proporcionality** a „vybrat“ které právo je důležitější
- **námitka proti zpracování pro účely přímého marketingu** – vždy je třeba upřednostnit právo na soukromí
- **námitka proti zpracovávání pro účely vědeckého či historického výzkumu nebo pro statistické účely** podle čl. 89 odst. 1 GDPR – rovněž se provádí **test proporcionality**; pokud vymazání jednoho údaje statistiku neovlivní, je třeba soukromí upřednostnit, ale pokud by mohlo statistiku výrazně narušit, je možné, že se upřednostní narušení práva na soukromí

V případě zpracování na základě **životně důležitého zájmu GDPR** námitku nepřipouští, což je z ústavněprávního hlediska obhajitelné. Přednost má vždy ochrana života a zdraví.

Test proporcionality

Jde v podstatě o test oprávněnosti prováděný pro konkrétní případ dle tří kroků:

- **test vhodnosti** – zkoumá se, zdali je zájem schopen dosáhnout stanoveného cíle
- **test potřebnosti** – zkoumá se, zdali by stanoveného cíle nemohlo být dosaženo jinak, avšak bez zásahu do soukromí
- **test poměřování** – porovnáváme právo na soukromí a daný zájem, což spočívá ve zvažování empirických, systémových, kontextových i hodnotových argumentů

Poučovací povinnost o námitce

V případě možnosti podat **námitku proti zpracování na základě oprávněného nebo veřejného zájmu nebo pro účely přímého marketingu** je nutné subjekt údajů o tom **vždy speciálně poučit**.

čl. 21 odst. 4 GDPR

Subjekt údajů je na právo vznést námitku […] výslovně upozorněn a toto právo je uvedeno **zřetelně a odděleně od jakýchkoli jiných informací**, a to **nejpozději v okamžiku první komunikace se subjektem údajů**.

AUTOMATIZOVANÉ ROZHODOVÁNÍ A PROFILOVÁNÍ

Právo nebýt předmětem pouhého rozhodování strojů

- právní úprava se zabývá otázkou, kdy **o právech a povinnostech rozhoduje algoritmus** (předem stanovený automatizovaný postup)
- jde o první právní úpravu **regulace algoritmického rozhodování**, včetně **rozhodování umělou inteligencí**
- **automatizované individuální rozhodování** – rozhodování založené výhradně na automatizovaném zpracování, včetně profilování
- automatizované individuální rozhodování vytváří v současné době řadu právních otázek – je sporné, zda je obecně povoleno, či zakázáno

Právo nebýt předmětem pouhého rozhodování strojů

Právo nebýt předmětem rozhodování robotů – subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká

„Jednej tak, abys používal lidství jak ve své osobě, tak i v osobě každého druhého vždy zároveň jako účel a nikdy pouze jako prostředek.“

kategorický imperativ Immanuela Kanta

„Robot nesmí ublížit člověku nebo svou nečinností dopustit, aby bylo člověku ublíženo.“

první zákon robotiky dle Isaaca Asimova

Možnosti uplatnění rozhodování strojů – výkladový problém

Právo „nebýt předmětem rozhodování robotů“ se nacházelo již ve směrnici a bylo státy transponováno v podstatě dvěma způsoby:

- **generální zákaz automatizovaného individuální rozhodování s výjimkami** – ČR
- **obecné povolení automatizovaného individuální rozhodování s možností vznést námitku** – Velká Británie

- autoři praktického komentáře od Wolters Kluwer se přiklánějí k názoru, že jde o generální zákaz
- autor této prezentace se přiklání k opačnému názoru, tzn. že **o žádosti o práva je nutné postupovat podle čl. 12 GDPR**, ale **o námitce proti zpracování je možné rozhodovat automatizovaně** („v prvním kole“; nakonec vždy musí rozhodnout živá bytost, tedy ne-stroj)

Automatizované individuální rozhodování na základě profilování

Je nutné odlišovat profilování a automatizované rozhodování o právech na základě profilování:

- **profilování** obecně zakázáno v žádném případě není
- **automatizované rozhodování o právech na základě profilování** již ovšem vytváří stejnou otázkou – jde o generální zákaz s výjimka, anebo o obecné povolení s možností vznést námitku?

Autor této prezentace se opět přiklání k názoru, že **je možné rozhodovat automatizovaně na základě profilování**, ale vždy jen „v prvním kole“, protože to obecně není zakázáno. Subjekt má pouze „jen“ právo nebýt předmětem takového rozhodování v konečném důsledku. Nakonec tedy vždy musí rozhodnout živá bytost, tedy ne-stroj. Proti tomuto výkladu ovšem hovoří fakt, že **GDPR používá „právo nebýt předmětem rozhodování“, nikoli „právo nebýt předmětem rozhodnutí“**.

Příklady automatizovaného individuálního rozhodování na základě profilování

- posouzení úvěruschopnosti, např. stanovení výše spotřebitelského úvěru, kterou je možné získat bez doložení příjmů
- výpočet prémie zaměstnance softwarem, který hodnotí výkonnost, např. měří odvolané minuty v call-centru
- rozhodnutí o výmazu fotky ze sociální sítě na základě „skenu“ fotografie
- rozhodování o tom, která stránka se ve vyhledávači zobrazí jako první
- rozhodování o tom, komu se zobrazí status uživatele na Facebooku
- rozhodování obchodu o tom, kterému uživateli je zaslán katalog luxusnějších produktů na základě předchozích nákupů

Ne každé z těchto rozhodování je ovšem **rozhodování o právech a povinnostech**. Právo nebýt předmětem individuálního automatizovaného rozhodování se týká jen rozhodování o právech a povinnostech či s **významnými právními důsledky**. Zbylé příklady jsou jen **obyčejným profilováním**.

Příklady automatizovaného individuálního rozhodování na základě profilování

bod 71 recitálu GDPR

Subjekt údajů by měl mít **právo nebýt předmětem žádného rozhodnutí, a to včetně opatření, které hodnotí osobní aspekty týkající se jeho osoby, vychází výlučně z automatizovaného zpracování** a které má pro něj **právní účinky** nebo se jej **podobně významně dotýká**, jako jsou automatizované **zamítnutí on-line žádosti o úvěr nebo postupy elektronického náboru bez jakéhokoliv lidského zásahu**. Takové zpracování zahrnuje „profilování“, jehož podstatou je jakákoliv forma automatizovaného zpracování osobních údajů hodnotící osobní aspekty vztahující se k fyzické osobě, zejména za účelem **analýzy či předvídání aspektů souvisejících s pracovním výkonem subjektu údajů, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo chováním, místem pobytu či pohybu**, pokud má pro něj právní účinky nebo se jí podobným způsobem významně dotýká. […]

Příklady automatizovaného individuálního rozhodování na základě profilování

bod 71 recitálu GDPR

[…] **Rozhodování založené na takovém zpracování, včetně profilování, by však mělo být umožněno, pokud jej výslovně povoluje právo Unie nebo členského státu, které se na správce vztahuje, mimo jiné pro účely monitorování podvodů a daňových úniků** a jejich předcházení, jež jsou v souladu s předpisy, normami a doporučeními orgánů Unie nebo vnitrostátních dozorových úřadů, a s cílem zajistit bezpečnost a spolehlivost služby poskytované správcem, nebo pokud **je nezbytné pro uzavření nebo plnění smlouvy mezi subjektem údajů a správcem** nebo pokud k tomu subjekt údajů **dal svůj výslovný souhlas**. V každém případě by se na takové zpracování měly vztahovat vhodné záruky, které by měly zahrnovat konkrétní informování subjektu údajů a **právo na lidský zásah**, na vyjádření svého názoru, na získání vysvětlení o rozhodnutí učiněném po takovém posouzení a na napadnutí tohoto rozhodnutí. Toto opatření by se nemělo týkat dítěte. […]

