METODIKA ČJF k harmonizaci s GDPR

Dne 27. dubna 2016 schválil Evropský parlament NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 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 (obecné nařízení o ochraně osobních údajů), které pro celou EU nově vymezuje práva a povinnosti v oblasti osobních údajů, více známé pod zkratkou „**GDPR**".

Nařízení GDPR bylo přijato jednak na základě čl. 8 Listiny základních práv Evropské unie, jednak článku 16 Smlouvy o fungování Evropské unie.

Nařízení GDPR je závazné v celém rozsahu a přímo použitelné ve všech členských státech EU s tím, že v účinnost vstupuje dne 25. 5. 2018 - tímto okamžikem dojde ke sjednocení ochrany osobních údajů na celém území Evropské unie a Evropského hospodářského prostoru.

Účelem metodiky ČJF je pomoc členským subjektům s harmonizací požadavků GDPR v rámci specifického postavení sportovního klubu v českém sportovním prostředí.

I. Základní pojmy uvedené v GDPR, které je třeba vnímat, jsou:

- **Osobní údaj (OÚ)** – jakákoliv informace, která se týká konkrétní fyzické osoby (subjektu údajů), ať už jde o identifikační a kontaktní údaje (např. jméno, příjmení, datum narození, adresa pobytu, rodné číslo, IČO/DIČ, telefonní číslo, e-mail, IP adresa, v podmínkách klubu či ČJF se může jednat o popisné údaje vypovídající o fyziologii člověka (např. výška, váha, velikost boty), informace z fotografií a kamerových záznamů, sociodemografické údaje (věk, pohlaví, rodinný stav, vzdělání, zaměstnání, příjmy a výdaje, počet dětí) nebo údaje o jeho chování a preferencích.

- **Zvláštní kategorie osobních údajů** (dříve citlivé osobní údaje) – některé osobní údaje zvlášť rizikové z pohledu možných zásahů do garantovaných práv a svobod fyzických osob, například údaje o zdravotním stavu, které jsou v klubu či ČJF vedeny u některých jezdců, údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, genetické či biometrické údaje.

- **Subjekt údajů** – každá fyzická osoba, jejíž OÚ jsou zpracovávány.
  V podmínkách ČJF se jedná o členy – fyzické osoby. Pojem „Subjekt údajů" (tedy nositel osobních údajů) je pevným slovním spojením používaným v legislativě GDPR. Nezaměňovat s pojmem „subjekt" uvedeným např. v čl.5 Stanov ČJF.
- **Zpracování** – jakékoli nakládání s osobními údaji, např. shromáždění, zaznamenání, zpřístupnění, uložení, uspořádání, vyhledání, pozměnění, použití, šíření atd. U

zpracování osobních údajů v rámci klubu patří mezi typické příklady vedení evidence (elektronické i listinné) o stavu členské základny, placení členských příspěvků, výsledkových listin, přihlášek na závody, evidence udělených plných mocí, zaměstnanecká agenda atd.

- **Správce** – jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; v rámci činnosti členských subjektů ČJF je jím klub a ČJF.

- **Zpracovatel** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává pro správce osobní údaje, pokud ho tím správce pověří, a pouze ve správcem stanoveném rozsahu a ke stanoveným účelům; není vyloučeno, že jedna osoba bude zároveň správcem (například ve vztahu ke svým zaměstnancům) i zpracovatelem (ve vztahu k jinému správci).

- **Společní správci** – správci, kteří společně stanoví účely a prostředky zpracování OÚ.

- **Příjemce** – jakýkoli subjekt, kterému jsou osobní údaje poskytnuty (není rozhodující, zda přímo správcem, nebo zpracovatelem na pokyn správce), v některých případech se za příjemce nepovažují orgány veřejné moci.

- **Právo vznést námitku** – je-li zpracování založeno na oprávněném zájmu správce, případně prováděno ve veřejném zájmu nebo při výkonu veřejné moci, má subjekt údajů právo kdykoli proti takovémuto zpracování vznést námitku, subjekt údajů má právo vznést námitku také proti zpracování za účelem přímého marketingu a správce má v tomto případě povinnost dotčené OÚ dále nezpracovávat.

- **ÚOOÚ** – Úřad pro ochranu osobních údajů, kontrolní a dozorový úřad dle GDPR v ČR, se sídlem Pplk. Sochora 27, 170 00, Praha 7, telefon: +420 234 665 111, web: www.uoou.cz.

- **Záznamy o činnostech zpracování** – každý správce osobních údajů je povinen vést záznamy o činnostech zpracování osobních údajů, za něž zodpovídá. GDPR sice předepisuje formální vedení záznamů o činnostech zpracování především pro velké organizace (nad 250 zaměstnanců), ale vzhledem k tomu, že záznamy musí vést i každý správce a zpracovatel (tedy bez ohledu na počet zaměstnanců), pokud prováděné zpracování OÚ pravděpodobně představuje riziko pro práva a svobody subjektů údajů,

zpracování OÚ není příležitostné (týká se všech aktivních hráčů), nebo zpracování zahrnuje zpracování zvláštních kategorií údajů (viz např. shora uvedené zdravotní údaje některých hráčů – tréninkový systém). P**ovinnost vést tyto formalizované záznamy se tedy bude týkat všech klubů i ČJF.** Každý přitom musí zohlednit kontext, citlivost a rozsah vedených osobních údajů, tzn., někdo si vystačí se záznamy v jednodušší formě, zatímco „velcí" správci budou muset zohlednit zvýšený objem a rizikovost zpracovávaných OÚ, aby byly schopny prokázat soulad s GDPR při případné kontrole ze strany ÚOOÚ.

