

**Sdružení hasičů Čech, Moravy a Slezska – Starosta sdružení,  
Římská 45, Praha 2**

**Metodický pokyn starosty SH ČMS**

Ročník : 2018

V Praze dne: 25. května 2018

Číslo: 3

**Metodický pokyn starosty SH ČMS  
k plnění obecného nařízení EU o ochraně osobních údajů GDPR  
v Kanceláři SH ČMS**

**I.**

**Úvodní ustanovení**

V souladu s ustanovením čl. 50 Stanov SH ČMS v platném znění a na jejich základě vydaným Organizačním řádem čl. 15, je vydáván Metodický pokyn starosty SH ČMS k plnění obecného nařízení EU o ochraně osobních údajů GDPR v Kanceláři SH ČMS, který je závazný pro všechny kmenové a externí zaměstnance.

**II.**

**Evropské nařízení o ochraně osobních údajů fyzických osob**

GDPR – evropské nařízení o ochraně osobních údajů fyzických osob „General Data Protection Regulation“ účinné od 25. května 2018

**III.**

**Zákon č. 101/2000 Sb., o ochraně osobních údajů**

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů bude účinností Obecné nařízení o ochraně osobních údajů dne 25. května 2018 zrušen.

**IV.**

**Definice osobních údajů.**

Osobním údajem je jméno a příjmení konkrétní osoby, příp. jakýkoli jiný údaj, který umožní konkrétní osobu ztotožnit např. telefonní číslo, emailová adresa, bydliště, tedy veškeré údaje na základě kterých je fyzická osoba identifikovatelná (lze ji přímo či nepřímo identifikovat).

**Osobní údaje**

Jméno a příjmení	Pohlaví	IP adresa	Fotografie
Věk a datum narození	Občanství	stav	RČ nebo jiný identifikátor vydaný státem
Email adresa	Telefonní číslo	Adresa bydliště	Adresa pracoviště

## V.

### Vymezení pojmů správce, zpracovatel, zpracování a subjekt údajů.

Správce je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

Zpracovatelem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Zpracováním jakákoliv operace s osobními údaji např. ukládání, nahlédnutí, vyhledávání.

Subjektem údajů je fyzická osoba, jíž se osobní údaje týkají. Subjekt údajů není právnická osoba. Údaje vztahující se k právnické osobě tak nejsou osobními údaji. Osobní údaje mohou být pouze ve vztahu k žijící fyzické osobě, jelikož Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách.

## VI.

### Práva subjektů údajů

Mezi práva subjektu údajů, která jsou mnohdy založena na aktivitě subjektu údajů, patří právo na přístup k osobním údajům, právo opravu, resp. doplnění, právo na výmaz, právo na omezení zpracování, právo na přenositelnost údajů, právo vznést námitku a právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování.

Co se rozumí přístupem k osobním údajům?

Přístupem k osobním údajům se rozumí právo subjektu údajů získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

- účely zpracování,
- kategorie dotčených osobních údajů,
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- plánovaná doba, po kterou budou osobní údaje uloženy,
- existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
- právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

Subjekt údajů má právo na opravu nepřesných osobních údajů, které se ho týkají. Neznamená to povinnost správce aktivně vyhledávat nepřesné údaje (avšak nic mu v tom ani nebrání), ani to neznamená povinnost správce např. každoročně požadovat po subjektu údajů aktualizaci jeho údajů. Pokud se subjekt údajů domnívá, že správce zpracovává jeho nepřesné údaje, upozorní jej na to. Je povinností správce, pokud mu subjekt údajů oznámí, že požaduje opravu jeho osobních údajů, zabývat se jeho žádostí.

Právo na výmaz (být zapomenut) představuje v Obecném nařízení jinými slovy vyjádřenou povinnost správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna podmínka:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznesl námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně,

- osobní údaje musí být vymazány ke splnění právní povinnosti,

## VII.

### Zpracování a zveřejňování osobních údajů.

Kancelář SH ČMS a její zaměstnanci zpracovávají osobní údaje členů SH ČMS za účelem evidence odborností, funkcí, ocenění, dobrovolné činnosti, sportu, úrazového pojištění a pro účely dotační politiky ministerstev a krajských úřadů. Dále zveřejňují osobní údaje v médiích, na sociálních sítích, webových stránkách a na veřejných sportovních a společenských akcích zpracovatele a za účelem marketingu (zejména v propagačních materiálech a letácích).

