METODICKÝ POKYN PRÁVNÍHO ODDĚLENÍ FAČR Č. 3/2018

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ČLENŮ KLUBŮ A DALŠÍCH OSOB

Platnost od 25. 5. 2018

Verze: 01

OBSAH:

1. ÚVODNÍ SLOVO

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) („**Nařízení**“) s účinností od 25. května 2018 je přímo aplikovatelné ve všech členských zemích Evropské unie, včetně České republiky, a nahrazuje v tomto směru dosud platný český zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Pokuty a následky zaváděné Nařízením jsou výrazně přísnější, a proto si Fotbalová asociace České republiky („**FAČR**“) uvědomuje nezbytnost zpracování této problematiky do podoby, která odpovědným osobám přiblíží postupy a ulehčí seznámení s problematikou zpracování osobních údajů.

Cílem *Metodického pokynu Zpracování osobních údajů členů klubů a dalších osob* („**Metodický pokyn**“) je seznámit osoby jednající za klub se zpracováním osobních údajů členů klubu a dalších fyzických osob a se změnami úpravy ochrany osobních údajů v souvislosti s Nařízením.

Metodický pokyn je obecným vodítkem při aplikaci jednotlivých pravidel týkajících se nakládání s osobními údaji. Jejím záměrem je zjednodušení a přiblížení procesů, které by si měl klub, jakožto správce a zpracovatel osobních údajů, při zpracování osobních údajů svých členů osvojit. Jednotlivé postupy by se měly proměnit v pravidla, jejichž dodržování se stane samozřejmostí.

Cílem Nařízení je zajistit vysokou úroveň ochrany osobních údajů ve všech členských státech Evropské unie a spolu se zákonem[1] o zpracování osobních údajů („**Zákon**“) zajistit volný pohyb údajů a informací mezi členskými státy (zejména z důvodu stále se rozvíjejícího vnitřního trhu), stanovit společný rámec pro práci s osobními údaji a jejich ochranu na území Evropské unie a sladit národní legislativu a rozhodovací praxi státních orgánů na území jednotlivých států; členské státy si mohou nadále v národních předpisech upřesnit obecné podmínky a zákonitosti zpracování osobních údajů v oblastech, ve kterých to Nařízení připouští.

Nejen výše zmíněné cíle Nařízení, ale také cíle FAČR jsou s politikou ochrany osobních údajů naprosto identické, a proto si tento Metodický pokyn klade za cíl zvýšit povědomí a standard ochrany osobních údajů při zpracování osobních údajů členů klubů a dalších osob.

[1] *Předpis, který adaptuje některé oblasti vyplývající z Nařízení do českého právního řádu (ke dni vydání tohoto Metodického pokynu není dosud schválený Parlamentem ČR).*

2. ZÁKLADNÍ POJMY

V souladu se Zákonem a Nařízením se pro účely tohoto Metodického pokynu rozumí:

(a) **správcem** subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; pokud účely a prostředky zpracování osobních údajů stanoví právo Evropské unie či členského státu, může toto právo stanovit i kdo bude správcem nebo stanovit zvláštní kritéria pro určení správce. **Správcem podle tohoto Metodického pokynu a ve smyslu Zákona a Nařízení je klub (dále také „Správce“);**

(b) **zpracovatelem** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro Správce;

(c) **subjektem údajů** identifikovaná nebo identifikovatelná (tj. určená nebo určitelná) fyzická osoba, jinými slovy osoba, k níž se osobní údaje vážou, zejména **člen klubu**;

(d) **příjemcem** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu (osoba, která není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli), 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 vztahujícími se na dané účely zpracování;

(e) **osobním údajem** veškeré informace o identifikované nebo identifikovatelné fyzické osobě (subjektu 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;

(f) **zvláštní kategorií osobních údajů** osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;

(g) **souhlasem subjektu údajů** jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

(h) **databází/evidencí** jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

(i) **biometrickými údaji** osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

(j) **anonymním údajem** takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů;

(k) **pseudonymizací** zpracování osobních údajů takovým způsobem, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

(l) **zpracováním osobních údajů** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

(m) **shromažďováním osobních údajů** systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování;

(n) **uchováváním osobních údajů** udržování údajů v takové podobě, která je umožňuje dále zpracovávat;

(o) **likvidací osobních údajů** fyzické zničení jejich nosiče, jejich fyzické vymazání nebo trvalé vyloučení z dalších zpracování;

(p) **profilováním** jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;

(q) **porušením zabezpečení osobních údajů** porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

(r) **členem** fyzická osoba, která je v souladu se stanovami FAČR zaregistrována jako člen klubu;

(s) **zákazníkem** fyzická nebo právnická osoba fungující jako dodavatel klubu zabezpečující služby určitého charakteru.

3. PRÁVNÍ ÚPRAVA A ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

3.1 PRÁVNÍ ÚPRAVA

Ochrana osobních údajů nestojí v našem právním řádu samostatně, ale je součástí mnohem širší oblasti a tou je ochrana soukromí. Ochrana soukromí se v poslední době stala nedílnou součástí našeho života. Jako obecný fenomén je stále častěji vnímána jako něco, co vyžaduje zvláštní zájem. Je jí zejména v posledních několika letech věnována značná pozornost. To se projevuje například tím, že řada právních předpisů obsahuje zvláštní ustanovení týkající se ochrany soukromí a osobního života nebo ochrany osobních údajů, a jsou stanovovány daleko přesnější limity pro to, kdo a k jakým údajům či informacím má či může mít přístup.

Platná právní úprava stanovující způsob nakládání s osobními údaji je primárně obsažena v Nařízení, které prohlubuje stávající právní úpravu a spolu se Zákonem nahrazuje úpravu dosavadní. Pokud jde o stanovení práv a povinností, není mezi Nařízením a Zákonem rozdíl, oba dva právní předpisy přímo upravují práva a povinnosti adresátů. Jistou

zvláštností Nařízení oproti Zákonu je jeho Preambule, která obsahuje tzv. recitály, což jsou ustanovení před vlastním textem Nařízení a tato ustanovení slouží v některých případech jako výklad či do jisté míry jako důvodová zpráva k některým ustanovením vlastního textu Nařízení. **Je tak vhodné při práci s Nařízením sledovat i jednotlivé recitály, které se např. týkají konkrétního článku či institutu obsaženého v Nařízení.**

Nařízení působí přímo, vyvolává přímé účinky, a proto je třeba s ním pracovat jako s každým jiným zákonem, tj. být s ním v souladu a plnit povinnosti v něm uvedené. Smyslem Nařízení a Zákona je realizovat Listinou základních práv a svobod zaručené právo na ochranu před neoprávněným zasahováním do soukromého a osobního života neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů.

Z právních předpisů upravujících ochranu soukromí je na prvním místě vhodné zmínit zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů („**Občanský zákoník**"), který úzce souvisí s ochranou soukromí člověka, resp. s ochranou osobnosti. V zásadě platí, že do soukromí člověka nelze zasahovat. Zároveň pak platí, že nelze nezákonně zpracovávat osobní údaje těchto osob. Z této zásady existují zákonem vymezené výjimky, které jsou upraveny zejména ustanoveními § 87 až § 89 Občanského zákoníku.

Do práva na soukromí nezasahuje ten, anebo jinými slovy oprávněně zpracovává osobní údaje a případně je dále používá ten, kdo pořizuje osobní údaje (např. fotografie), za účelem ochrany nebo výkonu práv osob. Jako příklad lze uvést pořízení nebo použití fotografií nebo záznamů z kamerového systému pro účely občanskoprávního nebo trestního řízení (jako důkazní prostředek).

Dalším oprávněným zásahem do soukromí, tedy oprávněným zpracováváním osobních údajů, pořízením nebo použitím fotografií nebo jiných obrazových a zvukových záznamů, jsou tzv. vědecké, umělecké nebo zpravodajské licence. Jako příklad lze uvést **pořizování fotografií z veřejných akcí pořádaných klubem pro novinářské či reportážní účely. Od reportážních účelů je třeba odlišit pořizování fotografií výhradně za účelem propagace či zvýšení zájmu možných budoucích členů o klub. Na zmíněné situace tzv. zpravodajská licence nedopadá.** Proto je u jednotlivých fotografií/záznamů třeba rozlišovat, zda je zaznamenána konkrétní osoba, která o pořizování snímků/záznamů své osoby ví, konkludentně s ním souhlasí a zároveň, což je nezbytná podmínka, ví, jak bude s fotografií/záznamem dále nakládáno.

Výše zmíněné zákonné výjimky musí být využívány přiměřeným způsobem, v souladu s pravidly slušnosti a obvyklého chování v občanské společnosti a rozumného očekávání dotčené osoby.

Kromě výše uvedených právních předpisů, na činnost klubů v oblasti zpracování osobních údajů dopadají zejména následující právní přepisy:

(a) *115/2001 Sb., o podpoře sportu,* který upravuje povinnost zapsat některé osobní údaje o sportovcích do rejstříku sportovních organizací a sportovců;

(b) *373/2011 Sb., o specifických zdravotních službách*[2]*;*

(c) *391/2013 Sb., vyhláška o zdravotní způsobilosti k tělesné výchově a sportu.*

[2] *zejména § 51; Posuzování zdravotní způsobilosti ke vzdělávání, k tělesné výchově a sportu*

Dozorovým úřadem odpovědným za kontrolu a sledování dodržování zákonných povinností v oblasti ochrany osobních údajů bude zpravidla Úřad pro ochranu osobních údajů[3], ale od účinnosti Nařízení (25. 5. 2018) není vyloučena přeshraniční kontrola jakéhokoliv jiného dozorového úřadu v oblasti ochrany osobních údajů z členského státu Evropské unie.[4]

3.2 ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Zásady neboli principy zpracování osobních údajů a ochrany se vztahují na všechny druhy a operace zpracování osobních údajů prováděné Správcem. Výslovně jsou jednotlivé principy uvedeny v článku 5 odst. 1 Nařízení a jejich dodržování je pro klub zásadní nejen z toho důvodu, že se de facto jedná zároveň o povinnosti, ale i proto, že v Nařízení výslovně upravuje odpovědnost Správce za jejich dodržování. Dodržování plnění povinností v souladu se zásadami musí být Správce, tedy klub, schopen také doložit, neboli dokázat, že jedná v souladu s pravidly. Jde o vyjádření jedné ze základních zásad, které Nařízení upravuje, a to tzv. principu odpovědnosti Správce.

