Doporučení k provedení vnitřního auditu o nakládání s osobními údaji v TJ/SŽ

Vážení zástupci tělocvičných jednot a sokolských žup,

dne 25.5.2018 vstoupilo v účinnost Obecné nařízení EU č. 2016/679 (dále jen „GDPR“), které přináší sportovním klubům a tělocvičným jednotám (dále jen „jednotám“) nové povinnosti.

Společně s tímto návodem respektive doporučením na provedení analýzy nakládání s osobními údaji ve Vaší jednotě (župě) se k Vám dostávají také nové formuláře přihlášek, a formuláře pro souhlasy se zpracováním osobních údajů pro členy. Společně s nimi také dokumenty Odpovědi na nejčastější otázky k formuláři informace a souhlas člena a Doporučení k auditu. Tyto dokumenty vznikly v rámci společného postupu ČOS, ČOV, ČUS, Orla a některých sportovních svazů.

Současně je na webových stránkách ČOS k dispozici (odkaz v zápatí webu - PRO ČLENY > Dokumenty a info ke stažení) aktuální znění ***Řádu k ochraně osobních údajů v ČOS***, který je závazný pro všechny členy a zaměstnance ČOS a je použitelný v současné podobě (s novelizací se počítá po přijetí tzv. adaptačního zákona k GDPR) i po 25.5.2018. Po prostudování uvedených dokumentů by Vám měla být problematika nakládání s osobními údaji v rámci ČOS jasnější.

S GDPR bude určitě spojena nutnost většího papírování, a některé kroky si vyžádají Váš čas. Pomocí GDPR některé firmy straší nesmírně vysokými sankcemi a nabízí certifikaci a poradenství. Většina z těchto strašáků je přehnaná a nabídka placených služeb pro potřeby TJ/SŽ zcela zbytečná. To ale neznamená, že za nesplnění GDPR nehrozí vůbec žádná sankce. Proto je třeba se problematice věnovat i na úrovni TJ a nejprve se pokusit zpracovat si audit vlastními silami.

Bohužel není možné vyrobit univerzální vzor, kam by se vždy doplnil jen název jednoty, v každé jednotě to máte nastavené trochu jinak. Nicméně se pokusím uvést pár tipů, které Vám zpracování auditu usnadní .

Vřele doporučuji pročíst skvěle zpracovaný návod na GDPR od odborníka na ochranu osobních údajů Petra Kamínka na webu https://sites.google.com/site/jaknagdpr/. Tento návod Vám pomůže zorientovat se v základních pojmech a hlavně je výborným průvodcem pro zpracování datového auditu na skutečně vysoké úrovni.

Pokud by pro Vás postup dle uvedeného návodu byl příliš náročný, doporučuji provést alespoň níže uvedenou minimalistickou variantu auditu.

Pokud by i po prostudování všech zmíněných materiálů zůstávali nějaké nejasnosti, můžete se s dotazy obracet na email: janda@akjanda.cz a do předmětu prosím uvádějte “GDPR SOKOL”.

Minimalistická varianta audit v rámci TJ

Nařízení známé pod zkratkou “GDPR” je nastaveno tak, že důkazní břemeno přenáší na správce osobních údajů (TJ). Je tedy potřeba věnovat čas výrobě dokumentu, kde shrnete základní informace o nakládání s osobními údaji v TJ. Je vcelku jedno zda se bude jednat o složku v počítači, šanon, excelovou tabulku nebo rukou psaný sešit.

Pokud máte za to, že žádné osobní údaje nezpracováváte a tudíž nemusíte ve vztahu k GDPR nic dělat. Uvědomte si, že osobním údajem je takřka jakýkoliv údaj o fyzické osobě, prostě vše co ji může (pomoci) identifikovat. Osobním údajem je i jméno a příjmení nebo e-mailová adresa, kterou o sobě někdo veřejně sdělí nebo který je dostupná z veřejných zdrojů (například když si najdete telefonní číslo na webových stránkách a následně si ho uložíte do telefonu, už pracujete s osobními údaji). Osobní údaje tedy v TJ a SŽ evidujeme naprosto všichni.

V následujícím textu budu předpokládat, že audit budete zpracovávat v el. dokumentu, ale místo něj si můžete samozřejmě dosadit i ten zmiňovaný sešit, pokud si ho jako nosič zvolíte. Do dokumentu je třeba k začátku účinnosti GDPR zapsat základní informace a stav k 25.5.2018, následně průběžně další zápisy, které vyplynou ze závěrů auditu.