Okresní sdružení hasičů (OSH) u členů zpracovává **Jméno a příjmení, rodné číslo z jehož vyplývá datum narození, adresu bydliště, fotografie, emailové adresy a telefonního čísla.**

Odsouhlasené osobní údaje zpracovává zpracovatel OSH dle členské přihlášky v centrální evidenci SH ČMS a následně při další činnosti spolku. (viz Směrnice č.1 starosty SH ČMS k nakládání s osobními údaji členů SH ČMS ze dne 29. 9. 2016)

Dle čl. 15 odst. 2 Stanov SH ČMS vedou (OSH) v obvodu své působnosti seznam (evidenci), okrsků, sborů a členů sdružení, působících v registrovaných sborech čímž jsou hlavními zpracovateli osobních údajů.

SH ČMS jako hlavní spolek dle č. 16 odst. 1 stanov je zpracovatelem i správcem osobních údajů.

Dále tento Metodický pokyn obsahuje parametry a stanoví povinnosti jednotlivých kmenových i externích zaměstnanců Kanceláře SH ČMS.

## VIII.

### Kancelář SH ČMS jako zaměstnavatel

Zaměstnavatel zpracovává osobní údaje zaměstnanců většinou z několika různých „zákonných právních důvodů“:

- osobní údaj na pracovní smlouvě (ta bude jistě uložena v elektronické či listinné podobě u zaměstnavatele,
- dále zaměstnavatel poskytuje ze zákona osobní údaje zaměstnanců například správě sociálního zabezpečení za účelem řádné evidence apod.

V tomto ohledu nezavádí Nařízení pro zaměstnavatele žádné nové povinnosti.

Pro zveřejnění osobních údajů zaměstnanců na webových stránkách zaměstnavatele je nutné výslovný souhlas zaměstnanců. Pokud zaměstnanec nesouhlasí, zaměstnavatel údaje zveřejnit nemůže.

## IX.

### Kancelář SH ČMS

Kancelář SH ČMS zpracovává osobní údaje členů SH ČMS, kteří již dali souhlas ke zpracovávání jejich osobních údajů, a to:

- k evidenci registrace statutárních a revizních orgánů hlavního a pobočných spolků
- v přihláškách na spolkové soutěže a kulturní a společenské akce
- v přihláškách na sportovní soutěže

- v přihláškách na školení odborností
- v přihláškách k účasti na školní výuku
- v návrzích na ocenění
- zveřejňováním v sociálních sítích a na webových stránkách SH ČMS
- zveřejňováním v tištěných materiálech a médiích SH ČMS
- zveřejňováním na výukových a propagačních materiálech

Tyto osobní údaje, zpracovávané v Kanceláři SH ČMS je nutné chránit a zabezpečit.

Zabezpečením obecně rozumíme taková opatření, která zajistí, že objekt zabezpečení nebude dostupný neoprávněným osobám

- zabezpečení fyzické – znamená zabránit fyzicky tomu, aby se neoprávněná osoba dostala k našim aktivům
- zabezpečení dat – znamená zabránit tomu, aby neoprávněná osoba při fyzickém styku s počítačem (či jiným zařízením) mohla přistoupit k datům

## **X.**

### **Zabezpečení**

#### **Fyzické:**

- při odchodu (i dočasném) zamykání kanceláří, zavírání dveří budovy
- při odchodu od počítače (i dočasném) ukončit práci s aplikacemi zpřístupňující osobní údaje
- při odchodu od počítače (i dočasném) uzamknout počítač
- při odchodu od počítače (trvalém) vypnout počítač
- dbát bezpečnosti při práci s tištěnými výstupy obsahující osobní data. Tyto uzamykat do skříní a neponechávat na stolech.
- návštěvy zaměstnanců z řad členů SH ČMS a dalších fyzických osob přijímat pouze na vyhrazeném místě Kanceláře SH ČMS. Zasedací místnost na chodbě (skleník).

#### **Zabezpečení dat:**

Zabezpečením dat rozumíme opatření, které neoprávněnému uživateli zabrání přečíst data tam, kde k nim má fyzický přístup.

Fyzický přístup může být

- legální – [www.evidencesdh.cz](http://www.evidencesdh.cz) (dodržovat Směrnici starosty SH ČMS č.1/2016)
- ilegální – prolomení fyzické ochrany, odposlouchávání komunikace
- neurčitý – data zveřejněná nedopatřením

Existují dva základní způsoby zabezpečení dat a jejich ochrany proti neoprávněnému užívání ve skutečnosti se tyto způsoby prolínají a kombinují

#### **HESLA**

- pro přístup k datům je třeba znát heslo

#### **ŠIFROVÁNÍ**

- data jsou ve formátu, který při běžném čtení nedává smysl

## **XI.**

### **Hesla**

Skupina znaků, jejíž znalost je podmínkou pro přístup k daným datům

Základní principy práce s hesly:

- hesla/PINy/přístupové kódy nikomu nesdělujeme
- hesla na počítače v Kanceláři SH ČMS, volíme tak aby bylo dostatečně silné, ale které si zároveň můžeme zapamatovat

