GDPR pro veřejný sektor

JUDr. Michal Morawski

15. 11. 2017, Brno, OC NOSRETI, Křenová 409/52

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

Motivace účastníků a cíl semináře

- GDPR představuje nový právní rámec ochrany osobních údajů v evropském prostoru s cílem hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich daty a osobními údaji, chránit jejich digitální data
- zasáhne všechny fyzické i právnické osoby, ať už jako subjekty osobních údajů či správce osobních údajů
- cílem semináře je poskytnout účastníkům základní orientaci v problematice nové právní úpravy s přihlédnutím k veřejné správě a dát návod, jak v zajištění souladu s touto novou úpravou postupovat dále

Osnova přednášky

- **Úvod do problematiky;**
  co přináší GDPR nového oproti stávajícímu stavu
- **Veřejnoprávní subjekt**
- **Principy zpracování**
- **Tituly**
- **Oblasti veřejné sféry**
- **Pověřenec pro ochranu osobních údajů**
- **Specifické instituty GDPR**
- **Předávání osobních údajů do třetích zemí**
- **Postupy**
- **Dodržování základních zásad**
- **Dozorové úřady**
- **Sankce**

Úvod; co přináší GDPR nového

- **Účinnost** nabývá **25. května 2018**, GDPR je přímo závazné na území ČR i EU bez nutnosti implementace českým zákonem
- Všechny subjekty se musí na GDPR **dostatečně předem připravit**, aby zpracování osobních údajů probíhalo od 25. května 2018 zcela podle GDPR

- **Nové a širší pojmy**
- **Univerzální územní působnost**
- **Souhlas se zpracováním osobních údajů**
- **Rozšíření práv subjektů údajů**
- **Větší důraz na zajištění bezpečnosti zpracování**

Zpracování osobních údajů veřejnoprávním subjektem z pozice:

- **Subjektu, vykonávajícího veřejnou moc a plnícího úkoly ve veřejném zájmu**
- **Subjektu, jednajícího k plnění právní povinnosti**
- **Subjektu v pozici běžného správce**
- **Mohou být správcem, zpracovatelem, společným správcem**

Principy zpracování

- **Zákonnost, korektnost/férovost a transparentnost**
- **Účelové omezení**
- **Minimalizace údajů**
- **Přesnost**
- **Omezení zpracování/uložení údajů**
- **Integrita a důvěrnost**
- **Odpovědnost**
- **Proporcionalita**

Tituly

- **Souhlas**
- **Veřejný zájem, výkon veřejné moci**
- **Plnění smlouvy**
- **Splnění právní povinnosti**
- **Ochrana životně důležitých zájmů subjektu údajů**
- **Oprávněný zájem**

GDPR ve veřejné sféře

- **Široký okruh subjektů**
- **Zahrnuje úřady a instituce, které vykonávají veřejnou správu**
- **Orgán veřejné moci**

Oblasti veřejné sféry a druhy zpracovávaných osobních údajů I

Veřejná správa – přenesená působnost

- **Evidence obyvatel**
- **Občanské průkazy a cestovní doklady**
- **Živnostenské podnikání**
- **Řízení o některých přestupcích**
- **Sociálně-právní ochrana dětí**
- **Matriční knihy**
- **Hazardní hry**
- **Rozhodování o poskytování opakujících se peněžitých dávek**
- **Státní občanství**
- **Příspěvky na péči sociálních služeb**
- **Nakládání s komunálním odpadem**

Oblasti veřejné sféry a druhy zpracovávaných osobních údajů II

Veřejná správa – samostatná působnost

- **Sociální služby**
- **Kultura, sport, rekreace a cestovní ruch**
- **Školství – základní školy, školská zařízení a předškolní zařízení**
- **Nakládání s komunálním odpadem**
- **Jednotka dobrovolných hasičů**

Příspěvkové a další organizace (v rámci samostatné působnosti územně správního celku)

- **Mají vlastní subjektivitu, zpracovávají osobní údaje samostatně**
- Nejčastěji vystupují jako **správci osobních údajů, může u nich docházet ke sdílení osobních údajů** (např. příspěvková organizace a územně správní celek)
- Příklady:
  - **školy**
  - **domovy dětí a mládeže**
  - **domovy pro seniory a pro zdravotně handicapované**
  - **poskytovatelé zdravotní péče**
  - **kulturní zařízení - divadla, muzea apod.**
  - **další instituce**, např. lesní podnik, správa hřbitovů, správa komunikací

Oblasti veřejné sféry a druhy zpracovávaných osobních údajů III

- **Profesní samospráva**
  - profesní komory s povinným členstvím
  - profesní komory s nepovinným členstvím
- **Vysoké školy**
- **Poskytovatelé zdravotních služeb přímo řízené Ministerstvem zdravotnictví ČR**

Zaměstnanci; smluvní partneři; jiné

- **Personální evidence**
- **Dodavatelé** zboží a služeb
- **Veřejné budovy**

Pověřenec
pro ochranu osobních údajů I.

povinný pro

- **orgány veřejné správy a veřejné subjekty**
- **hlavní činnost spočívá v**
  - rozsáhlém pravidelném a systematickém monitorování osob
  - rozsáhlém zpracování zvláštních kategorií údajů

Pověřenec pro ochranu osobních údajů II.