Příklady automatizovaného individuálního rozhodování na základě profilování

bod 71 recitálu GDPR

[…] V zájmu zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů a s přihlédnutím ke konkrétním okolnostem a souvislostem, za kterých se dané osobní údaje zpracovávají, by měl správce použít **vhodné matematické nebo statistické postupy profilování**, zavést **technická a organizační opatření, která zejména zajistí opravu faktorů vedoucích k nepřesnosti osobních údajů a minimalizaci rizika chyb**, a zabezpečit osobní údaje takovým způsobem, který zohledňuje potenciální rizika pro zájmy a práva subjektu údajů a který mimo jiné **předchází diskriminačním účinkům vůči fyzickým osobám na základě rasy nebo etnického původu, politických názorů, náboženského vyznání nebo přesvědčení, členství v odborech, genetických údajů nebo zdravotního stavu či sexuální orientace** nebo předchází přijímání opatření, jež mají takové účinky. **Automatizované rozhodování a profilování založené na zvláštních kategoriích osobních údajů by mělo být povoleno pouze za určitých podmínek.**

Podmínky automatizovaného individuálního rozhodování

Automatizované individuální rozhodování (na základě profilování nebo i bez něj) je k každém případě **dovoleno v těchto případech** (čl. 22 odst. 2 GDPR):

- **automatizované individuální rozhodování nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů** – správce údajů musí zavést vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů
- **automatizované individuální rozhodování povolené právem Unie nebo členského státu**, které se na správce vztahuje a které rovněž stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů
- **automatizované individuální rozhodování založené na výslovném souhlasu subjektu údajů** – správce údajů musí zavést vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů

Podmínky automatizovaného individuálního rozhodování

Vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů v případě automatizovaného individuální rozhodování spočívají v následujícím:

- **právo obdržet lidský zásah ze strany správce**
- **právo vyjádřit svůj názor ohledně takového rozhodnutí**
- **právo napadnout dané rozhodnutí –** na toto rozhodování „v druhém kole“ se pak již uplatní čl. 12 GDPR (bezúplatné právo na vyřízení žádosti v 30denní lhůtě)

Rozhodnutí se musí opírat o následující:

- **vhodné matematické nebo statistické postupy**
- **technická nebo organizační opatření, která zajistí opravu faktorů vedoucích k nepřesnostem**

Automatizované individuálního rozhodování na základě citlivých osobních údajů

Ani povolená automatizovaná individuálního rozhodování dle čl. 22 odst. 2 GDPR se **nesmí opírat o zvláštní kategorie osobních údajů** (ve smyslu čl. 9 odst. 1 GDPR), vyjma těchto případů:

- automatizovaná individuálního rozhodování na základě čl. 9 odst. 2 písm. a) GDPR – **s výslovným souhlasem**
- automatizovaná individuálního rozhodování na základě čl. 9 odst. 2 písm. g) GDPR g) GDPR – **zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu**, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů

GDPR: SPRÁVCE OSOBNÍCH ÚDAJŮ A JEHO ODPOVĚDNOST

Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

Čl. 24 – 26 GDPR

LEKCE Č. 6

Správce

- správce je definován v čl. 4 odst. 7 GDPR

Rozlišujeme dva základní druhy správců:

- **správce určený účelem** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů
- **správce určený zákonem** – jsou-li účely a prostředky zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení

KLÍČOVÝ POJEM

Správce, zpracovatel a příjemce

- **správce** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který **sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů**; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení (čl. 4 odst. 7 GDPR)
- **zpracovatel** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který **zpracovává osobní údaje pro správce** (čl. 4 odst. 8 GDPR)
- **příjemce** – každá fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli; avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování (čl. 4 odst. 9 GDPR)

Společní správci

- GDPR zná nově institut tzv. **společných správce** – společní správci vymezují **účel zpracování společně**; společné správcovství nelze smluvně vyloučit, neboť jde o statusovou otázku
- **právní úprava vztahů mezi společnými správci** – společní správci mezi sebou musí transparentním ujednáním vymezit své podíly na odpovědnosti za plnění povinností dle GDPR, zejména pokud jde o výkon práv subjektu údajů, a své povinnosti poskytovat informace uvedené v čl. 13 a 14 GDPR
- v ujednání společných správců může být určeno **kontaktní místo pro subjekty údajů**
- právní účinky vůči subjektům – o ujednání musí být informován subjekt údajů, nicméně bez ohledu na podmínky ujednání může **subjekt údajů vykonávat svá práva u každého ze správců i vůči každému z nich**

Zástupci správců nebo zpracovatelů, kteří nejsou usazeni v Unii

- správce nebo zpracovatel se sídlem mimo EU v případě extrateritoriální působnosti GDPR, tzv. **zahraniční správce nebo zpracovatel**, musí **písemně jmenovat svého zástupce v EU**
- **zástupce** – jakákoli fyzická nebo právnická osoba usazená v EU, která je správcem nebo zpracovatelem určena písemně k tomu, aby správce nebo zpracovatele zastupovala, pokud jde o příslušné povinnosti správce nebo zpracovatele dle GDPR (čl. 4 odst. 17 GDPR)
- zástupce je **usazen v jednom z členských států**, ve kterém se vyskytují subjekty údajů, jejichž osobní údaje jsou zpracovávány v souvislosti s nabízeným zbožím či službami, nebo jejichž chování je monitorováno
- **na zástupce se mohou obracet dozorové úřady a subjekty údajů ohledně všech otázek** – tím není nijak dotčena odpovědnost správce nebo zpracovatel

VÝJIMKY Z POVINNOST JMENOVAT ZÁSTUPCE:

- zpracování, které je příležitostné, nezahrnuje, ve velkém měřítku, zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů a je nepravděpodobné, že by s ohledem na svou povahu, kontext, rozsah a účely představovalo riziko pro práva a svobody fyzických osob
- orgán veřejné moci nebo veřejný subjekt

Princip odpovědnosti

Princip odpovědnost spočívá ve dvou základních povinnostech:

- **povinnost zajistit soulad s GPDR** – spočívá v sérii dílčích povinností a institutů, např. povinnost přijmou vhodná technická a organizační opatření k zabezpečení osobních údajů (čl. 24 GDPR), zásada záměrné a standardní ochrany osobních údajů (čl. 25 GDPR), vedení záznamů o zpracování (čl. 30 GDPR) či jmenování pověřence pro ochranu osobních údajů (čl. 37 až 39 GDPR)
- **povinnost být schopen tento soulad aktivně prokázat** – klíčový princip nové právní úpravy; spočívá ve vedení různé dokumentace (dokumentace o posouzení rizik, dokumentace právního základu zpracování, bezpečnostní dokumentace vč. dokumentace porušení zabezpečení, záznamy o prováděných zpracování, pokyny udělené pracovníkům, …)

