AKADEMIE GDPR

GDPR V PODNIKATELSKÉ PRAXI – OPROŠTĚNO OD MÝTŮ A DEZINFORMACÍ

Mgr. Tereza Šamanová

Seminář „Ochrana osobních údajů ve firmách v době účinnosti GDPR“

Ostrava, 30. 10. 2018

AKADEMIE GDPR

OBSAH

I. OPAKOVÁNÍ: ZÁKLADNÍ ZÁSADY, PRINCIPY A PODMÍNKY ZPRACOVÁNÍ OÚ DLE GDPR

AKADEMIE GDPR

AKADEMIE GDPR

CO PRO VAŠI FIRMU ZNAMENÁ GDPR?

Memento, že osobní údaje zaměstnanců, klientů, partnerů.. je třeba pečlivě chránit

+

- **Přímo platný právní předpis a sladění pravidel pro ochranu osobních údajů napříč EU**
- **Možnost posílení postavení firmy na trhu, pokud k tématu přistoupíte seriózně**

-

- **Vyšší administrativní zátěž vzhledem k novým povinnostem správců a právům subjektů údajů**
- **Nebezpečí komplikací v konkurenčním boji nebo při kverulacích subjektů údajů**
- **Nebezpečí zbytečných výdajů při nepochopení nebo špatné implementaci**

LEGISLATIVNÍ RÁMEC

I. **Nařízení č. 2016/679 – obecné nařízení o ochraně osobních údajů (GDPR)**
    I. Zásada přímé aplikace a aplikační přednosti → vůči zvláštním zákonům poměr subsidiarity / speciality

II. **Obecné právní předpisy**
    I. Z. č. 89/2012 Sb., občanský zákoník
    II. Z. č. 101/2000 Sb., o ochraně osobních údajů + sněmovní tisk č. 138 – návrh zákona o zpracování osobních údajů
    III. Z. č. 480/2004 Sb., o některých službách informační společnosti
    IV. Z. č. 40/2009 Sb., trestní zákoník
        I. § 180 – Neoprávněné nakládání s osobními údaji

III. **Zvláštní právní předpisy**
    I. Z. č. 499/2004 Sb., o archivnictví a spisové službě
    II. Z. č. 262/2006 Sb., zákoník práce + z. č. 312/2002 Sb., o úřednících územně samosprávných celků
    III. Z.č. 340/2015 Sb., o registru smluv + z. č. 250/2000 Sb., o rozpočtových pravidlech územích rozpočtů
    IV. Z. č. 106/1999 Sb., o svobodném přístupu k informacím
    V. Z. č. 500/2004 Sb., Správní řád
    VI. Z. č. 256/2013 Sb., katastrální zákon
    VII. Z. č. 561/2004 Sb., školský zákon + další školské předpisy
    VIII. Daňové a účetní předpisy

AKADEMIE GDPR

ZDROJE INFORMACÍ

Stanoviska | autoritativní názory | informace

- **Stanoviska WP 29:** http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360
- **Stanoviska ÚOOÚ a české překlady stanovisek WP 29:** https://www.uoou.cz/gdpr-obecne-nbsp-narizeni/ds-3938/p1=3938
- **Evropský sbor pro ochranu osobních údajů:** https://www.mpo.cz/cz/podnikani/ochrana-osobnich-udaju-gdpr/obecne-narizeni-o-ochrane-osobnich-udaju---gdpr--228672/
- **Návrh zákona o zpracování osobních údajů – Sněmovní tisk č. 138:** (www.psp.cz/sqw/historie.sqw?o=8&t=138)

Instituce | organizace

- **Úřad pro ochranu osobních údajů:** www.uoou.cz
- **Ministerstvo průmyslu a obchodu ČR:** www.mpo.cz/gdpr
- **Ministerstvo vnitra ČR:** www.mvcr.cz/gdpr

VĚCNÁ A MÍSTNÍ PŮSOBNOST GDPR

- **Všechny formy zpracování**
  - Zcela/částečně automatizované
  - Manuální, jsou-li anebo mají-li OÚ být součástí evidence
- **Veškeré zpracování osobních údajů na území EU/EHP, občanů EU a pohyby OÚ v rámci EU/EHP, když:**
  - Správce / zpracovatel OÚ sídlí v zemích EU
  - Správce / zpracovatel OÚ nesídlí v zemích EU, ale zpracovává data občanů EU za účelem nabídky zboží, služeb anebo za účelem monitoringu jejich chování na území EU
- **Výluky působnosti GDPR**
  - Osoby bez právní ochrany včetně osob zemřelých + právnické osoby × ochrana OÚ zaměstnanců
  - Zpracování osobních údajů v oblasti ochrany zákonnosti a bezpečnosti
  - Anonymní a anonymizované údaje, (neidentifikující) údaje pro statistické a výzkumné účely
  - **Osobní nebo domácké zpracování osobních údajů** fyzickou osobou bez souvislosti s profesní nebo obchodní činností

ZÁSADY ZPRACOVÁNÍ A OCHRANY OÚ

I. **Čl. 5 GDPR**

I. Zásada **zákonnosti, korektnosti a transparentnosti** zpracování
II. Zásada **účelového omezení** shromažďování osobních údajů
III. Zásada **minimalizace** zpracovávaných osobních údajů
IV. Zásada **přesnosti** osobních údajů
V. Zásada **omezeného uložení** osobních údajů
VI. Zásada **integrity a důvěrnosti** zpracování
VII. Zásada **odpovědnosti**
    I. Povinnost správce dodržet všechny povinnosti vyplývající ze zásad
    II. Povinnost správce dodržení shody prokázat

