

GDPR v archivní praxi

PhDr. Jiří Úlovec, Mgr. Karolína Šimůnková

Setkání archivů

Praha

18. 1. 2018

Evropské předpisy

- **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 bez dalšího**
- Nařízení – právně závazné v celém rozsahu EU a přímo použitelné
- **Nevztahuje se na údaje zesnulých osob**

Evropské předpisy - GDPR

- *Nepracuje s termínem „osobní citlivý údaj“ – členské státy mohou definovat samostatně*
- *„osobními údaji“* veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby
- *Mezi osobní údaje o zdravotním stavu by měly být zahrnuty veškeré údaje související se zdravotním stavem subjektu údajů, které **vypovídají o minulém, současném či budoucím tělesném nebo duševním zdraví** subjektu údajů.*

Evropské předpisy – GDPR – základní pojmy

- **správce** - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;
- **zpracovatel** - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
- **příjemce** - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané **účely zpracování**;

Evropské předpisy - GDPR

- **zákonnost, korektnost a transparentnost**
- 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.

Evropské předpisy - GDPR

- bezpečnost a důvěrnost údajům zabránění neoprávněnému přístupu k osobním údajům a k zařízení
- správce nebo zpracovatel musí posoudit rizika spojená se zpracováním a přijmout opatření ke zmírnění těchto rizik, například šifrování. Tato opatření by měla zajistit náležitou úroveň bezpečnosti, včetně důvěrnosti, s ohledem na stav techniky, náklady na provedení v souvislosti s rizikem a povahu osobních údajů, které mají být chráněny.
(náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předaných, uložených nebo jiným způsobem zpracovaných osobních údajů, které by mohly zejména vést k fyzické, hmotné nebo nehmotné újmě).

Evropské předpisy – GDPR - VYHOVĚT, VE LHŮTĚ, ODŮVODNIT, POUČIT, BEZPLATNĚ – tj. neplatí ceníky/sazebníky archivů

Čl. 12 – procesní lhůty k vyřízení žádostí dle GDPR

- Správce **neodmítne vyhovět žádosti** subjektu údajů, ledaže doloží, že nemůže zjistit totožnost subjektu údajů.
- Správce poskytne **informace o přijatých opatřeních, a to bez zbytečného odkladu a v každém případě do jednoho měsíce** od obdržení žádosti. Lhůtu **je možné** v případě potřeby a s ohledem na složitost a počet žádostí **prodloužit o další dva měsíce**. Správce **informuje** subjekt údajů **o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad**. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.
- **Pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti subjekt údajů o důvodech nepřijetí opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.**
- **Informace podle článků 13 a 14 a veškerá sdělení a veškeré úkony podle článků 15 až 22 a 34 se poskytují a činí bezplatně.**
- Jsou-li **žádosti** podané subjektem údajů **zjevně nedůvodné nebo nepřiměřené**, zejména protože se opakují, **může správce buď: a) uložit přiměřený poplatek** zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo sdělení nebo s učiněním požadovaných úkonů; nebo **b) odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti dokládá správce.**

Evropské předpisy – GDPR - lhůty

- Poskytnu:
1 měsíc, pokud více – povinnost oznámit
prodloužení žadateli – maximálně další dva měsíce
= celkem 3 měsíce
- Nepřijmu opatření:
**1 měsíc + odůvodnění + poučení o možnosti podat
stížnost** na dozorový úřad (ÚOOÚ) případně **se
obrátit na soud**

Rekapitulace stavu



Evropské předpisy – GDPR – Kdo se ptá?



- KDOKOLIV, jehož osobní údaje prochází dokumenty či archiváliemi archivu
- Badatel
- Zaměstnanec
- Dodavatel

Rekapitulace stavu – archivnictví



Evropské předpisy - GDPR

- **Čl. 15 Právo subjektu údajů na přístup k osobním údajům**
- **Čl. 16 Právo na opravu**
- **Čl. 17 Právo na výmaz – právo „být zapomenut“ (výjimka pro archivnictví přímo v GDPR čl. 17 odst. 3 písm. d)**
- **Čl. 18 Právo na omezení zpracování**
- **Čl. 19 Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování**
- **Čl. 20 Právo na přenositelnost údajů**
- **Čl. 21 Právo vznést námitku**
- Sankce až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obrátu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší

