Směrnice k nakládání s osobními údaji SK Teplice, z. s.

vypracovaná v souladu s Nařízením 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)

Datum poslední aktualizace: 01. 08. 2018

1 Úvod do problematiky ochrany osobních údajů

Dne 27.4.2016 bylo přijato 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), v anglickém jazyce General Data Protection Regulation – GDPR) (dále jen „**Nařízení**" nebo „**GDPR**").

GDPR představuje nový právní rámec ochrany osobních údajů a má za úkol maximálně chránit práva občanů EU proti neoprávněnému nakládání s jejich osobními údaji. Toto Nařízení bylo přijato formou evropského nařízení, znamená to tedy, že je jednotně platné napříč všemi státy EU, a je přímo účinné v celém evropském prostoru dne 25.5.2018.

Řadu pravidel oblasti osobních údajů již známe z předchozí právní úpravy, GDPR však zavádí celou řadu pravidel nových. Mezi taková práva patří např. právo na výmaz a také právo „být zapomenut". Jejich platnost a dodržování musí každý správce osobních údajů (takže nepochybně i **SK Teplice, z. s.**) zajistit a musí být také schopen doložit, že k zákonnému zpracování osobních údajů opravdu dochází.

GDPR poskytuje lidem, kterým údaje patří (tj. subjektům údajů - např. zaměstnancům **SK Teplice, z. s.**, hráčům, rozhodčím a dalším členům) nové možnosti, jak mít o nakládání se svými osobními údaji přehled. Kromě toho došlo k rozšíření pojmu „osobní údaje" – nově sem patří i e-mail, IP adresa, cookies v zařízení uživatele, či genetické a biometrické údaje. Právě poslední jmenované budou podléhat přísnějšímu režimu.

Nově je zavedena také oznamovací povinnost v případě narušení zabezpečení ochrany osobních údajů. Správce musí nahlásit únik či ohrožení osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o tom dozvěděl, Úřadu pro ochranu osobních údajů.

2 Základní pojmy

1. **Co je to GDPR?**

   Obecné nařízení EU, podle kterého se řídí ochrana osobních údajů.

2. **Co je to osobní údaj?**

   Jedná se o **jakoukoli informaci** o fyzické osobě, která napomůže k její identifikaci. Např. pokud o někom víme, že je to volejbalista Motoru České Budějovice, nejedná se samo o sobě o osobní údaj, neboť osobu na základě této informace neidentifikujeme. Jestliže ale víme, že nosí číslo 10 a jmenuje se Jiří, lze už snadno dohledat konkrétní osobu. Proto už by se o osobní údaje jednalo.
   Osobními údaji jsou zejména jméno, příjmení, pohlaví, věk a dátum narození, osobní stav, fotografie, ale také např. i IP adresa.
   Dále lze za osobní údaje považovat v hokeji např. statistiku úspěšnosti zákroků brankářů, ve fotbale úspěšnost střelby útočníků nebo počet odběhaných kilometrů hráčů atp.

3. **Co to je zpracování osobních údajů?**

Jakákoliv činnost, která je prováděna s osobními údaji. Např. pokud jsou zapisovány, vyplňovány nebo je někdo focen např. na registrační kartu (tzv. „registračku"). Taková činnost vždy podléhá pravidlům GDPR.

4. **Kdo je to Správce a Zpracovatel osobních údajů?**

   Správcem je subjekt, který rozhoduje o účelu a způsobu zpracování osobních údajů (např. **SK Teplice, z. s.** ve vztahu k zaměstnancům, členům, hráčům, rozhodčím atp.). Zpracovatelem se rozumí ten, kdo pro něj osobní údaje zpracovává (např. účetní firma).

5. **Kdo je to Subjekt osobních údajů?**

   Fyzická osoba, jejíž osobní údaje jsou zpracovávány.

6. **Kdo je to třetí strana?**

   Kdokoli mimo svaz, komu jsou předávány osobní údaje.