Možnost **omezení aplikace zásad a práv subjektů OÚ za účelem výslovného veřejného zájmu** → čl. 23 GDPR

II. **Čl. 25 a 32 GDPR**

I. **Standardní ochrana osobních údajů**
II. **Záměrná ochrana osobních údajů**
III. **Organizační a technická opatření k zajištění shody s GDPR**

ZÁKONNOST ZPRACOVÁNÍ OÚ

- **Právní tituly zpracování osobních údajů**
  - Plnění právní povinnosti
  - Plnění smlouvy
  - Oprávněné zájmy příslušného správce anebo třetí strany
  - Ochrana životně důležitých zájmů subjektů údajů nebo jiné fyzické osoby
  - Úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci
    - Výkon veřejné moci hlavním právním titulem pro zpracování OÚ OVM

- Souhlas subjektu údajů
  - Vždy zákonné zpracování? → Souhlasem není možné nahradit neexistenci důvodu ke zpracování
  - Kdy potřebujete souhlas? → Když nelze využít jiný právní titul

SOUHLAS - ZÁSADY NOVÉ ÚPRAVY

- **Vyšší standardy pro souhlas než podle stávající úpravy → Souhlas je:**
  - Jednoznačný (projev vůle)
  - Svobodný
  - Konkrétní
  - Informovaný
  - Oddělitelný → Oddělený
  - Aktivní (komisivní)

- **Jednoznačný projev vůle**
  - Psaný projev nebo jednoznačná akce → podpis listiny, dvojklik
  - Ne pasivní / konkludentní → Ne předvyplněná pole / tickboxy souhlasu

CHECKLIST PRO SOUHLAS

- **Je souhlas správný právní titul pro zpracování OÚ?**
- **Je žádost o souhlas jasná, zřetelná a oddělená od ustanovení uživatelských podmínek?**
- **Žádáme o aktivní opt-in? Nepoužíváme předem zatržená políčka?**
- **Je text souhlasu jednoduchý a všeobecně srozumitelný?**
- **Informujeme subjekt, proč chceme OÚ zpracovávat a jak to budeme dělat?**
- **Žádáme o souhlas položkově?**
- **Uvádíme jmenovitě naši organizaci a všechny třetí strany?**
- **Informuje subjekt OÚ, že může svůj souhlas kdykoliv odvolat?**
- **Zajistili jsme, že souhlas je možné odvolat snadno a rychle?**
- **Nepodmiňujeme souhlasem poskytnutí naší služby?**
- **Pokud poskytujeme online služby přímo dětem, žádáme o souhlas pouze v souladu s našimi opatřeními pro ověření věku a získání souhlasu rodičů?**

PRÁVA SUBJEKTU ÚDAJŮ

a) Automatická:

- **Právo na informace o zpracování OÚ**
- **Právo na výmaz („právo být zapomenut“)**
- **Právo na opravu**
- **Právo na omezení zpracování**
- **Právo nebýt předmětem automatizovaného rozhodnutí založeného na profilování**

b) Na žádost subjektu údajů:

- **Právo na přístup subjektu k OÚ**
  - Právo získat od správce OÚ potvrzení o zpracování OÚ
  - Právo získat kopii zpracovávaných OÚ
- **Právo na přenositelnost údajů**
- **Právo vznést námitku** v případě, že zpracování provádí správce na základě svých oprávněných zájmů

POVINNOSTI SPRÁVCŮ A ZPRACOVATELŮ

- **Povinnost vést záznamy o činnostech zpracování (čl. 30)**
  - Písemné záznamy, dostupné na vyžádání dozorovému úřadu
- **Povinnost zajistit odpovídající zabezpečení OÚ (čl. 32 + 25)**
  - Přijmout vnitřní koncepce a opatření pro zabezpečené zpracování OÚ
  - Zásady záměrné a standardní ochrany osobních údajů
- **Povinnost ohlašovat a dokumentovat bezpečnostní incidenty (*data breaches*; čl. 33, 34)**
  - Bez zbytečného odkladu, nejpozději do 72 hodin dozorovému orgánu
  - Bez zbytečného odkladu v případě závažného úniku i subjektům OÚ
- **Povinnost provést posouzení vlivu na ochranu osobních údajů (DPIA) a předchozí konzultace (čl. 35, 36)**
- **Povinnost zavést a obsadit funkci DPO pro určité typy organizací správců (čl. 37)**

POVĚŘENEC PRO OCHRANU OÚ

- **Pověřenec pro ochranu OÚ – Data Protection Officer (DPO)**
  - Čl. 37 a násl. GDPR
  - Vodítko WP 29 o pověřencích (WP 243 rev. 01)

- **Kdo musí jmenovat pověřence**
  - Každý orgán veřejné moci nebo veřejný subjekt
  - Subjekty provádějící v rámci svých hlavních činností:
    - Rozsáhlé pravidelné a systematické monitorování subjektů OÚ
    - Rozsáhlé zpracování OÚ zvláštní kategorie a údajů týkajících se rozsudků ve věcech trestních
  - Ten, po němž to bude vyžadovat právo EU anebo právo členského státu EU

- **Klíčové úkoly DPO**
  - Monitorování zpracování OÚ s cílem zajistit soulad s GDPR
  - Zajišťování provádění práv subjektů údajů
  - Evidenční a reportovací činnost DPO
  - Posuzování vlivu na zpracování OÚ (DPIA, konzultace s dozorovým orgánem)
  - Konzultace a spolupráce DPO s ÚOOÚ
  - Ohlašování a řešení bezpečnostních incidentů
  - Vzdělávání a školení zaměstnanců, případně externích dodavatelů

POVĚŘENEC PRO OCHRANU OÚ

- **Klíčové atributy pověřence**
  - Hluboká praktická **znalost ochrany OÚ**
  - Nezávislost × Soustavný **konflikt zájmů**
  - **Znalost místního prostředí** včetně jazyka
  - Fyzická **dostupnost**

- **DPO ve firemním kontextu**
  - Materiální **zdroje**
  - Časová **disponibilita**
  - Odpovídající **kompetence**
  - **Přístup** k informacím, databázím, procesům ad.