- **Kvalifikovaná osoba - požadavky**
  - znalost práva včetně evropského a praxe ochrany osobních údajů
  - znalost prostředí
  - znalost informačních technologií
  - doporučené - etické předpoklady, komunikační dovednosti, systematičnost
- Jak **fyzická osoba**, tak i **právnická osoba**
- **Zaměstnanec nebo externí spolupracující osoba**
- **Společný pověřenec**

Pověřenec
pro ochranu osobních údajů III.

- **Nezávislost**
- **Nestrannost**
- **Mlčenlivost**
- **Zákaz střetu zájmů**

Pověřenec pro ochranu osobních údajů IV.

- **Náplň činnosti**

  - monitorování souladu s nařízením
  - posuzování nutnosti provést posouzení vlivu na ochranu osobních údajů
  - kontaktní osoba vůči ÚOOÚ a vůči subjektům údajů
  - musí být snadno dosažitelný

Záznamy o činnostech zpracování
Posouzení vlivu na ochranu osobních údajů

- Výjimky v GDPR z obecné povinnosti vést **záznamy o činnostech zpracování**

- **Posouzení vlivu** – povinné zejména při automatizovaném zpracování, včetně profilování, při rozsáhlém zpracování zvláštní kategorie údajů nebo při rozsáhlém systematickém monitorování veřejně přístupných prostor

- **Obecné zásady pro hodnocení dopadů regulace (RIA)**

Kodexy chování; osvědčení o ochraně údajů

- **Kodexy**

  - správcům mají sloužit jako **vodítko správné praxe při zpracování osobních**

    údajů s ohledem na specifičnost daného odvětví

  - u **orgánu veřejné moci** je **vyloučeno jejich monitorování** zvláštním akreditovaným subjektem – nejsou však vyloučeny pravomoci dozorového úřadu

- **Osvědčení**

  - **dobrovolný** institut, nikoliv povinnost

  - možnost zohlednění např. při ukládání sankcí jako přijatá technická a

    organizační opatření

Předávání osobních údajů do třetích zemí

- Pouze při **splnění podmínek** daných GDPR
- **Úroveň ochrany** fyzických osob zaručená GDPR nesmí být znehodnocena
- Předání **založené na rozhodnutí o odpovídající ochraně**
- Předání **založené na vhodných zárukách**

Postupy I.

- **Základní audit zpracování osobních údajů**
- zmapovat faktickou situaci
- zjistit, do jaké míry se instituce GDPR dotkne
- **Nastavení vnitřních procesů a zajištění odpovídající dokumentace**
- nastavit vnitřní organizaci
- připravit odpovídající dokumentaci
- proškolit zaměstnance, kteří nakládají s osobními údaji

Postupy II.

- **Revidování směrnic a dokumentů na ochranu osobních údajů**
- zajistit, aby byl text zásad zpracování osobních údajů nebo souhlasů se zpracováním v souladu s GDPR psán srozumitelně a jasně
- dodržet transparentnost a zohlednit zvláštní požadavky na srozumitelnost ve vztahu k dětem
- upravit vnitřní směrnice organizace týkající se zpracování osobních údajů
- **Revidování smluvních vztahů**
- správce
- zpracovatel
- zpracovatelské smlouvy

Postupy III.

- **Zajištění bezpečnosti zpracování osobních údajů**
- zabezpečit osobní údaje po technické a organizační stránce
- kategorizovat bezpečnostní opatření v závislosti na riziku zpracování
- zabezpečit přičitatelnost
- zajistit mechanismus detekce incidentů

Postupy IV.

- **Příprava procesů při uplatnění práva subjektů údajů**

- právo na **přístup** k osobním údajům
- právo na **opravu**
- právo na **výmaz** (právo být zapomenut)
- právo na **omezení** zpracování
- právo na **přenositelnost** údajů
- právo vznést **námitku**
- právo nebýt předmětem **automatizovaného rozhodování**

- **Příprava mechanismů pro případy porušení ochrany osobních údajů (tzv. incident)**

- ohlašovací povinnost vůči ÚOOÚ
- oznamovací povinnost vůči dotčeným subjektům údajů
- vedení evidence všech incidentů

Kontinuální dodržování základních zásad I.

- **Jasné stanovení účelu**
- **Platný právní titul zpracování**
- **Minimalizace údajů**
- **Náležité informování**
- **Bezpečnost osobních údajů**

Kontinuální dodržování základních zásad II.

- **Mlčenlivost**
- **Odpovědnost**
- **Edukace**
- **Zajištění právního titulu k případnému předání osobních údajů mimo EU/EHS**
- **Nebát se poradit s odborníky**

Dozorové úřady

- **Orgán veřejné moci**
- **Nezávislost postavení**
- **Příslušnost**
- **Evropský sbor pro ochranu osobních údajů**

Sankce

- **sankce** až do 20 mil. EUR nebo 4% ročního celosvětového obratu (podle toho, co je vyšší)
- pro **orgány veřejné moci a veřejné subjekty** mohou členské státy stanovit pravidla, zda a do jaké míry je možné jim ukládat pokuty
- problematická vágnost řady ustanovení

Závěr

Je nezbytné začít pracovat na uvedení zpracování osobních údajů do souladu s novou právní úpravou bezodkladně, tedy ihned.

Kontakt:

Advokátní kancelář Kříž a partneři, s.r.o.
Tým pro služby v oblasti GDPR

kontaktní osoba:
michal.morawski@ak-kp.cz

ADVOKÁTNÍ KANCELÁŘ
KŘÍŽ A PARTNEŘI

Děkuji za pozornost!

Tento seminář pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz