

# GDPR při výkonu spisové služby u veřejnoprávních původců dle zákona č. 499/2004 Sb.

Mgr. Karolína Šimůnková

Národní archiv

duben 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 údajů
- 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

## 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.**

# Procesní úprava – GDPR

## Lhůty čl. 12

GDPR – nemá procesní úpravu, jen lhůty

- **Jsem schopen poskytnout odpověď**

- ✓ písemně nebo jinak,
- ✓ stručně,
- ✓ srozumitelně:

Lhůta - 1 měsíc, pokud více – povinnost oznámit prodloužení žadateli – maximálně další dva měsíce

**1 měsíc + 2 měsíce = celkem 3 měsíce**

- **Nejsem schopen přijmout opatření:**

**odůvodnění + poučení o možnosti podat stížnost** na dozorový úřad (ÚOOÚ) případně **se obrátit na soud**

**= lhůta 1 měsíc**

# Procesní úprava

- do nového zákona o zpracování osobních údajů – nejasné
- Zákon 106/1999 Sb. o svobodném přístupu k informacím?
- Správní řád 500/2004 Sb.

# Užitečné webové stránky

Úřad pro ochranu osobních údajů

Ministerstvo vnitra

Ministerstvo školství, mládeže a tělovýchovy

Ministerstvo zdravotnictví



» 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

» Nevýžádaná obchodní sdělení

» Registr

» Narušení bezpečnosti v  
elektronických komunikacích

» Předávání osobních údajů do  
zahraničí

» Zahraničí

» Informační systémy EU  
(Schengen)

» Informační systém ORG

» Publikace

» Pro míšeď

» 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 rizikovost, 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)



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

[Mapa serveru](#)

[Textová verze](#)

[English](#)

[Rozšířené vyhledávání](#)

OK

Rychlé menu

eGovernment

[Úvod](#)

[O nás](#)

[Služby pro veřejnost](#)

[Informační servis](#)

[eGovernment](#)

[EU](#)

[Nabídky a zakázky](#)

[Projekty](#)

[Legislativa](#)

[Kontakty](#)

## ZPRAVODAJSTVÍ

### [Výběrové řízení na pozici generálního ředitele České pošty](#)



Ministerstvo vnitra České republiky vyhlašuje transparentní výběrové řízení na pozici...

### [Setkání ministra vnitra Lubomíra Metnara se sportovci OLYMPU](#)



Ministr vnitra Lubomír Metnar se včera, 21. března 2018, sešel s úspěšnými sportovci ...

Marika Vitnerová - 22.3.2018

### [V Praze se konala mezinárodní konference k rozvoji dobrovolnictví](#)



Odbor prevence kriminality Ministerstva vnitra pořádal ve dnech 20. – 21. března 2018 ...

## FOTOGRAFIE DNE



### [Setkání ministra vnitra Lubomíra Metnara s eurokomisařem Julianem Kingem](#)

Ministr vnitra Lubomír Metnar se dnes, 23. 3. 2018, setkal s komisařem Evropské komise pro bezp...

[Další fotogalerie](#)

## INFORMACE

### [Společné století](#)

1918  
100  
2018

Informace k oslavám společného století

### [Prodej zajištěného majetku](#)



Automobily, televizory, počítače, domácí spotřebiče a další

## RYCHLÉ ODKAZY

[CIZINCI - FOREIGNERS](#)

[VOLBY](#)

[NEPLATNÉ PŘÍKAZY](#)

[RADA VLÁDY PRO IS](#)

[Policie ČR](#)

[Hasiči ČR](#)

[Státní služba](#)

[Registr smluv](#)



CENTRUM PROTI TERORISMU  
A HYBRIDNÍM HROZBÁM

[GDPR](#)



# Ochrana osobních údajů

[Úvod](#)[Aktuality](#)[Legislativa](#)[Metodická podpora a konzultace](#)[Otázky a odpovědi](#)[Systémové analýzy](#)[Další dokumenty](#)

## ANALÝZA OBCÍ

[Úvodní strana](#) / [Systémové analýzy](#) / [Analýza obcí](#)

### Systémová analýza obcí

Ministerstvo vnitra převzalo od dodavatele, společnosti Pražská znalecká kancelář, s.r.o., Systémovou analýzu působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů.