Evropské předpisy - GDPR

Mýtus = „GDPR se archivů netýká“

Čl. 89

Záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely

- 1. Zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podléhá v souladu s tímto nařízením vhodným zárukám práv a svobod subjektu údajů. Tyto záruky zajistí, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit **dodržování zásady minimalizace údajů. Tato opatření mohou zahrnovat pseudonymizaci za podmínky**, že lze tímto způsobem splnit sledované účely. Pokud mohou být sledované účely splněny dalším zpracováním, které neumožňuje nebo které přestane umožňovat identifikaci subjektů údajů, musí být tyto účely splněny tímto způsobem.
- 2. Jsou-li osobní údaje zpracovány pro účely vědeckého či historického výzkumu nebo pro statistické účely, může právo Unie nebo členského státu stanovit odchylky od práv uvedených v člancích 15, 16, 18 a 21, s výhradou podmínek a záruk uvedených v odstavci 1 tohoto článku, pokud je pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění zvláštních účelů, a tyto odchylky jsou pro splnění těchto účelů nezbytné.
- 3. Jsou-li osobní údaje zpracovány **pro účely archivace ve veřejném zájmu, může právo Unie nebo členského státu stanovit odchylky od práv uvedených v člancích 15, 16, 18, 19, 20 a 21, s výhradou podmínek a záruk uvedených v odstavci 1 tohoto článku**, pokud je pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění zvláštních účelů, a tyto odchylky jsou pro splnění těchto účelů nezbytné.
- 4. Pokud typ zpracování uvedený v odstavcích 2 a 3 slouží zároveň k jinému účelu, povolené odchylky se vztahují pouze na zpracování pro účely uvedené ve zmíněných odstavcích.

Evropské předpisy - GDPR

Mýtus = „GDPR se archivů netýká“

Promítnutí čl. 89 do novely archivního zákona – poslední verze návrhu – prosinec 2017

„V § 78 se doplňují odstavce 4 a 5, které včetně poznámky pod čarou č. 38 znějí:

- „(4) Právo subjektu údajů na přístup k osobním údajům obsaženým v archiváliích podle čl. 15 přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů³⁸⁾ se vykonává pouze nahlížením do archiválií podle tohoto zákona.
- (5) Čl. 16 a čl. 18 až 21 přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů³⁸⁾ se na zpracování osobních údajů pro účely archivnictví nepoužijí.
- 38) Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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).“
- **Pokud bude novela schválena – nebude se GDPR v čl. 15 – 21 vztahovat na archiválie**

Evropské předpisy - GDPR

Mýtus = „GDPR se archivů netýká“

- Pokud bude novela schválena – nebude se GDPR – čl. 15 -21 vztahovat na archiválie, ale při dodržení **čl. 89 odst. 1 – minimalizace, pseudonymizace**

Čl. 89

- **Záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely**
- 1. Zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podléhá v souladu s tímto nařízením vhodným zárukám práv a svobod subjektu údajů. Tyto záruky zajistí, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit dodržování **zásady minimalizace** údajů. Tato opatření mohou zahrnovat **pseudonymizaci** za podmínky, že lze tímto způsobem splnit sledované účely. Pokud mohou být **sledované účely splněny dalším zpracováním, které neumožňuje nebo které přestane umožňovat identifikaci subjektů údajů, musí být tyto účely splněny tímto způsobem.**

Evropské předpisy - GDPR

Archiválie – badatelské nahlížení podle § 37 a § 38 zákona o archivnictví

- Osobní údaj a citlivý údaj žijící osoby zpřístupnit jen s jejím souhlasem
- Archivní soubory uvedené ve výjimce v § 37 odst. 11 zákona o archivnictví – osobní údaje lze předložit k nahlížení bez souhlasu – nelze ale bez souhlasu dál publikovat, zveřejňovat – odpovědnost přechází na badatele (nález Ústavního soudu Pl. ÚS 3/14)
- Novela § 37 – definice citlivého údaje přímo do našeho zákona, zákon o zpracování osobních údaj a GDPR pracují s obecným pojmem „osobní údaj“