II. REMINDER:
ZÁKLADNÍ KROKY KE SHODĚ S GDPR

AKADEMIE GDPR

AKADEMIE GDPR

MINIMÁLNÍ SHODA S GDPR

I. Vypracování dokumentace osvědčující naplňování zásad zpracování, ochrany a zabezpečení osobních údajů (OÚ) podle čl. 5, 6, 25 a 32 GDPR

II. Vypracování záznamů o činnostech zpracování v minimálním rozsahu vyžadovaném čl. 30 GDPR

III. Zavedení role pověřence (DPO) do organizace a vybavení odpovídajícími kompetencemi

IV. Zavedení a popis systému procesů (přinejmenším jednoho generického procesu) reakcí organizace na práva subjektů osobních údajů

V. Vypracování dokumentace a zavedení a popis procesů naplňování informační povinnosti vůči subjektům údajů

VI. Zavedení procesů identifikace, dokumentace a hlášení bezpečnostních incidentů na poli osobních údajů
(tzv. *data breaches*)

VII. Revize smluv s nejvýznamnějšími zpracovateli osobních údajů

VIII. Provedení úvodního posouzení vlivů na zpracování osobních údajů (DPIA) v oblastech, kde bude identifikováno vysoké riziko zpracování osobních údajů

IX. Systém sběru, evidence a zpracování souhlasů se zpracováním OÚ

AKADEMIE GDPR

KROKY KE SHODĚ

I. **Znát základní principy a požadavky GDPR aneb *Poznej nepřítele, aby ses mohl účinně bránit!***

II. **Být si vědomi všech praktických dopadů GDPR do firemního života**
   I. Naplňování práv subjektů osobních údajů
   II. Plnění povinností firmy coby správce osobních údajů
   III. Vztahy se zpracovateli osobních údajů a nebo povinnosti firmy jako zpracovatele
   IV. Zaměstnanecké osobní údaje
   V. Klientská a obchodní agenda (B2B i B2C)
   VI. B2G smluvní vztahy
   VII. Zabezpečení a ochrana osobních údajů
   VIII. Pověřenec na ochranu osobních údajů
   IX. Minimální rozsah souladu s GDPR

III. **Zajistit prvotní soulad s GDPR**
   ✓ Identifikace informačních aktiv a lokalizace osobních údajů – *Co? / Kde?*
   ✓ Popis osobních údajů, účelů, zákonných titulů a procesů – *Kdo? / Proč? / Jak?*
   ✓ Prvotní analýzy rizik *Kde jsou úzká místa?*
   ✓ Nastavení zabezpečení a ochrany údajů *Jak úzká místa eliminovat?*

IV. **Průběžně dále zajišťovat soulad s GDPR**
   I. Dlouhodobé sledování a aktualizace rizik a jejich řešení
   II. Analýzy veškerých nových procesů z pohledu ochrany dat
   III. Průběžná revize způsobu zabezpečení a ochrany osobních údajů

III. UPOZORNĚNÍ: ČASTÉ OMYLY A MÝTY O GDPR

AKADEMIE GDPR

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

1. **GDPR je směrnice => musíme počkat na vnitrostátní právní úpravu**

Omyl: **GDPR =** nařízení 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) **= (General Data Protection Regulation)**

Proč?

U GDPR platí:

- **Zásada přímé aplikace** → k plné účinnosti nařízení není třeba vnitrostátního předpisu
- **Zásada aplikační přednosti** → základní principy se subsidiárně uplatní vždy, speciální právní úprava však má přednost

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

2. GDPR ruší dosud platnou národní legislativu a zavádí revoluci v práci s osobními údaji

Omyl: I nadále platí právní předpisy upravující práci s osobními údaji ve specifických oblastech, změnou je dotčen pouze zákon č. 101/2000 Sb. o zpracování osobních údajů a v souvislosti s ním měněné předpisy

Proč? Platí i nadále národní legislativa, zejména:

I. Obecné právní předpisy

I. Zák. č. 101/2000 Sb., o ochraně osobních údajů → zákon o zpracování osobních údajů (Sněmovní tisk č. 138)
II. Zák. č. 89/2012 Sb., občanský zákoník
III. Zák. č. 40/2009 Sb., trestní zákoník
- § 180 – Neoprávněné nakládání s osobními údaji

II. Zvláštní právní předpisy

I. Zák. č. 499/2004 Sb., o archivnictví a spisové službě
II. Zák. č. 262/2006 Sb., zákoník práce
III. Zák.č. 340/2015 Sb., o registru smluv + z. č. 250/2000 Sb., o rozpočtových pravidlech územích rozpočtů
IV. Zák. č. 106/1999 Sb., o svobodném přístupu k informacím
V. Zák. č. 500/2004 Sb., Správní řád
VI. Zák. č. 256/2013 Sb., katastrální zákon
VII. Zák. č. 561/2004 Sb., školský zákon + další školské předpisy
VIII. Daňové a účetní předpisy

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

3. GDPR zavádí revolučně nové zásady zpracování osobních údajů a práva subjektů

Omyl: V převážné většině jsou práva subjektů osobních údajů i zásady pro zpracování osobních údajů již zakotveny v nyní platné směrnici 95/46 a zákoně č. 101/2000 Sb.

Proč?

