GDPR – spisová služba a původci v předarchivní péči Národního archivu
Národní archiv (Mgr. Karolína Šimůnková)
22. 11. 2017

Nařízení Evropského parlamentu a Rady 2016/679 **o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) nabývá účinnost 25. května 2018**
http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1510084697564&uri=CELEX:32016R0679

- Nařízení – právně závazné v celém rozsahu EU a přímo použitelné
- **Nevztahuje se na údaje zesnulých osob**
- sankce za porušení povinností při ochraně osobních údajů **zatím** národní úpravou v případě orgánů veřejné moci v České republice navrhována na 10.000.000 Kč.

Národní archiv důrazně upozorňuje, že povinnost řádného vyřazování dokumentů ve skartačním nebo mimo skartační řízení, která je adresována původcům dle ust. § 3 zákona č. 499/2004 Sb., **není tímto evropským Nařízením dotčena. Národní archiv** stejně jako ostatní archivy dle zákona č. 499/2004 Sb. **je oprávněn ukládat** trvale **archiválie**, včetně archiválií **obsahujících osobní údaje žijících osob**, což vyplývá mj. z čl. 17 a čl. 89 GDPR.

Co bych měl udělat:

- Analýza činností souvisejících s informacemi (zejména pak s osobními údaji) – přehled agend a systémů (vedení seznamu o činnostech zpracování) – případně vytěžit a aktualizovat obdobnou analýzu provedenou v instituci z důvodu kyberbezpečnosti
- Analýza právních předpisů, na základě jejichž zmocnění shromažďujeme údaje (případně souhlas subjektu údajů, smlouva, plnění veřejného zájmu atp.)
- Stanovení postupů a politiky ochrany - analýza přístupových oprávnění, bezpečnosti uložení – dokumentů, spisů, systémů, informací.
- Proškolování zaměstnanců - správná správa hesel, řádné návyky zaměstnanců, nastavení odpovědnosti, procesy při ukončení pracovního/služebního poměru, pracovní náplně odpovídající práci s osobními údaji atp.
- **Revize spisového a skartačního řádu (doplnit všechny evidence vedené v instituci) včetně spisového a skartačního plánu (provést revizi skartačních lhůt z hlediska zákonného zmocnění a provozní potřebnosti)**
- Revize eSSSl a dalších samostatných evidencí s osobními údaji a přijetí opatření – různé cesty - logování nahlížení, přesné stanovení pole „věc“ v agendách s osobními či citlivými údaji příprava procesů včetně šablon odpovědí a nastavení lhůt na podání, která přijdou podle GDPR (čl. 12 – 22 GDPR)
- Správa dat a jejich záloh
- Stanovení postupů pro detekování bezpečnostních incidentů a řešení porušení zabezpečení

K tomu doporučujeme:

- **Ustanovení pracovního týmu/skupiny** pro provedení analýz a návrhů řešení implementace GDPR do provozu úřadu (včetně spisové služby a dalších informačních systémů), který provede výše uvedené analýzy včetně analýzy rozporů, konfliktních, rizikových míst, předloží návrhy řešení rozporů a návrhy postupů pro nově vzniklé agendy (čl. 13 – 21) a postupy pro kontrolu a ohlašovací povinnost v případě incidentu

- proškolit zaměstnance na téma GDPR a s ním související činnosti a nové agendy – rozhodně nestačí proškolit jen personalisty!
- zavést výstupy z analýz do praxe

Základní principy GDPR:

- zákonnost, korektnost, transparentnost, účel, minimalizace, přesnost, integrita, důvěrnost, omezení uložení
- konkrétní **účely**, pro které jsou osobní údaje zpracovávány, mají být **jednoznačné a legitimní** a aby byly **stanoveny v okamžiku shromažďování osobních údajů**
- osobní údaje mají **být přiměřené, relevantní a omezené** na to, co je nezbytné z hlediska účelů, pro které jsou zpracovávány
- **přesné** a v případě potřeby aktualizované;
- osobní údaje by měly být **zpracovány pouze tehdy, nemůže-li být účelu** zpracování **přiměřeně dosaženo jinými prostředky**.
- osobní údaje **zpracovávány na základě souhlasu subjektu údajů nebo s ohledem na nějaký jiný legitimní základ** stanovený právními předpisy
- je nezbytné zejména zajistit, aby byla **doba, po kterou jsou osobní údaje uchovávány, omezena na nezbytné minimum**.
- správce by měl **stanovit lhůty pro výmaz** nebo **pravidelný přezkum**. Měla by být přijata veškerá vhodná opatření, aby nepřesné osobní údaje byly opraveny nebo vymazány.
- osobní údaje by měly být **zpracovávány způsobem**, který zaručí náležitou **bezpečnost a důvěrnost** těchto údajů, mimo jiné za účelem **zabránění neoprávněnému přístupu** k osobním údajům (ISO 27001)
- správce nebo zpracovatel musí **posoudit rizika** spojená se zpracováním a **přijmout opatření** ke zmírnění těchto rizik, například **šifrování**

Pověřenec pro ochranu osobních údajů

Po 25. 5. 2018 nejpozději uvede veřejnoprávní původce kontaktní údaje na tzv. „pověřence na ochranu osobních údajů“

K činnosti a ustanovení pověřence pro ochranu osobních údajů odkazujeme na materiál:

- „Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí podle právního stavu k 10. srpnu 2017“ http://www.mvcr.cz/odk2/
- „Pověřenci ochrany osobních údajů ve služebních úřadech – metodické doporučení" http://www.mvcr.cz/sluzba/clanek/ministerstvo-vnitra-zverejnuje-metodicke-doporuceni-k-problematice-poverencu-pro-ochranu-osobnich-udaju.aspx
- „Pokyn týkající se pověřenců pro ochranu osobních údajů“ z 13. 12. 2016 z činnosti pracovní skupiny WP 29 publikovaný mj. na webových stránkách Úřadu pro ochranu osobních údajů https://www.uoou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju/d-21750

Další výklady – web Úřadu pro ochranu osobních údajů:

- **Odkazy na** https://www.uoou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju/d-21750