MĚSTA A OBCE V PASTI GDPR A KYBERNETICKÉ BEZPEČNOSTI

Plnění role správce a zpracovatele, proč je potřeba mít kvalitního pověřence, jak probíhají kontroly činnosti pověřence ze strany dozorových orgánů.

Bc. Radek Kubíček, MBA

Komunální veletrh Olomouc, 18.5.2023

2K CONSULTING

GDPR V ČESKÉ LEGISLATIVĚ

- ***Zákon č. 110/2019 Sb. o zpracování osobních údajů***, *který ruší zákon č. 101/2000 Sb. o ochraně osobních údajů*
- **Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů**

V nově podepisovaných dokumentech už nesmí být zák. č. 101/2000 Sb. uváděn!

2K CONSULTING

POVINNOSTI SPRÁVCE A POVINNÁ DOKUMENTACE

2K CONSULTING

ROLE PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- Správce osobních údajů
- Zpracovatel
- Pověřenec pro ochranu osobních údajů

2K CONSULTING

SPRÁVCE OSOBNÍCH ÚDAJŮ – CO JE TŘEBA MÍT ZPRACOVANÉ

* auditu připravenosti na GDPR
* aktualizace vnitřních předpisů úřadu s pravidly ochrany osobních údajů (např. změna organizačního řádu - jmenování pověřence)
* jmenování pověřence pro ochranu osobních údajů, změna pověřence pro ochranu osobních údajů, zveřejnění na webových stránkách
* výkaz činnosti pověřence pro ochranu osobních údajů/metodická, koncepční a kontrolní činnost = výkaz činnosti pověřence je požadovaným výstupem, pokud je v organizaci externí pověřenec pro ochranu osobních údajů, pro potřeby FÚ a auditu hospodaření je vhodné doložit za jaké služby daná osoba/subjekt fakturuje. Doporučení vést výkaz činnosti pověřence, aby bylo jasně dokumentováno, jak si plní povinnosti vůči správci a dle legislativy
* výroční zpráva organizace v oblasti ochrany osobních údajů

2K CONSULTING

SPRÁVCE OSOBNÍCH ÚDAJŮ – CO JE TŘEBA MÍT ZPRACOVANÉ

* zpracování a aktualizace záznamů o činnostech zpracování dl č. 30 Nařízení GDPR dle počtu agend, které organizace zpracovává (počet 33 – 50)
* zásady ochrany osobních údajů zveřejněné v elektronické a listinné podobě
* plán pověřence pro ochranu osobních údajů na kalendářní rok
* identifikace správcovsko-zpracovatelských vztahů, evidence zpracovatelských smluv
* identifikace aktiv v informačních systémech a jejich vyhodnocení v rámci rizikovosti, navržení protiopatření (analýza rizik, revize analýzy rizik), dle čl. 24, 25, 32 Nařízení GDPR
* směrnice a vnitřní předpisy pro oblasti IT, kamerové systémy, spisové služby ..
* prověření mediálních toků a obsahu informací, které jsou zveřejňovány ve vztahu k Nařízení (webové stránky, sociální sítě, webové a mobilní aplikace..)

2K CONSULTING

SPRÁVCE OSOBNÍCH ÚDAJŮ – CO JE TŘEBA MÍT ZPRACOVANÉ

* prověření smluvních vztahů se zpracovateli a doplnění nedostatečných smluv o dodatky zpracování osobních údajů
* posouzení vlivu na ochranu osobních údajů (DPIA)
* pracovní smlouva a pracovní náplň v souladu s GDPR
* zajištění spisové služby a archivnictví, vnitřní předpisy pro skartaci a likvidaci dokumentů
* zajištění pravidelného proškolení zaměstnanců v rámci ochrany osobních údajů
* jiné povinnosti vyplývající dle doporučení ÚOOU a NÚKIB

= s kvalitním pověřencem pro ochranu osobních údajů, to jde lépe.