- **GDPR není revolucí** v práci s osobními údaji, avšak přesto zavádí některé novinky
- **Příklady již platných práv a zásad**:
  - Právo na výmaz (§ 5 odst. 1 písm. e) zák.č. 101/2000 Sb.)
  - Právo na informace a na přístup k údajům (§ 11 a § 12 zák. č. 101/2000 Sb.)
  - Zákonnost zpracování osobních údajů (§ 5 odst. 2 zák.č. 101/2000 Sb.)
  - Účelové omezení zpracování osobních údajů (§ 5 odst. 1 písm. f) zák. č. 101/2000 Sb.)
  - Transparentnost zpracování údajů (§ 5 odst. 1 písm. g) zák. č. 101/2000 Sb.)
  - Přesnost zpracování (§ 5 odst. 1 písm. c) zák. č. 101/2000 Sb.) apod.
- **Příklady novinek**:
  - Právo na přenositelnost (čl. 20 GDPR)
  - Povinnost vést záznamy o činnostech zpracování (čl. 30 GDPR)
  - Ohlašovací povinnost u bezpečnostních incidentů (čl.33+34 GDPR)
  - Povinnost jmenovat pověřence pro ochranu osobních údajů (čl. 37 a následující GDPR)
  - Povinnost provádět posouzení vlivu na ochranu osobních údajů (čl. 35+36 GDPR)

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

4. Souhlas je univerzální právní titul pro zpracování údajů

Omyl: Souhlas je titulem „ultima ratio“ tam, kde nepřichází v úvahu jiné právní tituly pro zpracování osobních údajů

Proč?

- **Právní tituly zpracování osobních údajů**
  - Plnění právní povinnosti
  - Plnění smlouvy
  - Oprávněné zájmy příslušného správce anebo třetí strany
    - Vyloučený pro plnění úkolů veřejné správy orgány veřejné moci ×
    - Použitelný pro výkon úkolů samosprávy → Celá řada aplikací
  - Ochrana životně důležitých zájmů subjektů údajů nebo jiné fyzické osoby
  - Úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci
    - Výkon veřejné moci hlavním právním titulem pro zpracování OÚ OVM

- Souhlas subjektu údajů
  - Vždy zákonné zpracování? → **Souhlasem není možné nahradit neexistenci důvodu ke zpracování**
  - Kdy potřebujete souhlas? → Když nelze využít jiný právní titul

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

5. Souhlas se zpracováním osobních údajů je nutný i u zpracování podoby fyzické osoby nebo zasílání obchodních sdělení

Omyl: Souhlas se zpracováním osobních údajů je nadužíván a aplikován i v případech, kdy postačí formálně i obsahově jednodušší úkony dotčených subjektů údajů

Proč?

- **Souhlas se zpracováním osobních údajů je třeba využít skutečně pouze tam, kde:**
  a) Není k dispozici žádný jiný právní titul ke zpracování údajů a
  b) Dochází ke zpracování komplexu osobních údajů
- **GDPR = lex generalis (obecný právní předpis) pro zpracování osobních údajů**
- **Lex specialis (speciální právní úprava) pro zpracování podoby fyzické osoby:**
  - Občanský zákoník, Hlava II, Oddíl 6: Ochrana osobnosti, Poddoddíl 2: Ochrana soukromí a podoby:
    - Podobu člověka lze zachytit a rozšiřovat jen s jeho svolením – může být i konkludentní, tj. nikoli explicitně udělené ani písemně zaznamenané
    - Bylo-li svolení bez rozumného důvodu nebo podstatné změny okolností odvoláno, lze žádat odvolávajícího o náhradu škody
- **Lex specialis pro zasílání obchodních sdělení:**
  - Zákon o některých službách informační společnosti
    - Šíření obchodních sdělení je možné pouze na základě:
      a) předchozího obchodního kontaktu s adresátem sdělení tak, aby byl možný „opt-out“ (tj. vyjádření nesouhlasu)
      b) předchozího souhlasu adresáta sdělení, s kterým doposud odesílatel neměl žádný obchodní kontakt

AKADEMIE GDPR

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

6. GDPR obsahuje výjimky/úlevy pro malé firmy a organizace

Omyl: GDPR neobsahuje žádné výjimky co do vztahu velikosti firem a organizací a plnění základních povinností správců a zpracovatelů údajů. Jediná výjimka z evidenční povinnosti (pro organizace správců s počtem zaměstnanců do 250) je velmi řídce použitelná

Proč?

- **Evidenční povinnost (povinnost vést záznamy o činnostech zpracování) je upravena takto:**
  - Preambule GDPR stanoví, že:
    - „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.“ (rec. 13)
  - Avšak současně:
    - Výjimka platí pouze pro zpracování, které je:
      - Příležitostné
      - Nezahrnuje zpracování zvláštních kategorií údajů

=> V prostředí podnikajících subjektů pravděpodobně **nelze výjimku použít**

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

7. Pověřence mohu bez omezení sdílet s ostatními firmami/organizacemi

Omyl: Pro výkon funkce pověřence platí zákaz střetu zájmů. Nesmí tedy vykonávat funkci ve více firmách nebo organizacích, které jsou v potenciálně konkurenčním postavení

Proč?