- **DPO – pověřenec pro ochranu osobních údajů** (z angl. data protection officer); DPO je jakýmsi interním auditorem zpracování a ochrany osobních údajů; dohlíží nad tím, že osobní údaje jsou zpracovávány a chráněny v souladu s GDPR. Povinnost jmenovat DPO není plošná (lze ho však ustavit dobrovolně). Bude se zřejmě týkat jen minimálního počtu klubů. Blíže o DPO viz čl. IV odst. 4. této Metodiky.

- **Analýza rizik** – posouzení zpracování osobních údajů s cílem zjistit, jak závažná rizika plynou ze zpracování pro práva a svobody fyzických osob, a na základě toho přijmout opatření, která tato rizika minimalizují. Každý klub a ČJF by si měl zpracovat analýzu rizik ve vztahu ke zpracování osobních údajů, která provádí. Blíže o analýze rizik viz text v čl. IV odst. 1. této Metodiky.

- **DPIA** – posouzení vlivu na ochranu osobních údajů (z angl. data protection impact assessment); formalizovaná riziková analýza, jejímž úkolem je zjistit, zda i přes vysoká rizika zpracování osobních údajů, zjištěná v rámci zpracování záznamů o činnostech zpracování, lze tyto údaje legálně zpracovávat za použití opatření, která sníží vysoká rizika na přijatelnou úroveň.

- **Hlášení bezpečnostních incidentů** – GDPR obsahuje povinnost správce hlásit porušení zabezpečení, integrity a ztrátu osobních údajů ÚOOÚ bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o nich dozvěděl; z této povinnosti jsou vyloučeny pouze incidenty s nízkou rizikovostí pro subjekty osobních údajů. Navíc správci musí oznámit toto porušení neprodleně všem dotčeným subjektům údajů, pokud je pravděpodobné, že příslušné porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Blíže o hlášení bezpečnostních incidentů viz čl. IV odst. 6. této Metodiky.

II. Odhadované požadavky na shodu s GDPR

Vzhledem k obsahu činnosti zpracovatele a s tím související nutnosti evidovat osobní údaje je nutné, aby došlo k naplnění přinejmenším požadavků minimální shody s GDPR:

- Vypracování dokumentace osvědčující naplňování zásad zpracování, ochrany a zabezpečení osobních údajů (OÚ) zejména podle čl. 5, 6, 25 a 32 GDPR – touto dokumentací bude v podmínkách klubů a ČJF vedle revize stávajících interních předpisů zejména vypracování pravidel IT bezpečnosti a pravidel bezpečného nakládání s dokumenty, včetně režimových a organizačních opatření[1], jakož i vypracování závazné dokumentace (interní směrnice) o zpracování osobních údajů. Součástí směrnice mohou být rovněž záznamy o činnosti zpracování (alternativně mohou být tyto záznamy samostatným dokumentem). Viz článek „IV. Interní směrnice o zpracování osobních údajů“ této metodiky níže.

- Zavedení a popis přinejmenším jednoho procesu reakcí na práva subjektů osobních údajů – blíže viz čl. IV odst. 2. této Metodiky a vzory žádosti subjektu údajů a odpovědi na žádost, obsažené v příloze č. 1 a č. 2 této Metodiky.

- Zavedení procesu naplňování informační povinnosti vůči subjektům osobních údajů – definovaný vzor souhlasu.

- Zavedení procesů identifikace, dokumentace a hlášení bezpečnostních incidentů na poli osobních údajů – blíže viz čl. IV odst. 6. této Metodiky.

- Revize smluv s dodavateli klubu či ČJF, kteří jsou zpracovateli osobních údajů – blíže viz č. IV odst. 3. této Metodiky.

- Systém sběru, evidence a zpracování souhlasů se zpracováním OÚ – blíže viz čl. IV odst. 5. této Metodiky.

III. Zásady zpracování

[1] Jestliže takovou dokumentaci nepořídí klub či ČJF ve spolupráci s dodavatelem informačních technologií mohou být vhodnými podkladovými materiály pro vypracování této dokumentace odborná literatura v oblasti bezpečnosti informací, kybernetické bezpečnosti, případně zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, resp. příloha č. 4 k jeho prováděcí vyhlášce č. 316/2014 Sb.

GDPR vychází z několika obecných zásad zpracování a ochrany osobních údajů (obsažených především v čl. 5, 6, 25 a 32 GDPR, dále ze zásady přístupu založeného na řízení rizik a informačního sebeurčení subjektů údajů). Tyto zásady jsou následující:

- **Zásada zákonnosti, korektnosti a transparentnosti** znamená, že osobní údaje musejí být ve vztahu k subjektu údajů zpracovávány vždy korektně, zákonným a transparentním způsobem.

- **Zásada zákonnosti** vyžaduje, aby osobní údaje byly zpracovávány na základě právem stanovených legitimních důvodů (právních titulů, které vymezuje čl. 6 GDPR)[2], jimiž jsou: nezbytnost dodržení zákonné povinnosti, která se na správce vztahuje, nezbytnost pro splnění úkolů správce prováděných ve veřejném zájmu nebo při výkonu veřejné moci, nezbytnost pro plnění smlouvy, jejíž stranou je subjekt údajů, nebo za účelem přijetí opatření na žádost subjektu údajů před uzavřením smlouvy, nezbytnost pro účely oprávněných zájmů nebo zpracování založené na souhlasu subjektu údajů.

- **Zásada transparentnosti** souvisí s plněním informačních povinností vůči dotčeným subjektům údajů vymezených v čl. 12 až 14 GDPR. Kluby naplní tuto zásadu mimo jiné realizací vnitřního předpisu ČJF v rámci podpisu přihlášky, jejíž součástí je vzorová informace, resp. zajištěním informování u stávajících členů. Na shora uvedenou informační povinnost doporučujeme pamatovat rovněž v rámci webových stránek klubů.

