GDPR z pohledu dozorového úřadu

odborný seminář ISSS 2017 *GDPR – už nezbývá mnoho času*

Vít Zvánovec

úřad pro ochranu osobních údajů
the office for personal data protection

Poděkování

- PhDr. Miroslavě Matoušové, zakladatelce oboru ochrany osobních údajů v ČR a hlavní gestorce implementace GDPR do právního řádu ČR v ÚOOÚ za laskavé vytvoření první verse presentace

úřad pro ochranu osobních údajů
the office for personal data protection

Pilíře

- **kontinuita** (zásady a klíčové instrumenty)
- přesnější a podrobnější úprava oprávnění subjektu údajů
- propracovanější a náročnější pravidla pro správce a zpracovatele
- sjednocený nezávislý dozor
- předpoklad prováděcích unijních i vnitrostátních předpisů

úřad pro ochranu osobních údajů
the office for personal data protection

Hlavní novinky v GDPR

- směrnice → **nařízení**: harmonisace → unifikace (× prostor pro 120 národních výjimek)
- **rozšíření** zásad zpracování osobních údajů
- záměrná a standardní ochrana – článek 25
- přístup založený na risiku (RBA)

úřad pro ochranu osobních údajů
the office for personal data protection

Oprávnění subjektu údajů

- *být informován* – již nyní
- *mít přístup* – již nyní
- uplatnit námitky & žádat
  - opravu
  - výmaz
  - omezení
  - přenesení údajů

Zásady zpracování osobních údajů

- zákonnost, korektnost a transparentnost
- účelové omezení
- minimalisace údajů
- přesnost osobních údajů
- omezení uložení
- integrita a důvěrnost
- odpovědnost (lépe: *přičitatelnost*)

úřad pro ochranu osobních údajů
the office for personal data protection

Nástroje ochrany

- záznamy o činnostech zpracování (článek 30)
- **zabezpečení** zpracování (článek 32) ≠ bezpečnost
- posouzení vlivu na ochranu osobních údajů (DPIA, článek 35)
- předchozí konsultace (článek 36)
- pověřenec pro ochranu osobních údajů (článek 37 až 39)
- ohlášení porušení zabezpečení osobních údajů dozorovému úřadu (článek 33)
  - oznamování téhož dotčeným subjektům údajů (článek 34)
- mechanismus jediného kontaktního místa (§§ 119 a 128)
- mechanismus jednotnosti (článek 63)

úřad pro ochranu osobních údajů
the office for personal data protection

Záměrná a standardní ochrana

- článek 25
- **záměrná**: zvážená předem
- **standardní**: volby jsou nastaveny tak, aby co nejméně zasahovaly do soukromí

Záměrná ochrana

- vhodná technická a organisační opatření:
- minimalisace zpracování osobních údajů,
- co nejrychlejší pseudonymisace osobních údajů,
- transparentnost s ohledem na funkce a zpracování osobních údajů,
- umožnění subjektům údajů monitorovat zpracování osobních údajů
- umožnění správcům vytvářet a zlepšovat bezpečnostní prvky (zhotovitelé produktů, služeb a aplikací)

Standardní ochrana

- standardně se zpracovávají pouze osobní údaje, jež jsou nezbytné pro každý konkrétní účel ohledně:
  - množství
  - rozsahu zpracování
  - doba uložení
  - dostupnosti
- prevence nežádoucího zveřejnění

Přístup založený na risiku (RBA)

- risiko = pravděpodobnost × dopad
- zabezpečení zpracování
- **ohlášení** porušení zabezpečení osobních údajů: na **ÚOOÚ**
- **oznámení** porušení zabezpečení osobních údajů: **subjektu údajů**
- posouzení vlivu na ochranu osobních údajů (DPIA)
- předchozí konsultace
- pověřenec pro ochranu osobních údajů (DPO)
- předávání do třetích zemí

úřad pro ochranu osobních údajů
the office for personal data protection

Pseudonymisace

- zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez **dodatečných informací**
- dodatečné informace: uchovávány odděleně a vztahují se na ně taková opatření, že nebudou přiřazeny konkrétnímu člověku

Výsledek pseudonymisace

- vhodná záruka:
  - snížení risika pro práva subjektu údajů
  - změkčení některých povinnosti
    - práva subjektu údajů jsou totiž podmíněna schopností subjekt údajů identifikovat

Zákonnost

- Zpracování je zákonné, pouze pokud je v odpovídajícím rozsahu.
- Členské státy mohou zachovat/zavést konkrétnější ustanovení tím, že přesněji určí konkrétní požadavky na zpracování a jiná opatření k zajištění zákonného a spravedlivého zpracování.

úřad pro ochranu osobních údajů
the office for personal data protection

Zákonnost konkrétně

c) zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje

d) není

e) zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce/třetí strany – netýká se zpracování veřejnými úřady

Záznamy o činnostech zpracování

- riskantní zpracování
- citlivých údajů
- podniky s 250 a více zaměstnanci

Zabezpečení

- článek 32 odst. 1 GDPR
- schopnost
  - zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
  - obnovit dostupnost osobních údajů a přístup k nim v případě incidentů
- pravidelné testování, posuzování a hodnocení účinnosti zavedených opatření pro zajištění bezpečnosti zpracování

Výslovný pokyn

- článek 32 odst. 4:
  - „Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.“

úřad pro ochranu osobních údajů
the office for personal data protection

DPIA

- v samostatné ani přenesené působnosti není povinnost DPIA
- DPIA učiní zákonodárce adaptačním zákonem na základě článku 35 odst. 10 GDPR

Závěr

Děkuji za pozornost.