2K CONSULTING

ZPRACOVATEL OSOBNÍCH ÚDAJŮ

- externí mzdová účetní
- dodavatel software informačních agendových systémů (Gordic, KEO, Triada) nebo IS pro evidenci čtenářů v knihovně (Clavius, Verbis)
- dodavatel software pro účetnictví, personalistiku a mzdy (Vema, Pohoda)
- IT technik nebo externí správce sítě
- poskytovatel e-mailového hostingu a hostingu webových stránek
- externí administrátor elektronického nástroje VZ
- externí služba zajišťující likvidaci fyzické dokumentace – skartace
- poskytovatelé služeb Mobilní rozhlas, Seniorpas nebo SeniorTaxi
- poskytovatelé školní matriky
- poskytovatelé služeb pro sledování služebních vozidel pomocí GPS

ZPRACOVATEL OSOBNÍCH ÚDAJŮ

- administrátor nebo organizace archivující záznamy z kamerového systému
- externí správce bytového fondu nebo lesního hospodářství
- správa a provoz útulku pro opuštěná zvířata

ZPRACOVÁNÍ OS. ÚDAJŮ – PŘÍKLADY Z ČINNOSTI OBCE

- práce v agendovém informačním systému (nahlížení, úpravy, zápisy)
- export údajů z IS a vytváření seznamů občanů v excelu, wordu
- předávání informací o dětech mezi PO a obcí
- úhrada místních a správních poplatků
- přidělování čísla popisného, povolení kácení dřevin
- zveřejňování fotografií na webových stránkách obce, na nástěnkách, ve zpravodaji apod.
- vítání občánků, blahopřání jubilantům
- výběrové řízení na nové pracovní místo
- personální a mzdová agenda – příprava podkladů ke mzdám, vedení osobní složky zaměstnance, vzdělávání

ZPRACOVATELSKÉ SMLOUVY

- smlouva je uzavírána mezi správcem a zpracovateli – obvykle formou dodatku ke stávající smlouvě o poskytování služeb

Povinné a doporučené náležitosti:

- předmět, doba trvání, povaha a účel zpracování, typ osobních údajů
- závazek mlčenlivosti
- závazek řídit se pokyny správce
- povinnost zabezpečit osobní údaje (technická a organizační opatření)
- povinnost oznámit správci případy narušení bezpečnosti
- po skončení povinnost osobní údaje vrátit nebo vymazat (včetně všech kopií)

ZPRACOVATELSKÉ SMLOUVY

- seznam sub-zpracovatelů jako příloha smlouvy (stačí i kategorie)
- kontaktní osoba za zpracovatele a pověřence na ochranu osobních údajů
- náhrada škody, vč. v případě zneužití nebo úniku osobních údajů ze strtrany zpracovatele

Doporučení ze strany kontrolních orgánů: ISO normy 27001, 27701, 90001 nově 27702 a teď bude nově NIS 2!

POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ (DPO)

- povinnost jmenovat pověřence pro ochranu osobních údajů vyplývá z Nařízení GDPR, čl. 37, odst. 1a)
- správce je povinnen zveřejnit kontaktní údaje na pověřence pro ochranu osobních údajů (v rozsahu jméno a příjmení, e-mailová adresa a telefonní číslo)
- pověřenec musí komunikovat se subjekty údajů a pravidelně řešit věci se správcem

POVINNOSTI POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ (DPO)

- **poskytování informací a poradenství** správci či zpracovateli, včetně zaměstnanců, kteří se na zpracování podílejí
- pravidelně **informovat o změnách v legislativě**, které mohou mít dopad na zpracování osobních údajů v organizaci
- provádí **pravidelné školení zaměstnanců a vedoucích pracovníků** – školení je vhodné realizovat v intervalu jednou za rok, vedení organizace si uloží prezenční listinu z takového školení nebo potvrzení o školení v případě e-learningu
- **monitorování souladu** zpracování osobních údajů s Nařízením GDPR a dalšími souvisejícími předpisy
- poradenství, pokud jde o **posouzení vlivu na ochranu osobních údajů**
- **spolupráce s dozorovým orgánem** v případě kontroly bezpečnostního incidentu

2K CONSULTING

KVALIFIKACE POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ (DPO)

- osoba disponující praxí a profesními kvalitami, odbornou znalostí práva v oblasti ochrany osobních údajů
- pověřenec musí dostatečně znát Nařízení GDPR a jiné právní předpisy
- kvalifikační předpoklady pověřence se vztahují rovněž k hlavním činnostem správce (viz požadavek čl. 37 odst. 5 Nařízení GDPR)
- pověřenec je povinen zajistit svoji snadnou dosažitelnost pro správce, subjekty údajů i dozorové orgány

POVINNOSTI POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ (DPO)