Nebezpečné mýty a legendy

- „archiválie, jejichž původcem je KSČ jsou volně přístupné bez ochrany i podle jiného zákona než je zákon č. 499/2004 Sb., to bylo uzákoněno už dávno“
- „vědci mohou nahlížet bez omezení“
- „sčítací operáty mohou poskytovat i širší rodině a genealogům“
- „archivář si může nahlížet, kam chce a publikovat, co chce“
- „po sto letech od data narození můžu osobní údaje třetí osoby poskytnout každému, kdo si řekne“
- „archiválie jsou chráněné jen 30 let, pak je mohu překládat komukoliv bez dalšího“
- „jako badatel si můžu publikovat, co chci“

GDPR a předarchivní péče

Metodiky na stránkách MV

- <http://www.mvcr.cz/clanek/metodicka-podpora-a-konzultace.aspx>
- „Ochrana osobních údajů při výkonu spisové služby, zejména v informačních systémech spravujících dokumenty u veřejnoprávních původců“





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

[Mapa serveru](#)

[Textová verze](#)

[Rozšířené vyhledávání](#)

OK

Rychlé menu

Ochrana osobních údajů

Úvod

Aktuality

Legislativa

Metodická podpora a konzultace

Otázky a odpovědi

Systémové analýzy

Další dokumenty

AKTUALITY

[Implementace GDPR ve Francii](#)



Ministerstvo vnitra připravuje obdobné články s implementací GDPR i v dalších zemích.

[Ministerstvo vnitra iniciovalo vznik robota na chatování tzv. Chatbota GDPR](#)



Otázky k obecnému nařízení o ochraně osobních údajů lze klást také na stránkách Svazu...

[Ministerstvo vnitra připravuje vzorové systémové analýzy](#)



Ministerstvo vnitra připravuje zpracování systémových analýz ve vztahu ke krajům a ob...

[Katalog prací nově upravuje činnost pověřence](#)



Dne 1. ledna 2018 nabývá účinnosti nařízení vlády č. 399/2017 Sb., kterým se mění nař...

ÚVODNÍ SLOVO

Vážené dámy a pánové,

Ministerstvo vnitra připravilo pro zájemce z řad veřejné správy nové internetové stránky k problematice ochrany osobních údajů. Také touto cestou metodicky podporujeme úřady obcí, měst a krajů a jimi zřizované organizace při přípravách na účinnost nového evropského nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů známé pod zkratkou GDPR.

Na webových stránkách naleznete kromě právních předpisů, metodická doporučení, odpovědi na nejčastější otázky stejně jako odkazy na další relevantní informace a zainteresované instituce. Zveřejněny jsou také vzdělávací pomůcky - průvodce umožňující jednoduchou orientaci nařízením i odkaz na Ministerstvem vnitra iniciovaného robota na chatování k GDPR, kterému je možné klást základní dotazy a získat tak primární přehled o této problematice.

Postupně budou na stránkách zveřejněny také vzorové systémové analýzy pro obce a kraje, které umožní úřadům popsat a zhodnotit stav ochrany osobních údajů a přinesou návody pro řešení případných problémů, a tzv. checklisty, které úřadům jednoduchým způsobem umožní zkontrolovat, zda splňují zákonné požadavky v této oblasti.

Této problematice se je třeba věnovat, rozhodně však není třeba se jí obávat. Je třeba nepodléhnout nabídkám části podnikatelské veřejnosti, řídící se heslem „vystrašit a vyfakturovat“. Úřady samy mohou nejlépe zhodnotit, jaké osobní údaje využívají, jak s nimi nakládají, kdo k nim má přístup a jak jsou zabezpečeny. V tom, aby tak dělali správně, jim mají za úkol pomoci tyto webové stránky.

JUDr. PhDr. Petr Mlsna, Ph.D.
náměstek pro řízení sekce legislativy a státní správy pověřený řízením sekce veřejné správy

OCHRANA OSOBNÍCH ÚDAJŮ



Obecné nařízení o ochraně osobních údajů, označované jako GDPR (General Data Protection)

MVČR

[Nařízení GDPR](#)

[Evropská komise](#)

[Úřad pro ochranu osobních údajů](#)

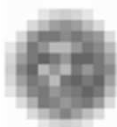
[Chatbot GDPR](#)

GDPR a předarchivní péče - **pověřenec**

- **25.5.2018 nejpozději uvede veřejnoprávní původce kontaktní údaje na tzv. „pověřence na ochranu osobních údajů“**
- **také archivy musí uvést kontakt**

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>



» Povinně zveřejňované
informace

» GDPR (Obecné nařízení)