7. **Co je to bezpečnostní incident?**

   Jakákoli situace, v jejímž rámci dojde k úniku, zničení nebo ztrátě osobních údajů.

8. **Co jsou to „osobní údaje dostupné z veřejných rejstříků"?**

   Jedná se o osobní údaje, které je teoreticky možné volně získat z veřejně dostupných seznamů (například z obchodního rejstříku).

9. **Co jsou to citlivé osobní údaje (zvláštní kategorie osobních údajů)?**

   Jedná se o osobní údaje, jejichž znalost může subjektu osobních údajů způsobit újmu. Jedná se např. o údaje vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuální orientaci subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů.

3 Obecně k povinnosti zajištění bezpečnosti zpracování osobních údajů

Každý sportovní svaz by měl zabezpečit osobní údaje po technické a organizační stránce, tj. organizačně v dokumentech určit např. přístupové role a stanovit technické prostředky k jejich zabezpečení, např.:

1. používat odpovídající technické zařízení a programové vybavení způsobem, který vyloučí neoprávněný či nahodilý přístup k osobním údajům ze strany jiných osob,

2. údaje v elektronické podobě uchovávat na zabezpečených serverech nebo na nosičích dat, ke kterým mají přístup pouze pověřené osoby na základě přístupových kódů či hesel,

3. zajistit dálkový přenos údajů buď pouze prostřednictvím veřejně nepřístupné sítě, nebo prostřednictvím zabezpečeného přenosu po veřejných sítích,

4. **písemné dokumenty obsahující osobní údaje uchovávat na zabezpečeném místě** (uzamykatelná skříň, místnost atd.) a zároveň vést řádnou evidenci o pohybu takových písemných dokumentů, dohlédnout na nemožnost nahrávat data na soukromé USB klíče apod.,

5. stanovit pravidla pro přístup k datům (hesla a role), zajistit logování tak, aby měl každý člen individuální přístup,

6. stanovit transparentní ujednání mezi svazem a jednotlivými sportovními kluby týkající se zpracování osobních údajů, stejně jako spolupracovat se zastřešující organizací co se týče ochrany osobních údajů (tedy např. s Českou unií sportu, z. s., dále také „**ČUS**").

4 Základní zásady zpracování osobních údajů

1. U každého osobního údaje je nezbytné jasně **stanovit účel jeho zpracování**, který není v rozporu s právními předpisy nebo oprávněnými zájmy subjektů údajů (měnit účel v průběhu zpracování principiálně lze, ale pouze ve značně omezeném rozsahu).

2. Každý osobní údaj musí být pro daný účel zpracován na základě platného právního titulu/důvodu, tj. zákonné zmocnění, oprávněný zájem, veřejný zájem, životně důležitý zájem, smlouva, výjimečně pak souhlas subjektu údajů.

3. Skutečnosti v bodech 1 a 2 této kapitoly jsou stanoveny v záznamech o činnosti zpracování, kterými svaz také disponuje a které by měl pravidelně aktualizovat.

4. Zpracovávat je možné pouze osobní údaje v nejmenším možném rozsahu, který ještě postačuje ke splnění účelu zpracování (zásada minimalizace). Tzn. není třeba zpracovávat všechny osobní údaje svého člena, jelikož například náboženské vyznání hráče není pro svaz důležité. Svaz by proto „zbytečné" osobní údaje neměl zpracovávat.

5. Je-li právním důvodem pro zpracování osobních údajů souhlas subjektu údajů, musí splňovat náležitosti dle GDPR (před udělením souhlasu náležité informování a poučení mimo jiné i o možnosti odvolání souhlasu). To, že byl souhlas udělen musí být **SK Teplice, z. s.** jakožto správce schopen kdykoliv prokázat (čl. 7 GDPR).

6. V každém případě zpracování osobních údajů musí být subjekt údajů ze strany správce náležitě **informován** o podmínkách zpracování osobních údajů a o svých právech.

7. Je nezbytné zajistit právní titul k případnému předání osobních údajů mimo EU/EHS (např. konání soutěže v nečlenském státu).