- působí jako **kontaktní místo pro dozorový úřad** v záležitostech týkajících se zpracování osobních údajů, včetně předchozí konzultace podle článku 36 Nařízení GDPR
- působí jako kontaktní místo pro subjekty údajů
- **Vzdělává se a prohlubuje své znalosti, dovednosti a zkušenosti** v souvislosti se zpracováním osobních údajů, sleduje změny a novinky v legislativě
- **Nenese odpovědnost za dodržování souladu s Nařízením GDPR v organizaci – tato odpovědnost zůstává vždy správci (tedy škole, obci, nemocnici apod.)!**

2K CONSULTING

KONTROLNÍ ČINNOST ÚOOÚ A SPRÁVNÍ TRESTY PRO OVM

2K CONSULTING

KONTROLNÍ ČINNOST ÚOOÚ

Zahájení a průběh kontroly

- rozhodnutí o kontrole
- vyrozumění správce o zahájení kontroly
- kontrola a místní šetření
- výsledek kontroly
- správní řízení

KONTROLNÍ ČINNOST ÚOOÚ

- Úřad pro ochranu osobních údajů zveřejnil mj. i témata, na která v letošním roce zaměří svoji kontrolní činnost.
  - zabezpečení osobních údajů u zpracovatele osobních údajů s tím související záznamy o činnostech zpracování (zpracovatelské smlouvy)
  - zpracování osobních údajů společností vyvíjející a provozující mobilní aplikace (Mobilní rozhlas)
  - zpracování související s rozvojem digitalizace služeb, které občanům poskytují orgány veřejné správy
- spolupráce probíhá v rámci kontrolní činnosti ve spolupráci s NÚKIB a OIP, zkušenosti jsou i ze strany České školní inspekce

KONTROLNÍ ČINNOST ÚOOÚ

- **povinnosti vyplývajících z právních předpisů a dodržování principu minimalizace údajů** (mj. v oblasti personalistiky a pracovních vztahů)
- **způsoby předávání osobních údajů a sdílení informací mezi správcem a zpracovateli** (účetnictví personalistika, IT systémy…)
- **dodržování principu transparentnosti a zveřejnění povinně zveřejňovaných dokumentů na webových stránkách organizace nebo na úřední desce**
- **plnění činnosti pověřence pro ochranu osobních údajů** – vhodné doložit písemným výkazem činnosti pověřence
- **nastavení vhodných organizačních a technických opatření** včetně zabezpečení IT systémů pro správu dat v elektronické podobě
- **kontrolní činnost výkonu činnosti pověřence**

BEZPEČNOSTNÍ INCIDENTY

Vždy je nutné vyhodnotit, k jak rozsáhlému úniku osobních údajů došlo a nakolik mohla být poškozena práva dotčených subjektů údajů.

Ne každý bezpečnostní incident je nutné hlásit Úřadu pro ochranu osobních údajů, správce by si však měl vést evidenci všech – i méně závažných – bezpečnostních incidentů!