- Základní příručka k GDPR
- Otázky a odpovědi k GDPR
- Pokyny Pracovní skupiny WP29
- Dokumenty k GDPR
- GDPR a role ÚOOÚ

» Právní předpisy

» Judikatura

» Dozorová činnost

» Nevyžádaná obchodní sdělení

» Registr

» Narušení bezpečnosti v
elektronických komunikacích

» Předávání osobních údajů do
zahraničí

» Zahraničí

» Informační systémy EU
(Schengen)

» Informační systém ORG

» Publikace

» Pro mládež

» Archiv

Cesta: Titulní stránka > Hlavní menu > GDPR (Obecné nařízení)

GDPR (Obecné nařízení)

Základní informace

[Nařízení \(EU\) 2016/679 \(GDPR\)](#) představuje právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejích občanů proti neoprávněnému zacházení s jejich daty a osobními údaji. GDPR přebírá všechny dosavadní zásady ochrany a zpracování údajů, na nichž unijní systém ochrany osobních údajů stojí a potvrzuje, že ochrana cestuje přes hranice současně s osobními údaji.

V souladu s tím dále Obecné nařízení rozvíjí a posiluje práva lidí dotčených zpracováním, a to v obou složkách: mít (získávat) informace o tom, které jejich údaje jsou zpracovávány a proč, a domáhat se dodržování pravidel, včetně nápravy stavu. GDPR klade systematicky důraz na vymahatelnost práv lidí a povinnosti správců (odpovědných za zpracování). Obsahuje proto propracovanější a náročnější pravidla pro zvláštní kategorie údajů a zpracování a současně vymáhá od správců a zpracovatelů výrazně aktivnější přístup, zejména se jedná o to, že před zahájením nového zpracování je třeba posoudit vliv jednotlivých zpracování na ochranu osobních údajů (DPIA) a zvolit vhodné nástroje ochrany údajů, za určitých podmínek si vyžádat předběžnou konzultaci u dozorového úřadu. Klíčem k nastavování povinností pro správce je rizikovitost, která je dovozována z rozsahu zpracování, zpracovávaných osobních údajů a používaných technologií.

Správci a zpracovatelé jsou za určitých podmínek povinni jmenovat pověřence pro ochranu osobních údajů. Podrobněji jsou stanoveny povinnosti při zabezpečení zpracování a nově je zavedena povinnost ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu a občanům, jichž se porušení zabezpečení týká.

Obecné nařízení výslovně upravuje nezávislost, obecné podmínky pro členy, úkoly a pravomoci dozorových úřadů v členských státech Evropské unie, EHP i Švýcarska a vzájemnou spolupráci těchto dozorových úřadů. Jednotný je také přístup k sankcím.

Rubriky

- [Základní příručka k GDPR](#)
Přehled základních pojmů a informací vztahujících se k Obecnému nařízení.
- [Otázky a odpovědi k GDPR](#)
Nejčastější otázky k Obecnému nařízení, na které je dotazován Úřad pro ochranu osobních údajů.
- [Pokyny Pracovní skupiny WP29](#)
Pokyny a ostatní materiály pracovní skupiny WP29 k Obecnému nařízení.
- [Dokumenty k GDPR](#)
Dokumenty vztahující se k Obecnému nařízení (směrnice, návrhy zákonů, brožury).
- [GDPR a role ÚOOÚ](#)
Shrnutí role Úřadu pro ochranu osobních údajů v souvislosti s Obecným nařízením.

[Rozbalit](#) celý strom složek dokumentů

Kontext

Umístění: [Složky dokumentů](#) > [Mapa stránek](#) > [Hlavní menu](#) > GDPR (Obecné nařízení)

Zobrazit aktuální dokumenty | [archiv dokumentů](#) | [dokumenty včetně archivu](#)

GDPR a předarchivní péče – web ÚOOÚ

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

- Vodítka k **ohlašování případů porušení zabezpečení osobních údajů** podle Nařízení 2016/679 (neoficiální překlad z anglického originálu)
- Vodítka k **automatizovanému individuálnímu rozhodování a profilování** podle Nařízení 2016/679 (neoficiální překlad z anglického originálu)
- Pokyny k **posouzení vlivu na ochranu osobních údajů** a ke stanovení, zda zpracování bude „pravděpodobně mít za **následek vysoké riziko**“ pro účely Nařízení 2016/679
- Pokyny WP29 **ke správnímu pokutování** (AJ)
- Pokyny týkající se **práva na přenositelnost údajů**
- Pokyny týkající se práva na přenositelnost údajů (často kladené otázky)
- Pokyny týkající se **pověřenců pro ochranu osobních údajů**
- Pokyny týkající se pověřenců pro ochranu osobních údajů (často kladené otázky) [
- Pokyny pro **určení vedoucího dozorového úřadu správce nebo zpracovatele**
- Pokyny pro určení vedoucího dozorového úřadu správce nebo zpracovatele (často kladené otázky)