První třetinu dokumentu věnujte analýze současné situace. Aby byl dokument dostatečně přehledný, nadepište si každou stránku nadpisem, který usnadní orientaci v dokumentu a práci s ním. Může jít například o následující nadpisy: **Zaměstnanci, Funkcionáři, Členové TJ, Nájemci, Partneři a dodavatelé, Ostatní**. Poslední zbytková kategorie je důležitá, budete do ní potřebovat zaznamenat vše, co se nebude dát přiřadit jinam.

K nadpisům doplňte všechny seznamy, databáze a osobní údaje, které v TJ evidujete (například seznam členů, seznam nájemců, seznam zaměstnanců, jsou-li vedeny tak také seznamy bývalých zaměstnanců, členů a nájemců, seznam vystavených faktur apod.)

Co? Kde? Proč? Jak? Jak dlouho?
U každého z uvedených seznamů je třeba vypsat odpovědi na tyto otázky:
Co je obsahem seznamu? (například *jméno a příjmení, adresa, členství v oddíle, doba členství*)
Kde údaje vedete? *(v papírovém sešitě* nebo *v PC*)
Proč je potřebujete, tedy zda existuje titul, kvůli němuž informace vedete. (Odpověď na tuto otázku je nejdůležitější: někdy údaje potřebujete ze zákona, z důvodu požadavku ČOS, jindy půjde o *oprávněný zájem spolku - údaje jsou potřeba pro vlastní činnost TJ*. Pokud žádnou odpověď na otázku "Proč?" nenajdete, vzniká problém, který vyřešíte dle odstavce Opatření k nápravě.
Jak máte zabezpečeno, že se se k seznamu nedostane neoprávněná osoba (například uklízečka nebo návštěva v kanceláři TJ). (Odpověď na tuto otázku bude také jednoduchá: někdo zamyká všechny šanony do skříně, jiný má vše v polici a zamyká jen kancelář).
Jak dlouho osobní údaje uchováváte bude poslední otázka, odpověď na ni bude sloužit k vyhodnocení, zda je doba přiměřená.

Opatření k nápravě
Druhá třetina dokumentu musí být věnována vylepšení stávající situace.
Například: *Máme šanony s osobními údaji v kanceláři v knihovně, pořídíme si zamykatelnou plechovou skříň, jak předpokládá Řád k ochraně osobních údajů v ČOS. Počítač není zabezpečený vstupním heslem, což napravíme v termínu do DD.MM.RRRR*. Vytvoříte si tak seznam úkolů, aby Úřad pro ochranu osobních údajů viděl, že jste se nad tím zamysleli a přijali nějaká opatření. Za půl roku zkontrolujte a zapište, zda jste všechny úkoly splnili, případně si nové uložíte.

Chyby a prolomení bezpečnostního rizika
Pokud se stane, že s osobními údaji naložíte nějak chybně, nemusíte to okamžitě nikam hlásit, ale musíte takové "přešlapy" evidovat. Na konec dokumentu si tak napište ještě jeden nadpis: **Prolomení bezpečnostního rizika** nebo **Chyby a omyly**. Právě sem pak zapisujte všechny kritické situace, omyly, maily se seznamem členů odeslané na špatnou adresu, ztrátu dokumentů s osobními údaji členů, odcizení klíčů od kanceláře, správně byste měli zapisovat i spuštěný počítač ponechaný bez dozoru v dosahu 3. osoby. Každou takovou zapsanou událost vyhodnotíte a dle velikosti rizika jen situace naprosto katastrofální ohlásíte ÚOOÚ (například když kancelář TJ vykradou a zmizí i listiny či počítače s osobními údaji členů).

Pro Českou obec sokolskou

Mgr. Pavel Janda, právník ČOS
květen 2018

Zdroje:
Návod jak na GDPR, Petr Kamínek - https://sites.google.com/site/jaknagdpr/odkazy
GDPR pro samostatné advokáty, Daniela Kovářová - https://www.epravo.cz/top/aktualne/gdpr-pro-samostatne-advokaty-107496.html
Řád k ochraně osobních údajů v ČOS - Směrnice ČOS 1/2015
Doporučení pro členské spolky vhodná pro sportovní kluby ČUS, ČOV, SSS ČR, ČOS, národní svazy a další sportovní subjekty