8. Je nezbytné zajistit, aby osoby, které přistupují k osobním údajům, či je dále zpracovávají, dodržovaly tento vnitřní předpis.

9. Je třeba náležitě vyškolit zaměstnance svazu, kteří s osobními údaji nakládají.

10. V případě jakýchkoliv pochybností při konkrétních zpracováních je třeba se vždy poradit s odborníky.

11. Ve smlouvách s obchodními partnery musí být stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie osobních údajů. Zejména by měla být se zpracovatelem smluvně ošetřena součinnost při výkonu práv subjektů údajů, oznamování a řešení bezpečnostních incidentů.

12. Je třeba prověřit z pohledu správce, zda zpracovatelé, které využívá, splňují uvedené požadavky a následně je nutné toto pravidelně prověřovat. Současně je třeba monitorovat smlouvy, které jsou uzavřeny se zpracovateli, a případně je doplnit či upravit.

5 Nakládání s dokumenty

5.1 Dokumenty v elektronické podobě

Elektronické dokumenty se nachází v paměti výpočetní techniky, tj. telefonů, tabletů, či počítačů. Je proto nutné, aby byla dodržována určitá pravidla při manipulaci s touto technikou:

1. Při ovládání PC je třeba zejména:

   i. Dodržovat následující nastavení zásad hesla a politiky konta:

      - nezobrazovat jméno posledně přihlášeného uživatele,
      - ochrana heslem:

        - vynutit použití historie hesel – počet hesel, které si systém pamatuje: obvykle 10,
        - maximální doba platnosti hesla – počet dní: obvykle 180
        - minimální doba platnosti hesla – počet dní: obvykle 1,
        - minimální délka hesla – počet znaků: obvykle 8,

- hraniční hodnota uzamčení účtu – počet povolených pokusů o přihlášení: obvykle 3,
- trvání uzamčení účtu: Uzamčení dočasné – obvykle 20 minut,
- vynulování počítadla uzamčení účtu po čase: obvykle 20 minut. (Tedy po uplynutí 20 minut dojde k vynulování počítadla uzamčení účtu a uživatel má opět 3 pokusy pro přihlášení.).

o uzamknutí počítače obvykle při neaktivitě delší než 30 minut.

ii. Dodržovat bezpečnost poskytovanou systémem správy hesel. Heslo je citlivé na jeho kompromitaci vždy, když je použito, uloženo nebo jinak zaznamenáno. Pro zajištění bezpečnosti musí být hesla zadávána s opatrností. Následující doporučení pomáhají hesla chránit.

o Nikdy nezapisovat heslo.
o Nikdy s nikým nesdílet heslo.
o Nikdy nepoužívat heslo pro přihlášení se do sítě pro jiné účely.
o Používat rozdílná hesla pro přihlášení se do sítě a pro účet Administrátor na počítači.
o Měnit své heslo do sítě každých 180 dní nebo dle požadavků vynucených lokálními politikami zabezpečení.
o Měnit heslo okamžitě, pokud existuje podezření, že by mohlo být kompromitováno.
o Aby heslo bylo silné, musí splňovat následující požadavky:

- musí být nejméně 8 znaků dlouhé,
- musí obsahovat znaky ze dvou z následujících tří skupin:

Popis	Příklady
Velká a malá písmena	A, B, C … a, b, c, …
Číslice	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symboly	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

- musí být signifikantně odlišné od předchozího,
- nesmí obsahovat jméno nebo uživatelské jméno,
- nesmí ho tvořit běžné slovo nebo jméno,
- nesmí být snadno uhodnutelné (např. Jméno + datum narození ...).

o Hesla administrátorů musí být po každé změně uložena do trezoru v zapečetěné obálce.

iii. Při krátkodobém opuštění PC aktivovat spořič obrazovky s heslem.

2. Pracovníci **SK Teplice, z. s.** mají právo nahlížet do souborů obsahujících osobní údaje jen za předpokladu, že je to nezbytné k výkonu jejich pracovního zařazení.