Zásady vztahující se na zpracování osobních údajů vyjádřené přímo v Nařízení:

(a) **zákonnost, korektnost, transparentnost**; podle těchto zásad musí Správce zpracovávat osobní údaje minimálně na základě jednoho právního důvodu/titulu vyjádřeného v článku 6 odst. 1 anebo článku 9 odst. 2 Nařízení (tj. na základě souhlasu subjektu údajů, na základě smlouvy, právní povinnosti atd.);

(b) **omezení účelu**; osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány způsobem neslučitelným s těmito účely (tj. klub jakožto správce osobních údajů musí mít určitý důvod/účel, proč osobní údaje shromažďuje, a tyto údaje smí zpracovávat pouze pro naplnění tohoto účelu – např. registrace);

(c) **minimalizace údajů**; osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány (klub nesmí shromažďovat a dále zpracovávat takové údaje, které nejsou nutné pro splnění účelu);

(d) **přesnost**; osobní údaje musí být přesné. Zásada souvisí s aktualizací údajů (klub by měl v případě potřeby údaje aktualizovat, aby nebyly zastaralé);

(e) **omezení uložení**; osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány (klub nesmí zpracovávat osobní údaje po delší dobu, než která je nutná pro naplnění účelu);

(f) **integrita a důvěrnost**; technické a organizační zabezpečení osobních údajů na nejvyšší možné úrovni tak, aby nebyly údaje zpracovávány neoprávněnými osobami.

Zásady dovozované z textu Nařízení a Zákona:

(a) rozlišovat zpracování na základě souhlasu a jiných právních důvodů;

(b) udělení souhlasu se zpracováním je právem a nikoli povinností (pokud je zpracování prováděno na základě souhlasu subjektu údajů, může subjekt údajů odmítnout udělení souhlasu);

(c) respektovat práva subjektu údajů a jejich uplatňování;

---

[3] https://www.uoou.cz/vismo/o_utvar.asp?id_u=10&p1=4252.

[4] *Článek 56 odst. 4 Nařízení stanoví, že pokud vedoucí dozorový úřad (Úřad pro ochranu osobních údajů) rozhodne, že se věcí zabývat nebude, zabývá se jí v souladu s články 61 a 62 Nařízení dozorový úřad, který informoval vedoucí dozorový úřad.*

(d) pohlížet na právní předpisy upravující zpracování osobních údajů jako na předpisy zvyšující bezpečnost a ochranu soukromého života člověka;

(e) respektovat dozorový úřad.

Výše uvedený výčet zásad lze doplnit o koncept odpovědnosti, na kterém Nařízení i Zákon spočívá. Jedná se o objektivní odpovědnost, která nevyžaduje zavinění (úmysl nebo nedbalost jednajícího). Klub bude tedy při neoprávněném zpracování, např. úniku dat, odpovídat vždy, i pokud neměl v úmyslu způsobit újmu. Přičemž dozorový úřad může od uložení správního trestu (pokuty) upustit anebo výši pokuty snížit, dospěje-li k názoru, že Správce vynaložil veškeré úsilí, aby neoprávněnému zpracování (takovému, které není v souladu s pokyny Nařízení nebo Zákona) zabránil.

V případě zpracovávání osobních údajů na základě souhlasu u dětí mladších 15 let se bude vyžadovat souhlas zákonného zástupce. Děti starší 15 let můžou souhlas udělit bez omezení.

Recitál Nařízení upozorňuje, že *děti zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů. Tato zvláštní ochrana by se měla zejména vztahovat na používání osobních údajů dětí pro účely marketingu nebo vytváření osobnostních i uživatelských profilů a shromažďování osobních údajů týkajících se dětí při využívání služeb nabízených přímo dětem. Souhlas nositele rodičovské zodpovědnosti by neměl být nutný v případě preventivních či poradenských služeb nabízených přímo dětem.*[5]

4. OSOBNÍ ÚDAJE A ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ

4.1 OSOBNÍ ÚDAJE

Pojem osobní údaj s technologickým rozvojem dostává nový rozměr. Klub zpracovává údaje a informace, které v určitém okamžiku mohou být údaji osobními, anebo také údaji citlivými, které mezi osobními údaji zaujímají zvláštní postavení (viz bod 4.2). Výklad pojmu osobní údaj blíže vymezuje kapitola 2. bod (e) Metodického pokynu a zjednodušeně lze říci, že osobním údajem je jakýkoliv údaj/informace, který lze vztáhnout k fyzické osobě (jméno, e-mail, rodinný stav apod.). Rozhodující je, zda lze údaje ke konkrétní fyzické osobě přiřadit. Osobním údajem může být jeden údaj nebo i více údajů, které teprve dohromady umožňují konkrétní osobu identifikovat/určit. Není přitom rozhodující, zda má Správce tyto údaje v jedné databázi nebo ve více oddělených databázích, seznamech či evidencích.

Podle rozhodnutí Nejvyššího správního soudu je pouhé telefonní číslo (tj. bez přiřazeného jména) osobním údajem, neboť právě v podmínkách technologicky vyspělé společnosti lze osobu v určitém časovém úseku přímo kontaktovat. Podle soudu se výklad pojmu osobní údaj nemůže omezit striktně jen na znalost např. rodného čísla, adresy či pracoviště subjektu údajů. Z tohoto pohledu je za osobní údaj třeba považovat i číslo mobilního telefonu určité osoby.[6]

Osobní údaje lze rozdělit do několika kategorií:

[5] *Recitál 38 Nařízení.*

[6] *Rozhodnutí Nejvyššího správního soudu spis. zn. 9 As 34/2008-68 Sb.*

(a) **Identifikační údaje**: umožňují osobu ztotožnit a odlišit od jiných. Mezi identifikační údaje se řadí: *jméno a příjmení, datum narození a místo narození, číselné kódy např. rodné číslo*[7]*;*

(b) **Adresní údaje**: charakterizují polohu. Mezi adresní se řadí *ulice, číslo, PSČ, stát anebo GPS souřadnice*;

(c) **Kontaktní údaje**: umožňující osobu kontaktovat. Mezi kontaktní údaje se řadí primárně *e-mailová adresa a telefonní číslo*;

(d) **Popisné údaje**: sloužící zejména k posuzování, hodnocení, příp. třídění a vyhledávání záznamů;

(e) **Finanční údaje:** obsahují informace o ekonomické činnosti;

(f) **Údaje o zdravotním stavu**: analyzující/hodnotící momentální stav/kondici člena.

4.2 ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ, TZV. CITLIVÉ ÚDAJE

Citlivé údaje jsou dle Nařízení zvláštní kategorií osobních údajů, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Zpracování těchto údajů vyžaduje zvláštní, přísnější režim, neboť mohou subjekt údajů samy o sobě ve společnosti, v zaměstnání, ve škole apod. poškodit, či mohou zapříčinit jeho diskriminaci.

Klub může, má-li právní základ pro takové zpracování osobních údajů, zpracovávat také údaje o zdravotním stavu. Formálně vzato je informací o zdravotním stavu určitého člověka také konstatování zdravotnického pracovníka, že je daná osoba zdráva, že je její zdravotní stav dobrý či vyhovující nebo že neprodělala určitý úraz či netrpí některou chorobou. **Účelu Nařízení a Zákona však bude plně dosaženo, pokud i v tomto případě budou za citlivé údaje považovány pouze informace o konkrétní prodělané či aktuální nemoci či úrazu dané osoby a o podstoupené léčbě (tedy nikoliv pouze údaj o způsobilosti/nezpůsobilosti)**. V některých případech mohou být citlivé údaje o zdravotním stavu odvoditelné i z informací o prodělaných vyšetřeních (na specifických lékařských pracovištích či pomocí určitých lékařských nástrojů), proto bude i takové údaje nutno považovat za citlivé. Výčet citlivých údajů v souvislosti s činností FAČR bude obsahovat především informace o zranění, ke kterému došlo při výkonu sportovní činnosti anebo nemoci, která brání členovi účastnit se sportovní činnosti.

5. PRAVIDLA EVIDENCE OSOBNÍCH ÚDAJŮ

Evidence neboli jinak řečeno vedení záznamů anebo přehledů má pro Správce význam z hlediska prokazování souladu své činnosti s Nařízením a Zákonem. Dle článku 30 Nařízení mají správci, kteří zaměstnávají více než 250 osob povinnost vést tzv. záznamy o zpracování osobních údajů, za které odpovídají. **Bez ohledu na počet zaměstnanců je Správce anebo také zpracovatel povinen vést záznamy** v takových případech zpracování, které i) představuje riziko pro práva a svobody subjektů údajů, ii) zpracování není příležitostné, nebo iii) zahrnuje zpracování zvláštních kategorií údajů (viz odstavec 4.2). Jelikož zpracování údajů klubem není příležitostné a zpracování může představovat zásahy do práva a svobod subjektu údajů, je vysoce pravděpodobné, že **Klub musí vést záznamy o zpracování údajů**. V neposlední řadě na základě

[7] *Rodné číslo se řadí mezi osobní údaje a v mnoha kontextech se používá jako jednoznačný identifikátor fyzické osoby. Lze ho však zpracovávat pouze na základě souhlasu subjektu údajů (nositele rodného čísla) anebo stanoví-li tak zvláštní zákon, nejedná-li se o činnost ministerstev.*

kineziologického rozboru (vyšetření fyzioterapeuta) bude klub zpracovávat též údaje o zdravotním stavu.

5.1 ZÁZNAMY POŘIZOVANÉ SPRÁVCEM

Správce je povinen vést záznamy o činnostech zpracování, za které je odpovědný. Vzorový příklad vedení/sepsání záznamů o činnostech zpracování (tzv. datová mapa) je uveden v příloze tohoto Metodického pokynu. Záznamy lze vést v papírové podobě anebo v elektronické ve formátu Excel, Word, apod.

Tyto záznamy dle č. 30 Nařízení obsahují minimálně následující informace:

Informace vedené Správcem	Vysvětlení
Kontaktní údaje	*Součástí záznamů jsou také informace o Správci, zejména: jméno a kontaktní informace, případně kontaktní informace společného Správce, zástupce Správce nebo pověřence pro ochranu osobních údajů.*
Účel/y zpracování	*Ze záznamů o zpracování musí být zřejmé, k jakému účelu jsou osobní údaje při konkrétní činnosti zpracovávány. Správce může v záznamech například uvést, že e-mailové adresy zpracovává za účelem zasílání marketingových sdělení.*
Popis kategorií subjektu údajů a kategorie osobních údajů	*Záznamy mají obsahovat informace o tom, jakých subjektů údajů se osobní údaje týkají (např. zákazníci). Stejně tak musí být ze záznamů jasné, jakých kategorií osobních údajů se zpracování týká (např. adresní a identifikační údaje).*
Kategorie příjemců	*Součástí záznamů musí být vymezení alespoň jednotlivých skupin příjemců osobních údajů (např. společnosti vymáhající dlužné pohledávky nebo ostatní členové skupiny podniků), a to včetně příjemců ve třetích zemích nebo v mezinárodní organizaci*
Předávání do zahraničí	*V záznamech musí být uvedena informace o předání osobních údajů do konkrétní třetí země nebo konkrétní mezinárodní organizaci. Správce je povinen doložit vhodné záruky pro ochranu osobních údajů, jestliže se jedná o předání osobních údajů do zahraničí, které je založeno na výjimce pro specifické situace podle druhého pododstavce článku 49 odst. 1 Nařízení.*
Plánované lhůta pro výmaz	*Je-li to možné, uvede Správce v záznamech lhůtu, ve které dojde k výmazu jednotlivých kategorií osobních údajů.*
Technická a organizační opatření.	*Je-li to možné, uvede Správce obecný popis technických a organizačních opatření, která přijal v souvislosti se zabezpečením osobních údajů podle článku 32 odst. 1 Nařízení. Lze tak učinit prostřednictvím výčtu interních a externích předpisů Správce, které tato opatření obsahují/upraví.*

Povinnost vést záznamy je stanovena také pro zpracovatele, např. dodavatele klubu, přičemž obsah záznamů se výrazně neliší od obsahu záznamů pořizovaných Správcem (klubem). Rozsah zaznamenávaných informací je však menší. Obsahem jsou kontaktní údaje zpracovatele a jeho případných zástupců, informace o případném předání osobních údajů do zahraničí a případně popis technických a organizačních opatření, je-li to možné.