- **GDPR stanoví obecnou povinnost správce zajistit, aby pověřenec nebyl ve střetu zájmů (čl. 38 odst. 6 GDPR)**
- **Výklad WP29 k tématu střetu zájmů stanoví, že:**
  - Ke střetu zájmů u externího pověřence může dojít v případě, že by vykonával svou činnost v několika firmách či organizacích, které jsou v potenciálně konkurenčním postavení

⇒ **Potenciální střet zájmů interní:**

⇒ **Může být odhalen správcem samotným a správce mu může předejít vymezením úkolů pověřence**

⇒ **Potenciální střet zájmů externí:**

⇒ **Nemůže být odhalen správcem samotným a je tedy vhodné řešit jeho zákaz ve smlouvě s pověřencem**

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

8. Pověřenec vůbec nesmí sám pracovat s osobními údaji, aby nebyl ve střetu zájmů

Omyl: Pro výkon funkce pověřence platí zákaz střetu zájmů. Nesmí tedy vykonávat žádné činnosti, při kterých rozhoduje o účelu a způsobu zpracování údajů

Proč?

- **GDPR stanoví obecnou povinnost správce zajistit, aby pověřenec nebyl ve střetu zájmů (čl. 38 odst. 6 GDPR)**
- **Výklad WP29 k tématu střetu zájmů stanoví, že:**
  - K internímu střetu zájmů může dojít, pokud je pověřenec zastává pozici, která jej nutí určovat účely a způsoby zpracování osobních údajů v organizaci správce
  - Příkladem takových pozic jsou:
    - **Senior manažerské pozice** – např. vrchní manažer organizace, finanční manažer, zdravotní manažer, marketingový manažer, vedoucí HR nebo IT oddělení
    - **Pozice zařazené na nižším stupni v organizační struktuře, pokud obnášejí rozhodování o způsobu a účelu zpracování údajů** (např. pracovník vydávající rozhodnutí o vyměření poplatkové povinnosti občanů, pracovník stavebního úřadu s právem činit úkony ve správním řízení apod.)

⇒ **Střet zájmů** je zapotřebí identifikovat nikoli podle názvu pozice, ale **podle skutečného obsahu pracovních úkolů a toho, zda obnášejí rozhodování o účelu a způsobu zpracování údajů**

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

9. Pověřenec musí být jmenován pro každý typ veřejnoprávní organizace

Omyl: Pověřence v českém prostředí musejí jmenovat **pouze organizace zřízené zákonem, které vykonávají veřejnou moc** (= autoritativně rozhodují o právech a povinnostech fyzických osob)

Proč?

- **GDPR (čl. 37)** stanoví obecnou povinnost správce a zpracovatele jmenovat pověřence v případech, kdy zpracování osobních údajů provádí **orgán veřejné moci či veřejný subjekt, s výjimkou soudů**
- **Zákon o zpracování osobních údajů** (§ 14 odst. 1, ve znění aktuální verze návrhu) stanoví, že povinnost jmenovat pověřence pro ochranu osobních údajů mají:
  - **Orgány veřejné moci**
  - **Orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu**.

⇒ Příklady organizací, které **pověřence mít musejí:**

- Základní, střední a mateřské školy

⇒ Příklady organizací, které **pověřence mít nemusejí:**

- Knihovny
- Základní umělecké školy
- Organizace provádějící bytovou správu nebo správu nebytových prostor
- Organizace poskytující sociální služby

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

10. Pro výkon funkce pověřence je nutná certifikace

Omyl: Pověřenec pro ochranu osobních údajů není v českém prostředí regulovaná živnost ani není kvalifikace pro výkon funkce závazně stanovena, oficiální certifikační schémata s certifikací pověřenců nepočítají

Proč?

- **GDPR (čl. 37 odst. 5)** stanoví obecné požadavky na kvalifikaci pověřence:
  - profesní kvality
  - zejména odborné znalosti práva a praxe v oblasti ochrany údajů
  - schopnost plnit úkoly stanovené nařízením
- **WP29 ve svém výkladovém stanovisku wp243 doplňuje:**
  - užitečné jsou znalosti odvětví podnikání a organizace správce
  - zapotřebí je porozumění procesním operacím, informačním systémům, bezpečnosti dat a potřebám správce v oblasti ochrany dat
  - jsou nutné i zevrubné znalosti procesních a administrativních pravidel platných v organizaci správce

⇒ **Pravidla pro kvalifikaci pověřence:**

- dána nařízením a výkladovými pravidly
- v ČR nejsou předmětem regulace na úrovni podmínek pro výkon živnosti nebo povolání
- odměna pověřence: optimálně v návaznosti na vykonávané úkoly, nikoli kvalifikaci

AKADEMIE GDPR

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

11. Je obecně lepší mít interního/externího pověřence

Omyl: Každá organizace správce by si měla identifikovat svou vlastní potřebu co do kapacity a odbornosti pověřence, nelze formulovat paušální doporučení

Proč?

- **GDPR stanoví obecnou povinnost pověřence plnit alespoň úkoly:**
  - poskytování informací a poradenství – obecně i na požádání
  - monitorování souladu s GDPR a dalšími předpisy EU i ČR
  - spolupráce na posouzení vlivu na ochranu osobních údajů
  - spolupráce s dozorovým úřadem
  - výkon funkce kontaktního místa pro dozorový úřad i subjekty údajů
- **Pověřenec dále může plnit i jiné úkoly a povinnosti:**
  - předpokladem je zamezení střetu zájmů

⇒ **Příklady možných řešení:**

- **Externí pověřenec s minimálním úvazkem**
  - Riziko: špatná znalost interních poměrů v organizaci správce => chyby v poskytovaných informacích a poradenství
- **Interní pověřenec pověřený i plněním jiných úkolů v organizaci správce**
  - Riziko: nedostatek kapacity na výkon funkce pověřence => prodlevy v poskytování informací, poradenství a součinnosti

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

12. Koupím si „typové GDPR řešení pro určitou velikost firmy/obor podnikání“ a mám vystaráno

Omyl: GDPR vyžaduje **individuální přístup každého správce**, Vy sami nejlépe víte, jak se ve Vaší organizaci pracuje s daty včetně osobních údajů

Proč?