- **Zásada účelového omezení** znamená, že každé zpracování osobních údajů musí být v souladu se svým legálním účelem. Osobní údaje musejí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Dostatečně určitě stanovený účel je např. „plnění smlouvy“, „zasílání marketingových nabídek“, „ochrana oprávněných zájmů – majetku správce“ nebo „plnění právní povinnosti“. Účel zpracování je výslovně vyjádřený, byl-li sdělen subjektům údajů. Legitimita účelu znamená, že je účel zpracování v souladu s právním řádem jako celkem, nikoliv tedy pouze v souladu s GDPR.

- **Zásada minimalizace údajů** znamená, že je možné zpracovávat osobní údaje pouze v minimálním rozsahu, počtu operací a množství evidencí, které jsou nezbytně nutné a potřebné pro splnění příslušného účelu zpracování. Ačkoliv tato zásada neznamená, že by měla existovat výlučně a pouze jedna evidence, každý správce musí usilovat o to, aby osobní údaje nebyly shromažďovány v rozsahu, který překračuje potřeby účelu (např. pro plnění smlouvy o dodávce kurzů výuky jezdectví shromažďovat rodná čísla účastníků kurzu), zpracovávány nadbytečnými procesy a operacemi, popř. rozmnožovány do většího množství evidencí, než je nutné (např. každý zaměstnanec klubu si pořizuje svoji kopii přihlášky, aniž by pro to byly důležité provozní důvody, či ČJF vyžaduje rodná čísla jezdců, ačkoli jejich jedinečnou identifikaci lze zajistit z ostatních OÚ).

[2] Tyto právní tituly obsahově odpovídají současnému § 5 odst. 2 písm. a) – e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

- **Zásada přesnosti** má vyjádření v povinnosti zpracovávat pouze přesná, správná a aktuální data. Znamená to, že v pravidelných časových intervalech (např. jednou v sezoně) by měla být osobní data členů aktualizována, např. formou dotazu na člena při odbavení ke hře, aby potvrdil správnost svých kontaktních údajů, případně je opravil. Také je vhodné upravit v interní směrnici o zpracování osobních údajů mechanismy a opatření určená k řízení životního cyklu sbíraných osobních údajů a vedoucí k včasné opravě a/nebo likvidaci nepřesných osobních údajů, jakož i postupy uplatňované v rámci aktualizace osobních údajů (zejména z podnětu subjektu údajů). Pravidelnost ověřování přesnosti a aktualizace osobních údajů by měla odpovídat potenciálnímu riziku vzniku újmy. Vyšší riziko vzniku újmy lze očekávat v případě pravidelného zpracovávání osobních údajů, než v případě jejich pouhého uložení.

- **Zásada omezeného uložení** znamená povinnost uchovávat osobní údaje jen po dobu nezbytně nutnou k naplnění účelu zpracování. Archivační (skartační) lhůty musejí být uvedeny v záznamech o činnostech zpracování osobních údajů a je nezbytné zajistit jejich dodržování. **Subjekt údajů by měl být informován o době, po kterou budou jeho osobní údaje zpracovávány –** kluby archivují OÚ člena po dobu 10 let po ukončení činnosti, jak vyplývá z požadavků zákona o podpoře sportu.

- **Zásada integrity a důvěrnosti** představuje zejména povinnost zajistit bezpečné zpracování osobních údajů. Při posuzování vhodné úrovně bezpečnosti zpracování osobních údajů se zohlední zejména rizika, která představuje zpracování osobních údajů, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim. Vhodná technická a organizační opatření poměrně stručně zmiňuje čl. 32 GDPR.[3] **Standardizované postupy**, vypracované za účelem zajištění náležité úrovně (tj. odpovídající danému riziku) zabezpečení osobních údajů, případně včetně:
    a) pseudonymizace a šifrování osobních údajů;
    b) zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování;
    c) obnovení dostupnosti osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
    d) pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování,

  musejí být upraveny v interní směrnici o zpracování osobních údajů a figurovat v záznamech o činnostech zpracování.

IV. Interní směrnice o zpracování osobních údajů

[3] Vhodnými vodítky pro identifikaci vhodných opatření je vedle čl. 32 GDPR i zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, popř. normy ISO a tzv. best practices v oblasti informační a kybernetické bezpečnosti.

Jak vyplývá ze shora uvedeného, každý zpracovatel by měl nejprve provést zhodnocení, kterým posoudí svoji činnost na poli zpracování OÚ z hlediska požadavků GDPR. Tímto zhodnocením by měl klub získat základní evidenci o zpracování osobních údajů, které provádí. Níže je pod bodem 1 uveden jako příklad soupis kategorií a charakteristik zpracování osobních údajů, které by měl klub posoudit i s vysvětleními, co by mělo být předmětem vyplnění s tím, že následně musí správce vypracovat Směrnici o zpracování osobních údajů, která by měla zahrnovat a řešit požadavky GDPR v podmínkách správce, kdy směrnice má následující části:

1. Evidence činností zpracování: na tučně zvýrazněné otázky které jsou kategoriemi a charakteristikami zpracování osobních údajů, je potřeba si ve smyslu kurzívou uvedeného návodu odpovědět a takovýto materiál může být následně použit jako základ pro vnitřní směrnici správce tak, jak je GDPR vyžadováno:

Jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů [článek 30 odst. 1 písm. a) GDPR]:

Uveďte jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů.

Identifikace příslušných zpracování osobních údajů [článek 30 odst. 1 písm. b) GDPR]:

Uveďte seznam všech zpracování osobních údajů, které provádíte, podle hlavních kategorií:

a) *členská agenda;*
b) *zaměstnanci;*
c) *provoz klubu, daně a účetnictví (dodavatelé);*
d) *obchod a marketing, komunikace online;*
e) *ostatní.*

Proč (za jakým účelem) a na základě jakého právního titulu se osobní údaje v rámci zpracovávání zpracovávají [článek 30 odst. 1 písm. b) GDPR]?

