Zlínský kraj

Implementace GDPR v prostředí Krajského úřadu Zlínského kraje a příspěvkových organizací zřizovaných Zlínským krajem

16. 5. 2018
Konference k problematice GDPR ve veřejné správě,
Národní archiv Praha

Zlínský kraj

Implementace GDPR – Jak na to?

Nezbytnost, která musí být zajištěna s ohledem na:

- adekvátnost vynaložených nákladů a úsilí,
- minimalizaci nezbytné dokumentace,
- zachování zdravého rozumu,
- přiměřenosti vůči reálným podmínkám,
- nevytvoření nadbytečné administrativní zátěže.

Smluvní partner pro implementaci - I3 Consultants, s.r.o.

Smlouva o dílo nabyla účinnosti dne 28. 9. 2017.

Zlínský kraj

Etapy implementace

- Etapa 1 - Vstupní a rozdílová analýza u Krajského úřadu Zlínského kraje (dále jen „KÚZK“) a vybraných 8-mi školských příspěvkových organizací (dále jen „PO“) a 6-ti dalších PO zřizovaných Zlínským krajem (2 sociální oblast, 2 kulturní oblast, 1 dopravní oblast, 1 zdravotnická oblast)
- Etapa 2 - Vstupní a rozdílová analýza u zbývajících 104 PO zřizovaných Zlínským krajem
- Etapa 3 - Provedení analýzy informačních rizik u vybraných 8-mi školských PO a 6-ti dalších PO zřizovaných Zlínským krajem
- Etapa 4 - Zpracování typové dokumentace pro ochranu osobních údajů v souladu s GDPR
- Etapa 5 - Implementace kroků k dosažení souladu s GDPR u KÚZK – typová dokumentace pro KÚZK.

Cíle etapy 1

- Zjištění a vyhodnocení rozsahu a potřebnosti zpracování osobních údajů,
- stanovení účelů a prostředků zpracování,
- zjištění prokazatelnosti a objektivní potřeby vyžadování souhlasů se zpracováním,
- posouzení smluvních vztahů se zpracovateli osobních údajů,
- posouzení rozsahu a úrovně organizačních a technických opatření k ochraně osobních údajů,
- posouzení rozsahu a úrovně zpracované dokumentace k ochraně osobních údajů,
- posouzení kontrolní činnosti k OOÚ.

Způsob provedení:

Osobními návštěvami vybraných „testovaných“ 14 PO s týmem smluvního partnera včetně zástupce kraje.

Zlínský kraj

Zmapování zpracování osobních údajů v agendách

- V jakých agendách a činnostech jsou zpracovávány osobní údaje? (např. při výkonu státní správy, samosprávy, interních procesech, při zajištění komunikace se subjektem údaj, řešení dotací atd.).
- Proč jsou tyto osobní údaje v dané agendě nebo činnosti zpracovávány? Nutí k tomu správce nějaký zákon nebo veřejný zájem, jsou shromažďovány za účelem uzavření smlouvy nebo potřeby oprávněného zájmu, nebo jsou zpracovávány na základě souhlasu dotčené osoby?
- Jsou všechny zpracovávané osobní údaje opravdu nezbytné pro naplnění účelu, pro které jsou v agendě nebo procesu shromažďovány? (typicky nadbytečnými údaji v mnoha agendách jsou národnost, rodné číslo, číslo občanského průkazu atd.)
- Kolik osobních údajů je v dané agendě zpracováváno? (řádově stovky, tisíce atd.; je nutné hodnotit dle počtu dotčených osob, údaj je důležitý pro případné hodnocení rizika při zpracování)
- Jak dlouho budou osobní údaje uchovávány? Je určeno skartačním plánem nebo je potřeba stanovit nějakou odpovídající lhůtu?
- Kdo osobní údaje v agendě zpracovává? Vlastní zaměstnanci nebo např. externí subjekt a jeho zaměstnanci?
- Jakými prostředky jsou údaje v agendě zpracovávány? (manuálně, v listinné podobě nebo elektronicky formou strukturovaných dat v nějaké aplikaci nebo formou nestrukturovaných dat např. na pevném disku počítače, sdíleném úložišti atd.)
- Jsou osobní údaje z agendy někomu předávány a pokud ano, na základě čeho? (např. orgánům finanční správy, vyššímu správnímu celku, soudu, policii atd. na základě zvláštních zákonů).

Posouzení pravidel ochrany osobních údajů

- **fyzická bezpečnost** (vstup do objektu, klíčový režim a evidence klíčů, zajištění servrovny a aktivních prvků sítě, dostatek uzamykatelných skříní, režim úklidu kanceláří atd.),
- **administrativní bezpečnost** (evidence dokumentů, pravidla pro kopírování dokumentů, pravidla pro předávání a likvidaci dokumentů atd.),
- **personální bezpečnost** (zejména přidělování a odebírání přístupových oprávnění do aplikací v rámci životního cyklu zaměstnance nebo dodavatele služby),
- **počítačová bezpečnost** (pravidla pro elektronickou komunikaci, pro ukládání a sdílení dat, ochranu paměťových médií, zabezpečení přenosných zařízení, řízení přístupů k datům obsaženým v aplikacích a sdílených discích, auditní záznamy k těmto přístupům, evidence a přidělování vzdálených přístupů k aplikacím nebo informačním systémům, využívání administrátorských práv atd.)