Zpracování a řádné vedení záznamů je jedním z prvních kroků, jak se přiblížit souladu s Nařízením.

5.2 SHROMAŽĎOVÁNÍ A TVORBA DATABÁZE

Je pravděpodobné, že klub bude vytvářet databáze osobních údajů. **Údaje musí být** vedeny v souladu se zásadou účelového omezení a minimalizace osobních údajů (viz odstavec 3.2), zásadami výslovně vyjádřenými v článku 5 odst. 1 písm. b) a c) Nařízení, tj. **shromažďovány pro** určité, výslovně vyjádřené a **legitimní účely a zpracovávány v rozsahu nezbytně nutném** pro naplnění předem stanoveného účelu zpracování.

Za **shromažďování** se považuje postup Správce**, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení** na nosič informací pro jejich okamžité nebo pozdější zpracování. Povinnost shromažďovat pouze osobní údaje přiměřené a nezbytné pro naplnění účelu se tedy vztahuje pouze k aktivní, volní činnosti Správce. Přiměřenost rozsahu zpracovávaných osobních údajů je nezbytné posuzovat vždy ve vztahu ke stanovenému účelu zpracování, neboť **každému samostatně určenému účelu (např. registrace, marketing atd.) bude odpovídat jiný rozsah nezbytných osobních údajů.** Již při stanovení účelu by měl proto Správce současně vymezit rozsah osobních údajů, které ve vztahu k tomuto účelu bude shromažďovat, a takto stanovený **rozsah by měl být minimální možný tak, aby Správce shromažďoval osobní údaje v nejmenším možném rozsahu, při kterém zamýšlené zpracování může dosáhnout stanoveného účelu.** Smyslem je tedy minimalizace rozsahu zpracovávaných osobních údajů již ve fázi jejich shromažďování (klub by například neměl vyžadovat e-mail subjektu údajů, pokud není nezbytný pro naplnění účelu zpracování). Současně by měl Správce zajistit, že zpracování požadovaných údajů bude mít trvale souvislost a význam pro stanovený účel zpracování. Například pro zasílání nabídek prostřednictvím elektronických prostředků (e-mail) by měly být dostačující údaje v rozsahu jméno, příjmení a e-mailová adresa. V databázi pro marketingové účely by Správce neměl shromažďovat údaje jako rodné číslo, zdravotní údaje apod. Účelem marketingové evidence/databáze je zasílání reklamy, čemuž musí odpovídat také rozsah shromažďovaných údajů. Správce by si měl položit otázku, bez jakých údajů se při odeslání obchodního sdělení neobejde. Předtím, než započne proces zpracování, je Správce povinen zvážit rozsah a účel zpracování, vzájemně jej posoudit a až následně proces zpracování osobních údajů zahájit.

Rozsah osobních údajů zpracovávaných klubem může být v zásadě vymezen dvojím způsobem. Jednak může vyplývat ze zákonné úpravy[8], která bude výslovně vyjmenovávat osobní údaje, které jsou nezbytné pro naplnění zákonem upraveného účelu zpracování. Zásada nezbytnosti a přiměřenosti tedy musí být zachována i v tomto případě.

Druhou možností je vymezení rozsahu shromažďovaných osobních údajů Správcem na základě svého rozhodnutí, který se bude odvíjet od jím stanoveného účelu, např. pro běžnou evidenci sportujících dětí není nezbytné uvádět rodné číslo dítěte. Nezbytným osobním údajem, ale zcela jistě bude např. pohlaví nebo věk dítěte, které budou rozhodující pro

[8] *Např. ustanovení § 3a odst. 3 písm. d) zákona č. 115/2001 Sb., dle kterého sportovní organizace je povinna bez zbytečného odkladu zapsat do rejstříku údaje jméno a příjmení, datum narození a adresu místa pobytu sportovce a trenéra evidovaného u sportovní organizace, která je v ní sdružena; nemá-li sportovec nebo trenér místo pobytu na území České republiky, adresu místa na území České republiky, kde se převážně zdržuje; v případě sportovce rovněž druh sportu, který sportovec vykonává; v případě cizinců rovněž státní občanství.*

možnost soutěžit v určité věkové kategorii. Zásada nezbytnosti a přiměřenosti však musí být také zachována i v tomto případě.

Výše uvedené platí obdobně i v případech, kdy subjekt údajů poskytl klubu souhlas se zpracováním osobních údajů. Správce se nemůže zbavit odpovědnosti tvrzením, že v případě, kdy shromažďuje nadbytečné údaje, tak činí legitimně, protože mu subjekt údajů s tímto postupem udělil souhlas.

Tím spíše se zásada nezbytnosti a přiměřenosti uplatní, požaduje-li Správce poskytnutí nadbytečných údajů povinně. Např. pokud Správce ve formuláři, který bude používat pro shromažďování osobních údajů pro účely fotbalové soutěže, stanoví jako povinnou položku rodné číslo, poruší tím povinnost shromažďovat a zpracovávat pouze nezbytně nutné údaje. Rozdílem by bylo, pokud tuto položku do formuláře Správce nepředepíše, a přesto mu subjekt údajů takový osobní údaj do tohoto formuláře vyplní. V tomto případě se nebude jednat o porušení povinnosti minimalizace osobních údajů, neboť Správce tento údaj neshromažďoval v tom smyslu, že jej vědomě a cíleně nepožadoval.

Dalším častým případem souvisejícím s plněním povinnosti minimalizace je rozsah osobních údajů shromážděný v souvislosti s pořizováním kopií osobních dokladů[9]. Právní úprava zakazuje pořizování kopie občanského průkazu bez prokazatelného souhlasu jeho držitele (s výjimkou zákonem[10] nebo mezinárodní smlouvou stanovených případů). Tento zákaz slouží k tomu, aby byla omezena možnost zneužití občanského průkazu, příp. cestovního dokladu před jeho padělám apod. Navíc k uvedenému zákonnému zákazu kopírování se ve vztahu k osobním údajům uvedeným na občanském průkazu nebo cestovním dokladu plně uplatní Nařízení. Z důvodu množství osobních údajů uváděných na tomto dokladu lze konstatovat, že až na výjimky[11] budou některé z těchto osobních údajů uvedených v občanském průkazu pro většinu zpracování nadbytečné – místo narození, rodinný stav, údaje o dětech nebo manželovi včetně jejich rodného čísla. V takovém případě musí klub zajistit, že v důsledku kopírování občanského průkazu nebudou shromažďovány nadbytečné údaje (toho lze docílit například kopírováním přes šablonu, která zakryje některé části, které obsahují nadbytečné údaje, a zbylé části s potřebnými údaji zůstanou odkryté). . Další možností je opsat údaje přímo z osobního dokladu, aniž by odpovědný zaměstnanec nebo jiná odpovědná osoba Správce doklad zkopírovala.

5.3 ÚČEL ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Klub může, jakožto Správce osobních údajů stanovit, že k určitému účelu, samozřejmě s přihlédnutím k jeho podnikatelským aktivitám, bude zpracovávat osobní údaje, aniž by takovou činnost zahrnující zpracování osobních údajů ukládal nějaký zvláštní právní předpis. Klub jakožto správce si tak sám určí účel zpracování osobních údajů (např. pořádání soutěže).

Účel zpracování osobních údajů však Správce nemůže zvolit zcela libovolně; stanovený **účel musí být legální a legitimní**. Legalita znamená soulad s platnými právními

---

[9] Kopírování osobních dokladů upravuje např. zákona č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a také zákon č. 329/1999 Sb., o cestovních dokladech ve znění pozdějších předpisů.

[10] Např. zákon č. 253/2008 Sb., některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.

[11] Identifikace podle § 8 odst. 7, § 9 odst. 1 zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

předpisy a legitimita znamená oprávněnost. Legalita i legitimita účelu zpracování musí být naplněny současně.

Smyslem povinnosti vymezit (stanovit) účel zpracování osobních údajů je zejména to, aby Správce ještě před začátkem samotného zpracování otevřeně deklaroval cíle (záměry) své činnosti a své úmysly. Dále, aby důkladně zvážil, čeho hodlá pomocí zpracování osobních údajů dosahovat a jaké důsledky to pro něj bude mít, případně zda je vůbec zapotřebí k dosažení daného cíle osobní údaje shromažďovat. V některých případech lze velmi podobného výsledku dosáhnout i prostřednictvím statistických dat (zjednodušeně řečeno pouze číselná data), a tedy bez nutnosti shromažďovat osobní údaje, např. sledování preferencí členů, kdy pro získání základní představy o dané problematice nejsou osobní údaje nezbytné.

Deklarování účelu zpracování osobních údajů musí být dostatečně určité a nelze se omezit pouze na obecné konstatování, že osobní údaje budou zpracovávány např. pro podnikatelskou činnost.

Příklady předpokládaných účelů zpracování osobních údajů klubem:

(a) registrace člena klubu a s tím spojené povinnosti vyplývající z Občanského zákoníku, zákona o podpoře sportu a daňových předpisů, jako např. vedení seznamu členů, vyúčtování členských příspěvků (bez souhlasu člena klubu);

(b) zveřejňování údajů členů v příslušné databázi/evidence (se souhlasem člena klubu);

(c) nabízení obchodu a služeb - marketingové účely (se souhlasem člena klubu a bez souhlasů zákazníků, jakožto dodavatelů).

5.4 PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ

Předávání osobních údajů třetím osobám (osobám, které nejsou subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli) anebo jinému Správci je zakázáno. Výjimku z tohoto zákazu tvoří předání zpracovateli osobních údajů členů a dalších osob klubu (viz odstavec 5.4.1) anebo příjemci, kterému je Správce oprávněn osobní údaje předávat na základě oprávnění vyplývajícího z článku 6 odst. 1 anebo článku 9 odst. 2 Nařízení. Takové oprávnění bude ve většině případů vyplývat z právního předpisu anebo souhlasu subjektu údajů. V mimořádných situacích může být předání údajů člena možné i pro ochranu životně důležitých zájmů[12].

