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

Posouzení vlivu na ochranu osobních údajů - DPIA

Posouzení vlivu na ochranu OÚ

Čl. 35 a 36 Nařízení

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

Posouzení vlivu na ochranu OÚ je nutné zejména v případech:

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

Posouzení vlivu na ochranu OÚ

Operace zpracování OÚ obsahující faktory s vysokým rizikem

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

Posouzení vlivu na ochranu OÚ

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

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

Posouzení vlivu na ochranu OÚ

Posouzení vlivu na ochranu OÚ - DPIA

- proces, který má identifikovat a podrobně popsat toky dat do a z organizace
- může se týkat i jediné operace zpracování OÚ
- může být provedena i pro několik podobných operací zpracování
- může být provedena i pro několik správců, kteří provádějí stejná zpracování (kamerové systémy, používání stejných aplikací, systémů apod.)

Posouzení vlivu na ochranu OÚ

DPIA není vyžadováno v případech:

- kdy není pravděpodobné, že zpracování ohrozí práva a svobody SÚ
- u zpracování podobných těm, u kterých již DPIA bylo provedeno
- pokud má zpracování právní základ v právu členského státu nebo EU, který stanovuje že:
  - není nutné provést DPIA
  - upravuje konkrétní zpracování
- zpracování je zahrnuto do nepovinného seznamu zpracování stanoveného DÚ

Posouzení vlivu na ochranu OÚ

Kdy je nutné provést DPIA

- mělo by být provedeno před zamýšleným zpracováním
- otázka povinnosti u již prováděných zpracování
- WP29 ovšem „důrazně doporučuje“ provedení u již existujících zpracování (mohou se měnit jedn. složky prováděné operace, účel zpracování, rozsah OÚ apod..)

Kdo má DPIA provést

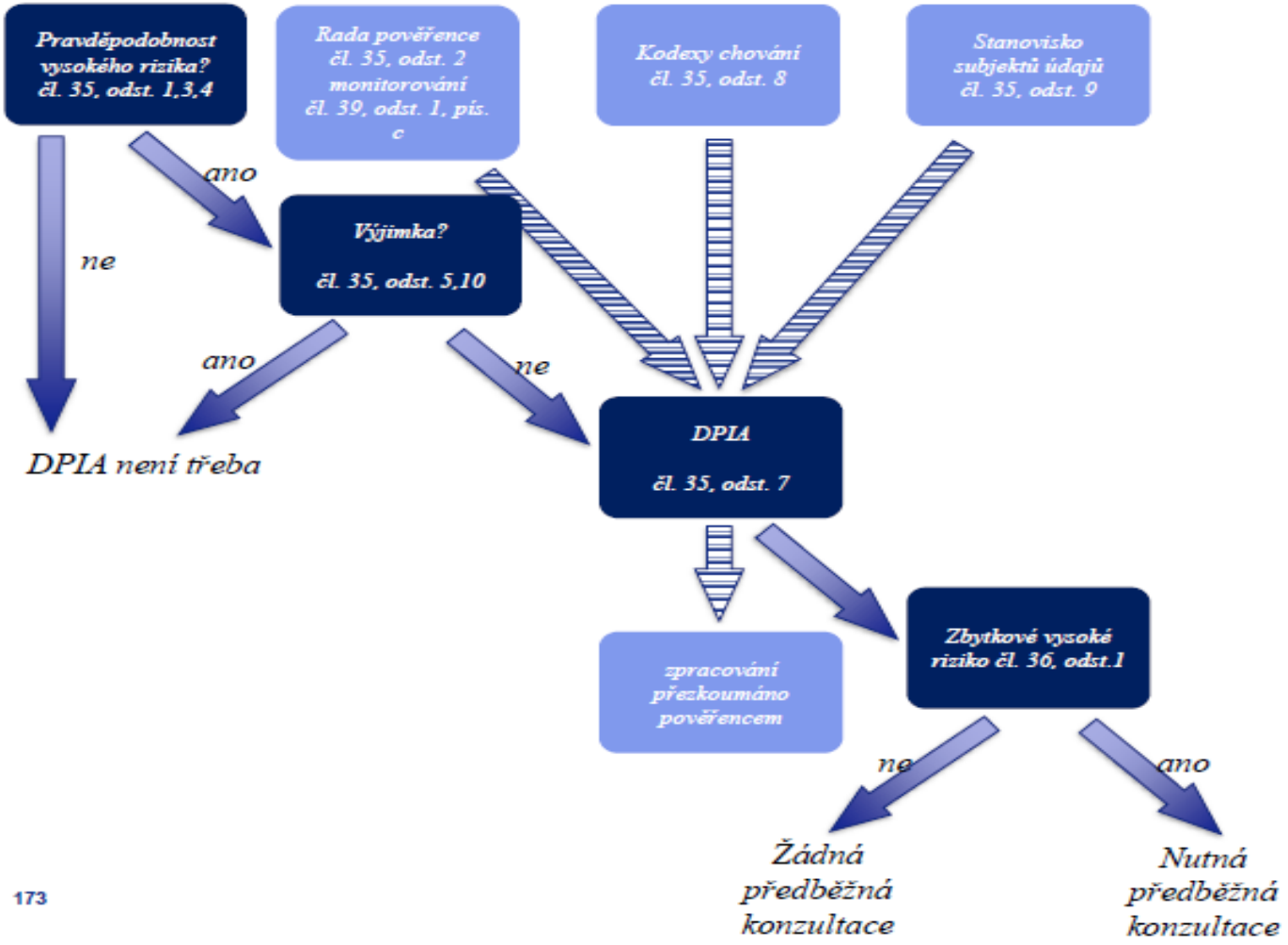
- zodpovídá vždy správce společně s DPO, pokud je jmenován
- možno provést v rámci organizace nebo zadat externě