Uveďte pro každé zpracování osobních údajů účel (cíl, smysl zpracování) a rovněž právní titul zpracování (půjde zejména o plnění smlouvy se subjektem - členem a plnění zákonných povinností; v případě právní povinnosti doporučujeme uvést i odkaz na příslušný právní základ); více viz zásada zákonnosti v čl. III. výše.

Tuto část lze sloučit s předchozím bodem ve formátu:
Zpracování – Účel – Právní titul.

Jaké osobní údaje jsou zpracovávány v rámci zpracování [článek 30 odst. 1 písm. c) GDPR]?

Pro každé zpracování uveďte všechny kategorie osobních údajů, které zpracováváte.

Z jakých zdrojů jsou osobní údaje získány [(článek 30 odst. 1 písm. c) GDPR]?

Uveďte všechny subjekty, od nichž získáváte osobní údaje, které v rámci své činnosti zpracováváte. Půjde především o subjekty údajů (členové ve vztahu ke svým vlastním osobním údajům, zaměstnanci, aj.).

Kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích:

Uveďte všechny kategorie osob a organizací, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích.

V jakém termínu a jak se osobní údaje likvidují [článek 30 odst. 1 písm. f) GDPR]?

Uveďte pro každé zpracování osobních údajů archivační a skartační lhůtu.
Je-li v klubu vydán a naplňován, lze odkázat na příslušný interní předpis (typicky archivační/skartační řád).

Jakým způsobem se osobní údaje aktualizují [článek 30 odst. 1 písm. g) GDPR]?

Uveďte způsob aktualizace osobních údajů – viz zásada přesnosti v článku III. výše (např. obdržením informace od člena o změně kontaktních údajů aj.).
Je-li v klubu vydán a naplňován, lze odkázat na příslušný interní předpis (např. „Směrnice o zpracování osobních údajů“).

Které listinné a elektronické evidence (spisovny, archivy, IT systémy, datová úložiště) provádějí zpracování [článek 30 odst. 1 písm. g) GDPR]?

Uveďte podrobně, jaké listinné evidence a IT systémy využíváte pro svou činnost a jejich vazbu na konkrétní zpracování (tzn. které evidence/IT systémy provádějí jaké zpracování osobních údajů).
Je-li v klubu vydán a naplňován, lze odkázat na příslušný interní předpis anebo dokumentaci informačního prostředí (např. popis IT systémů, „Směrnici o zpracování osobních údajů“).

Je prostředí klubu pravidelně bezpečnostně testováno (zejm. IT systémy)? Interně nebo externími konzultanty? [článek 30 odst. 1 písm. g) GDPR].

GDPR klade velký důraz na bezpečnost zpracování osobních údajů. Vaše IT systémy by měly být bezpečnostně testovány – interně nebo externě. V závislosti na objemu zpracovávaných osobních údajů je třeba zvolit délku časového období mezi dvěma testy.
Je-li v klubu vydán a naplňován, lze odkázat na příslušný interní předpis (např. bezpečnostní normu).

Jak je zajištěna bezpečnost šifrování dat při komunikaci se subjektem údajů [článek 30 odst. 1 písm. g) GDPR]?

Uveďte, jak řešíte komunikaci citlivých členských informací a dále např. jak zabezpečujete předání údajů o zaměstnancích externí účetní firmě.
Je-li v klubu vydán a naplňován, lze odkázat na příslušný interní předpis (např. bezpečnostní normu anebo „Směrnici o zpracování osobních údajů“).

Jak je zajištěna bezpečnost sdílení dat s externími subjekty? Mají všichni externí dodavatelé, zpracovávající osobní údaje, uzavřené smlouvy o zpracování osobních údajů, poskytující odpovídající záruky ochrany [článek 30 odst. 1 písm. g) ve spojení s článkem 28 GDPR]?

Uveďte, zda vaši dodavatelé, kteří mohou mít přístup ke zpracovávaným osobním údajům (např. účetní agentura nebo firma spravující váš webový systém), mají uzavřeny smlouvy o zpracování osobních údajů.
Je-li v klubu vydán a naplňován, lze odkázat na příslušný interní předpis (např. bezpečnostní normu anebo „Směrnici o zpracování osobních údajů“).

Je zajištěna nevratná likvidace dat v rámci databázového systému [článek 30 odst. 1 písm. g) GDPR]?

Uveďte, zda na konci životního cyklu příslušného zpracování osobních údajů je váš IT systém schopný nevratně osobní údaje vymazat.

Je k dispozici procedura k určení práv subjektů údajů a jejich výkon s ohledem na jejich data, která jsou zpracovávána v rámci zpracování?

Uveďte, zda máte zaveden interní proces vyřizování žádostí subjektů údajů ve vztahu k právům subjektů údajů – viz bod 2. níže, a jakou formou postupujete (např. odkaz na formuláře na vašem webu nebo v listinné podobě). Rovněž je potřeba vymezit, v jakých situacích jsou práva subjektů omezována a z jakých titulů.

Poskytují se oprávněným subjektům údajů předepsané informace, zejména o rozsahu a účelu zpracování, způsobu zpracování osobních dat a komu mohou být osobní údaje zpřístupněny?

Uveďte, kde a jakou formou poskytujete předepsané informace pro subjekty údajů.

Zabraňují nasazené technické prostředky a uplatňovaná organizační opatření nahodilému anebo neoprávněnému přístupu k osobním údajům, jejich změně, zcizení, zneužití, zničení nebo ztrátě [článek 30 odst. 1 písm. g) GDPR]?

