GDPR

PRO OBCE

Prezentace pro konferenci

GDPR A JEHO IMPLEMENTACE DO KRAJSKÉHO ÚŘADU

- Lukáš Lexa
- Data Protection Services, s.r.o.

Co je GDPR?

- GDPR, neboli **General Data Protection Regulation** je již platné nové Nařízení Evropského Parlamentu a Rady č. 2016/679
- Jedná se o Nařízení EU **upravující ochranu osobních údajů**
- **Je přímo použitelné**: členské státy jej nemusejí transponovat ani implementovat a jsou za jeho dodržování odpovědné (rozsudky Costa vs. E.N.E.L., Francovich vs. Itálie)
- Účinnosti nabude **25. května 2018**
- Stávající zákon č. 101/2000 Sb. bude do podstatné míry **zrušen**
- Přináší **zpřísnění požadavků** na správu a zpracování osobních údajů
- Sankce za nedodržení Nařízení jsou ve výši **až 20 milionů €** = více než 500 milionů CZK
- Zcela nově zavádí povinnost zřídit funkci **pověřence pro ochranu osobních údajů** (Data Protection Officer, dále „DPO“)

Jak se dotýká územních samospráv?

- Nová regulace explicitně dopadá i na orgány veřejné moci
- Mají povinnost zřídit funkci DPO
- Obce spravují a zpracovávají celou řadu osobních údajů, ať již v rámci samostatné nebo přenesené působnosti
- Měly by mít vyhotovené bezpečnostní směrnice (IT bezpečnost a fyzická bezpečnost) a plány pro postup v případě úniku osobních údajů
- Technická a organizační opatření za účelem ochrany osobních údajů

Kdo je DPO?

- Pověřenec pro ochranu osobních údajů (dále „*DPO*“ podle anglického označení Data Protection Officer)
- Musí disponovat odbornými znalostmi v oblasti práva a IT
- Jeho činnost může být outsourcována a může se jednat o právnickou osobu (WP 243 a FAQ)
- Je to funkce, která musí být ustanovena, nelze její plnění svěřit několika stávajícím zaměstnancům zčásti pro oblast IT a zčásti pro oblast práva a roztříštit tak zodpovědnost za výkon funkce

Postavení DPO

- Je stanoveno Článkem 38 Nařízení
  1. je správcem náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů
  2. je správcem podporován při plnění svých úkolů, jsou mu poskytovány zdroje nezbytné k jejich plnění, má přístup k osobním údajům a operacím s nimi a jsou udržovány jeho odborné znalosti
  3. správce zajistí, aby nedostával žádné pokyny, nemůže být propuštěn ani sankcionován a je přímo podřízený vrcholovým řídícím pracovníkům
  4. obrací se na něj subjekty údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů
  5. je vázán tajemstvím
  6. správce zajistí, aby nebyl ve střetu zájmů

Úkoly DPO

- Jsou stanoveny Článkem 39 Nařízení
  A. poskytuje informace a poradenství správci a jeho zaměstnancům o jejich povinnostech
  B. monitoruje soulad s Nařízením, rozdělení odpovědnosti, zvyšování povědomí a odbornosti
  C. poskytuje poradenství na požádání
  D. spolupracuje s dozorovým úřadem
  E. je kontaktním místem pro dozorový úřad

Odpovědnost DPO

- Podle Nařízení není odpovědný za nedostatky a nesmí být sankcionován ani propuštěn. **Odpovědný je vždy správce!**
- Odpovídá pouze za špatný výkon činnosti způsobenou škodou
- Pokud je zaměstnancem, odpovídá za škodu podle nařízení vlády do 4,5 násobku mzdy/platu

Proč outsourcing DPO?

- V současné době není na pracovním trhu v ČR dostatek expertů splňujících oba kvalifikační předpoklady: právo & IT
- Průměrná měsíční hrubá mzda takového experta v Praze a středních Čechách je 60-90.000 Kč (Zdroj: *Grafton Recruitment*, 2016)
- Obce si jej s ohledem na závaznou výši tabulkového odměňování nemohou dovolit
- Outsourcing je obchodně-právní vztah s určením vzájemných práv a povinností a je tak pro odběratele vyváženější, než pracovně-právní vztah
- V případě nespokojenosti lze kontrakt ukončit, kdežto zaměstnanec je s ohledem na Nařízení prakticky nepropustitelný (nelze jej propustit pro nadbytečnost nebo reorganizaci)
- V rámci outsourcingu odpovídá za skutečnou výši škody nesprávnou radou: uplatní se totiž odpovědnost za odbornou radu podle § 5 ve spojení s § 2950 občanského zákoníku
- **Outsourcing však není zbavení se odpovědnosti!**

Střet zájmů

- DPO nebude ve střetu zájmů, pokud vykonává činnost pro více obcí: obce vůči sobě navzájem nejsou v konkurenčním (soutěžním) postavení na volném trhu
- Zaměstnavatel je ovšem povinen zkoumat střet zájmů DPO (zásada Fit & Proper) v rámci organizace (funkci tedy nemůže vykonávat osoba odpovědná za IT) i mimo ni (monitoring jiných výdělečných aktivit, otázka blízkých osob)

Vaše osobní odpovědnost

- Za únik osobních údajů
- Za zneužití osobních údajů
- I pouhá nedbalost je podle § 180 trestního zákoníku trestný čin:

*„Kdo, **byť i z nedbalosti**, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné **v souvislosti s výkonem veřejné moci**, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, **bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti**.“*

Liberace

- Zbavení se objektivní odpovědnosti za správní delikt
- Pachatel vynaložil dostatečné úsilí, které je rozumné po něm požadovat, aby deliktu předešel/zabránil
- Lze preventovat selhání lidského faktoru/úmysl?
- Princip proporcionality: po malé obci nelze požadovat totéž, co po ORP/okresním/krajském městu
- Netýká se trestného činu

Není čas!

- Nařízení je již platné a účinné bude od **25. května 2018**
- Do té doby je nezbytné: ustanovit funkci DPO, provést analýzu, vyhotovit zprávu, vytvořit doporučení k nápravě, vyhotovit systém pro jejich sledování a mnohé další činnosti
- To nelze vyřešit přes noc ani za měsíc, mj. Nařízení předpokládá poskytnutí široké součinnosti ze strany správce

Co vám můžeme nabídnout?

- **Minimalistické řešení: dodávka pouze toho nejnezbytnějšího**
- Dodávání služeb vyhovujících požadavkům na funkci DPO v rámci outsourcingu, včetně provedení analýzy stavu
- Splnění kvalifikačních kritérií požadovaných Nařízením
- Hladký přechod do období účinnosti Nařízení
- Unifikované řešení přizpůsobené konkrétním požadavkům. Postupujeme podle standardů interního auditu
- Proškolení klíčových zaměstnanců
- Model společných agend a procesů

Děkujeme za pozornost

GDPR

PRO OBCE