Posouzení rizik

Posouzení rizik pro práva a svobody osob:	
/Uvést, zda je u tohoto zpracování přítomen některý z níže uvedených rizikových faktorů/	
• Automatizované, systematické vyhodnocování osobních aspektů týkající se fyzických osob včetně profilování s následným rozhodováním s právním nebo obdobně významným účinkem	
• Rozsáhlé systematické monitorování veřejně přístupných prostorů	
• Zpracování OÚ zvláštní kategorie	
• Zpracování je rozsáhlé	
• Soubory dat, které byly porovnány nebo zkombinovány	
• Zahrnutí údajů týkající se zranitelných subjektů údajů	
• Inovativní používání nebo uplatňování technologických nebo organizačních řešení (např. biometrika)	
• Přesun dat přes hranice mimo Evropskou unii	
• Pokud samotné zpracování zabraňuje subjektům údajů vykonávat právo nebo využívat službu nebo smlouvu	
Jedná se o zpracování s vysokým rizikem pro práva a svobody osob:	Ano/Ne

Posouzení vlivu na ochranu OÚ

Schéma posouzení vlivu na ochranu OÚ (DPIA)



Posouzení vlivu na ochranu OÚ

Příklady posouzení vlivu u některých zpracování

Př.: *nemocnice zpracovává údaje o zdravotním stavu pacientů. V tomto případě se jedná o rozsáhlé zpracování citlivých OÚ, přičemž mnozí pacienti mohou být současně osobami zvláště zranitelnými. Nemocnice proto bude muset provést posouzení vlivu na ochranu OÚ*

Př.: *e-shop při návštěvě jeho stránek zobrazuje zákazníkům reklamy na základě jejich dřívějších objednávek. Jedná se sice o profilování, nicméně nejedná se o systematické nebo rozsáhlé zpracování. V tomto případě nebude muset e-shop provádět posouzení vlivu na ochranu OÚ*