Výstupy analýzy vycházejí z posouzení situace u 15 vzorových měst, městských částí a obcí:

- Černošice; Děčín; Dobříš; Město Cheb; Město Karviná; Město Nymburk; Město Tábor; Město Velké Meziříčí; Město Vyškov;
- Městská část Praha 4; Městská část Praha - Zbraslav;
- Kamýk nad Vltavou; Mladý Smolivec; Srbsce; Vysoké Pole.

Těmto obcím patří poděkování za čas a úsilí, které věnovaly spolupráci s dodavatelem.

Dotazníková šetření, z nichž analýza vychází, proběhla u obcí na počátku roku 2018 a zobrazují stav připravenosti na obecné nařízení o ochraně osobních údajů v uvedené době.

Z analýzy lze vytěžit zejména následující podklady pro praxi územních samosprávných celků:

• náhled metodologie konkrétního nástroje k analýze rizik, která je dostatečně názorná, pokud by obec měla zájem rozlišk...

MVČR

[Nařízení GDPR](#)[Evropská komise](#)[Úřad pro ochranu  
osobních údajů](#)[Chatbot GDPR](#)

# GDPR a Ministerstvo vnitra

## Systémové analýzy pro kraje

## Systémové analýzy pro obce

Příloha č. 3 Systémové analýzy působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů

Přehled agend zpracovávajících osobní údaje v obcích I. stupně

Název agendy	Vedené OÚ	Právní základ zpracování	Účel zpracování	Přenositelnost	Námitka	Archivní doba
Poskytování informací dle zákona č. 106/1999 Sb.	Jméno, příjmení, titul, datum narození, trvalé bydliště, e-mail, datová schránka, podpis, rasový či etnický původ, politické názory, náboženské vyznání, filozofické přesvědčení, členství v odborech, genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu, údaje o sexuálním životě, údaje o sexuální orientaci	106/1999 Sb., - Zákon o svobodném přístupu k informacím,	Právní povinnost	Ne	Ne	84 Poskytování informací, styk s veřejností 84.1 Poskytování informací ze zákona 55 84.2 Poskytování informací - vyhodnocení A5

# GDPR a Ministerstvo vnitra - pověřenec

- **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/>
- 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>
- „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>

# GDPR a Ministerstvo vnitra

- vzorový záznam o činnostech zpracování
- volby

Záznam o činnostech zpracování - VOLBY Čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů (GDPR)
<i>Špráva: ... (název, adresa, datová schránka) ... Zástupce špráva: ... (jméno, příjmení, funkční zařazení osoby odpovědné za agendu) ... Pověřeno pro ochranu osobních údajů: ... (jméno, příjmení, e-mail) ...</i>
I. Účely zpracování
<b>ZAJIŠTĚNÍ AGENDY OBCE PODLE VOLEBNÍCH ZÁKONŮ</b>
Čl. 6 odst. 1 písm. a) GDPR - zpracování nezbytné pro plnění právní povinnosti: zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů, zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů a o změně některých zákonů, zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů, zákon č. 62/2003 Sb., o volbách do Evropského parlamentu a o změně některých zákonů, zákon č. 275/2012 Sb., o volbě prezidenta republiky a o změně některých zákonů (zákon o volbě prezidenta republiky), prováděcí právní předpisy k volebním zákonům.
II. Kategorie subjektů údajů
Občan obce – volič. Člen okrskové volební komise. Kandidát. Zmocněnec. Petent.
III. Kategorie osobních údajů
Základní identifikační údaje, státní občanství, volební právo a jeho případné omezení, číslo dokladu totožnosti, účast při hlasování; v případě členů okrskových volebních komisí údaje nezbytné pro výkon činnosti člena komise a pro jeho odměňování; v případě kandidátů a zmocněnců identifikační údaje dle kandidátní listiny a čestného prohlášení kandidáta; v případě petentů u nezávislých kandidátů identifikační údaje dle náležitosti petice.
IV. Kategorie přijemů
Členové okrskových volebních komisí pro účely plnění jejich povinností podle volebních zákonů. Kontrolní orgány (krajský úřad, státní volební komise).
V. Plánované lhůty pro výmaz kategorií osobních údajů
Platí skartační lhůty stanovené vyhláškami k volebním zákonům: ve vztahu ke kandidátním listinám a souvisejícím dokumentům - A10, pro ostatní volební dokumentaci - V5.
VI. Obecný popis technických a organizačních bezpečnostních opatření
Listinná vyhotovení volební dokumentace jsou ukládána v uzamčených prostorách a v průběhu voleb se pečeti. Přístup k elektronickým datovým souborům je zabezpečen hesly v souladu s nastavením přístupových práv vnitřními předpisy obce.