Při předávání osobních údajů musí Správce přijmout taková opatření, aby byla zajištěna bezpečnost těchto údajů a nedošlo k neoprávněnému zpracování předávaných osobních údajů. Správce proto uzavírá za účelem předá(vá)ní osobních údajů s příjemcem písemnou smlouvu, v níž se příjemce především zavazuje zajistit bezpečnost předaných osobních údajů. Příjemce se navíc zavazuje zastavit zpracování osobních údajů v případě, že subjekt údajů svůj souhlas odvolá a toto oznámí Správci. Povinnost podle předchozí věty se nevztahuje na předání anebo zpřístupnění osobních údajů příslušným státním orgánům a dalším osobám, jež upravují zvláštní právní předpisy (např. Policie ČR).

Získávání osobních údajů od jiných správců doporučujeme na základě písemné smlouvy s takovým jiným správcem. Smlouva o předá(vá)ní osobních údajů od jiného správce bude obsahovat zejména záruky týkající se oprávněnosti předchozího zpracování osobních údajů. Dále bude smlouva obsahovat záruky, že subjekty údajů poskytly souhlas

[12] *Např. předání údajů rychlé zdravotnické službě.*

s předáním jejich osobních údajů dalším správcům, aniž by vyloučily Správce, jemuž se údaje předávají. Pokud nebyl souhlas subjektů údajů získán, je nezbytné ověřit, zda pro předání osobních údajů existuje jiný právní titul uvedený v článku 6 odst. 1 písm. b) až f) Nařízení, příp. článku 9 odst. 1 písm. b) až j), jedná-li se o zvláštní kategorii osobních údajů. Pro každé předání je tak nezbytné zajistit poučení a/nebo získání souhlasu podle bodu 6.1 před dalším zpracováním.

5.4.1 Zpracovatel a náležitosti smlouvy

Správce může zpracováním osobních údajů pověřit třetí osobu (zpracovatele). Pověření lze udělit pouze v rámci smlouvy v souladu s článkem 25 Nařízení, která musí mít písemnou formu.

Smlouva musí zavazovat zpracovatele k dodržování vnitřních předpisů klubu upravujících zpracování osobních údajů, a to minimálně v obdobném rozsahu jako je musí dodržovat Správce. V této smlouvě musí být výslovně stanoven předmět a doba trvání zpracování, povaha a účel zpracování, kategorie osobních údajů a kategorie subjektů údajů, práva a povinnosti Správce a záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů a další náležitosti uvedené v článku 28 odst. 3 Nařízení.

Smlouva zejména stanoví, že zpracovatel:

(a) nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Správce;
(b) zpracovává osobní údaje pouze na základě doložených pokynů Správce, a to v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Unie nebo členského státu, které se na Správce vztahuje;
(c) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
(d) přijme opatření k zabezpečení osobních údajů;
(e) dodržuje podmínky pro zapojení dalšího zpracovatele;
(f) zohledňuje povahu zpracování, je Správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů;
(g) je Správci nápomocen při zajišťování souladu s povinnostmi při zabezpečení osobních údajů, ohlašování a oznamování případů porušení zabezpečení osobních údajů dozorovému úřadu a subjektu údajů, posouzení vlivu na ochranu osobních údajů a předchozí konzultace;
(h) v souladu s rozhodnutím Správce všechny osobní údaje buď vymaže, nebo je vrátí Správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;
(i) poskytne Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v článku 28 Nařízení, a umožní audity, včetně inspekcí, prováděné Správcem nebo jiným auditorem, kterého Správce pověřil, a k těmto auditům přispěje.

Pokud zpracovatel využívá ke zpracování osobních údajů třetích osob, je povinen zajistit, aby obdobně dodržovaly interní předpisy klubu upravující zpracování osobních údajů tak, aby nedošlo ke snížení úrovně ochrany osobních údajů zajištěné těmito předpisy.

5.5 ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Správce je povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování nebo jinému zneužití. Zjednodušeně řečeno jde o povinnost přijmout (vzhledem k účelu a prostředkům zpracování osobních údajů) ta nevhodnější bezpečnostní opatření.

Nařízení upravuje záměrnou a standardní ochranu osobních údajů, přičemž každý z těchto institutů slouží jiným způsobem k ochraně práv a svobod subjektů údajů.

- Záměrná ochrana osobních údajů spočívá v přijímání vhodných technických a organizačních opatření při určení prostředků pro zpracování i v době zpracování samotného, a to na základě posouzení závažnosti rizik pro práva a svobody subjektů údajů. Tím by měla být individuálně zajištěna optimální ochrana osobních údajů s přihlédnutím ke specifickým aspektům každého procesu zpracování.
- Standardní ochrana osobních údajů spočívá v povinnosti Správce přijmout vhodná organizační a bezpečnostní opatření k zajištění toho, aby byly standardně zpracovány jen osobní údaje nezbytně nutné pro daný účel.

Jednou z hlavních povinností je aktivní dokládání souladu, resp. možnost prokázat soulad zpracování s Nařízením dle článku 24 odst. 1 Nařízení. Nejvhodnější formou prokazování je dokumentace vedená Správcem prokazující soulad zpracování osobních údajů s povinnostmi plynoucími pro něj z Nařízení. Požadavek proaktivního přístupu Správce se pak promítá například do povinnosti provádět zabezpečení zpracování, provádět posouzení vlivu nebo předchozí konzultace s Úřadem pro ochranu osobních údajů. Pro zajištění souladu lze Správcům doporučit zavedení interních směrnic na ochranu a zpracování osobních údajů a vedení dokumentace takovým způsobem, aby z ní vyplýval soulad zpracování s Nařízením. Interní směrnice by měla přesně vymezovat postupy a stanovit pravidla a podmínky osobám/subjektům podílejícím se na zpracování osobních údajů. Zjednodušeně řečeno, interní předpis určuje způsob chování v konkrétních situacích tak, aby jednání odpovídalo a zejména bylo přizpůsobeno potřebám Správce. Interní předpisy pomáhají předvídat a očekávat chování osob seznámených s interní směrnicí, neboť vymezení určitých pravidel dovoleného a předpokládaného chování snižuje rizika, že dojde kneoprávněným zpracováním osobních údajů, a tím chrání Správce.

Veškeré písemnosti a jiné fyzické nosiče informací, kterými Správce disponuje a které obsahují osobní údaje, musí být chráněny před volným přístupem neoprávněných osob. Toho lze dosáhnout především skladováním v uzamykatelných skříňkách a zamykatelných místnostech chráněných proti požáru. Tato povinnost platí obdobně i pro údaje obsažené v elektronické formě na datovém nosiči.

Bezprostřední přístup k osobním údajům subjektu údajů mohou mít pouze oprávněné osoby, které Správce určil, a to pouze v rozsahu, který Správce určil.

Server, na kterém jsou případně data obsahující osobní údaje uložena, musí být chráněn proti útoku z internetu firewallem a antivirovým systémem či obdobnými zabezpečovacími prostředky. Tento server musí být umístěn v uzamykatelné skříni a zabezpečené místnosti s přístupem pouze pro oprávněné osoby určené Správcem.

Datové soubory obsahující osobní údaje, jejichž ztráta nebo změna by mohly mít negativní důsledky pro subjekty údajů, musejí být Správcem denně zálohovány. Tyto zálohy se

v pravidelných, maximálně dvoutýdenních, intervalech musejí následně přepisovat tak, aby byly osobní údaje stále zabezpečeny a byla zachována zásada integrity a důvěrnosti informací (viz odstavec 3.2).

Pokud klub využívá informační systémy, měly by být vybaveny následujícími bezpečnostními funkcemi:

(a) nepřetržité zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému před neautorizovaným přístupem, zejména modifikací nebo zničením. Zaznamenávají zejména použití identifikačních a autentizačních informací, pokusy o zkoumání přístupových práv, činnost autorizovaných subjektů informačního systému ovlivňující bezpečnost informačního systému;
(b) možností zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele, bezpečnostního správce nebo správce informačního systému.
(c) ošetření paměťových objektů (médií) před jejich dalším použitím;
(d) ochrana důvěrnosti dat během přenosu mezi zdrojem a cílem a jejich integrita,
(e) možnost pseudonymizace a šifrování osobních údajů;
(f) schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
(g) možnost pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

V případě opravy systému (Windows apod.), na kterém jsou instalovány informační systémy, anebo v případě opravy hardware[13], je třeba zajistit, že osoby, které budou tuto opravu provádět, jsou důvěryhodné a budou vázány povinností mlčenlivosti ve smyslu bodu 5.6 a ujednání dle odstavce 5.4.1 tohoto Metodického pokynu, a to pod hrozbou smluvní pokuty.

5.6 POVINNOST MLČENLIVOSTI

Všechny osoby, které zpracovávají osobní údaje pro Správce, jakož i další osoby, které přijdou do styku s osobními údaji u Správce nebo zpracovatele, jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních přijatých Správcem. Povinnost mlčenlivosti trvá i po skončení pracovního poměru, nebo poměru obdobného. Výjimky z povinnosti mlčenlivosti mohou být obsaženy v zákoně.

5.7 KATEGORIE ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ A JEJICH VYUŽITÍ

Pro zabezpečení souladu zpracování osobních údajů s právními předpisy je nutné nejprve vymezit přesně rozsah osobních údajů, které bude klub shromažďovat. Ty se můžou lišit v závislosti na konkrétních podmínkách, proto je jejich výčet v odstavci 5.7.1 pouze demonstrativní.

Není vyloučeno, že osobní údaje bude klub zpracovávat i prostřednictvím informačních systémů. I v takovém případě je potřebné zajistit, aby zpracování probíhalo v souladu s obecnými požadavky ochrany osobních údajů, jak jsou vymezeny v tomto Metodickém pokynu. Jelikož ale každý klub může využívat vlastní informační systém, jsou postupy v této kapitole popsány pouze obecně bez vazby na konkrétní systém.

[13] *Technické vybavení počítače.*

Ke správnému fungování databází osobních údajů je třeba zajistit zejména kvalitní zápis klíčových informací o jednotlivých osobách, tj. členech, zákaznících a dalších osobách, o vazbách mezi nimi a dále o aktivitách mezi klubem a těmito osobami.

5.7.1 Základní možné kategorie subjektu údajů

(a) Člen – osoba, která v daném kalendářním roce skutečně vykonává sportovní činnost, pro kterou je u sportovní organizace (viz kapitola 2);
(b) Zákonný zástupce – osoba, která zastupuje člena klubu pro nedostatek věku;
(c) Zákazník – dodavatelé a další osoby spolupracující se Správcem (viz kapitola 2).