GDPR a předarchivní péče

Metodiky na stránkách
ostatních ministerstev -
zdravotnictví

- http://www.mzcr.cz/Legislative/obsah/implementace-gdpr_3805_11.html



GDPR a předarchivní péče



Metodiky na stránkách ostatních ministerstev - školství

- <http://www.msmt.cz/dokumenty-3/metodicka-pomucka-k-aplikaci-obecneho-narizeni-o-ochrane>

Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství

K čemu slouží tato metodika?

Tato pomůcka si klade za cíl seznámit osoby, které vykonávají činnosti v oblasti zpracování osobních údajů v kontextu školství, s nadcházející úpravou osobních údajů představovanou nařízením Evropského parlamentu. Metodika chce být obecným interpretačním vodítkem při aplikaci jednotlivých pravidel. Jejím záměrem tudíž není rozbor konkrétních situací, které s ohledem na šíři adresátů tohoto doporučení nelze ani obsáhnout a které jsou z tohoto důvodu zpracovány pouze příkladem. Naopak se věnuje výkladu budoucí právní úpravy způsobem, který by měl její aplikaci v prostředí škol a školských zařízení zjednodušit.

Tomuto záměru odpovídá i struktura metodického doporučení, přičemž v úvodní části doporučení je popsáno, o jakou právní úpravu se jedná, na co je třeba se v souvislosti s ní připravit a dále jsou tamtéž uvedeny zásady pro další nakládání s osobními údaji. Tyto zásady se dále prolínají závěrečnou částí, která je věnována výkladu vybraných ustanovení nařízení, se kterými se v prostředí školství můžeme setkat.

Pro koho je tato metodika určena?

Metodika je adresována všem osobám, které v rámci své činnosti v oblasti školství přicházejí do styku s problematikou osobních údajů. Může se jednat například o:

- ředitele škol a školských zařízení,
- rektory vysokých škol a další akademické pracovníky,
- učitele,
- hospodáře a účetní škol,
- zaměstnance krajských a obecních úřadů,
- správce sítí, jiné pracovníky IT a další.

Co je GDPR?

Dne 25. 5. 2018 nabývá účinnosti **nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 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)** (dále jen „nařízení“), které spolu se zákonem o zpracování osobních údajů (jehož návrh je aktuálně v legislativním procesu) nahradí dosavadní právní úpravu, tj. zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

GDPR a předarchivní péče

Připravovaná novela archivního zákona –
verze prosinec 2017 - § 64 archivního
zákona

- u eSSI bude zavedena **povinnost vedení
jmenného rejstříku v el. podobě**

GDPR a předarchivní péče

Archivy by měly upozornit původce, 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. Archivy dle zákona č. 499/2004 Sb. jsou oprávněny ukládat trvale archiválie, včetně archiválií obsahujících osobní údaje žijících osob, což vyplývá mj. z čl. 17 a čl. 89 GDPR.

!

GDPR a provoz archivu



- KDOKOLIV, jehož osobní údaje prochází dokumenty/informačními systémy ve správě archivu mimo archivní fondy
- Badatel
- Zaměstnanec
- Dodavatel

Evropské předpisy - GDPR

- Čl. 15 Právo subjektu údajů na přístup k osobním údajům
- Čl. 16 Právo na opravu
- Čl. 17 Právo na výmaz – právo „být zapomenut“
- Čl. 18 Právo na omezení zpracování
- Čl. 19 Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování
- Čl. 20 Právo na přenositelnost údajů
- Čl. 21 Právo vznést námitku
- Sankce až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obrátu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší
- Národní předpis počítá se sankcí do výše 10 000 000 Kč

Evropské předpisy – GDPR - Informace poskytované v případě, že osobní údaje byly/nebyly získány od subjektu údajů čl. 13 a 14