Je zapotřebí podrobně a s ohledem na situaci Vaší organizace řešit:

I. **Praktické dopady GDPR do organizace správce údajů**
   I. Práva subjektů osobních údajů
   II. Povinnosti firmycoby správce osobních údajů
   III. Data občanů / Zaměstnanecké osobní údaje
   IV. Zabezpečení a ochrana osobních údajů
   V. Pověřenec na ochranu osobních údajů
   VI. Dosažení minimálního rozsahu souladu s GDPR

II. **Zajištění souladu s GDPR**
   I. Identifikace informačních aktiv a lokalizace osobních údajů – *Co? / Kde?*
   II. Popis osobních údajů, účelů, zákonných titulů a procesů – *Kdo? / Proč? / Jak?*
   III. Analýzy rizik a jejich dlouhodobé udržování – *„malá/velká“ DPIA*
   IV. Nastavení zabezpečení a ochrany osobních údajů

AKADEMIE GDPR

NEJČASTĚJŠÍ OMYLY A MÝTY O GDPR

13. GDPR se nedotkne zahraničního obchodu naší firmy

Omyl: GDPR platí pro ochranu osobních údajů občanů, rezidentů i osob pohybujících se v EU kdekoli na světě

Proč?

- **Předávání je možné pouze na základě:**
  - Rozhodnutí o odpovídající ochraně
  - Záruk
  - Výjimek pro specifické situace
- **Evropská komise vydává rozhodnutí o odpovídající ochraně - whitelist - seznam zemí, které podle jejího přezkumu zajišťují odpovídající úroveň ochrany**
  - Aktuálně součástí seznamu: Andorra, Argentina, Faerské ostrovy, jurisdikce Guernsey, Izrael, Jersey, Kanada, ostrov Man, Nový Zéland, Švýcarsko, Uruguay, USA (pouze Privacy Shield) – u všech avizován přezkum do účinnosti GDPR
  - Stejná pravidla pro ochranu dat platí i v zemích EES – Norsko, Lichtenštejnsko, Island
- **Výjimky pro specifické situace:**
  - Informovaný výslovný souhlas subjektu údajů
  - Předání nezbytné pro plnění smlouvy nebo předsmluvních opatření mezi subjektem údajů a správcem
  - Předání nezbytné pro uzavření nebo splnění smlouvy uzavřené se správcem osobou odlišnou od subjektu údajů, v jejím zájmu
  - Předání nezbytné z důležitých důvodů veřejného zájmu
  - Předání nezbytné pro určení, výkon nebo obhajobu právních nároků
  - Předání nezbytné k ochraně životně důležitých zájmů subjektu/jiných osob (+ subjekt není způsobilý udělit souhlas)
  - K předání dochází z rejstříku (veřejně přístupného / oprávněný zájem k nahlížení)

V. ČASTÉ ŽIVOTNÍ SITUACE FIREM A OCHRANA DAT

AKADEMIE GDPR

1. PERSONÁLNÍ PRAXE A VÝBĚROVÁ ŘÍZENÍ

- **Příklady relevantních účelů zpracování:**
  - Zpracování životopisů a dalších podkladů (např. doklad o vzdělání, doklady o dosavadní praxi, výpis z Rejstříku trestů aj.)
  - Vedení evidence uchazečů
  - Vypracování zprávy o posouzení a hodnocení uchazečů
  - Uzavření smlouvy / postup po ukončení výběrového řízení
  - Personálně-mzdová agenda zaměstnanců
- **Právní titul pro zpracování údajů:**
  - Plnění zákonné povinnosti
  - Oprávněný zájem firmy jako (potenciálního) zaměstnavatele
  - Souhlas s oslovením pro účely dalšího výběrového řízení
- **Související legislativa:**
  - Zákoník práce
- **Časté problémy:**
  - Uchovávání údajů o uchazečích a zaměstnancích po dobu delší, než je nutné vzhledem k účelu
  - Excesivní požadavky na údaje od uchazečů

2. MONITORING VNITŘNÍCH A VNĚJŠÍCH PROSTOR KAMEROVÝMI SYSTÉMY

- **Příklady relevantních účelů zpracování:**
  - Provoz kamerových systémů v provozovnách a areálech firmy
  - Provoz kamerových systémů na veřejných prostranstvích
- **Právní titul pro zpracování údajů:**
  - Oprávněný zájem (ochrana majetku firmy)
  - Veřejný zájem (ochrana veřejného pořádku a majetku třetích osob)
- **Související legislativa:**
  - Zákoník práce
  - Občanský zákoník
- **Časté problémy:**
  - Okruh osob, které mají přístup ke sledování a záznamu z kamerového systému
  - Uchovávání záznamů po dobu delší, než je nezbytně nutné
  - Shromažďování excesivního rozsahu (množství) záznamů, které je nepřiměřené danému účelu

3. AGENDA DANÍ, POPLATKŮ A SOCIÁLNÍHO ZABEZPEČENÍ

- **Relevantní operace zpracování:**
  - Výběr daně/pojistného na sociální zabezpečení a s ním související operace:
    - shromáždění, uspořádání a vedení evidence poplatníků / zaměstnanců (personální agenda, evidence ubytovaných apod.)
    - Přístup správce daně k evidencí vedené firmou jako plátcem daně, poplatku nebo pojistného na sociální zabezpečení
    - Zpřístupnění osobních údajů oprávněným příjemcům
- **Právní titul pro zpracování údajů:**
  - Plnění zákonné povinnosti
- **Související legislativa:**
  - Zákon o daních z příjmů
  - Zákon o DPH
  - Zákon o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti
  - Zákon o místních poplatcích
  - Obecně závazné vyhlášky
- **Časté problémy:**
  - Okruh zaměstnanců, kteří mají přístup k evidenci poplatníků
  - Dostatečné zabezpečení papírové dokumentace, informačních systémů a databází
  - Vztah s externími zpracovateli a datové transfery