- pokud možno volíme pro různé přístupy různá hesla

### **Složení hesel u přístupu k datům:**

- heslo by mělo mít alespoň 9 znaků
- mělo by se skládat alespoň z velkých a malých písmen a číslic, lépe přidat speciální znaky  
náhodná kombinace: xS4A.2()2xG8
- zapamatovatelná kombinace: (hAs3).iCi
- heslo by mělo být zapamatovatelné
- hesla zásadně nikam nepíšeme, takové heslo nemá smysl

### **Tři základní způsoby prolomení hesla, kterým se musí zpracovatel vyvarovat:**

- **vyzrazení hesla** – zde útočník ve skutečnosti nic neprolamuje, přistupuje k datům jako řádný uživatel s řádným heslem – velmi častá situace
- **slovníkový útok** – útočník zkouší hesla ze seznamu, případně se pokouší heslo odvodit
- **útok hrubou silou** – útočník postupně zkouší všechny kombinace znaků, až najde to pravé. Útočník zkouší postupně (s pomocí stroje) všechny kombinace znaků a bezpečnost záleží na tom, kolik takových hesel může existovat. Počet možných kombinací je ovlivněn délkou hesla a počtem možných znaků. Krátké heslo je málo bezpečné, protože čas vynaložený na vyzkoušení všech kombinací je také krátký.

Složitost hesla by měla odpovídat tomu, jak „citlivá“ jsou chráněná osobní data

## **XII.**

### **Přenos informací (komunikace)**

V mnoha případech je nutné zabezpečit, aby neoprávněné osoby neměly přístup k přenášeným informacím:

- z důvodu zákona
- z důvodu osobní preference

### **Přenos elektronickou cestou:**

- předání na elektronickém médiu
- e-mail (elektronická pošta)
- veřejná úložiště
- privátní úložiště

### **Předání na elektronickém médiu:**

Jedná se o média:

- CD, DVD, flash

Kromě speciálních flash disků nejsou data nijak chráněná proti neoprávněnému přístupu v případě získání fyzického média.

Smazání souboru z média běžným způsobem neznamená odstranění souboru – obnovení je pro znalého člověka otázkou vteřin.

**Osobní údaje na elektronické médiu se nesmí nikdy kopírovat a nikomu poskytovat.**

### **Elektronická pošta (e-mail):**

Elektronická pošta (e-mail) je v běžné podobě nešifrovaná tzn. že text prochází internetem tak, že není problém jej odposlechnout a přečíst. Pokud posíláte citlivé přílohy, měly by být chráněny šifrováním a heslem.

Pro heslo platí obecné zásady pro tvorbu a použití hesel odst. 9 Metodického pokynu.

**Hesla samotná přitom NIKDY neposíláme e-mailem, ale jiným kanálem (např. SMS, ústně)**

### **Veřejné úložiště:**

Primárně je určeno pro veřejné sdílení informací, pokud vložíme data, jsou veřejně přístupná. Data lze chránit heslem, ale stále samotný soubor bývá veřejně přístupný.

Pro heslo platí obecné zásady pro tvorbu a použití hesel odst. 9 Metodického pokynu.

**Bez šifrování a hesla je použití veřejného úložiště zapovězeno a pro osobní data nelze tento způsob doporučit vůbec.**

### **Privátní úložiště:**

Optimální možnost přenosu osobních dat.

- úložiště je privátní prostor organizace
- úložiště je zabezpečeno šifrováním a vícefaktorovou autentizací

### **Jak tedy komunikovat?**

Vždy záleží na „citlivosti“ informací:

Osobní údaje a další citlivé informace nikdy neposíláme bez dostatečného zajištění ochrany heslem (ideálně zabalit do archivu ZIP a chránit heslem, případně alespoň zaheslovat soubory DOC a XLS) a omezit veřejné úložiště.

## **XIII.**

### **Odpovědnost zpracovatelů a správců osobních údajů**

Každý zaměstnanec Kanceláře SH ČMS, který musí při zpracovávání osobních údajů postupovat dle tohoto Metodického pokynu s veškerou pečlivostí. Osobní údaje pečlivě chránit proti zcizení třetí osobou. Nesmí údaje předávat třetí osobě k jakýmkoliv účelům a v případě úniku dat toto okamžitě nahlásit řediteli Kanceláře SH ČMS, případně Úřadu na ochranu osobních údajů.

## **XIV.**

### **Závěrečná ustanovení**

Metodický pokyn starosty SH ČMS k plnění obecného nařízení EU o ochraně osobních údajů GDPR v Kanceláři SH ČMS nabývá platnosti dnem schválení starostou SH ČMS 25. 5. 2018.

V Praze dne 25. 5. 2018

Ing. Karel Richter v.r.  
Starosta SH ČMS