3. Pracovníci mají právo **zpřístupňovat** dokumenty obsahující osobní údaje **třetím osobám** či subjektům jen za předpokladu, že mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, předpisem SK Teplice, z. s.**, případně uloží-li jim takovou **povinnost vedoucí pracovník.**

4. Pracovníci **SK Teplice, z. s.** mají zakázáno ukládat osobní údaje do veřejně přístupných rozhraní, prohlížečů a databází, ledaže mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, předpisem sportovního svazu, předpisem SK Teplice, z. s.**, případně uloží-li jim takovou **povinnost vedoucí pracovník.**

5. Osobní údaje je možné vkládat do předem připravených databází, které jsou k tomu určené nebo do vlastních (nesdílených) dokumentů, do kterých mají přístup jen sami pracovníci.

6. Pracovníci nemají bez výslovného povolení vedoucího pracovníka právo tisknout osobní údaje obsažené ve sdílených databázích.

7. Je **zakázáno** pořizovat **skeny občanských průkazů** vyjma situací, kdy je to pořizovaná stanoveno jako zákonná povinnost nebo kdy k tomu subjekt osobních údajů předá výslovný a svobodný souhlas se všemi zákonnými náležitostmi.

8. Registrační a jiné informační systémy, které svaz spravuje a do kterých mají přístup fyzické osoby, nebo jednotliví členové svazu (sportovní kluby) musí být spravovány s nejvyšším zřetelem na ochranu osobních údajů v nich obsažených.

5.2 Dokumenty v papírové podobě

1. Listiny obsahující jakékoli osobní údaje (např. zápisy o utkání, faktury) nesmí být ponechány nechráněny na volně a dostupném místně. Ideální variantou je tyto listiny ukládat do uzamykatelných skříní, nicméně v místnostech přístupných pouze pro zaměstnance mohou být uloženy **i v neuzamykatelných skříních.**

2. Pracovníci, kteří mají uložené listiny s osobními údaji v neuzamčené skříni dle bodu 1. jsou povinni uzamykat kancelář pokaždé, když ji opouští.

3. Žádné dokumenty nebudou ponechávány bez dozoru na pracovní ploše stolu, při odchodu z práce, příp. opuštění kanceláře (jednání, přestávka na oběd atd.) budou dokumenty obsahující osobní údaje uklizeny v šuplících.

4. Listiny obsahující **citlivé osobní údaje** (karta zaměstnance, dotazník zaměstnance, jakékoli informace o zdravotním stavu) mohou být uložené jen v **uzamčených** skříních, a to jak na místech veřejně přístupných, tak i na místech přístupných pouze zaměstnancům.

5. Pracovníci mají právo **nahlížet** do dokumentů obsahujících osobní údaje jen za předpokladu, že je to **nezbytné** k výkonu jejich pracovního zařazení.

6. Pracovníci mají právo **zpřístupňovat** dokumenty obsahující osobní údaje **třetím osobám** či subjektům jen za předpokladu, že mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, předpisem svazu**, případně uloží-li jim takovou **povinnost vedoucí pracovník**.

7. Je **zakázáno** pořizovat **kopie občanských průkazů** vyjma situací, kdy je to pořizovaná stanoveno jako zákonná povinnost nebo kdy k tomu subjekt osobních údajů předá výslovný a svobodný souhlas se všemi zákonnými náležitostmi.

5.3 Porušení ochrany dat

1. Každý svaz je povinen ohlásit únik či ohrožení zabezpečení osobních dat Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o incidentu dozvěděl.

   Ohlášení musí obsahovat minimálně:

   i. popis povahy daného případu porušení zabezpečení osobních údajů,
   ii. popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
   iii. popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení,
   iv. zabezpečení osobních údajů.

2. Každý člen **SK Teplice, z. s.** je povinen o jakémkoli podezření o úniku osobních údajů informovat předsedu SK Teplice, z. s.