DŮLEŽITÉ

SOULAD S NAŘÍZENÍM (JEDNOTLIVÉ POVINNOSTI)

Posouzení rizik

Způsob zajištění souladu s GDPR by měl vždy odpovídat riziku, které zpracování představuje pro práva a svobody fyzických osob. GDPR rozlišuje tři stupně rizika:

- **riziko** – obecné měřítko pro zavádění technických a organizačních opatření; správce musí riziko co nejvíce snížit
- **vysoké riziko** – pokud správce dospěje k závěru, že hrozí vysoké riziko, pak se aplikuje povinnost provést posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR, povinnost provést předchozí konzultace dle čl. 36 GDPR a v případě porušení zabezpečení povinnost notifikovat subjekty dle čl. 34 GDPR (viz bod 91 odůvodnění GDPR)
- **nízké riziko** – nízké riziko aplikuje některé výjimky z povinností, např. není nutné ohlašovat porušení zabezpečení

Vysoké riziko

bod 91 odůvodnění GDPR

To by mělo platit zejména pro **rozsáhlé operace zpracování**, jež mají sloužit ke zpracování **značného množství osobních údajů na regionální, celostátní nebo nadnárodní úrovni**, jež by mohly mít dopad na velký počet subjektů údajů a u nichž je pravděpodobné, že budou představovat vysoké riziko, například vzhledem k jejich citlivosti, pokud se **v souladu s dosaženou úrovní technických znalostí použije ve velkém rozsahu nová technologie**, jakož i pro jiné operace zpracování, které představují vysoké riziko pro práva a svobody subjektů údajů, zejména **v případech, kdy s ohledem na tyto operace je pro subjekty údajů obtížnější uplatnit svá práva**. Posouzení vlivu na ochranu osobních údajů by mělo být vypracováno i v případech, kdy se osobní údaje zpracovávají **za účelem přijetí rozhodnutí o konkrétních fyzických osobách v návaznosti na jakékoliv systematické a rozsáhlé hodnocení osobních aspektů týkajících se fyzických osob na základě profilování těchto údajů nebo v návaznosti na zpracování zvláštních kategorií osobních údajů, biometrických údajů, nebo údajů o odsouzení v trestních věcech a o trestných činech či souvisejících bezpečnostních opatřeních**. […]

Vysoké riziko

bod 91 odůvodnění GDPR

[…] Posouzení vlivu na ochranu osobních údajů je rovněž zapotřebí v případě **monitorování veřejně přístupných prostor prováděného ve velkém rozsahu, zejména pokud se k němu používá optických elektronických přístrojů**, nebo v případě jakýchkoliv jiných operací, kdy má příslušný dozorový úřad za to, že je pravděpodobné, že **zpracování bude představovat vysoké riziko pro práva a svobody subjektů údajů, zejména proto, že tyto úkony brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy, nebo proto, že jsou prováděny systematicky a ve velkém rozsahu**. […]

Vysoké riziko

bod 91 odůvodnění GDPR

[…] Zpracování osobních údajů by nemělo být považováno za zpracování velkého rozsahu, pokud se jedná o **zpracování osobních údajů pacientů nebo klientů jednotlivými lékaři, zdravotníky nebo právníky**. V takových případech by posouzení vlivu na ochranu osobních údajů **nemělo být povinné**.

Kritéria při posuzování rizik

Posouzení rizik zahrnuje následující kroky:

- **identifikace hrozeb** – nevhodné zpracování, které přesahuje legitimní očekávání subjektu, riziko překročení zásady minimalizace údajů, uchování údajů po delší dobu, znemožnění nebo ztížení výkonu práv, …
- **identifikace potenciální újmy** – riziko diskriminace, krádeže, zneužití identity, poškození pověsti, … (viz bod 75 odůvodnění GDPR)
- **zhodnocení pravděpodobnosti vzniku újmy** – více osob zapojených do zpracování či zapojení třetích stran zvyšují tuto pravděpodobnost
- **zhodnocení závažnosti potenciální újmy** – citlivost osobních údajů (nikoli nutně ve smyslu čl. 9 GDPR), objem údajů, zranitelnost fyzických osob (sociálně slabí, děti, …), možný dopad na události v životě subjektů údajů

Metodiky při posuzování rizik

- **Methodology for Privacy Risk Management. How to implement the Data Protection Act** – metodika vydaná francouzským dozorovým úřadem CNIL, přístupná online na www.cnil.fr
- **Conducting privacy impact assessment: code of practice** – metodika britského dozorového úřadu ICO

Seznam všech povinností správce

- **zásada záměrné a standardní ochrany osobních údajů** (čl. 25 GDPR) – viz dále
- **povinnosti společných správců** (čl. 26 GDPR) – povinnost upravit si vzájemné vztahy
- **povinnosti zahraničních správců** (čl. 27 GDPR) – povinnost jmenovat zástupce
- **povinnosti v souvislosti se zapojením zpracovatele** (čl. 28 až 29 GDPR) – podrobnosti v lekci č. 7
- **vedení záznamů o zpracování** (čl. 30 GDPR) – viz dále
- **povinnost spolupracovat s Úřadem pro ochranu osobních údajů** (čl. 31 GDPR) – viz dále
- **povinnost přijmou vhodná technická a organizační opatření k zabezpečení osobních údajů** – podrobnosti v lekci č. 8 (čl. 24, 32 až 34 GDPR)
- **posouzení vlivu na ochranu osobních údajů** (čl. 35 GDPR)
- **provedení předchozí konzultace** (čl. 36 GDPR)
- **povinnost jmenovat pověřence pro ochranu osobních údajů** – podrobnosti v lekci č. 9 (čl. 37 až 39 GDPR)

Seznam povinností všech správců

POVINNOSTI VŠECH SPRÁVCŮ:

- **zásada záměrné ochrany osobních údajů** (čl. 25 odst. 1 GDPR) – povinnosti při vývoji aplikací, služeb či produktů, ochrana „by design“
- **zásada standardní ochrany osobních údajů** (čl. 25 odst. 2 GDPR) – povinnosti související s výkonem práv, zpracování pro dané účely po nutnou dobu, …
- **povinnost spolupracovat s Úřadem pro ochranu osobních údajů** (čl. 31 GDPR) – viz dále
- **povinnost přijmou vhodná technická a organizační opatření k zabezpečení osobních údajů** – podrobnosti v lekci č. 8 (čl. 24, 32 – 34 GDPR)

Seznam povinností některých správců

POVINNOSTI NĚKTERÝCH SPRÁVCŮ:

- **povinnosti společných správců** (čl. 26 GDPR) – povinnost upravit si vzájemné vztahy
- **povinnosti zahraničních správců** (čl. 27 GDPR) – povinnost jmenovat zástupce
- **povinnosti v souvislosti se zapojením zpracovatele** (čl. 28 až 29 GDPR) – podrobnosti v lekci č. 7
- **vedení záznamů o zpracování** (čl. 30 GDPR) – viz dále
- **povinnost jmenovat pověřence pro ochranu osobních údajů** – podrobnosti v lekci č. 9 (čl. 37 až 39 GDPR)

POVINNOSTI V PŘÍPADĚ VYSOKÉHO RIZIKA:

- **posouzení vlivu na ochranu osobních údajů** (čl. 35 GDPR)
- **provedení předchozí konzultace** (čl. 36 GDPR)

Záměrná a standardní ochrana osobních údajů

- **záměrná ochrana osobních údajů** (čl. 25 odst. 1 GDPR, data protection **by design**) – zatímco čl. 24 GDPR stanoví povinnost přijmout technická a organizační opatření, čl. 25 odst. 1 GDPR stanoví **povinnost jak a kdy je přijmout** – již v době určení prostředků zpracování, tzn. při návrhu (designu), tj. v okamžiku vývoji produktu či služby – GDPR zde zdůrazňuje tzv. pseudonymizaci a používání aplikací a programů, které ochranu a minimalizaci údajů umožňují (bod 78 odůvodnění GDPR)
- **standardní ochrana osobních údajů** (čl. 25 odst. 2 GDPR) – povinnost stanovit účel a zajistit, že (a) bude zpracováno nejmenší nezbytně nutné množství osobních údajů (b) pouze po nutnou dobu a (c) budou dostupné pouze nejmenšímu nutnému počtu osob

Záměrná ochrana osobních údajů (ochrana „by design“)

bod 78 odůvodnění GDPR

Pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů je třeba přijmout vhodná technická a organizační opatření, aby se zajistilo splnění požadavků vyplývajících z tohoto nařízení. Aby správce mohl doložit soulad s tímto nařízením, měl by přijmout vnitřní koncepce a zavést opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů. Tato opatření by mohla mimo jiné spočívat v minimalizaci zpracování osobních údajů, co nejrychlejší pseudonymizaci osobních údajů, transparentnosti s ohledem na funkce a zpracování osobních údajů, umožnění subjektům údajů monitorovat zpracování osobních údajů a umožnění správcům vytvářet a zlepšovat bezpečnostní prvky. **Pokud jde o vývoj, koncepci, výběr a používání aplikací, služeb a produktů, které jsou založeny na zpracování osobních údajů nebo osobní údaje za účelem plnění svých funkcí zpracovávají, je třeba zhotovitele těchto produktů, služeb a aplikací vybízet k tomu, aby při vývoji a koncipování těchto produktů, služeb a aplikací zohledňovali právo na ochranu údajů a brali náležitý ohled na stav techniky s cílem zajistit, aby správci a zpracovatelé mohli plnit své povinnosti v oblasti ochrany údajů. Zásady záměrné a standardní ochrany osobních údajů by rovněž měly být zohledněny v souvislosti s veřejnými zakázkami.**

Standardní ochrana osobních údajů

- **povinnosti vyplývající z jednotlivých práv** – např. informační povinnost dle čl. 13 a 14 GDPR, povinnost přenést osobní údaje k jinému správci, povinnost vymazat včas údaje
- **povinnost stanovit účel** – základní povinnost; jde o znak odlišující správce od zpracovatele
- **povinnost shromažďovat údaje odpovídají stanovenému účelu a pouze v rozsahu pro daný účel** – zbylé by se měly likvidovat, popř. je vůbec nezačínat shromažďovat; možná budoucí potřeba informací není dostatečným důvodem; mnohdy není účelné shromažďovat vedle sebe datum narození, rodné číslo i kopii občanského průkazu
- **povinnost zpracovávat údaje pouze v souladu s účelem, ke kterému byly shromážděny** – informovaný souhlas byl vždy dán předem k určitému účelu, který pak nelze měnit; není možné je ani předávat jiným správcům za jiným účelem („přeprodej informací“)

Standardní ochrana osobních údajů

- **povinnost uchovávat informace pouze po nezbytně nutnou dobu** – po uplynutí této doby mohou být informace uchovávány pouze pro státní statistické účely, pro účely vědecké a pro účely archivnictví; mnohdy je nutné je anonymizovat; východiskem jsou někdy promlčecí či prekluzivní doby
- **povinnost zpracovávat údaje pouze otevřeně** – subjekt musí o zpracování i o účelu zpracovávání vědět
- **povinnost nesdružovat osobní údaje, které byly získány k rozdílným účelům**
- **povinnost získávat údaje zákonným způsobem** – údaje nelze získávat nekalým nebo podvodným jednáním

Typická porušení standardní ochrany osobních údajů

- **zveřejnění osobních údajů v souvislosti ve vznikem dluhu** – ačkoli toto může být vnímáno jako určitá sankce pro dlužníka, zveřejňování informací o dlužnících může být nepřípustným zásahem do práva na soukromí
- **získání informací pod záminkou jiného účelu**
- **získání informací pro více účelů, ačkoli souhlas byl poskytnut pouze ve vztahu k jedinému účelu**
- **sdružování osobních údajů, které byly získány k rozdílným účelům**

Povinnost vést záznamy

- záznamy správce jsou podstatně obsáhlejší než záznamy, které vede zpracovatel
- záznamy se musí vést **písemně** (postačí elektronicky)
- **na požádání** musí být předány **Úřadu pro ochranu osobních údajů**

KDO MUSÍ VÉST ZÁZNAMY?

- správci s alespoň **250 zaměstnanci**
- správci, kde zpracování pravděpodobně představuje **riziko pro práva a svobody subjektů** údajů
- správci, kde **zpracování není příležitostné**
- správci, kde jde o **zpracování zvláštních kategorií osobních údajů** (vč. rozsudků v trestních věcech)

Záznamy o zpracování

Záznamy o zpracování musí obsahovat:

- **kontaktní údaje** – jméno a kontaktní údaje správce, příp. společného správce, zástupce správce či pověřence pro ochranu osobních údajů
- **účel zpracování** – nutno uvést všechny účely zpracování
- **kategorie subjektů osobních údajů a osobních údajů** – rozdělit subjekty do kategorií (např. zaměstnanci, zákazníci, uchazeči o zaměstnání), následně pak rozlišit kategorie údajů (kontaktní údaje, údaje o zdravotním stavu, …); všechny kategorie je nutné slovy popsat
- **kategorie příjemců** – vymezení alespoň skupin příjemců osobních údajů (externí účetní, vymáhací agentura, dceřiná společnost, …)
- **předávání do zahraničí** – informace o předávání osobních údajů do třetích zemí či mezinárodním organizacím, nutné je uvést také záruky pro ochranu údajů (viz čl. 29 odst. 1 GDPR)
- **lhůta pro výmaz** – je-li možné, správce uvede rovněž plánované lhůty pro výmaz
- **technická a organizační opatření** – je-li možné, správce uvede obecný popis technických a organizačních opatření dle čl. 32 odst. 1 GDPR

Povinnost spolupráce s dozorovým úřadem

- správce, zpracovatel a případný zástupce správce nebo **zpracovatele spolupracují na požádání s dozorovým úřadem při plnění jeho úkolů**
- dozorovým úřadem je v České republice **Úřad pro ochranu osobních údajů** v Praze (Pplk. Sochora 27, Praha 7)

DOLOŽENÍ SOULADU S NAŘÍZENÍM

Doložení souladu s GDPR

Soulad s GDPR se zpravidla dokládá **přiměřenou dokumentací** (listinnou nebo elektronickou).