5.7.2 Seznam možných zpracovávaných osobních údajů člena klubu

(a) jméno a příjmení
(b) adresa místa pobytu
(c) datum narození
(d) pohlaví
(e) e-mailová adresa
(f) mobilní číslo
(g) údaje o zdravotním stavu, které obsahuje lékařský posudek ze zdravotní prohlídky
(h) členský poplatek
(i) případný souhlas zákonného zástupce u dětí do 15 let

5.7.3 Seznam možných zpracovávaných osobních údajů zákonného zástupce

(a) jméno a příjmení
(b) adresa místa pobytu
(c) e-mailová adresa
(d) mobilní číslo

5.7.4 Seznam možných zpracovávaných osobních údajů pro zákaznické kontakty

(a) jméno a příjmení
(b) obchodní jméno společnosti
(c) e-mailová adresa
(d) mobilní číslo, příp. telefonní číslo zaměstnání

5.7.5 Pravidla pro zavádění nových záznamů a jejich změnu – Evidence klubu

(a) kontrola, zda stejný kontakt již nebyl do databáze zaveden. Pokud v databázi již stejný kontaktní záznam existuje, nevytvářet paralelně nový záznam;
(b) používání české diakritiky (háčky, čárky);
(c) kontrola zaváděných informací oproti veřejně dostupným databázím[14]. V případě zákazníků lze kontrolu zaměřit na název společnosti, její sídlo a identifikační číslo;
(d) vkládání telefonních čísel v příslušném tvaru: např. +420xxxxxxxxx.

5.7.6 Využívání údajů

Osobní údaje z databáze/evidence klubu lze využívat pouze v souladu s účelem, pro který byly tyto údaje shromážděny. O účelech zpracování blíže pojednávají body 5.2 a 5.3 tohoto Metodického pokynu. Údaje v databázi/evidenci budou zřejmě primárně shromažďovány

[14] *Např.* https://is.fotbal.cz/clenove/databaze-clenu.aspx, www.justice.cz, http://wwwinfo.mfcr.cz/ares/ares_es.html.cz.

přímo od subjektu údajů, tj. členů, zákonných zástupců anebo zákazníků prostřednictvím osobního jednání, anebo prostřednictvím prostředků vzdálené komunikace (telefon, fax, atd). Dalším možným zdrojem osobních údajů mohou být veřejně dostupné informace a také informace/údaje, které správce získal od třetích osob[15].

Údaje člena klubu lze využívat v souvislosti s činností klubu, tj. evidence a vedení záznamů, kontaktování, vyúčtování členských příspěvků apod.

Pro účely marketingu lze zpracovávat údaje zákazníka či člena v rozsahu jméno, příjmení, telefon a e-mailová adresa. O**bchodní sdělení lze zákazníkovi zaslat prostřednictvím elektronických prostředků (e-mailová zpráva, telefon) bez předchozího souhlasu v případech, kdy zákazník využil služeb klubu[16].** V případě členů je pro zasílání obchodních sdělení nezbytný jejich souhlas. Vzorový souhlas s poskytnutím údajů pro účely marketingu je přílohou tohoto Metodického pokynu.

Úprava obchodních sdělení se ale uplatní pouze v případě, že obsah bude mít ziskový charakter, tedy bude určen k přímé či nepřímé podpoře služeb. **Pokud bude klub informovat pouze o svých nepodnikatelských aktivitách, nebude se jednat o obchodní sdělení, tj. transakční sdělení** (např. vyrozumění o konání zápasů, informace o zrušení tréninku apod.)

Údaje sdělené třetí osobou nelze využívat za jiným účelem než za tím účelem, pro který byly příslušné údaje touto třetí osobou Správci předány/sděleny. Přístup do databází/evidence mohou mít pouze osoby dle svých oprávnění (viz blíže bod 5.5).

5.7.7 Profilování subjektů údajů

Nařízení zavádí nová ustanovení, která se týkají profilování a automatizovaného rozhodování, zejména z hlediska rizik pro soukromí subjektu údajů. Ve světle Nařízení se profilováním rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména za účelem rozboru nebo odhadu, resp. analýzy či předvídání aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu. Neboli se jedná o takové zpracování, které vede k hodnocení nebo rozboru nějakých osobních aspektů fyzické osoby.

Profilování není nutné vnímat jako zakázanou aktivitu, ale jako rizikovější zpracování související právě s některými zvláštními povinnostmi vyplývajícími z Nařízení. Jsou tři možné způsoby, jak může být profilování využito, i) obecné profilování,[17] ii) rozhodování založené na profilování,[18] a iii) výhradně automatizované rozhodování, včetně profilování.[19]

---

[15] *Např. rodinný příslušník.*

[16] *Za zákazníka (ať už fyzickou nebo právnickou osobu) ve smyslu zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), je nutno považovat jen takový subjekt, se kterým již v minulosti odesílatel obchodního sdělení (klub) uzavřel obchod.*

[17] *Např. hodnocení návštěvnosti klubu, frekvence využití a určení členů, kterým lze služby klubu v budoucnu nabízet. Jedná se tedy o profilování členů, aniž by byl profil vytvářen pomocí automatizovaných prostředků.*

[18] *Např. určení člena, který obdrží dárkový poukaz, a to na základě profilu vytvořeného pomocí čistě automatizovaných prostředků. Zhodnocení doby „strojově", ale rozhodnutí o přiřazení poukazu může být na Správci.*

[19] *Např. automatické stanovování výše členského poplatku na základě údajů o zdravotním stavu a délce členství, tedy profilování bez možnosti ovlivnění člověkem.*

Článek 22 Nařízení stanoví, že jako pravidlo platí zákaz plně automatizovaného individuálního rozhodování, včetně profilování, které má pro osoby právní účinky nebo se jich obdobným způsobem významně dotýká, avšak s výjimkami uvedenými v čl. 22 odst. 2 Nařízení.

Dochází-li k obecnému profilování nebo k rozhodování založeném na profilování, lze jej provádět bez souhlasu subjektu. Pouze v případě, že dochází k výhradně automatizovanému rozhodování včetně profilování je Správce povinen vyžádat si výslovný souhlas subjektu údajů, pokud není takové rozhodování včetně profilování nezbytné k uzavření smlouvy nebo povoleno právem státu.

5.8 PROVOZOVÁNÍ KAMEROVÉHO SYSTÉMU

Oblast zpracování osobních údajů prostřednictvím kamer se vztahuje nejenom na členy klubu, ale jakékoli třetí osoby, které se momentálně nacházejí v místě, kde je kamerový systém provozován. Proto je vhodné tuto problematiku zmínit zvlášť.

Provozování kamerového systému samo o sobě není považováno za zpracování osobních údajů. **Ke zpracování** dochází až v momentě, kdy je vedle kamerového sledování **prováděn záznam pořizovaných záběrů**, nebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním.

Z důvodu neexistence speciálního zákona, který by režim kamerových systémů upravoval, se pro tento druh zpracování osobních údajů uplatní Nařízení a Zákon. Využití kamerových systémů na sportovišti podléhá obecnému režimu Nařízení a vyžaduje existenci zákonného důvodu. Tím může být v případě klubu ochrana důležitého zájmu Správce. Přesto bude nezbytné:

- stanovit účel zpracování, kterým bude u klubu zmíněná ochrana majetku a zdraví osob na stadionu před krádeží nebo zničením, zároveň ale nesmí být možné dosáhnout daného účelu za použití méně omezujících opatření, jako je např. osobní dohled organizátorů;
- dodržovat zásady zpracování osobních údajů prostřednictvím kamer, zejména nezasahovat nadměrně do soukromí subjektů údajů, jako je instalace kamer v místech určených k soukromým účelům, jako jsou převlékárny, toalety apod.;
- stanovit lhůtu pro uchování záznamů, která nepřesáhne dozorovým úřadem (Úřad pro ochranu osobních údajů) doporučovaný 1 týden. Kamerový systém, spolu s datovými nosiči, na kterých jsou záznamy uchovávány, musí být dostatečně chráněny před neoprávněným přístupem;
- informovat subjekty údajů o existenci kamerového systému, např. pomocí informační tabulky s textem a piktogramem kamery. Informace musí obsahovat údaje o Správci a odkaz na osobu/místo, kde se dají získat podrobnější informace. Povinnost správců v souvislosti s kamerovým systémem jsou blíže popsány v metodice Úřadu pro ochranu osobních údajů – *Provozování kamerových systémů*[20];

[20] https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf

- vyhotovit interní směrnici popisující oprávněnost pořizování záznamů, přístup osob k těmto záznamům, způsoby uchování záznamů apod.

Na žádost FAČR a klubů připravil resort Ministerstva vnitra ČR manuál k řešení diváckého násilí, který se mimo jiné dotýká provozování kamerového systému na stadionech.[21]

V ostatním se při zpracování osobních údajů prostřednictvím kamerového systému plně uplatní obecná úprava ochrany osobních údajů tak, jak je popsána v tomto Metodickém pokynu.

5.9 NAKLÁDÁNÍ S FOTOGRAFIEMI

K pořizování, používání, šíření či zveřejňování fotografií či jiných záznamů členů klubu může docházet jak v režimu zpracování osobních údajů (tedy v režimu Nařízení), tak pouze v režimu Občanského zákoníku. V obou případech je významné, zda fyzická osoba (člen klubu) sama ze své vůle používá (šíří, zveřejňuje) svou vlastní fotografii nebo záznam, nebo se jedná i o fotografie či záznamy jiných osob. Při používání a šíření fotografií a audiovizuálních záznamů fyzických osob je zejména třeba brát také v úvahu, zda dochází k jejich zveřejňování v prostředí internetu, kde je zvýšené nebezpečí jejich zneužití.[22]

Kluby musí rozlišovat situace, k jakým účelům budou fotografie dále zpracovávány (např. zveřejnění na stránkách klubu). Využívání fotografií v souvislosti s prodejem a předáváním neoprávněným osobám není dovoleno.

Občanský zákoník zakazuje zachycovat a rozšiřovat podobu člověka bez jeho svolení. Zachycená osoba se může úspěšně domáhat stažení fotografie, k jejímuž pořízení a šíření souhlas nedala. Svolení není potřeba v případě, že fotografie klub užívá k ochraně svých práv (např. shromažďování důkazů). Bez souhlasu členů klubu lze zpracovávat fotografie na základě tzv. zpravodajské licence.