Uveďte, jaká bezpečnostní opatření používáte pro zajištění bezpečnosti zpracovávaných osobních údajů (provozní opatření, IT opatření).
Je-li v klubu vydán a naplňován, lze odkázat na příslušný interní předpis (např. bezpečnostní normu).

Jsou zpracovávané osobní údaje přenášeny do zahraničí nebo jsou přístupné ze zahraničí [článek 30 odst. 1 písm. e) GDPR]?

Uveďte, zda jsou vámi zpracovávané osobní údaje přenášeny do zahraničí nebo přístupné ze zahraničí. Více viz část V. níže.

Jsou pracovníci, mající přístup k osobním údajům v rámci zpracování osobních údajů, proškoleni? Mají tito pracovníci ve svých smlouvách sjednánu povinnost mlčenlivosti ve vztahu ke zpracovávaným osobním údajům [článek 30 odst. 1 písm. g) GDPR]?

Uveďte, zda jsou pracovníci klubu proškoleni o GDPR a zásadách ochrany osobních údajů. Dále uveďte, zda pracovníci klubu včetně např. vašeho IT experta, mají smluvní závazek mlčenlivosti ve vztahu ke zpracovávaným osobním údajům, k nimž mají přístup.

2. Vyřizování žádostí a stížností subjektů zpracování

GDPR obsahuje řadu práv subjektů údajů. Kluby a ČJF musí zajistit hladký výkon těchto práv subjektů údajů. To bude pravděpodobně jedna z priorit ÚOOÚ při kontrolách shody s GDPR. Pro účely výkonu práv subjektů údajů zde proto uvádíme zásadní doporučení, spočívající v tom, že kluby musejí pro účely shody s GDPR zajistit hladký výkon práv subjektů údajů, např. prostřednictvím online formulářů na svých webech nebo v listinné podobě **tak, aby bylo uplatnění práv subjektu co nejjednodušší a nejefektivnější.** Usnadnit subjektům údajů výkon jejich práv lze dále např. v případě ČJF implementací standardizovaných procesů (postupů) zakotvených v interních předpisech a uplatňovaných v případě podání příslušné žádosti subjektem údajů, jakož i ustanovením veřejně přístupného jednotného kontaktního místa pro uplatnění nároků subjektů údajů. Důležitý je rovněž pravidelný audit výkonu činností regulovaných GDPR, evidovaná kontrola organizačních opatření a činností správců osobních údajů. Je-li jmenován pověřenec pro ochranu osobních údajů, vykonává v rámci činnosti správce osobních údajů výše uvedený audit, dohled a další kontrolní činnosti.

Elektronické žádosti. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob. Vždy je třeba ověřit identitu toho, kdo žádost v elektronické formě podal, aby se informace nedostaly neoprávněným osobám (způsob a míra ověření by měly odpovídat kontextu, rozsahu a citlivosti požadované informace). K ověření je možné použít např. telefon nebo SMS členovi, výjimečně lze požadovat i osobní identifikaci.

Lhůta. Informace musí být poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení.

Poplatek. Zásadně platí, že informace se poskytují bezplatně. Pouze v případě, pokud jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce. Zneužitím nelze a priori rozumět výkon práv subjektu údajů.
Níže uvádíme stručné informace o jednotlivých právech. V příloze jako jeden ze vzorů uvádíme vzor žádosti a odpovědi na žádost.

a) Právo na přístup

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,
- že má právo požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
- že má právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů, - o skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.

Pokud správce o fyzické osobě žádné údaje nezpracovává, poskytuje se informace, že osobní údaje tazatele nejsou předmětem zpracování osobních údajů ze strany správce.

Ve vztahu k členům lze jen doporučit, aby kluby na žádosti členů o přístup k osobním údajům reagovali vstřícně a poskytli alespoň hlavní kategorie osobních údajů, které klub/ČJF zpracovává. I když právní úprava umožňuje informace neposkytnout a žádost subjektu zamítnout s odkazem na to, že mu již všechny informace byly poskytnuty, proaktivní postoj k žádostem vlastních členů nepochybně lépe vyhoví požadavkům GDPR a výrazně eliminuje rizika případných kontrol ze strany ÚOOÚ.

Upozorňujeme, že **i zamítnutí žádosti musí být vyřízeno ve stanovené lhůtě**.
Více informací o právech subjektu údajů je k dispozici na internetových stránkách Úřadu pro ochranu osobních údajů. (https://www.uoou.cz/6-prava-subjektu-udaj/d-27276)

b) Právo na výmaz

Právo na výmaz představuje povinnost správce zlikvidovat osobní údaje, které o žadateli zpracovává, 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 vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovávány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 GDPR.

Výše uvedené podmínky se neuplatní, pokud je zpracování OÚ nezbytné:

a) pro určení, výkon nebo obhajobu právních nároků;
b) pro výkon práva na svobodu projevu a informace;
c) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
d) z důvodu veřejného zájmu v oblasti veřejného zdraví podle GDPR;
e) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely podle GDPR, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování.

V naprosté většině případů žádostí o výmaz, v souvislosti s vedením seznamu členů, bude třeba je odmítnout s odkazem na určení, výkon nebo obhajobu právních nároků, resp. na plnění právních povinností vyplývajících ze zákona o podpoře sportu nebo v souvislosti s ním.

c) Právo na přenositelnost

Právo na přenositelnost představuje právo subjektu údajů získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, a to v případě, že zpracování osobních údajů je založeno na souhlasu nebo na smlouvě a zpracování se provádí elektronicky (kumulativní podmínky).