- **dokumentace o posouzení rizik** – zhodnocení rizik (dle zásad výše) či přímo **posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR**
- **dokumentace právního základu zpracování** – karty jednotlivých zpracování s uvedením právního titulu (často formou **zásad ochrany osobních údajů**)
- **bezpečnostní dokumentace vč. dokumentace porušení zabezpečení** – popis přijatých technických a organizačních opatření k ochraně osobních údajů; dokumentace porušení zabezpečení je obligatorní, pojem „bezpečnostní dokumentace“ GDPR nezná
- **záznamy o prováděných zpracování** – např. záznamy o likvidaci či anonymizaci („skartační protokol“) či přímo **záznamy o zpracování dle čl. 30 GDPR**
- **pokyny udělené pracovníkům** – např. interní směrnice pro zaměstnance, dohody o mlčenlivosti, … či přímo **koncepce ochrany osobních údajů dle čl. 24 odst. 2 GDPR**

Koncepce ochrany osobních údajů („politika ochrany osobních údajů“)

Pokud je to s ohledem na činnosti zpracování přiměřené, zahrnují přijatá opatření také uplatňování vhodných **koncepcí v oblasti ochrany údajů** správcem (v angličtině „**data protection policy**“). Koncepce ve smyslu čl. 24 odst. 2 GDPR by měla obsahovat:

- jasně stanovené povinnosti a odpovědnost zaměstnanců a pracovníků
- jasně stanovené postupy zpracování
- jasně stanovené postupy při zajištění zabezpečení, např. při předávání údajů v rámci korporace
- kontrolní mechanismy – postupy k ověřování, zda je koncepce dodržována

Další možnosti dokládání souladu

Správce může doložit, že plní příslušné povinnosti, také pomocí následujících institutů:

- **schválené kodexy chování dle čl. 40 GDPR** – souhrnné dokumenty vypracováné sdruženími zastupující různé kategorie správců (sektorové organizace), které obsahují způsob, jak provést implementaci; kodex je schválen dozorovým úřadem (čl. 40 a 41 GDPR)
- **schválené mechanismy pro vydávání osvědčení dle čl. 42 GDPR** – správce sám zvolí postupy a následně požádá akreditovaný subjekt pro vydávání osvědčení, aby u něj provedl audit a posoudil soulad s nařízením; platnost osvědčení je tři roky (čl. 42 a 43 GDPR)

GDPR: ZPRACOVATEL A ZPRACOVATELSKÁ SMLOUVA

Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

Čl. 28 – 31 GDPR

LEKCE Č. 7

Zpracovatel

- na zpracování osobních údajů se může podílet **zpracovatel či více zpracovatelů**
- **zpracovatel** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce (viz čl. 4 odst. 8 GDPR)
- český zákon, na rozdíl od GDPR, rozlišoval dva druhy ustanovení zpracovatele (z pověření správce; zákonné zmocnění – to řeší čl. 28 odst. 3 GDPR)
- není možné, aby docházelo ke zpracování pouze zpracovatelem, tj. bez správce
- správce musí být odlišný zpracovatele, nemůže jít ani o část správce, např. HR oddělení

Další osoby, které se podílí na zpracování (§ 14, 15 zákona o ochraně osobních údajů; čl. 29 GDPR) – na zpracování se podílí i další osoby (zaměstnanci správce, externí IT technik při jednorázové opravě apod.), které nelze považovat kvůli ad hoc práci s daty za zpracovatele – je vhodné na ně myslet a zajistit jejich mlčenlivost a plnění povinností dle čl. 29 GDPR („dle pokynů správce“) a čl. 32 odst. 5 GDPR („zabezpečení osobních údajů“).

KLÍČOVÝ POJEM

Příklady zpracovatelů

- **externí poradenské služby** – externí mzdový účetní, externí personální agentura, ...
- **poskytovatelé cloudového řešení** – vzdálený server, služby typu Google Disk, OneDrive, …
- **externí archivy**
- **zajišťování bezpečnosti** – bezpečnostní agentura provozující kamerový systém, služby vrátnice či recepce, …
- **provozovatel redakčního systému e-shopu**

Obecné požadavky na zpracovatele

- **obecné požadavky na zpracovatele** – pouze takoví zpracovatelé, kteří poskytují dostatečné záruky, že zavedou vhodná technická a organizační opatření – toto lze prokázat kodexem chování (dle čl. 40 GDPR) nebo mechanismem pro vydávání osvědčení (dle čl. 42 GDPR)

VHODNÁ TECHNICKÁ OPATŘENÍ V CLOUD COMPUTINGU (dle WP29)**:**

- **integrita** – nesmí dojít k pozměnění údajů, údaje jsou pravé a nenarušené,
- **důvěrnost** – šifrování nebo pseudoanonymizace; zajištění a vymáhání povinnost mlčenlivosti, správa přístupových práv,
- **transparentnost** – zpracovatel své postupy sdělí a popíše správci,
- **izolovanost** – zpracovatel nemíchá údaje od různých správců,
- **součinnost** – okamžitá spolupráce se správcem při řešení žádostí,
- **odpovědnost** – zajištění sankcí vůči zaměstnancům a ostatním pracovníkům, kteří poruší své povinnosti.

Povinnosti zpracovatele

Všichni zpracovatelé mají tyto základní povinnosti:

- **povinnost zpracování pro účely správce** (čl. 28 odst. 10)
- **povinnost zpracování údajů podle pokynů správce** (čl. 29 a čl. 32 odst. 4 GDPR)
- **povinnost spolupráce s dozorovým úřadem** (čl. 31 GDPR)
- **povinnost zabezpečit osobní údaje** (čl. 32 GDPR)
- **povinnost hlásit porušení zabezpečení správci** (čl. 33 GDPR)

Někteří zpracovatelé pak mají rovněž následující povinnosti:

- **povinnost vést záznamy o zpracování** (čl. 30 GDPR)
- **povinnost jmenovat pověřence pro ochranu osobních údajů** (čl. 37 GDPR)

Základní povinnosti zpracovatele

- **povinnost zpracování pro účely správce** (čl. 28 odst. 10) – správce vymezuje účel, který zpracovatel nesmí měnit ani z něj vybočit; zpracování musí být stále v mezích vymezeného účelu
- **povinnost zpracování údajů podle pokynů správce** (čl. 29 a čl. 32 odst. 4 GDPR) – platí rovněž pro další osoby, které se podílejí na zpracování (tyto osoby však dle GDPR nejsou odpovědné); nezákonný pokyn musí zpracovatel odmítnout (čl. 28 odst. 3 písm. a) GDPR) a toto sdělit správci
- **povinnost spolupráce s dozorovým úřadem** (čl. 31 GDPR) – obecná povinnost součinnosti s ÚOOÚ zejména při dozoru, kontrole, správním či povolovacím řízení, příp. při porušení bezpečnosti
- **povinnost zabezpečit osobní údaje** (čl. 32 GDPR) – povinnost zavést vhodná technická a organizační opatření
- **povinnost hlásit porušení zabezpečení správci** (čl. 33 GDPR)

Povinnost vést záznamy

- záznamy zpracovatele jsou užšího rozsahu než záznamy správce
- záznamy se musí vést **písemně** (postačí elektronicky)
- **na požádání** musí být předány **Úřadu pro ochranu osobních údajů**

KDO MUSÍ VÉST ZÁZNAMY?