Cíle etapy 2

- Seznámit ředitele příspěvkových organizací se změnami, které přináší do způsobu zpracování a ochrany osobních údajů Nařízení Evropského parlamentu a Rady (EU) 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).
- Projednat rozsah zpracovávaných osobních údajů na základě zpracovaného přehledu účelů zpracování osobních údajů, který do vzorového dokumentu vyplňovala každá zúčastněná příspěvková organizace.
- Projednat rozsah a způsob ochrany osobních údajů na základě příspěvkovou organizací vyplněného on-line dotazníku.
- Navrhnout potřebné změny ke splnění požadavků obecného nařízení o ochraně osobních údajů.

Získání přehledu o :

- Účelech zpracování,
- rozsahu zpracovávaných osobních údajů,
- reálných možnostech ochrany osobních údajů,
- reálných možnostech obsazení role pověřence pro ochranu osobních údajů,
- specifikách při zpracování.

Způsob provedení:

Cca 1 – hodinové individuální pohovory se zástupci každé zbývajících 104 PO nad vyplněnými dotazníky s týmem smluvního partnera a zástupce kraje.

Cíle etapy 3

Navrhnout metodiku analýzy informačních rizik (posouzení rizik).

Provést analýzu rizik dle metodiky I3 Consultanst,s.r.o. s cílem posoudit a navrhnout:

- hodnotu informačních aktiv obsahující osobní údaje dle metrik stanovených zákonem o kybernetické bezpečnosti,
- zranitelnosti a hrozby působící na aktiva,
- velikost a závažnost rizik z pohledu jejich dopadů a pravděpodobnosti výskytu,
- která explicitně definovaná opatření v GDPR jsou relevantní pro eliminaci identifikovaných rizik (pseudonymizace, šifrování, minimalizace atd.),
- zda stávající technická a organizační opatření jsou vzhledem k závažnosti rizik dostatečná, v případě potřeby navrhnout další potřebná opatření
- návrh a odůvodnění akceptovatelných rizik,
- zpracování plánu zvládání rizik.

Cíle etapy 4 a 5

Zajistit soulad s GDPR na PO a KÚZK schopností prokázat:

- zákonnost zpracování osobních údajů,
- záměrnou a standardní ochranu osobních údajů,
- minimalizaci zpracovávaných osobních údajů,
- korektnost a transparentnost při zpracování osobních údajů,
- odpovídající důvěrnost, integritu a dostupnost osobních údajů,
- odpovědnost správce osobních údajů.

Soulad prokázat prostřednictvím:

- provozní dokumentace ke zpracování a ochraně osobních údajů,
- stanovením role pověřence pro ochranu osobních údajů resp. referenta ochrany osobních údajů (u PO, které nemusí jmenovat pověřence),
- systémem vzdělávání zaměstnanců.

Typová dokumentace k implementaci GDPR

Pro PO (1. a později 2. aktualizovaná verze):

- Politika ochrany osobních údajů
  - Záznamy o činnostech zpracování
- Směrnice „Povinnosti osob při zpracování osobních údajů“,
- Směrnice „Výkon práv subjektu údajů“,
- Směrnice „Záměrná a standartní ochrana osobních údajů“,
- Směrnice „Bezpečnost ICT“,
- Směrnice „Ochrana osobních údajů v kamerovém systému“,
- Metodika analýzy rizik GDPR,
  - Seznam hrozeb a opatření,
  - Plán zvládání rizik,
  - Nástroj pro hodnocení rizik GDPR,

Pro KÚZK - 1 komplexní vnitřní norma:

SM/82 – Systém zpracování a ochrany osobních údajů

Zlínský kraj

Základní ustanovení vnitřní normy KÚZK

- **působnost –** pravidla závazná pro radu, zastupitelstvo, zaměstnance kraje,
- **definování základních pojmů, hlavních cílů a zásad** zpracování a ochrany osobních údajů,
- **stanovení odpovědností a povinností** pověřence, vedoucích zaměstnanců a oprávněných osob,
- **zavedení celkové evidence** osobních údajů, která je v terminologii označena jako „**Záznamy o činnostech zpracování“** dle čl. 30 GDPR, podklady pro tuto evidenci tvoří výstupy z inventury účelů zpracování osobních údajů provedených jednotlivými odbory KÚZK,
- **souhlas se zpracováním osobních údajů v** souladu s požadavky GDPR,
- **stanovení postupu pro uplatňování práv subjektů údajů,** správce musí odpovědět bez zbytečného odkladu, v každém případě do 1 měsíce od obdržení žádosti a ztotožnění žadatele (lze prodloužit max. o 2 měsíce); předpokládanou zátěží může být zejména uplatňování práva na přístup ke zpracovávaným osobním údajů,
- **stanovení postupu** pro řešení situace, kdy mohlo dojít (bezpečnostní událost) nebo došlo (bezpečnostní incident) **k porušení zabezpečení osobních údajů** s přihlédnutím k nutnosti ohlášení incidentu Úřadu pro ochranu osobních údajů a v případě vysokého rizika dopadů na práva a svobody subjektů udajů i dotčeným subjektům údajů.

Typová dokumentace – vzory, informace o zpracování

- **Vzory:**
  - dodatky ke smlouvám se zpracovateli,
  - sdělení kontaktních údajů pověřence ÚOOÚ,
  - doporučení k pracovnímu poměru pověřence,
  - souhlasů se zpracováním.

- **Informace o zpracování osobních údajů:**
  - obecná informace o zpracování osobních údajů na web organizace a kraje,
  - informace o pořizování fotografií, obrazových a zvukových záznamů z akcí,
  - informační povinnost k vybraným účelům zpracování osobních údajů.

Zlínský kraj

Děkuji za pozornost.

Mgr. Ing. Zdeněk Vašátko
vedoucí útvaru interního auditu
telefon: 577 043 580
e-mail: zdenek.vasatko@kr-zlinsky.cz