Při výkonu svého práva na přenositelnost má žadatel – subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

V podmínkách klubů a ČJF zřejmě toto právo nebude nijak frekventováno a to zejména s ohledem na to, že každý klub při přijetí nového člena jednak MUSÍ poskytnout informaci o zpracovávání OÚ (viz vzor textu na přihlášce) bez ohledu na to, že do klubu vstupuje člen sice nový, ale mající již v minulosti (nebo stále) členství v jiném klubu, jednak každý klub musí být schopen prokázat své ev. právní nároky – typicky přihláškou za člena klubu.

d) Právo na opravu nebo doplnění

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů.

Pokud se správce domnívá, že zpracovávané osobní údaje jsou přesné, informuje o tom žadatele s odůvodněním.

Toto právo se v podstatě kryje s povinností správce dodržovat již výše uvedenou zásadu přesnosti – tedy dbát o to, aby klub měl v komunikaci se členem na paměti, že je primárně především jeho povinností dbát o to, že údaje mají být správné a nespoléhat se až na to, že člen uplatní své právo na opravu.

e) Další práva subjektů údajů

GDPR obsahuje i další práva subjektů údajů, a to právo na omezení zpracování a právo podat námitku proti automatizovanému rozhodování, přičemž tato práva budou pravděpodobně jen minimálně frekventována.

Ve vztahu ke všem shora uvedeným právům odkazujeme na vzor žádosti subjektu údajů a vzor odpovědi na žádosti uvedené v příloze č. 1 a č. 2 této Metodiky.

3. Revize smluv s dodavateli

Většina klubů/ČJF bude muset revidovat smlouvy se svými dodavateli a odběrateli služeb (např. poskytovatelé informatických služeb – dodavatelé software, externí účetní, daňové a auditorské společnosti apod.). Dodavatelé velmi často v rámci své činnosti zpracovávají osobní údaje na základě pokynů objednatelů – správců a jsou tedy koncovými zpracovateli osobních údajů, s nimiž musejí mít kluby/ČJF coby správci uzavřené písemné smlouvy o zpracování osobních údajů, které obsahově vyhoví čl. 28 odst. 3 GDPR.

Kluby/ČJF jakožto správci by měly ve smlouvách se svými dodavateli – zpracovateli osobních údajů mít dohodnuta následující ujednání:

- Specifikovat osobní údaje, které jsou zpracovávány (např. zpracování mezd zaměstnanců).
- Uvést účel zpracování osobních údajů (např. zajišťování údržby IT systému klubu). Tímto účelem je omezen rozsah zpracování osobních údajů dodavatelem.

- Uvést závazek zpracovatele zpracovávat osobní údaje v souladu s příslušnými právními předpisy, smlouvou nebo pokyny správce vydanými v souladu s příslušnými právními předpisy. Nebude-li dodavatel moci z jakýchkoli důvodů zajistit dodržování zákonných povinností či pokyny správce, zavazuje se o tom správce neprodleně informovat.
- Uvést do smlouvy vždy povinnost dodavatele
    a) zpracovávat pouze osobní údaje odpovídající stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,
    b) nesdružovat osobní údaje, které byly získány k rozdílným účelům či
    c) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování.
- Uvést povinnost dodavatele přijmout před zpracováním osobních údajů odpovídající organizační a technická bezpečnostní opatření pro zajištění ochrany osobních údajů. Tato opatření zahrnují pro kluby přinejmenším zabezpečený přístup do prostor, v nichž probíhá zpracování osobních údajů, přístup k osobním údajům jen pro vybrané pracovníky dodavatele, kteří tento přístup potřebují pro účely plnění smlouvy, aj.
- Uvést závazek dodavatele proškolit své zaměstnance a další případné zástupce, kteří zpracovávají osobní údaje, o jejich povinnosti (trvající i po skončení zaměstnání nebo příslušných prací) zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.
- Uvést závazek dodavatele neprodleně oznamovat správci veškeré případy náhodného nebo neoprávněného přístupu k osobním údajům.

Je nutné, aby kluby/ČJF vybíraly své dodavatele také podle toho, jak dokáží plnit povinnosti ochrany osobních údajů podle GDPR. Současně by kluby/ČJF, jakožto správci, měly v přiměřených lhůtách pravidelně kontrolovat plnění závazků dodavatelů podle uzavřených smluv o zpracování osobních údajů. Zápisky z takových kontrolních dnů budou sloužit k doložení úsilí zpracovatele plnit své povinnosti správce osobních údajů při případné kontrole ÚOOÚ. Postupy a harmonogram kontrol plnění závazků dodavatelů podle uzavřených smluv o zpracování osobních údajů je třeba standardizovat v interní směrnici na ochranu osobních údajů.

4. Pověřenec pro ochranu osobních údajů

GDPR zavádí pro některé správce a zpracovatele osobních údajů povinnost ustavit a obsadit funkci tzv. pověřence pro ochranu osobních údajů (DPO), který plní funkci koordinátora a supervizora ochrany osobních údajů. GDPR uvádí několik charakteristických situací, kdy správci nebo zpracovatelé jsou povinni jmenovat DPO, v čl. 37.

Pro kluby bude povinné jmenování DPO spíše výjimkou. Bude to na základě následující podmínky GDPR:
Spočívají Vaše hlavní činnosti v rozsáhlém zpracování zvláštních kategorií osobních údajů?

Zvláštní kategorie osobních údajů jsou údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje a biometrické údaje a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Jak již bylo uvedeno výše, někteří správci zdravotní stav svých členů sledují, ale nejde o „hlavní činnost v rozsáhlém zpracování“ – to lze v podmínkách klubů a ČJF konstatovat i s vědomím, že měřítka toho, kdy je zpracování osobních údajů rozsáhlé, GDPR nestanoví a ani ve výkladové praxi nejsou zatím nijak ustálena, a budou se dále upřesňovat.