- zpracovatelé s alespoň **250 zaměstnanci**
- zpracovatelé, kde zpracování pravděpodobně představuje **riziko pro práva a svobody subjektů** údajů
- zpracovatelé, kde **zpracování není příležitostné**
- zpracovatelé, kde jde o **zpracování zvláštních kategorií osobních údajů** (vč. rozsudků v trestních věcech)

DŮLEŽITÉ

Záznamy o zpracování

Pokud **zpracovatel** musí vést **záznamy o zpracování**, pak by tak měl činit pro každého správce zvlášť. Tyto záznamy musí obsahovat zejména:

- **kontaktní údaje** – jméno a kontaktní údaje zpracovatele, každého správce, pro něhož jedná, a případných zástupců či pověřenců pro ochranu osobních údajů,
- **kategorie zpracování** – účel či účely zpracování pro každého ze správců, popř. popis kategorií osobních údajů, subjektů osobních údajů a příjemců osobních údajů (obsahově v užším rozsahu než u správce),
- **předávání do zahraničí** – informace o předávání osobních údajů do třetích zemí či mezinárodním organizacím, nutné je uvést také záruky pro ochranu údajů (viz čl. 29 odst. 1 GDPR),
- **technická a organizační opatření** – je-li možné, správce uvede obecný popis technických a organizačních opatření dle čl. 32 odst. 1 GDPR.

Zpracovatelská smlouva

- pokud zpracování nevyplývá ze zákona (např. ze zákona o základních registrech), musí správce se zpracovatelem uzavřít zpracovatelskou smlouvu
- zpracovatelská smlouva = **data processing agreement**
- **písemná forma** – postačí elektronická, může tedy být **součástí všeobecných obchodních podmínek**
- může jít o **adhezní smlouvu** – typicky u cloudových služeb
- může mít formu **standardních smluvní doložek**, které přijme Komise podle čl. 93 odst. 2 GDPR nebo dozorový úřad podle čl. 63 GDPR (čl. 28 odst. 6 GDPR)

VZOR

Obsah zpracovatelské smlouvy

- **předmět a doba trvání smlouvy, povaha zpracování** – vymezení kategorií osobních údajů, kategorií subjektů, povaha a účel zpracování, vše nikoli obecně; je možné i na dobu neurčitou,
- **závazek řídit se pokyny správce** – esenciální náležitost, zpracovatel musí být schopen pokyny vždy prokázat
- **mlčenlivost** – závazek mlčenlivosti, pokud nejde o případy zákonné mlčenlivosti,
- **zabezpečení a součinnost** – závazek přijmout technická a organizační opatření, která jsou nutná k zabezpečení, a poskytovat součinnost (zejména při vyřizování žádostí, auditech a inspekcích a v souvislosti se zabezpečením), součinnost může být zpoplatněna pouze vůči správci
- **řetězení zpracovatelů** – stanovení podmínek pro řetězení zpracovatelů, např. potřeba souhlasu správce
- **ukončení zpracování** – závazek vymazat údaje v souvislosti s ukončením smlouvy

VZOR

Zapojení dalších zpracovatelů

- dle historického stanoviska Úřadu pro ochranu osobních údajů č. 1/2009 bylo řetězení zpracovatelů zakázáno – tento právní názor byl následně překonán
- možnost zapojení dalších zpracovatelů potvrdilo rozhodnutí Evropské komise č. 2010/87/EU
- GDPR zapojení dalšího zpracovatele umožňuje vždy jen **po předchozím písemném povolení správce** – povolení může být **obecné nebo konkrétní**
- v případě obecného povolení musí mít správce možnost uplatnit námitku
- mezi jednotlivými zpracovateli musí být rovněž uzavřena **zpracovatelská smlouva** se stejnými náležitostmi – odpovědnost se nepřenáší, ale nevylučují se regresivní nároky

GDPR: ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

Čl. 32 – 36 GDPR

LEKCE Č. 8

Obecně k zabezpečení osobních údajů

Dochází ke **zpřísnění právní úpravy**, byť se povaha tohoto institutu nijak nemění; volba prostředků zabezpečení je stále na správci/zpracovateli. Povinnost zabezpečit osobní údajů je stále formulována obecně (**bez použití technických norem**), je vymezena v podstatě jako **povinnost prevence**.

- tato povinnost stíhá **správce i zpracovatele**
- **odpovědnost za protiprávní stav** – jde o ochranu jak před úmyslným, tak před nedbalostním jednáním, dokonce i před vyšší moci (přírodní katastrofy, …)
- **časově neomezená povinnost** – trvá, dokud údaje existují jako osobní údaje
- **důkazní břemeno** – správce i zpracovatel musí být schopen přijatá opatření prokázat; musí tedy vést **bezpečnostní dokumentaci**

Technologická neutralita

bod 15 recitálu

*S cílem zabránit vzniku vážného rizika obcházení by **ochrana fyzických osob měla být technologicky neutrální a nezávislá na použitých technologiích**. Ochrana fyzických osob by se měla vztahovat jak na automatizované zpracování osobních údajů, tak na manuální zpracování, pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy. Záznamy nebo soubory záznamů ani jejich titulní strany, které nejsou uspořádány podle určených hledisek, by do oblasti působnosti tohoto nařízení spadat neměly.*

Účel povinnosti zabezpečit osobní údaje

PORUŠENÍ ZABEZPEČENÍ (čl. 4 odst. 12 GDPR):

- náhodné nebo protiprávní zničení osobních údajů
- ztráta osobních údajů
- pozměnění osobních údajů
- neoprávněné zpřístupnění při přenosu, uložení nebo jiném zpracování

K porušení může dojít:

- **zvenčí správce/zpracovatele** – např. kybernetický útok, průmyslová špionáž
- **zevnitř správce/zpracovatel** – např. neoprávněné zpřístupnění třetí osobě
- **úmyslně** – např. záměrné vyzrazení informací
- **nedbalostně** – např. nedostatečným zabezpečením

Povinnost zabezpečit osobní údaje

Povinnost zabezpečit osobní údaje spočívá ve třech krocích:

- 1. krok – **posouzení rizik** – správce/zpracovatel musí posoudit rizika zpracování s přihlédnutím k povaze zpracování; toto vyhodnocování musí probíhat pravidelně (viz 3. krok)
- 2. krok – **přijetí vhodných technických a organizačních opatření** – GDPR nestanoví přesně, jaká opatření je nutné zavést; toto rozhodnutí je odpovědností správce/zpracovatele
- 3. krok – **dodržování, monitorování a revidování bezpečnostních opatření** – nejde jen o jednorázovou činnost, ale má být prováděno pravidelně (rovněž s ohledem na vývoj stavu vědy a techniky)

DŮLEŽITÉ

Posouzení rizik

Obecné posouzení rizik dle čl. 24 GDPR – ačkoli se čl. 24 GDPR dle systematiky nařízení vztahuje pouze ke správci, s ohledem na povinnosti dle čl. 32 GDPR je nutné jej přiměřeně vztáhnout i na zpracovatele.

Posouzení bezpečnostních rizik dle čl. 32 GDPR – nejde pouze o zabezpečení IT systémů, nutné vzít v potaz také lidský faktor, fyzické prostředí, důvěrnost subdodavatelů či obchodních partnerů; v potaz tedy bereme:

- **objektovou bezpečnost** – bezpečnost místa,
- **personální bezpečnost** – vyhodnocení důvěryhodnosti osob,
- **technologickou bezpečnost** – bezpečnost techniky, softwaru či jiných technologií.