4. UZAVÍRÁNÍ A ZVEŘEJŇOVÁNÍ SMLUV

- **Příklady relevantních účelů zpracování:**
  - Smluvní agenda související s výkonem podnikání (smlouvy s dodavateli a odběrateli)
  - Poskytování služeb potřebných pro výkon podnikání (externí účetnictví, správa IT..)
  - Smlouvy s veřejnoprávními subjekty (viz další modelová situace)
- **Právní titul pro zpracování údajů:**
  - Plnění zákonné povinnosti
  - Plnění smlouvy
- **Související legislativa:**
  - Občanský zákoník
- **Časté problémy:**
  - Zpracování osobních údajů v rozsahu širším, než je nezbytné k danému účelu
  - Uchovávání smluvní dokumentace po dobu delší, než je nutné
  - Předávání údajů třetím stranám (externí účetní apod.), aniž by o tom byl dotčený subjekt údajů informován
  - Okruh zaměstnanců s přístupem ke smluvní dokumentaci
  - Zabezpečení papírové dokumentace, informačních systémů, databází a úložišť

5. SMLUVNÍ VZTAHY S VEŘEJNOU SPRÁVOU

- **Relevantní operace zpracování:**
  - Zpracování osobních údajů pro uzavření smlouvy
  - Evidence smluv
  - Zveřejnění u smluvní strany (úřední deska, web, veřejné projednávání smlouvy..) nebo v registru smluv
- **Právní titul pro zpracování údajů:**
  - Plnění smlouvy
  - Plnění zákonné povinnosti smluvní protistrany – veřejnoprávního subjektu
- **Související legislativa:**
  - Zákon o registru smluv
  - Zákon o rozpočtových pravidlech územních rozpočtů
- **Časté problémy:**
  - Zveřejňování smluv automaticky (registr smluv, úřední deska) nebo na žádost (svobodný přístup k informacím)
  - Proporcionalita a vztah k veřejnému zájmu
  - Novinářská činnost x veřejný zájem
  - Zápisy z jednání zastupitelstev
  - Zveřejňování registru uskutečněných majetkových transakcí (nájmy apod.)

6. OBCHODNÍ AKTIVITY V RÁMCI EU

- **Relevantní operace zpracování:**
  - Smluvní vztahy s dodavateli, odběrateli a dalšími partnery
  - Vysílání zaměstnanců
  - Vztahy se zahraničními orgány veřejné moci
  - = Vždy pohyb osobních údajů na jednotném vnitřním trhu EU = volný pohyb dat
- **Právní titul pro zpracování údajů:**
  - Oprávněný zájem
  - Plnění smlouvy
  - Plnění zákonné povinnosti
- **Související legislativa:**
  - Občanský zákoník
  - Zákoník práce
  - Zákon o zpracování osobních údajů + místní legislativa ostatních členských států a jurisdikcí
- **Časté problémy:**
  - Vztahy se zahraničními dozorovými úřady
  - Neznalost zahraniční legislativy pro ochranu osobních údajů

7. OBCHODNÍ STYKY SE TŘETÍMI ZEMĚMI

- **Relevantní operace zpracování:**
  - Smluvní B2B, B2C i B2G vztahy
  - Vysílání zaměstnanců
  - Pohyb zboží obsahujícího osobní údaje
- **Právní titul pro zpracování údajů:**
  - Plnění smlouvy
  - Plnění zákonné povinnosti
- **Související legislativa:**
  - Občanský zákoník
  - Zákon o mezinárodním právu soukromém a procesním
  - Zákon o zpracování osobních údajů
- **Časté problémy:**
  - Neznalost pravidel, která je potřeba respektovat, a to:
    - Předávání založené na rozhodnutí o odpovídající ochraně
    - Předávání založené na vhodných zárukách
    - Předávání založené na výjimkách
  - Rozhodnutí o odpovídající ochraně dosud vydáno pouze pro: Andorra, Argentina, Faerské ostrovy, jurisdikce Guernsey, Izrael, Jersey, Kanada, ostrov Man, Nový Zéland, Švýcarsko, Uruguay, USA (pouze Privacy Shield)

8. ZVEŘEJŇOVÁNÍ INFORMACÍ NA FIREMNÍM WEBU

- **Relevantní operace zpracování:**
  - Zveřejnění informací o aktivitách firmy
  - PR, udržování vztahů s veřejností a podpora image firmy
- **Právní titul pro zpracování údajů:**
  - Oprávněný zájem firmy jako správce údajů
- **Související legislativa:**
  - Občanský zákoník
  - Zákoník práce
  - Zákon o zpracování osobních údajů
- **Časté problémy:**
  - Hranice oprávněného zájmu a ochrany osobních údajů:
    - Zveřejňování fotografií a kontaktů zaměstnanců a zástupců firmy
  - Hranice novinářské licence a ochrany osobních údajů:
    - Informace a fotografie z akcí firmy
    - Ilustrace života firmy
  - Ochrana osobnosti:
    - Zákaz zveřejňování fotografií jednotlivých osob bez jejich svolení dle OZ
    - NENÍ zapotřebí souhlasu dle GDPR!