Zpravodajstvím je třeba rozumět informování veřejnosti o věcech oprávněného veřejného nebo obecného zájmu, zejména prostřednictvím hromadných sdělovacích prostředků, kterými je šířeno zpravodajství. Občanský zákoník příkladmo uvádí zpravodajství tiskové, rozhlasové a televizní. Typickým vybočením ze zákonné zpravodajské licence je pořízení nebo použití podobizny či záznamu člena klubu např. pro účely reklamní, aniž by dal člen klubu k pořízení souhlas.[23]

Fotografie by měly být primárně zpracovávány se souhlasem dotčených osob, tj. členů klubu, zejména jedná-li se o děti, tak se souhlasem jejich zákonného zástupce. Aby mohl klub udělení souhlasu prokázat, měl by disponovat podepsaným souhlasem člena klubu či zákonného zástupce se zpracováním (zveřejněním) fotografie na webových stránkách.

V ostatním se při nakládání s fotografiemi plně uplatní obecná úprava ochrany osobních údajů tak, jak je popsána v tomto Metodickém pokynu.

6. INFORMAČNÍ A POUČOVACÍ POVINNOST

V souladu se zásadou transparentnosti, která se prolíná celým Nařízením, je Správce povinen informovat subjekt údajů o zpracování osobních údajů, které se tohoto subjektu údajů týkají. Ve většině případů budou Správci v souvislosti s činností klubu informovat své členy. Informační

[21] http://www.mvcr.cz/clanek/ministr-vnitra-predstavil-manual-pro-fotbalove-kluby-k-reseni-divackeho-nasili.aspx

[22] https://www.uoou.cz/stanovisko-c-12-2012-k-nbsp-pouziti-fotografie-obrazoveho-a-nbsp-zvukoveho-zaznamu-fyzicke-osoby/d-2769

[23] *Rozsudek Nejvyššího soudu České republiky ze dne 26. 7. 2000, sp. zn. 30 Cdo 2304/99*

povinnost lze plnit různou formou a způsoby. Povinnost lze plnit jak tištěnou formou, např. prostřednictvím informačního letáku anebo také elektronicky přes webové stránky klubu. Správce však bude prokazovat dozorovému úřadu v oblasti ochrany osobních údajů (ne)plnění této povinnosti vůči členům, a proto by měl zvolit formu a způsob, který je nejen „users friendly“, ale také prokazatelný. Vzorový příklad plnění informační povinnosti je uveden v příloze tohoto Metodického pokynu.

6.1 INFORMAČNÍ POVINNOST PŘI SHROMAŽĎOVÁNÍ ÚDAJŮ

V zásadě platí, že aby zpracování osobních údajů bylo možno považovat za legální i legitimní, musí být mj. prováděno otevřeně a transparentně. Dotčená fyzická osoba musí být informována o zpracování svých osobních údajích. V případech, kdy klub, jakožto Správce, získá osobní údaje od subjektu údajů, je povinen jej poučit ve smyslu článku 13 Nařízení. Za tím účelem je Správce povinen zajistit, aby se subjekt údajů řádně seznámil s informacemi uvedenými níže, a které je Správce povinen poskytnout již v okamžiku získání osobních údajů od subjektu údajů.

Správce poskytne subjektu údajů následující informace:

(a) totožnost a kontaktní údaje klubu (název, sídlo, IČO, kontakt);
(b) účely zpracování, pro které jsou osobní údaje zpracovávány;
(c) právní základ pro zpracování;
(d) příjemce nebo kategorie příjemců osobních údajů;
(e) případný úmysl Správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny;
(f) doba, po kterou budou osobní údaje uloženy;
(g) pokud je zpracování založeno na souhlasu, existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
(h) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;
(i) existenci práva požadovat od Správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů a existenci práva subjektu údajů podat stížnost u dozorového úřadu.

Informace uvedené pod písm. a) až i) poskytne Správce také v případě, že osobní údaje nebyly získány přímo od subjektu údajů, ale například z veřejných zdrojů nebo od třetích osob. V takovém případě výše uvedené informace doplní ještě o kategorii dotčených osobních údajů a zdroj osobních údajů. Nejsou-li údaje získány přímo od subjektu údajů, poskytne Správce informace v přiměřené lhůtě po získání osobních údajů, ale nejpozději do 30 dnů s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány (např. emailovou zprávou). V případech kdy mají být osobní údaje použity pro účely komunikace se subjektem údajů, poskytne tyto informace v okamžiku, kdy poprvé dojde k této komunikaci, anebo pokud mají být osobní údaje zpřístupněny jinému příjemci, poskytne klub informace při prvním zpřístupnění osobních údajů.

S ohledem na výše uvedené lze shrnout, že Správce poskytuje informace při získání údajů anebo v přiměřené lhůtě, nezískal-li údaje od subjektu údajů.

Z informační povinnosti existují výjimky. Správce není povinen poskytnout informace v případech, kdy subjekt údajů již informace o zpracování má, a do té míry, v níž je má. Klub však musí pamatovat na to, že bude muset prokazovat splnění této informační povinnosti dozorovému úřadu, a proto **je vždy vhodné subjekt údajů informovat prokazatelným způsobem**, který snižuje míru rizika odpovědnosti při zpracování osobních údajů.

Klub je povinen plnit výše uvedenou povinnost jak v případech, kdy údaje shromažďuje se souhlasem, tak bez souhlasu. Není nezbytné informovat v každém okamžiku procesu zpracování, důležité je podat informace u „vstupu" sběru dat (při získávání údajů, viz výše), aby měl subjekt údajů představu, jak bude s jeho údaji nakládáno, např. při registraci člena.

6.2 POUČOVACÍ POVINNOST PŘI UPLATŇOVANÍ PRÁVA NA PŘÍSTUP K ÚDAJŮM

Uplatní-li subjekt údajů právo na přístup ke svým osobním údajům dle článku 15 Nařízení, je mu Správce povinen tuto informaci předat bez zbytečného odkladu, anebo nejpozději do 30 dnů ode dne doručení žádosti. Informace jsou poskytnuty ve formě, ve které subjekt údajů uplatňuje své právo (např. písemně, ústně). Správce má právo za poskytnutí dalších kopií požadovat přiměřený poplatek na administrativní náklady.

K ověření identity subjektu údajů, který žádá o přístup k osobním údajům, využije Správce všech vhodných opatření. Není-li schopen identifikovat subjekt údajů, pak ho o tom, pokud je to možné, informuje. Ověřování identity nemá být Správcem zneužíváno k získávání dalších údajů a k jejich uchování za účelem reakce na případné další žádosti.

Obsahem informace je sdělení o:

(a) účelu zpracování osobních údajů,
(b) osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování, včetně veškerých dostupných informací o jejich zdroji,
(c) příjemci, případně kategoriích příjemců,
(d) době, po kterou budou osobní údaje uloženy,
(e) existenci práva požadovat od Správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování a právo podat stížnost u dozorového úřadu,
(f) veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
(g) skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování a v těchto případech smysluplné informace týkající se použitého postupu, jakož i sdělení o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů.

Poučovací povinnost plní předem určená osoba Správce, přičemž informace jsou poskytovány zejména v elektronické formě, pokud subjekt údajů nepožádá o jiný způsob poskytnutí informací o zpracování. Právo na přístup je doplněno právem uvedeným v bodě 7.4.

7. PRÁVA SUBJEKTU ÚDAJŮ

Práva subjektu údajů jsou důležitým prvkem ochrany osobních údajů jako celku, jelikož subjekt údajů je často ve slabším postavení než Správce. Jeho práva tak narovnávají vztah mezi subjektem

údajů a správcem, zejména mezi členem a klubem. Většina práv subjektu údajů byla do Nařízení převzata ze současné platné právní úpravy anebo byla zavedena na základě rozhodovací praxe evropských soudů.

Ochranu práv posiluje zavedení přístupu založeného na riziku, kdy je v rámci zpracování vždy nutné zvažovat možné nepříznivé dopady do práv a svobod subjektu údajů. Pro vyřízení žádosti subjektu údajů Nařízení stanoví i poměrně přísné lhůty, ve kterých musí Správce subjekt údajů vyrozumět o přijatých opatřeních. Lhůty zní na „bez zbytečného odkladu“ anebo „nejpozději do jednoho měsíce“, s možností za určitých podmínek tuto lhůtu prodloužit o další dva měsíce, samozřejmě s odůvodněním a s povinností o prodloužení subjekt údajů informovat.

V jednotlivých právech se promítají zásady, které jsou uvedeny v bodě 3.2; například v právu na přístup k osobním údajům se promítá zásada transparentnosti a doplňuje jí plnění informační povinnosti. Na toto právo je často nahlíženo jako na podmnožinu zcela nového práva na přenositelnost údajů. V právu na opravu, právu na výmaz či být zapomenout a právu na omezení zpracování se zase promítají zejména zásady omezení uložení a přesnosti. Zásada zákonnosti se pak mimo jiné promítá také do práva odvolání souhlasu se zpracováním osobních údajů. V neposlední řadě je nutné zmínit právo vznést námitku a zcela specifické právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování osobních údajů. Nakonec je nutné zmínit práva související s právní ochranou subjektu údajů, a to právo podat stížnost u dozorového úřadu a právo na účinnou soudní ochranu.

7.1 PRÁVO NA OPRAVU

Jednou ze základních zásad Nařízení je přesnost osobních údajů. To znamená, že Správce musí přijmout veškerá rozumná opatření, aby zpracovával přesné a aktuální údaje a nepřesné údaje buď vymazal, nebo opravil.

Správce je povinen ověřit, zda jsou osobní údaje, k nimž se žádost subjektu o opravu vztahuje, přesné. Do doby, než Správce přesnost údajů ověří, by mělo být zpracování těchto osobních údajů omezeno[24]. Po jejich ověření musí Správce subjekt údajů informovat, že omezení bude zrušeno a že bude ve zpracování osobních údajů pokračovat.

Subjekt údajů má právo také doplnit neúplné osobní údaje. Tohoto práva může využít v situaci, kdy chce Správci z vlastní vůle o sobě poskytnout dodatečné osobní údaje. Při uplatňování tohoto práva se přihlíží k účelům zpracování tak, aby Správce nebyl nucen zpracovávat na základě požadavku subjektu údajů i osobní údaje, které nejsou potřebné pro účely zpracování.

Na základě požadavku člena provede klub opravu údajů, které se ho týkají. Mají-li být údaje rozšířeny o další osobní údaje, je nezbytné postupovat v souladu se zásadou minimalizace osobních údajů a neshromažďovat údaje, které jsou nadbytečné. Člen může svůj požadavek vznést, jak ústně osobně, tak písemně. Pro účely ověřování identity lze vyžadovat dodatečné informace umožňující jeho identifikaci.