Kritéria při posouzení rizik

- **stav vědy a techniky** – péče de lege artis vždy vyžaduje použití nejmodernějších technologií
- **náklady na provedení** – na straně správce/zpracovatele jde o důležité kritérium
- **kontext zpracování** – povaha, rozsah a účel zpracování
- **pravděpodobnost rizika** pro práva a svobody subjektů údajů
- **míra rizika** pro práva a svobody subjektů údajů – bude např. rozdíl mezi zabezpečením zvláštní kategorie citlivých osobních údajů (např. informací o sexuálním životě) a údaji, které jsou běžné (např. věk), popř. je subjekt údajů sám běžně zveřejňuje (např. fotografie na jeho facebookovém profilu)

Volba bezpečnostních opatření

- **volba způsobu ochrany** i odpovědnost za ni je na správci a zpracovateli, sami musí najít **odpovídají úroveň zabezpečení** s ohledem na všechna možná rizika a náklady, s výjimkou povinného opatření souvisejícího s přístupem zaměstnanců či smluvních partnerů (dle čl. 32 odst. 4 GDPR)
- jedním z prvků, kterými lze splnit tuto povinnost je dodržování schváleného **kodexu chování** (dle čl. 40 GDPR) nebo uplatňování schváleného **mechanismu pro vydávání osvědčení** (dle čl. 42 GDPR)
- je možné využít **technické normy**, zejména z rodiny ISO 27000
- je vhodné využít **příklady bezpečnostních opatření uvedených přímo v GPDR**, např. pseudoanonymizaci či šifrování

Využití technickým norem

Při zavedení opatření lze vycházet z jiných bezpečnostních norem a standardů, např. **norem z rodiny ISO 27000**, což jsou již **technické normy**. Jedná se zejména o normy:

- **norma ISO 27002** (Information technology - Security techniques - Code of practice for information security management) – vydání mezinárodní normy, která obsahuje více než 114 strukturovaných oblastí doporučení rozdělených do 14 kapitol, ve kterých je obsaženo více než 5000 přímých a odvozených bezpečnostních opatření
- **norma ISO 27001** – implementace systému řízení bezpečnostních informací – poskytuje model pro zavedení efektivního systému řízení bezpečnosti informací (ISMS) v organizaci a doplňuje tak normu ISO 27002
- **norma ISO 27018** – zpracování osobních údajů v prostředí veřejného cloudu

Příklady bezpečnostních opatření v GPDR

- **pseudoanonymizace** – dochází k oddělení přímých identifikátorů osoby, např. jména či rodného čísla, od ostatních údajů; i po provedení pseudoanonymizace zůstávají údaje osobními, na rozdíl od anonymizace,
- **šifrování osobních údajů** – opatření, při němž jsou osobní údaje převedeny do podoby, která není čitelná bez znalosti šifrovacího klíče
- **zavedení krizových scénářů** –zavedení organizačních procedur, pokud dojde k fyzickému nebo technickému incidentu

Příklady bezpečnostních opatření v GPDR

- **opatření k zajištění integrity systémů a služeb zpracování** – zabezpečení přístupu, např. metodou autentizace, autorizace, existence hesel či zavedení systému úrovní práv
- **opatření k zajištění dostupnosti systémů a služeb zpracování** – ochrana před zničením, ztrátou či pozměněním, např. monitorování přístupů jednotlivých osob a změn, které provedly, limitování přístupů, mechanismus, který brání zkopírování celé databáze, zálohování, pravidelná kontrola údajů, ukládání otisků souborů (hashování)
- **opatření k zajištění odolnosti systémů a služeb zpracování** – schopnost odolávat hrozbám, např. využívání bezpečnostního softwaru proti virovým hrozbám

Dodržování bezpečnostních opatření a přístup dalších osob

- **z**volená opatření je nutné dodržovat
- v případě, že má správce či zpracovatel **zaměstnance**, musí je vždy smluvně zavázat k tomu, aby údaje zpracovávaly pouze dle pokynů správce, popř. zavést interní předpis
- zaměstnanci také musí být náležitě proškoleni
- k mlčenlivosti je vhodné zavázat i **další osoby, které se mohou podílet na zpracování**, např. externí servisní technik či úklidová služba

Poznámka: Opatření související s přístupem zaměstnanců a dalších osob, je jediné, které GDPR výslovně uvádí jako povinné (čl. 32 odst. 4 GDPR). Výjimkou je pouze takové zpracování, které osobě ukládá přímo právo EU nebo předpisy členského státu, např. pro účely výkonu státního dozoru nebo kontroly.

Monitoring bezpečnostních opatření

- v průběhu zpracování se může měnit riziko, které zpracování představuje, a proto je vhodné nastavit **účinnou politiku pravidelného testování, posuzování a hodnocení všech přijatých opatření**
- vhodné je provádět **bezpečnostní audity** a **simulace bezpečnostních incidentů**
- může se jednat např. o nástroje prevence ztráty dat (data loss prevention, DLP) či systémy pro odhalení průniků do počítačových systémů (intrusion detection system, IDS)
- opatření je vhodné v písemné podobě uchovávat vč. výsledků kontrol a průběžných zpráv (viz čl. 24 GDPR); porušení bezpečnosti je nutné písemně v každém případě

Notifikační a ediční povinnost

Porušení zabezpečení (čl. 4 odst. 12 GDPR) je nutné v některých případech **ohlašovat** (notifikační povinnost) a vždy pak **zdokumentovat** (ediční povinnost).

Rozlišujeme:

- **notifikační povinnost správce vůči Úřadu pro ochranu osobních údajů** – vždy, ledaže je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody subjektů údajů; i takové porušení je ovšem nutné zdokumentovat
- **notifikační povinnost správce vůči subjektům údajům** – v případě vysokého rizika pro práva a svobody subjektů údajů, pokud údaje nebyly pseudoanonymizované či šifrované
- **notifikační povinnost zpracovatele vůči správci** – zpracovatele nestíhá povinnost ohlašovat porušení Úřadu ani subjektům, ale vždy pouze správci

Další ohlašovací povinnosti

Pro některé správce vyplývala ohlašovací povinnost již v minulosti z různých zákonů:

- ze **zákona o kybernetické bezpečnosti** – pro tzv. povinné osoby
- ze **zákona o elektronických komunikacích** – od transpozice směrnice ePrivacy
- ze **zákona o platebních styku** – pro poskytovatele platebních služeb v souvislosti s transpozicí směrnice PSD2

Může se tedy stát, že osoba bude muset **provést více notifikací**. Typicky půjde např. o banku.