5.4 Likvidace osobních údajů

Ve chvíli, kdy opadne poslední oprávněný zájem pro zpracovávání osobních údajů, je nutné tyto údaje zlikvidovat. V případě přepisovatelných medií lze údaj vymazat, v případě nepřepisovatelných médií či papírové podoby musí dojít k fyzickému zničení v podobě:

i. rozdrcení (diskety, disky),
ii. skartování (papír)
iii. formátování či přepsání (elektronické přepisovatelné disky),
iv. demagnetizace (diskety).

6 Pravidla využívání sítě Internet

1. Zaměstnanci a členové svazu budou používat síť Internet tak, aby se minimalizovala možná rizika vyplývající z jeho používání. Nesprávné používání a zneužití služeb Internetu představuje hrozbu pro informační systém.

2. Zaměstnanci a členové svazu mají zakázáno navštěvovat stránky s neznámým obsahem.

6.1 Zákazy pro uživatele

Je zejména zakázáno:

1. používat informační prostředky pro zobrazování, ukládání, zpracování nebo šíření materiálů, které omezují lidská práva a práva menšin, jsou rasistické, sexuálně zaměřené, nebo jiným způsobem nezákonné,
2. poskytnout služební identifikační prostředky využívané při práci s informačními technologiemi prostřednictvím internetu (např. heslo) cizí osobě,
3. stahovat z internetu nelegální software,
4. svévolně instalovat jakýkoli software, včetně různých plug-in modulů na pracovní stanici uživatele,
5. svévolně měnit nastavení programů umožňujících komunikaci s internetem,
6. poskytnout neautorizovanému subjektu přístup ke službám internetu ze služebních počítačů,
7. posílat informace s osobními údaji v otevřeném tvaru elektronickou poštou,
8. připojovat se z pracovních stanic na privátní internetové účty,
9. jakýmkoli způsobem provádět vyhledávání, monitorování a zjišťování stavu portů na serverech podnikového informačního systému.

7 Vstupy do budov a kanceláří

1. Zaměstnanec nemá povoleno umožnit vstup do budovy (resp. prostoru využívaném **SK Teplice, z. s.**) za jiným než pracovním/spolkovým účelem.

2. V případě, že zaměstnanci nejsou přítomni na pracovišti, jsou zodpovědní za zamykání a jiné zabezpečení svých kanceláří, jakož i uložení dokumentů obsahujících osobní údaje do míst dle této směrnice.

8 Bezpečnostní incidenty

1. Může se stát, že dojde k tzv. bezpečnostnímu incidentu. To je situace, ve které dochází k narušení bezpečí osobních údajů. Za takový incident považujeme např.:

    i. neoprávněný přístup do informačních systémů a úložišť,
    ii. pokus o neoprávněný přístup do informačních systémů a úložišť.

2. Tento přístup nebo pokus o něj může být jak fyzický, tak elektronický (např. cílené zaslání e-mailu „infikovaného" virem, …).

3. V případě, že zaměstnanec zjistí, že došlo k narušení bezpečí osobních údajů, neprodleně tuto skutečnost nahlásí předsedovi SK Teplice, z. s.

8.1 Postup při vzniku bezpečnostních incidentů

1. Po zjištění vzniku bezpečnostního incidentu zaměstnanec informuje předsedu SK Teplice, z. s. Vedoucí zásadou při vzniku bezpečnostního incidentu je, že zaměstnanec bude vždy nápomocen k tomu, aby došlo k bezodkladnému napravení porušení a k rychlému prošetření incidentu.

2. V závislosti na typu incidentu je třeba přijmout adekvátní bezpečnostní opatření, která minimalizují škody a vznik dalších rizik.

3. Pokud incident jakýmkoli způsobem ohrozí osobní údaje je třeba neprodleně informovat předsedu SK Teplice, z. s., případně do 72 hodin i dozorový úřad.

V Teplicích 30. 6. 2021

SK TEPLICE, spolek
U Červeného kostela 110
415 01 Teplice
IČ: 26645939

Mgr. et Mgr. Daniel Pokorný
předseda VV SK Teplice, z. s.