KYBERNETICKÁ BEZPEČNOST A SPISOVÁ SLUŽBA = OCHRANA OSOBNÍCH ÚDAJU

2K CONSULTING

SPISOVÁ SLUŽBA

- „**(3)** Určení původci evidují dokumenty opatřené jednoznačným identifikátorem v evidenční pomůcce. Záznam o dokumentu v evidenční pomůcce určení původci spojí s dokumentem jednoznačným identifikátorem.
- **(4)** Vykonávají-li určení původci spisovou službu v elektronické podobě v elektronickém systému spisové služby, vedou jako samostatnou funkční část evidenční pomůcky jmenný rejstřík v elektronické podobě určený pro automatické zpracovávání údajů o odesílatelích a adresátech dokumentů evidovaných v evidenční pomůcce a jiných osobách, jichž se dokumenty evidované v evidenční pomůcce týkají. Vykonávají-li určení původci spisovou službu v listinné podobě, mohou vést jako samostatnou funkční část evidenční pomůcky jmenný rejstřík v listinné podobě určený pro zpracovávání údajů o odesílatelích a adresátech dokumentů evidovaných v evidenční pomůcce a jiných osobách, jichž se dokumenty evidované v evidenční pomůcce týkají.
- **(5)** Určení původci vedou ve jmenném rejstříku o odesílateli dokumentu, adresátu dokumentu nebo jiné osobě, jíž se dokument týká, alespoň
- **a)** jméno, popřípadě jména, a příjmení, jde-li o fyzickou osobu,
- **b)** jméno, popřípadě jmena, a příjmení, popřípadě dodatek odlišující osobu podnikatele nebo druh podnikání vztahující se zpravidla k této osobě nebo druhu podnikání, jde-li o podnikající fyzickou osobu nezapsanou v obchodním rejstříku,
- **c)** obchodní firmu nebo název, jde-li o podnikající fyzickou osobu zapsanou v obchodním rejstříku nebo právnickou osobu,
- **d)** identifikační číslo osoby, pokud bylo přiděleno,
- **e)** identifikátor datové schránky, pokud byla zřízena, a
- **f)** bezvýznamový identifikátor pro potřeby výkonu spisové služby, pokud byl určeným původcem přidělen.
- **(6)** Určení původci mohou vést ve jmenném rejstříku o odesílateli dokumentu nebo adresátu dokumentu, který je fyzickou osobou, a o jiné fyzické osobě, jíž se dokument týká, aniž by byl vyžadován jejich souhlas, údaje spadající do minimálního souboru osobních identifikačních údajů jedinečně identifikujících fyzickou nebo právnickou osobu podle přímo použitelného předpisu Evropské unie upravujícího rámec interoperability[37]), nejde-li o údaje podle odstavce 5.
- **(7)** Určení původci stanoví nejvýše **tříletou skartační lhůtu** pro údaje o fyzické osobě vedené ve jmenném rejstříku počínající běžet předáním dokumentů a spisů, ke kterým se údaje o fyzické osobě vztahovaly, nebo archivu nebo jejich zničením.
- **(8)** Určení původci jsou oprávněni využívat pro účely vedení jmenného rejstříku údaje o odesílateli dokumentu, adresátu dokumentu nebo jiné fyzické osobě, jíž se dokument týká, pokud je jejich zdrojem jimi vedený spis.

2K CONSULTING

LIKVIDACE TISKÁREN, KOPÍREK A SKENERŮ

- správná forma likvidace multifunkčních zařízení
  - podle *zákona č. 185/2001 Sb. o odpadech a o změně některých dalších zákonů*, jsou elektronická zařízení pro účely tohoto zákona vybranými zařízeními, která je nutno ekologicky likvidovat – potvrzení o ekologické likvidaci
  - moderní kancelářská zařízení mají zabudovaný pevný disk, na který se ukládají všechny dokumenty, které se na přístroji tisknou, kopírují, skenují, či posílají faxem – nutná řádná likvidace disku – pozor také při reklamaci a výměně disků – mohou obsahovat osobní údaje

KAMEROVÝ SYSTÉM

2K CONSULTING

INFORMAČNÍ POVINNOST PŘI VYUŽITÍ KAMEROVÉHO SYSTÉMU

- neuvádět informaci o tom, zda je s nebo bez záznamu

2K CONSULTING

KAMEROVÝ SYSTÉM

- před instalací kamerového systému je nutné zvážit, zda pro jeho pořízení **existují relevantní důvody** a vyhodnotit nejvhodnější umístění kamer
- sledování kamerovým systémem **nesmí nadměrně zasahovat do soukromí** osob
- kamerový systém je možné využít **jen v případě, kdy sledovaného účelu nelze** účinně **dosáhnout jinou cestou** (např. lepším zabezpečením majetku)
- užití kamerového systému je **vyloučeno v prostorách určených k ryze soukromým úkonům** (např. toalety, sprchy) – v prostorách např. šaten nebo osobních skříněk (např. na plaveckých bazénech) je monitorování kamerovým systémem povoleno pouze v případě, že jsou k dispozici vymezené prostory pro převlékání, které nejsou kamerami sledovány

2K CONSULTING

KAMEROVÝ SYSTÉM

- kamerové systémy pro zajištění bezpečnosti v obcích a městech
- kamerové systémy za účelem ochrany majetku
- kamerové systémy za účelem ochrany zdraví osob
- kamerové systémy v bytových domech
- kamerové systémy v rodinných domech
- fotopasti
- atrapy kamer

KAMEROVÝ SYSTÉM

Dokumentace k provozu kamerového systému

- interní postupy pro provoz kamerového systému a pravidla pro nakládání se záznamy z bezpečnostních kamer je vhodné zpracovat v podobě interní bezpečnostní směrnice
- základní informace o bezpečnostním kamerovém systému včetně informace o správci osobních údajů by měly být součástí provozního řádu objektu
- v prostorách vstupu je vhodné umístit piktogramy s kamerou, které informují přicházející osoby o tom, že vstupují do monitorovaného prostoru
- v případě umístění kamerového systému a pracovišti musí být stávající i noví zaměstnanci poučeni podle § 316 zákoníku práce
- správce je povinen vést záznam o činnostech zpracování dle čl. 30 Nařízení GDPR – tyto nahrazují registrační povinnost podle původního zákona č. 101/2000 Sb. o ochraně osobních údajů (zrušen 04/2019), správce si záznam o činnostech zpracování uchovává, neodesílá se ÚOOÚ
- pokud je využit kamerového systému a zpracování takto získaných osobních údajů probíhá na základě oprávněného zájmu (viz Nařízení GDPR, čl. 6, odst. 1f), je správce povinen provést tzv. test proporcionality neboli balanční test

JAK TO U NÁS FUNGUJE?