9. ZVEŘEJŇOVÁNÍ INFORMACÍ VE FIREMNÍCH PERIODIKÁCH

- **Relevantní operace zpracování:**
  - Zveřejnění informací o aktivitách firmy
  - PR, udržování vztahů s veřejností a podpora image firmy
- **Právní titul pro zpracování údajů:**
  - Oprávněný zájem firmy jako správce údajů
  - Plnění smlouvy (s partnery nebo autory článků)
- **Související legislativa:**
  - Občanský zákoník
  - Autorský zákon
  - Zákon o zpracování osobních údajů
- **Časté problémy:**
  - Hranice oprávněného zájmu a ochrany osobních údajů + ochrany osobnosti zaměstnanců a partnerů:
    - Obchodní strategie nesmí „pohltit“ ochranu osobních údajů a osobnosti
  - Hranice novinářské licence a ochrany osobních údajů:
    - Informace a fotografie z akcí firmy
    - Sportovní, kulturní a společenský život firmy

10. POŘÁDÁNÍ AKCÍ, ZVANÍ ÚČASTNÍKŮ A DOKUMENTACE

- **Relevantní operace zpracování:**
  - Adresné poskytování informací o akcích firmy (obvykle e-mailem nebo osobními pozvánkami)
  - Zpracování zahrnuje zvaní, uspořádání akcí, realizaci programu + ex post informování o proběhnuvších akcích
- **Právní titul pro zpracování údajů:**
  - Oprávněný zájem
  - Souhlas (minoritně a ve zcela výjimečných případech)
- **Související legislativa:**
  - Občanský zákoník
  - Zákon o zpracování osobních údajů
  - Zákon o některých službách informační společnosti
- **Časté problémy:**
  - Hranice oprávněného zájmu a ochrany osobnosti + osobních údajů:
    - Nepřístojné osobní podrobnosti v pozvánce, adresné pozvánky zahrnující i citlivé osobní údaje
  - Hranice novinářské licence a ochrany osobních údajů:
    - Informace a fotografie z akcí firmy
    - Sportovní, kulturní a společenský život nebo odborná činnost, na které se firma podílí

11. SKARTACE, ARCHIVACE A PRÁVO NA VÝMAZ

- **Relevantní operace zpracování:**
  - Retence osobních údajů po dobu nezbytnou pro jejich zpracování
  - Praktická realizace zásady omezeného zpracování údajů
  - Realizace práva subjektů údajů na výmaz údajů
- **Právní titul pro zpracování údajů:**
  - Myslitelné jsou všechny, je vždy zapotřebí reflektovat, který z právních titulů k pokračujícímu zpracování/uchovávání údajů trvá
  - Může jít i o kombinaci několika právních titulů
- **Příklady povinné retenční doby:**
  - Účetní a daňové doklady – 5/10 let (podle druhu dokumentu)
  - Seznam společníků obchodní společnosti - 6 let
  - Mzdové listy a účetní záznamy pro důchodové pojištění – 30 let
- **Časté problémy:**
  - Neexistence skartačních a archivačních plánů:
    - Firmy často nevědí, které dokumenty jsou archiváliemi a jak s nimi nakládat
    - Častým nešvarem je neexistence systematického nastavení skartačních lhůt
  - O právu na výmaz se uvažuje i tam, kde trvá právní titul pro zpracování údajů

12. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ V PRAXI

- **Příklady relevantních opatření k zabezpečení údajů:**
  - Uzamykatelné místnosti a kusy nábytku
  - Politika bezpečných a nesdílených hesel do zařízení a systémů
  - Politika „zamčeného stolu a zamčené obrazovky“ při přechodném opuštění pracovního místa
  - Heslování flashdisků
  - Šifrování nebo zipování příloh e-mailů
  - Eliminace otevřených kopií na navzájem si neznámé adresáty
- **Povinnost správce související se zpracováním údajů:**
  - Zásada důvěrnosti a zabezpečení zpracování
  - Odpovědnost správce
- **Časté problémy:**
  - Nejasná nebo absentující pravidla pro zabezpečení údajů uvnitř organizace správce
  - Nezodpovědnost a nebo nevědomost zaměstnanců
  - Neřešení bezpečnostní situace u externích zpracovatelů

13. HLÁŠENÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ ÚDAJŮ

- **Příklady bezpečnostních incidentů:**
  - Ztracené nebo odcizené telefony, notebooky, flashdisky
  - Zapomenutá, ztracená nebo odcizená papírová dokumentace
  - Vloupání do kanceláře
  - Kybernetický útok
- **Povinnosti správce související se zpracováním údajů:**
  - V případě existence rizika hlásit do 72hod dozorovému úřadu (www.uoou.cz)
    - Povinnost zaměstnance bezodkladně hlásit incident zaměstnavateli, aby ten mohl dostát své povinnosti správce
  - V případě vysokého rizika i oznámit dotčeným subjektům údajů
    - Povinnost zaměstnance jednak hlásit zaměstnavateli a současně i identifikovat okruh osob, jichž by se incident mohl týkat
  - Odpovědnost správce za škodu způsobenou porušením povinností i vzniklou dotčeným subjektům údajů
- **Časté problémy:**
  - Nejasná nebo absentující pravidla pro hlášení případů porušení zabezpečení uvnitř organizace správce
  - Nezodpovědnost a nebo nevědomost zaměstnanců
  - Neřešení bezpečnostní situace u externích zpracovatelů

DĚKUJI ZA POZORNOST

AKADEMIE GDPR

WWW.VYSKOLENO.CZ

Tereza Šamanová | tsamanova@spcr.cz
Jindřich Kalíšek | jindrich.kalisek@prkpartners.com
Miroslava Matoušová | miroslava.matousova@uoou.cz
Daniel Joksch | daniel_joksch@cz.ibm.com
Ivan Makatura | ivan_makatura@cz.ibm.com

AKADEMIE GDPR