# GDPR a zdravotnictví

Metodiky na stránkách  
ostatních ministerstev -  
zdravotnictví

- [http://www.mzcr.cz/Legislative/obsah/implementace-gdpr\\_3805\\_11.html](http://www.mzcr.cz/Legislative/obsah/implementace-gdpr_3805_11.html)

Ministerstvo zdravotnictví ČR  
Ústav zdravotnických informací a statistiky ČR

**Jak implementovat  
NAŘÍZENÍ  
EVROPSKÉHO  
PARLAMENTU A RADY  
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 do resortu zdravotnictví



2018

# GDPR a školství



## 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 zapracovány 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 sítě, 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.



## MŠMT PŘIPRAVILO PRO ŠKOLY PRAKTICKÝ NÁVOD K GDPR



Praha, 15. března 2018 - Ministerstvo školství, mládeže a tělovýchovy připravilo pro školy Stručný návod na zabezpečení procesů souvisejících s GDPR ve školách. Manuál usnadní školám přípravu na obecné evropské nařízení o ochraně osobních údajů, které začne platit letos v květnu. Školy v něm najdou praktické příklady, jak bezpečně zpracovávat a uchovávat osobní údaje související s GDPR.

"Školy by si měly nejprve zmapovat, jak zpracovávají osobní údaje, a zkontrolovat také smlouvy, které se zpracování těchto dat týkají, například smlouvy s poskytovateli IT či čipových karet ke vstupu do škol. V příručce pak najdou postup, jak správně nastavit vnitřní procesy, dále také vzorové záznamy o činnostech zpracování osobních údajů, které musí každá škola povinně připravit, či vzorovou směrnici o nakládání s osobními údaji, kterou mohou využít," uvedla náměstkyně pro řízení sekce legislativy a mezinárodních vztahů Ministerstva školství, mládeže a tělovýchovy **Dana Prudíková**. Školy by také měly mít pověřence pro ochranu osobních údajů, přičemž MŠMT v tomto doporučuje spolupracovat se zřizovatelem školy. Informace o zpracování osobních údajů by pak školy měly uveřejnit například i na svém webu.

Materiál je členěný do pěti částí, které se tematicky věnují obsahu zpracovatelských smluv, vzoru vnitřního předpisu, příkladům zpracování osobních údajů až po podrobné vzorové záznamy o činnostech zpracování pro mateřské, základní, střední i vyšší odborné školy. Jeho přípravu MŠMT konzultovalo s Úřadem pro ochranu osobních údajů a Ministerstvem vnitra, kteří jsou gestory předpisu.

[Kontakty pro média](#)[Tiskové zprávy](#)[Ministr](#)[Logo MŠMT](#)[Archiv tiskových zpráv](#)

# GDPR a školství

- Stručný návod na zabezpečení procesů souvisejících s GDPR ve školách (nástin pracovního postupu)
- Záznamy o činnostech zpracování

# GDPR a školství - Záznamy o činnostech zpracování

## Záznam o činnostech – školní matrika, evidenční listy

### Činnosti

1. Evidence ve školní matrice
2. Evidenční listy školy dítěte/žáka/studenta
3. Evidence doplňujících údajů pro předávání údajů

Jméno a  
kontaktní  
údaje správce:

Jméno a  
kontaktní údaje  
pověřence:

Osobní údaje

Subjekt údajů

Účel zpracování

Popis technických  
opatření

Popis bezpečnostních  
a organizačních  
opatření

Kategorie příjemců  
(včetně zahraničních  
subjektů)