7.2 PRÁVO NA VÝMAZ

Podstatným právem subjektu údajů je právo na to, aby byly jeho údaje vymazány a nebyly dále zpracovávány, pokud nastane jeden z důvodů stanovených v Nařízení. Prvním důvodem je, že údaje již nejsou potřebné pro účely, pro které byly zpracovány. Dalším

[24] *Podle článku 18 odst. 1 písm. a) Nařízení má subjekt údajů právo na to, aby Správce omezil zpracování, v případě popírá-li subjekt údajů přesnost osobních údajů, a to na dobu potřebnou k tomu, aby Správce mohl přesnost osobních údajů ověřit.*

důvodem je odvolání souhlasu subjektem údajů, pokud neexistuje žádný další (jiný) důvod pro zpracování jeho osobních údajů. V neposlední řadě také skutečnost, že subjekt údajů vznesl námitku proti zpracování osobních údajů, které se ho týkají, nebo pokud je zpracování jeho osobních údajů v rozporu s Nařízením. Jinými slovy právo být zapomenut dává subjektu údajů (člen, zákazník apod.) za splnění určitých podmínek právo požadovat vůči Správci, aby zlikvidoval jeho osobní údaje a dále je neuchovával.

Klub má povinnost osobní údaje na žádost člena vymazat, pouze pokud je splněna některá ze zmíněných podmínek pro výmaz (viz *7.2.1 Podmínky pro výmaz*) a zároveň nelze aplikovat výjimku z povinnosti provést výmaz (viz *7.2.2 Výjimky z práva na výmaz*).

7.2.1 Podmínky pro výmaz:

(a) Správce nepotřebuje osobní údaje pro účel, za kterým je shromáždil, anebo je nepotřebuje jinak zpracovávat. V souladu se zásadou omezení uložení (viz odstavec 3.2) osobní údaje vymaže;

(b) Správce zpracovává osobní údaje na základě souhlasu a subjekt údajů souhlas odvolá. Povinnost provést výmaz údajů však Správci vznikne, pokud nebude mít jiný právní titul pro pokračování ve zpracování. Pokračující zpracování by pak bylo v rozporu se zásadou zákonnosti;

(c) subjekt údajů vznese námitku proti zpracování dle článku 21 odst. 1 Nařízení a při posouzení dle tohoto ustanovení vyjde najevo, že v konkrétní situaci převažuje zájem subjektu údajů nad zájmem Správce na zpracování těchto osobních údajů. Dalším případem je, že subjekt údajů vznese námitku proti zpracování dle článku 21 odst. 2 Nařízení. Po dobu, po kterou Správce provádí posouzení námitky, nesmí Správce dané osobní údaje zpracovávat, dokud neprokáže, že jeho oprávněný zájem v daném případě převáží. Pokud dojde k závěru, že převáží zájem nebo práva subjektu údajů, musí Správce osobní údaje vymazat, pokud jej o to subjekt údajů požádá. V poslední řadě, pokud Správce **zpracovává osobní údaje** subjektu údajů na základě právního titulu oprávněného zájmu **za účelem přímého marketingu** a tento subjekt údajů vznese námitku proti takovému zpracování dle článku 21 odst. 2 Nařízení, **musí Správce osobní údaje vymazat rovnou**, bez vážení a posuzování oprávněného zájmu;

(d) osobní údaje byly zpracovány protiprávně. V souladu s pojetím zásady zákonnosti bude mít subjekt údajů právo na výmaz nejen v případě, že budou osobní údaje zpracovány v rozporu s Nařízením, ale případně i s jakýmkoliv jiným právním předpisem, např. předpisem uvedeným v bodě 3.1;

(e) na Správce se vztahuje právní povinnost vyplývající z práva EU nebo z práva členského státu, která mu ukládá osobní údaje vymazat;

(f) jedná se o **osobní údaje dětí** shromážděné Správcem v souvislosti s nabídkou služby informační společnosti dle článku 8 Nařízení. Toto právo se uplatní na všechny osobní údaje, které Správce shromáždil od nezletilých subjektů údajů. Subjekt údajů má na výmaz právo i poté, co již hranici zletilosti překročil, ohledně údajů, které o něm Správce shromáždil, když byl ještě nezletilý.

7.2.2 Výjimky z práva na výmaz:

(a) osobní údaje je nezbytné zpracovávat pro výkon práva na svobodu projevu a informace. Tato výjimka se tak uplatní např. v žurnalistice, v níž jsou vydané články projevem svobody projevu. Stejně tak nebudou moci subjekty údajů žádat

výmaz osobních údajů např. z veřejných rejstříků, u nichž se zase jedná o právo na informace. Uplatňování bude také vždy záviset na konkrétní situaci daného subjektu údajů. Způsob, jakým je nutné vážit právo na ochranu osobních údajů proti právu na svobodu projevu a informace, však bude ve finále záviset na rozhodnutích a argumentacích soudů;

(b) osobní údaje je nezbytné zpracovávat pro plnění právních povinností. Pokud se na Správce vztahuje právní povinnost, která Správci ukládá, aby osobní údaje uchovával, nebude muset subjektům údajů v jejich žádosti vyhovět. Kromě zákona o zdravotních službách může vyplývat povinnost zpracovávat údaje např. ze zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů;

(c) pokud Správce potřebuje osobní údaje zpracovávat ke splnění úkolu prováděného ve veřejném zájmu, kterým je pověřen, nebo při výkonu veřejné moci. Správce by měl vždy posoudit konkrétní situaci žadatele a zvážit, jestli osobní údaje skutečně potřebuje zpracovávat či nikoliv;

(d) zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví v souladu s článkem 9 odst. 2 písm. h) a i) Nařízení. Tyto údaje musejí být zároveň příslušným pracovníkem zpracovávány v souladu s článkem 9 odst. 3 Nařízení;

(e) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely a toto zpracování splňuje podmínky stanovené v článku 89 odst. 1 Nařízení[25]. V takovém případě může Správce výmaz těchto osobních údajů odmítnout provést, pokud by tím bylo znemožněno nebo vážně ohroženo splnění cílů takového zpracování;

(f) zpracování osobních údajů je nezbytné pro určení, výkon nebo obhajobu právních nároků.[26] Zde je nutné důsledně uplatňovat zásadu nezbytnosti. Osobní údaje by měly být dle této podmínky uchovány pouze tehdy, pokud nelze určit, vykonat nebo obhájit určitý právní nárok bez jejich zpracování. Zároveň se musí jednat o potřebu objektivní. Správce jednoduše nemůže o určitých osobních údajích prohlásit, že je pro takové účely potřebuje bez toho, aby toto odůvodnil faktickou potřebou.

V každém případě je nutné vždy zvažovat rozsah zpracovávaných údajů v souvislosti se zásadou minimalizace údajů (viz odstavec 3.2), tedy na základě výjimek nesmí Správce zpracovávat více údajů, než je pro daný účel nezbytně nutné. Výjimky se uplatní pouze tehdy, pokud daného cíle nelze dosáhnout jiným způsobem než zpracováním osobních údajů. Všechny výše uvedené výjimky je tedy nutné posuzovat v souladu se základními zásadami. Právo na výmaz není nezbytné dle výše uvedených podmínek zkoumat v případě účelu vyjádřeného v bodě 5.3 písm. (c) Metodického pokynu. Údaje určené k marketingovému účelu tak lze vymazat bez dalšího.

Je však nutné mít na paměti, že v některých případech má Správce povinnost osobní údaje vymazat sám od sebe, bez toho, aby musel subjekt údajů Správce o výmaz žádat. Pokud pomine účel zpracování, bude muset Správce osobní údaje sám od sebe zlikvidovat. Stejně

[25] *Zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podléhá v souladu s tímto nařízením vhodným zárukám práv a svobod subjektu údajů. Tyto záruky zajistí, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit dodržování zásady minimalizace. Tato opatření mohou zahrnovat pseudonymizaci za podmínky, že lze tímto způsobem splnit sledované účely. Pokud mohou být sledované účely splněny dalším zpracováním, které neumožňuje nebo které přestane umožňovat identifikaci subjektů údajů, musí být tyto účely splněny tímto způsobem.*

[26] *Právním* nárokem lze rozumět možnost uplatnit své subjektivní právo, tedy domáhat se jeho realizace u soudu nebo úřadů.

tak bude muset Správce osobní údaje zlikvidovat, pokud pro určité kategorie osobních údajů ztratí právní titul (oprávnění).

7.3 PRÁVO NA OMEZENÍ ZPRACOVÁNÍ[27]

Právo na omezení zpracování dává subjektu údajů možnost požádat Správce, aby omezil zpracování osobních údajů, které se ho týkají. Pokud jsou splněny podmínky Nařízení uvedené níže, Správce tak musí učinit.

7.3.1 Podmínky pro omezení zpracování

(a) subjekt údajů uplatní právo na opravu (viz odstavec 7.1). Subjekt údajů může v tomto případě Správce žádat, aby omezil jejich zpracování po dobu, kdy bude Správce ověřovat správnost osobních údajů;

(b) zpracování je v rozporu se zákonem, ale nevyžaduje jejich výmaz (viz odstavec 7.2), nýbrž pouze jejich omezení;

(c) Správce nepotřebuje zpracovávat údaje pro potřeby naplnění účelu zpracování, ale subjekt údajů je potřebuje pro určení, výkon nebo obhajobu právních nároků. Cílem tohoto omezení je, aby Správce údaje nemohl vymazat a subjekt údajů je mohl použít;

(d) subjekt údajů vznesl námitku proti zpracování dle článku 21 Nařízení. Omezení se vztahuje na dobu, po kterou bude Správce posuzovat, jestli námitce vyhoví. Správce posuzuje, jestli zájmy a práva daného subjektu údajů převažují nad oprávněnými důvody Správce či zájmy Správce při zpracování ve veřejném zájmu či při výkonu veřejné moci.

7.4 PRÁVO NA PŘENOSITELNOST ÚDAJŮ

Právo na přenositelnost umožňuje subjektům údajů získat osobní údaje, které poskytli Správci údajů, a to ve strukturovaném, běžně používaném a strojově čitelném formátu, a předat tyto údaje jinému správci údajů.

Cílem nového práva je posílení pravomocí a kontroly subjektů údajů, pokud jde o jejich vlastní osobní údaje. Toto právo usnadňuje jejich schopnost své osobní údaje snadno přemísťovat, kopírovat nebo předávat z jednoho informačního prostředí do jiného (ať už do svých vlastních systémů, systémů důvěryhodných třetích stran, nebo do systémů nových správců).

7.4.1 Podmínky pro uplatnění práva na přenositelnost

Právo na přenositelnost lze uplatnit, pouze pokud je zpracování osobních údajů prováděno:

(a) automatizovaně a zároveň je založeno na právním důvodu/titulu:

(aa) souhlasu subjektu údajů anebo

(ab) plnění smlouvy, jejíž smluvní stranou je subjekt údajů.

Vylučovací metodou dojdeme k tomu, že právo na přenositelnost se neuplatní vůči Správci, který provádí zpracování osobních údajů, jež je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je tento správce pověřen (např.