2K CONSULTING

Chcete mít kvalitního pověřence pro ochranu osobních údajů?

Fungujeme rychle, spolehlivě a klient je pro nás partner, kterého nikdy v „ průseru“ nenecháme, řešíme ochranu osobních údajů a kybernetickou bezpečnost dohromady☺

Nabízíme součástí služeb i právní poradenství, vzory dokumentu a směrnic….

2K CONSULTING

UŽIVATELSKÁ SEKCE

2K Consulting

- Hlavní stránka
- Soubory
- Organizace
- Uživatelé
- Kategorie

- Nastavení aplikace

Vítejte v uživatelské sekci společnosti 2K CONSULTING s.r.o.

V uživatelské sekci naleznete dokumentaci pro **Vaši cílovou skupinu**. Sekce zahrnuje potřebné informace a aktuality, včetně výkladu legislativy, změny v oblasti práva ve vztahu k GDPR, nov
Úřadu pro ochranu osobních údajů ČR a Evropského sboru pro ochranu osobních údajů. Dále zde najdete veškeré pokyny, vyjádření a doporučení pověřence pro ochranu osobních údajů, kte
poštou, datovou schránkou nebo e-mailem. Uživatelská sekce také obsahuje některé metodiky týkající se ochrany osobních údajů a kybernetické bezpečnosti z oblasti personalistiky a spisové

**Cílem vytvoření této uživatelské sekce bylo ušetřit Vám čas věnovaný administrativě a vytvořit ucelený systém dokumentů, který budete mít k dispozici pro Vaši potřebu, či připad
strany dozorových orgánu ČR a EU.**

Uživatelská sekce je tedy souborem dokumentů korespondujících s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti s
osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) **označované jako GDPR (General Data Protection Regulation). G
právní rámec ochrany osobních údajů platný na celém území Evropské unie**. Naleznete zde také dokumenty týkající se Zákona č. 110/2019 Sb., *Zákon o zpracování osobních údajů a jin
a vyhlášek resortu ministerstev (MV ČR, MŠMT ČR, MZ ČR, MPSV ČR) ve vztahu ke GDPR.*

Dokumenty, které zde naleznete jsou v následujících formátech.

Obrázky ve formátu jpeg, png, pdf, zip. Ostatní dokumenty ve formátu DOCX a XLSX určené pro verze Microsoft Office (formát Word a Excel).

**V uživatelské sekci máte k dispozici vzorovou dokumentaci a některé změny poznačené žlutou barvou stačí doplnit a zelenou barvou pouze aktualizovat nebo vymazat, pokud se
organizace nebo neodpovídají aktuální situaci.**

Dokumenty pro Vás budeme pravidelně revidovat, doplňovat a měnit dle stanovisek Úřadu pro ochranu osobních údajů ČR nebo vývoje legislativy. Pokud dojde k aktualizaci dokumentu, bude
aktualizace a v tomto případě v obsahu dokumentu došlo ke změně a je tak vhodné si jej stáhnout do svého PC nebo jiného uložiště v nové verzi.

Dokumenty jsou rozdělené do jednotlivých sekcí. Mohou je tak využívat zaměstnanci napříč organizací (účetní, personalistky apod.). Do uživatelské sekce máte **bezplatný** přístup po dobu trvá
poskytování služeb pověřence pro ochranu osobních údajů. V případě ukončení smluvního vztahu Vám bude přístup zrušený.

V případě obtíží se prosím obraťte na zákaznický servis 2K CONSULTING s.r.o. zastoupený Bc. Martinou Dostálovou, tel: 585 155 100, email: sekretariat@2kconsulting.cz nebo na Bc. Radka

2K CONSULTING

BEZPEČNÁ ORGANIZACE

BEZPEČNÝ ÚŘAD

https://2kconsulting.cz/kontakt/

Pojďte do toho s námi.

2K CONSULTING