Notifikační povinnost vůči ÚOOÚ

- **prvotní posouzení porušení zabezpečení** – nejprve je nutné posoudit, zda jde skutečně o porušení zabezpečení a zda představuje riziko pro práva a svobody subjektů údajů; prvotní posouzení je také vhodné **zdokumentovat**
- **riziko pro práva a svobody údajů** – např. omezení práv, ztráta možnosti získat úvěr, nemajetková újma, riziko krádeže, diskriminace, finanční ztráta, poškození pověsti, sdělení významných hospodářských či společných skutečností, …
- **lhůta pro ohlášení** – bez zbytečného odkladu, nejpozději do 72 hodin od okamžiku, kdy se správce o porušení dozvěděl; pokud je ohlašováno později, je nutné uvést důvody zpoždění
- **obsah hlášení** – popis povahy porušení, kategorie a přibližný počet dotčených subjektů a údajů, kontaktní údaje pověřence, popis možných důsledků, popis přijatých či navržených opatření [ÚOOÚ může nařídit **nápravné opatření dle čl. 58 odst. 2 písm. e) GDPR**]

DŮLEŽITÉ

Notifikační povinnost vůči subjektům

- **ohlašování porušení** – v případě vysokého rizika pro práva a svobody subjektů údajů je nutné ohlášení provést rovněž vůči subjektům údajů, popř. vždy tehdy, rozhodne-li tak Úřad pro ochranu osobních údajů [čl. 58 odst. 2 písm. e) GDPR]
- **vysoké riziko pro práva a svobody subjektů údajů** – nenastává tehdy, byly-li včas přijata náležitá bezpečnostní opatření, která riziko minimalizovala, popř. jsou-li údaje nesrozumitelné (pseudoanonymizované či šifrované)
- **lhůta pro ohlášení** – bez zbytečného odkladu; není stanovená žádná horní hranice
- **forma ohlášení** – stručně a srozumitelně (čl. 12 GDPR); pokud by ohlášení vyžadovalo od správce nepřiměřené úsilí, je možné tak učinit pomocí veřejného oznámení, např. prostřednictvím médií
- **obsah hlášení** – obdobně jako vůči ÚOOÚ, ale stručně a srozumitelně

Bezpečnostní dokumentace

- **bezpečnostní dokumentace** – ačkoli GDPR nestanoví výslovnou povinnost vést bezpečnostní dokumentaci, s ohledem na čl. 24 GDPR je nutné vést záznamy o zpracování, tedy i o přijatých bezpečnostních opatřeních; musí být vedena v písemné formě (nemusí být nutně listinná); s ohledem na znění čl. 32 se doporučuje, aby přiměřenou dokumentaci vedl také zpracovatel, byť na něj čl. 24 GDPR nedopadá
- **dokumentace porušení zabezpečení** – GDPR výslovně stanoví, že správce musí vytvářet a uchovávat dokumentaci všech případů porušení zabezpečení (tedy i těch, která nebyla hlášení ÚOOÚ); obsah dokumentace

VZOR

GDPR: POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

Advokátní kancelář
Křížka Kuckirová Legal

www.kklegal.cz

Čl. 37 – 39 GDPR

LEKCE Č. 9

Pověřenec pro ochranu osobních údajů

- pověřenec pro ochranu osobních údajů = **Data Protection Officer (DPO)**
- v některých evropských zemích (Německo, Francie, Maďarsko, Polsko) tento institut již existoval
- nově je zaveden pro všechny členské země EU

- **poradní orgán správce** – pověřenec bude konzultovat se správcem dodržování GDPR
- **kontaktní místo pro subjekty** – pověřenec zajišťuje komunikaci se subjekty (např. občany obce) a dozorovým orgánem (Úřad pro ochranu osobních údajů)
- **nezávislé postavení** – pověřenec nesmí být přímo úkolován, pověřenec správce také kontroluje a může se proti jeho postupům vymezit

Povinné jmenování DPO

Pověřenec musí být organizací jmenován, pokud:

- zpracování provádí **orgán veřejné moci či veřejný subjekt** (s výjimkou soudů při výkonu jejich rozhodovací činnosti) – bez ohledu na to, jaké údaje jsou zpracovávány
- **hlavní činnosti** správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují **rozsáhlé pravidelné a systematické monitorování subjektů údajů** [čl. 37 odst. 1 písm. b) GDPR]
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém **zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů**

Ostatní organizace mohou pověřence jmenovat **dobrovolně** na základě vlastního uvážení.

Členské státy navíc mohou okruh osob, které musí pověřence jmenovat, rozšířit vlastními národními předpisy.

Povinné jmenování podle čl. 37 odst. 1 písm. b) GDPR

Je nutné zkoumat všechny tyto podmínky:

- **hlavní činnost** – např. činnost nemocnice při vedení údajů o zdravotním stavu, ale již ne činnost nemocnice při vypracování mezd zaměstnanců
- **rozsáhlost** – např. činnost nemocnice, zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu; zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky
- **pravidelnost** – průběžný nebo v pravidelných intervalech a po určitou dobu se opakující zpracování
- **systematičnost** – zpracování vyskytující se podle určitého systému; přednastavené, organizované nebo metodické; uskutečňující se jako součást obecného plánu pro sběr dat; vykonávané jako součást strategie
- **monitorování** – např. sledování či profilování na intenretu za účelem behaviorálního marketingu (bod 24 odůvodnění)

Příklady správců s DPO

Pověřence pro ochranu osobních údajů **budou muset jmenovat** zejména:

- **úřady, obce a kraje**
- **školy, nemocnice, banky, pojišťovny, dopravní podniky**
- **internetové vyhledávače** a **poskytovatelé služeb sociálních sítí**
- **některé soukromé bezpečnostní agentury** – např. provozující kamerový systém v několika nákupních centrech
- **provozovatelé telekomunikačních sítí**
- **instituce provádějící profilování a hodnocení za účelem řízení rizika** – např. registry dlužníků pro potřeby úvěrového hodnocení

Kvalifikace DPO

POŽADAVKY NA POVĚŘENCE DLE GDPR:

- *"…musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39 GDPR"*

ROZVEDENÍ POŽADAVKŮ DLE PRACOVNÍ SKUPINY WP29:

- **znalost národního a unijního práva** v oblasti ochrany dat a hluboké znalosti GDPR
- praktické zkušenosti aplikace požadavků ochrany dat
- znalost prováděných zpracovatelských operací
- **znalost informačních technologií a bezpečnosti dat**
- znalost dané organizace
- schopnost propagovat kulturu ochrany dat v dané organizaci

Nezávislost DPO

- musí být zajištěno nezávislé postavení, a proto se doporučuje **nezávislý externí pověřenec**
- musí být zajištěno, aby se **vyvaroval střetu zájmů**
- s ohledem na jeho funkci mu **nesmějí být ukládány žádné pokyny**

- **pověřenec z řad vlastních zaměstnanců** – GDPR nevylučuje, aby byl pověřenec jmenován z vlastních řad, ale klade na něho určité nároky (kvalifikace, zamezení střetu zájmů, přístup k nejvyššímu vedení, …)
- nikdy nepůjde o řadového zaměstnance, **neměl by jím být např. vedoucí ochrany osobních údajů** (Chief Privacy Officer, CPO)

Zveřejnění údajů na DPO

- Správce nebo zpracovatel je povinen **zveřejnit kontaktní údaje pověřence na svém webu** nebo jiným vhodným způsobem
- Kontaktní údaje pověřence je třeba také **sdělit Úřadu pro ochranu osobních údajů**

Kontaktní údaje:

- poštovní adresa
- telefonní číslo
- e-mailová adresa

Pro lepší dostupnost lze zřídit **kontaktní webový formulář** či **specializovanou linku**.

Činnosti DPO

Činnosti pověřence:

- **mechanismus jediného kontaktního místa** – kontaktní místo pro všechny subjekty, vyřizován žádostí, konzultace
- **přístup k nejvyššímu vedení** – konzultace při jakýchkoli změnách, které se mohou dotknout ochrany osobních údajů
- **komunikace s Úřadem pro ochranu osobních údajů**

DĚKUJEME ZA VAŠI POZORNOST

Videa a další materiály včetně vzorů najdete na:

www.skoleni.brnenskypravnik.cz