K problematice DPO je namístě podotknout, že DPO není osobou, která by schvalovala nebo určovala soulad postupů s GDPR – zde vždy odpovídá pouze správce.

5. Souhlasy subjektů se zpracováním osobních údajů

Jak již bylo několikrát vyloženo, ČJF přistupuje k otázce zpracování OÚ z pozice, podle které není třeba souhlasu subjektů údajů se zpracováním. Výjimkou je **rodné číslo**, k jehož zpracování je zatím souhlas nutný.

V této souvislosti je taktéž třeba, aby si kluby/ČJF, jakožto správci, byly vědomy rozdílů mezi „Členskými informacemi“ rozesílanými například ve formě newsletterů a osloveními (dopisy, e-maily, telefonáty), která jsou reklamními sděleními. Jinými slovy – budou-li kluby rozesílat svým členům pouze základní informace z klubového života (novinky, akce, členské příspěvky aj.), nepotřebují souhlas. Ve všech ostatních případech musí mít klub před tím, než zašle marketingovou informaci či reklamní sdělení od subjektu údajů souhlas.

Žádost o souhlas musí být konkrétně formulována a musí být doprovázena informacemi o účelu a prostředcích zpracování osobních údajů, o tom, s kým budou osobní údaje sdíleny, jak budou zabezpečeny a jaká práva má člen ve vztahu ke svým údajům.

Souhlas může subjekt údajů kdykoliv odvolat. Souhlasy je nutné interně evidovat, přičemž tato evidence musí být systematická a přehledná (s vyznačením doby, po kterou jsou osobní údaje na základě souhlasu zpracovávány). Právě z tohoto důvodu se doporučuje zpracování založené na souhlasu subjektů údajů využívat minimálně.

6. Hlášení bezpečnostních incidentů

GDPR klade velký důraz na systematickou ochranu a zabezpečení osobních údajů. GDPR zavádí povinnost jednak hlásit bezpečnostní incidenty ÚOOÚ, a v případě, že hrozí rizika pro práva a svobody dotčených subjektů údajů, také tyto incidenty neprodleně oznamovat těmto subjektům údajů.

Nařízení GDPR definuje bezpečnostní incidenty jako případy porušení zabezpečení osobních údajů, tedy velmi široce. Spadají sem nejenom přímé útoky na zpracovávaná data zvenčí anebo zevnitř (ať již úmyslné, jako je „vynesení“ informací, anebo nedbalostní, jako je např. smazání částí údajů v IT systému), ale i celá řada drobnějších a méně nápadných situací, kdy klub/ČJF ztratí kontrolu nad daty, která spravuje – např. i ztráta nezabezpečeného mobilního telefonu s kontakty na členy klubu anebo notebooku se seznamem členů (!)

Hlášení bezpečnostních incidentů je povinné vždy, ledaže je nepravděpodobné, že by konkrétní porušení bezpečnosti mělo za následek riziko pro práva a svobody fyzických osob (např. ztráta zaheslovaného mobilního telefonu anebo krádež notebooku, jehož disk je standardně šifrován). Bohužel, prozatím není k dispozici přesnější vodítko k určení, které případy se musí ÚOOÚ hlásit, a které ne. Vždy je proto vhodné provést předběžné posouzení existujícího nebo potenciálního rizika a vyhodnotit jeho závažnost pro práva a svobody fyzických osob.

Jako příklad velmi závažného porušení bezpečnosti zpracovávaných osobních údajů je možné uvést ztrátu členské agendy – například přihlášek ke členství v klubu (ve fyzické i elektronické podobě) nebo zjištěný neoprávněný přístup k databázi členů. Takovéto bezpečnostní incidenty bude potřeba ohlásit ÚOOÚ i dotčeným subjektům údajů.

Přestože ne každé porušení zabezpečení bude nutné hlásit dozorovému úřadu anebo subjektu údajů, je potřeba jej vždy zaznamenat do evidence takovýchto porušení, kterou musí mít každý správce osobních údajů.

Každý klub by měl mít jako součást interní směrnice vypracovaný postup řešení bezpečnostních incidentů. **Tento postup zahrnuje nejen neprodlené hodnocení incidentu a jeho ohlášení ÚOOÚ a případně dotčeným subjektům údajů, ale také co nejrychlejší řešení incidentu a přijetí opatření k tomu, aby se pokud možno podobný bezpečnostní incident nemohl opakovat.**

V. Předávání osobních údajů do zahraničí

V podmínkách standardní členské správy a činnosti klubu se takováto situace nepředpokládá, nicméně je potřeba důsledně rozlišovat, kam se OÚ případně předávají. Pokud je předávání osobních údajů v rámci EU anebo EHP, nemusí se provádět žádné zvláštní postupy a data lze předat stejně, jako by se jednalo o předání v rámci ČR, výhodu zemí s dostatečnou ochranou OÚ požívají Faerské ostrovy, Jersey, Ostrov Man, Guermsey, Argentina, Švýcarsko, Uruguayská republika, Andorra a Nový Zéland. U několika dalších států, např. Izrael, Kanada nebo USA platí zvláštní režim – více informací lze nalézt na webových stránkách ÚOOÚ.

VI. Závěr

Cílem této metodiky je pomoci jezdeckým klubům v lepší orientaci v problematice GDPR s tím, že kromě vysvětlení klíčových pojmů předkládá určitá konkrétní řešení z hlediska dokumentace, která je pro kluby jakožto správce předepsaná a ze strany ÚOOÚ bude při provádění kontroly vždy prověřována.