Informace o  
případném  
předání do třetí  
země

Plánovaná  
lhůta pro  
výmaz

1. Evidence ve školní matrice

# GDPR a knihovny – Národní knihovna

Oborové  
báze dat

Odborné  
činnosti

Legislativa,  
standards

Akce,  
vzdělávání

Statistika,  
dokumenty

Adresáře, e-  
konference

Spolky,  
sdružení

Soutěže a  
ceny

Programy  
podpory

Oborová  
brána KIV



Nacházíte se zde: [Úvod](#) > [Legislativa, standardy](#) > [Legislativní dokumenty](#) > [Ochrana osobních údajů](#) > [Ochrana osobních údajů - Příručka pro knihovny](#)

## Ochrana osobních údajů - Příručka pro knihovny

*Tato příručka si klade za cíl konkretizaci povinností vyplývajících knihovnám z 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, známého též pod zkratkou GDPR (dále jen Nařízení). Příručka odráží stav problematiky k 7. 2. 2018. Postupně budou doplňovány další příklady a úpravy podle vývoje legislativy a získaných zkušeností.*

### Náměty a dotazy

### Obsah

Účel příručky a práce s ní

- [Legislativa, standardy](#)
- [Legislativní dokumenty](#)
  - [Knihovní zákon 257/2001 Sb. a návazné prováděcí přepisy](#)
  - [Povinný výtisk](#)
  - [Autorské právo](#)
  - [Svobodný přístup k informacím](#)
  - [Osiřelá díla](#)
  - [Ochrana osobních údajů](#)
    - [Ochrana osobních údajů - Příručka pro knihovny](#)

# GDPR a předarchivní péče

Připravovaná novela archivního zákona –  
verze prosinec 2017

POZOR na § 64 archivního zákona (zákon  
č. 499/2004 Sb.)

# 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

# Právo být zapomenut – ne v úřadě!

- Činnost úřadů – obvykle definována v právních předpisech – tj. zákonné zmocnění
- Není-li zákonné zmocnění – nutný souhlas subjektu údajů
- Veřejnoprávní původci – povinnost spisového řádu a plánu dle § 66 zákona č. 499/2004 Sb.
- Spisový plán – skartační lhůty – některé ze zákona
- Princip skartační lhůty – ne neodůvodnitelně dlouhá, ne neodůvodnitelně krátká – archivy nejsou provozní spisovny státní správy a samosprávy
- Čl. 17 – neplatí v archivnictví

# Právo být zapomenut – ne v úřadě!

Spisový znak	Popis věcné skupiny	Skartační znak a lhůta
-----------------	---------------------	---------------------------

27/9	Služební cesty – zahraniční i tuzemské	V- 5
------	--	------

27/10	Dovolená a zastupování	S -5
-------	------------------------	------

27/11	Oficiální návštěvy ze zahraničí - přijetí	A -2
-------	---	------

**Skartační lhůta – ne krátká, ne dlouhá - správná**

# GDPR a předarchivní péče

- **Všichni původci dle zákona č. 499/2004 Sb. by měli vědět, 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 – ukládání vybraných archiválií veřejnoprávních původců v síti veřejných archivů

- Dokumenty/spisy vybrané za archiválie dle zákona č. 499/2004 Sb. lze bez jakéhokoliv rizika uložit ve veřejném archivu – archivy mají zmocnění k ukládání archiválií včetně jakéhokoliv typu osobního údaje
- Čl. 89 – odpovědnost za řádnou správu a zabezpečení osobních údajů přechází na archiv
- Národní úprava může přijmout výjimku pro archivnictví z čl. 15 – 21 GDPR

# Co je špatně v této reportáži?

- <http://www.ceskatelevize.cz/porady/1097181328-udalosti/217411000100921/video/569990>
- Jako úředník se nevrhám ke skartovačce jen proto, že úřední dokument obsahuje osobní údaje! Dokumenty/spisy s osobními údaji vyřazují v procesu skartačního řízení poté, co jim uplynuly skartační lhůty, příslušný archiv dokumenty/spisy posoudil, některé z nich vybral k trvalému uložení (předávám do archivu) nebo dal souhlas s jejich zničením (zničím). NE DŘÍVE!

## 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

# 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 – 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.).

Děkuji za pozornost