- Informace, které mají být subjektům údajů poskytnuty podle článků 13 a 14, mohou být doplněny standardizovanými ikonami s cílem poskytnout snadno viditelným, srozumitelným a jasným způsobem přehled o zamýšleném zpracování. Pokud jsou ikony prezentovány v elektronické formě, musí být strojově čitelné.
- Informace o pověřenci

Rekapitulace stavu



Evropské předpisy - GDPR

- Povinnost **spolupracovat s ÚOOÚ** (čl. 31)
- Povinnost **zabezpečit** (čl. 32)
- Povinnost **ohlásit porušení zabezpečení** s rizikem pro narušení práv subjektu/ů údajů ÚOOÚ (do 72 hodin), při vysokém riziku narušení práva povinnost oznámit i subjektu údajů (čl. 33 a 34) (srv. s povinností nahlašovat bezpečnostní incidenty podle zákona o kybernetické bezpečnosti)
- Povinnost **vést záznamy o činnostech zpracování** (výjimky pro organizace zaměstnávající méně než 250 osob pro archivy v podstatě nepoužitelná – neplatí, když zpracování není příležitostné a představuje riziko pro práva a svobody subjektu údajů) (čl. 30)
- Povinnost **posouzení vlivu na ochranu osobních údajů** (DPIA) – jen při automatizovaném zpracování, zpracování mimo právní rámec– rozsáhlé systematické monitorování veřejných prostor (rozsáhlé monitorování veřejných prostor) – čl. 35+36
- Povinnost **jmenovat pověřence** pro ochranu osobních údajů, zveřejnit kontaktní údaje a sdělit je ÚOOÚ (DPO) (čl. 37)

Evropské předpisy – GDPR - DESATERO

1. Analýza činností původce souvisejících s informacemi (zejména pak s osobními údaji); zjištění agend a systémů, ve kterých se vyskytují osobní údaje (vedení seznamu o činnostech zpracování); možnost využít obdobnou analýzu provedenou v organizaci z důvodu zákona o kybernetické bezpečnosti.
2. Analýza právních předpisů, na základě jejichž zmocnění shromažďujeme údaje (případně souhlas subjektu údajů, smlouva, plnění veřejného zájmu atp.).
3. Stanovení postupů a politiky ochrany – analýza přístupových oprávnění, bezpečnosti uložení (dokumentů, spisů, systémů, informací).
4. Proškolení zaměstnanců: správná správa hesel, řádné návyky zaměstnanců, nastavení odpovědnosti, procesy při ukončení pracovního / služebního poměru, pracovní náplně odpovídající práci s osobními údaji atp. (GDPR se netýká „jen personalistů“!).
5. Revize pracovních smluv se zaměstnanci, doplnění doložky o ochraně osobních údajů

Evropské předpisy – GDPR - DESATERO

6. Revize spisového řádu (doplnit všechny evidence vedené u původce) a revize spisového a skartačního plánu (provést revizi skartačních lhůt z hlediska zákonného zmocnění a skutečné provozní potřeby).

7. Revize výkonu spisové služby, ISSD a dalších evidencí s osobními údaji a přijetí opatření.

8. Ověření správy dat a jejich záloh (v případě externího dodavatele prověření smluv a ošetření ochrany osobních údajů ve smlouvách).

9. Příprava procesů včetně šablon odpovědí a nastavení lhůt vyřízení podání, která přijdou podle GDPR (čl. 12 až 22 a 34 GDPR).

10. Stanovení postupů pro detekování bezpečnostních incidentů a řešení porušení zabezpečení (kdo odpovídá za nahlášení incidentu, kam oznamuji, komu atp.).

Evropské předpisy – GDPR - DESATERO

Ad) Analýza činností původce souvisejících s informacemi (zejména pak s osobními údaji); zjištění agend a systémů, ve kterých se vyskytují osobní údaje (vedení seznamu o činnostech zpracování);

<http://www.szrcr.cz/registr-prav-a-povinnosti/udaje-o-registrovanых-agendach-podle-zakona-111-2009>

+ provozní agendy + technická zařízení

2. Analýza právních předpisů, na základě jejichž zmocnění shromažďujeme údaje (případně souhlas subjektu údajů, smlouva, plnění veřejného zájmu atp.) – využít data o archivních činnostech ze základního registru práv a povinností, doplnit ostatní předpisy u dalších činností

Děkujeme za pozornost