Touto dokumentací je myšlena „***Směrnice o zpracování osobních údajů jezdeckého klubu …x.y…***“, jejíž součástí by měly být minimálně shora popsané a okomentované následující pasáže:

1. Evidence činností zpracování – vždy k dané konkrétní otázce uvést údaje dle skutečnosti - viz čl. IV odst. 1. shora
2. Vyřizování žádostí a stížností subjektů zpracování – viz čl. IV odst. 2. shora (příloha č. 1 „VZOR – žádost subjektu údajů o uplatnění práv“, příloha č. 2 „VZOR – odpověď subjektu údajů“)
3. Revize smluv s dodavateli – viz čl. IV odst. 3. shora
4. Pověřenec pro ochranu osobních údajů – do textu v interní směrnici v této části postačí uvést, že s odkazem na čl. 37 GDPR není DPO vyžadován – viz čl. IV odst. 4. shora
5. Souhlas člena se zpracováním osobních údajů – viz. definovaný vzor souhlasu
6. Hlášení bezpečnostních incidentů - viz čl. IV odst. 6. shora
7. Náležitosti Informace členům – viz povinná součást přihlášky

Jezdecké kluby nejsou a velmi pravděpodobně nebudou primární cílovou skupinou z hlediska kontrolní činnosti ze strany ÚOOÚ, neboť, jak vyplývá z důvodové zprávy k GDPR, celá tato problematika směřuje především k tzv. velkým správcům. Tomu ostatně odpovídá i povinnost zřizování pověřence (byla rozebrána výše), která se na jezdecké kluby až na výjimky nebude vztahovat. Zároveň je však třeba mít na paměti, že problematika ochrany osobních údajů tak, jak je pojata, je skutečně významným mezníkem v chápání, nakládání, správě, údržbě a především ochraně před zneužitím osobních údajů fyzických osob v rámci jednotného prostředí EU a EHP.

Právě z těchto důvodů tedy nelze k problematice GDPR přistupovat formálně, ale s plnou vážností, neboť ochrana osobních údajů se stává velkým společenským tématem a je nutné, aby kluby předpokládaly, že může ze strany některých jejich členů docházet k podnětům k ÚOOÚ, na základě kterých bude v rámci výkonu své kontrolní pravomoci ÚOOÚ u klubů jakožto správců provádět kontrolní činnost.

GDPR se nevztahuje na údaje zemřelých osob a údaje zpracované pro osobní potřebu bez dalšího šíření.

Tato metodika je tedy zaměřena na to, by si kluby mohly vytvořit svoji interní „směrnici“, která nebude formální, ale vyhovující.

Je plně na místě v této souvislosti upozornit, že tato metodika je cílena na standardní jezdecký klub, tedy klub, který se zabývá výhradně svojí sportovní činností (tedy jezdeckým servisem pro své členy, o kterých spravuje informace v rozsahu nezbytném k tomu, aby klub mohl plnit

svůj účel v souladu se svými stanovami). Je tedy zřejmé, že jedná-li se o klub velký – vztaženo nikoliv na počet členů ale na příjmy, od nichž se odvíjí zákonem předvídané méně než poloviční příjmy z vedlejší hospodářské činnosti – mající vysoké příjmy z vedlejší hospodářské činnosti, bude interní směrnice specificky rozsáhlejší. V dnešní době je na trhu poměrně široká nabídka agentur či právních kanceláří, které mnohdy za značné částky nabízejí provedení analýzy rizik a vypracování vnitřní směrnice. Jak již bylo řečeno, cílem této metodiky je to, aby kluby s její pomocí splnily požadavky GDPR bez nutnosti dalších výdajů.

Závěrem je potřeba věnovat zvláštní pozornost otázce prevence. Interní směrnice slouží především k tomu, aby byla zanalyzována problematika ochrany osobních údajů v daném konkrétním klubu s tím, že je třeba, v případě potřeby, ji průběžně doplňovat či opravovat, typicky dojde-li ke změně SW či IT specialisty či dojde-li k vyjasnění, resp. ke zpřesnění či zúžení nebo rozšíření okruhu zpracovávaných osobních údajů. Zároveň je třeba mít neustále na paměti záměr a cíl interní klubové směrnice, tedy předcházet bezpečnostním incidentům (blíže popsáno shora). Otázka průběžného doplňování, resp. úprav interní směrnice je záležitostí velmi subjektivního posuzování, a lze proto očekávat, že jakmile jednou klub vytvoří interní směrnici, obvykle nebude mít tendenci se k ní vracet, s výjimkou jediného případu – a tím bude bezpečnostní incident. Dojde-li totiž k bezpečnostnímu incidentu, má zpracovatel povinnost „*bez zbytečného odkladu a pokud možno do 72 hodin ……*“ toto oznámit ÚOOÚ, „ *… ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob*“. Tato variabilita v rozhodování klubu o „závažnosti bezpečnostního incidentu“ je záležitostí, kterou si musí klub v případě neoznámení incidentu obhájit. Je však zcela jisté, že vždy bude nezbytné bez ohledu na „oznámení či neoznámení“ upravit interní směrnici ve smyslu „poučení se“ z bezpečnostního incidentu.

Lze s určitostí očekávat, že se problematika GDPR, resp. aplikační pravidla k harmonizaci, budou postupně vyvíjet a měnit, přičemž je otázkou, jak by bylo případné očekávání zjednodušení administrativní zátěže (tedy „vyčkávání“) klubů jakožto správců, ze strany kontrolních orgánů hodnoceno, resp. jak by bylo sankcionováno, z čehož vyplývá jednoznačné doporučení ČJF svým členským subjektům realizovat postupy specifikované v této metodice co nejdříve.

Praha, květen 2018

Schváleno VV ČJF , dne 24.5.2018

Příloha č.1 - VZOR – žádost subjektu údajů o uplatnění práv

Příloha č.2 – VZOR – odpověď subjektu údajů