[27] *Např. bude-li subjekt údajů namítat, že zpracovávané datum narození není přesné, měl by Správce po dobu potřebnou k prokázání správnosti zpracování data narození omezit jeho zpracování, např. je zablokovat pro další zpracování, včetně předávání jiným subjektům.*

zpracování údajů prostřednictvím kamerového systému). Proto je správné určení právního základu zpracování údajů zcela základním a nezbytným požadavkem Nařízení.

Rozsah osobních údajů, které se poskytují v rámci práva na přenositelnost, je užší než u práva na přístup (viz pro srovnání bod 6.2). Poskytnout lze totiž jen osobní údaje, které se týkají subjektu údajů a zároveň které subjekt údajů poskytl Správci. Jedná se o osobní údaje, které subjekt údajů přímo, vědomě a aktivně sdělil Správci, třeba prostřednictvím formuláře (např. e-mailová adresa, jméno, příjmení, věk), a zároveň i o osobní údaje, které jsou generovány na základě aktivity člena v souvislosti s činností klubu. Nepůjde ale o údaje odvozené nebo dovozené z osobních údajů subjektu údajů na základě analýz, hodnocení, profilování a podobných procesů prováděných klubem.

Nařízení ukládá všem správcům povinnost poskytnout osobní údaje požadované fyzickou osobou ve formátu, který podporuje opakované použití. Konkrétně stanoví, že osobní údaje musí být poskytnuty „*ve strukturovaném, běžně používaném a strojově čitelném formátu*".

Pojmy „strukturovaný", „běžně používaný" a „strojově čitelný" představují soubor minimálních požadavků, které by měly usnadnit interoperabilitu formátu údajů poskytnutých Správcem, neboli schopnost předávat údaje z jednoho informačního prostředí do jiného. Strojově čitelným formátem lze rozumět soubor strukturovaný tak, aby v něm softwarové aplikace mohly snadno nalézt, rozpoznat a získat konkrétní údaje. Za strojově čitelné údaje se považují údaje zakódované v souborech strukturovaných ve strojově čitelném formátu. Strojově čitelné formáty mohou být otevřené nebo chráněné vlastnickým právem; mohou být formálně normalizované, či nikoli.

Osobní údaje, které subjekt údajů poskytl Správci, mohou obsahovat údaje třetích osob. Pokud by výkonem práva na přenositelnost ve vztahu k určitým údajům měla být nepříznivě dotčena práva a svobody jiných osob, nelze tyto údaje v rámci práva na přenositelnost poskytnout.

Jsou-li naplněny výše uvedené podmínky pro přenositelnost údajů, je klub povinen předat údaje ve formátu a způsobem uvedeným výše.

7.5 PRÁVO VZNÉST NÁMITKU

Nařízení dává subjektu údajů v některých případech možnost vznést námitku proti zpracování. Jedná se zejména o situace, kdy subjekt údajů neměl možnost ovlivnit to, že jsou jeho údaje zpracovány, a zároveň se nejedná o plnění právní povinnosti nebo životně důležitý zájem, kdy je tato nemožnost ovlivnit zpracování obhajitelná. Subjekt údajů má takto možnost vznést tři druhy námitek proti zpracování prováděném:

(a) na základě právního titulu oprávněného zájmu a plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci;
(b) pro účely přímého marketingu na základě právního titulu oprávněného zájmu;
(c) pro účely vědeckého či historického výzkumu nebo pro statistické účely.

7.5.1 Námitka proti zpracování na základě oprávněného zájmu či plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci

Jakmile Správce námitku proti zpracování obdrží, musí osobní údaje subjektu údajů, který vznesl námitku, bez zbytečného odkladu přestat zpracovávat. I zde se však uplatní pravidla, která Správci dávají možnost žádost odmítnout. Jedná se o případy, kdy je žádost/námitka i) zjevně neodůvodněná nebo ii) nepřiměřená. Zároveň se uplatní obecné pravidlo o tom,

že Správce musí subjekt údajů s dostatečnou jistotou identifikovat, aby předešel možnému zneužití tohoto práva. Správce tedy bude mít předtím, než bude muset přestat osobní údaje zpracovávat, nějaký čas na to, aby posoudil, jestli se nejedná o zjevně neodůvodněnou nebo nepřiměřenou žádost a jestli ji skutečně podal subjekt údajů. Pokud Správce dojde k závěru, že námitka je opodstatněná měl by zpracování osobních údajů omezit a provést věcné posouzení námitky. Pokud chce Správce následně začít osobní údaje opět zpracovávat, musí v rámci věcného posouzení námitky prokázat, že má pro zpracování závažné oprávněné důvody, které převažují nad zájmy a svobodami subjektů údajů.

7.5.2 Námitka proti zpracování pro účely přímého marketingu

Jakmile ji subjekt údajů vznese, musí Správce přestat osobní údaje subjektu údajů pro účely přímého marketingu zpracovávat.

7.5.3 Námitka proti zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely

Správce posoudí zpracování všech údajů, které zpracovává pro účely vědeckého či historického výzkumu, nebo pro statistické účely. V případech, že dle retenčního schématu (schéma doby uchování osobních údajů Správcem) je zpracování údajů nadále nezbytné, námitce subjektu údajů nevyhoví a informuje jej dopisem o dalším zpracování např. z důvodu uchování pro vědecké účely.

8. LIKVIDACE OSOBNÍCH ÚDAJŮ A RETEČNÍ DOBA

8.1 LIKVIDACE OSOBNÍCH ÚDAJŮ

Likvidací osobních údajů se rozumí postup jehož výsledkem je nevratné znemožnění osobní údaje nadále využívat, a to jak ze strany likvidaci provádějícího Správce, tak jakéhokoli jiného subjektu. Výsledkem likvidace dat musí být jejich faktické zničení či znepřístupnění pro správce i jakýkoliv další subjekt. Správce nebo zpracovatel na základě pokynu Správce je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány. Správce je povinen zlikvidovat osobní údaje v případech, pomine-li důvod, pro který byly zpracovávány. Povinnost likvidace je vztažena k okamžiku naplnění účelu zpracování, jenž byl Správce povinen stanovit na samotném začátku zpracování osobních údajů (viz blíže odstavec 5.3). Jednotlivá doba zpracování osobních údajů je vyjádřena v odstavci 8.2.

Likvidaci je třeba provést také v případě, kdy subjekt údajů požádá o ukončení zpracování osobních údajů (viz odstavec 7.2), anebo odvolá svůj souhlas se zpracováním osobních údajů, je-li tento souhlas nezbytný pro další zpracování a Správci nesvědčí jiný právní titul pro zpracování osobních údajů (např. plnění smlouvy nebo právní povinnosti).

Vzhledem k tomu, že Nařízení ani Zákon nestanoví konkrétní formu likvidace osobních údajů poté, co pomine účel zpracování, anebo požádá-li o ukončení zpracování subjektu údajů, je způsob jejího provedení na Správci. Mezi základní způsoby likvidace lze řadit:

(a) anonymizace identifikačních, adresních a kontaktních údajů (viz kapitola 2.);
(b) jejich vymazání, a to bez možnosti jejich opětovného obnovení (např. pomocí příslušných softwarových nástrojů), tzv. tvrdé mazání, tedy nikoli jejich znečitelnění;
(c) skartování či jiné zničení neumožňující zpětnou rekonstrukci písemných dokumentů.

O likvidaci se provede zápis, který Správce důkladně uloží pro potřeby doložení splnění své povinnosti při případné kontrole dozorovým úřadem anebo žádosti subjektu údajů. Tento zápis bude obsahovat identifikaci příslušné databáze, ve které byly údaje uloženy, a kategorie zlikvidovaných osobních údajů a dále důvod, pro který byla likvidace provedena. Likvidaci je nezbytné provést jak v informačních systémech, tak v papírových složkách.

8.2 RETENČNÍ DOBA

Osobní údaje mohou být uchovávány pouze po dobu nezbytnou k dosažení účelu zpracování a po uplynutí této doby je třeba provést likvidaci osobních údajů v souladu s odstavcem 8.1.

Informační systémy Správce by měly umožnit nastavení automatického mazání osobních údajů. Správce by měl rozhodnout o délce doby uchování údajů tak, aby byla nastavena v informačním systému v souladu se zásadami Nařízení a zvláštními právními předpisy. V případě, že jsou osobní údaje vedeny mimo informační systémy v papírové podobě, bude muset klub vymezit retenční dobu, nejlépe v interním předpise a tuto poté důsledně vynucovat.

9. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

Případy povinného jmenování, které Nařízení výslovně předpokládá, lze dovozovat pouze výkladem, jelikož povinnost jmenovat pověřence pro ochranu osobních údajů je vztažena (i) k povaze, rozsahu, nebo účelu rozsáhlého pravidelného a systematického zpracování a také (ii) ke kategorii osobních údajů, které jsou zpracovávány. Rozhodujícími faktory při určování rozsáhlosti zpracování jsou faktory jako např.: počet subjektů údajů, objem dat (rozsah), doba trvání a nepřetržitost zpracování a územní rozsah zpracování a podstata hlavní činnosti. Posouzení, zdali bude klub povinen jmenovat pověřence pro ochranu osobních údajů („**Pověřenec**“ nebo „**DPO**[28]“), záleží vždy na konkrétní situaci. Dle aktuálně dostupných informací k výkladu daného ustanovení lze v souvislosti se zpracováním údajů členů předpokládat, že kluby nemusí svého Pověřence jmenovat. Nicméně FAČR doporučuje ustanovit osobu, která v klubu bude odpovědná za otázky zpracování osobních údajů, zejména v souvislosti s plněním mimořádných a krizových situací uvedených v bodě 10. Bude-li klub Pověřence jmenovat, musí splňovat požadavky uvedené v bodě 9.1 a plnit úkoly uvedené v bodě 9.2 tohoto Metodického pokynu.

9.1 POŽADAVKY NA POVĚŘENCE

Základní požadavky na osobu Pověřence vyplývají z článku 37 odst. 5 Nařízení, dle kterých by měl být Pověřenec ustanoven na základě svých profesních kvalit. Požadavky na profesní kvality definuje Nařízení tak, že se jedná zejména o odborné znalosti práva a praxe v oblasti ochrany osobních údajů. Je zřejmé, že vyžadována bude znalost národního a evropského práva v oblasti ochrany osobních údajů, odpovídající praxe a samozřejmě zejména precizní znalost Nařízení a Zákona. DPO by měl být podrobně seznámen s procesy a technologiemi zpracování osobních údajů u Správce, pro kterého bude tuto funkci vykonávat. Míra jeho potřebné odbornosti bude však různá, a to v závislosti na citlivosti, složitosti a rozsahu zpracovávaných osobních údajů, tj. v závislosti na operacích zpracování konkrétního správce osobních údajů. Dále lze předpokládat, že v souvislosti

[28] *Data Protection Officer.*

s možnými přeshraničními kontrolami dozorových úřadů členských států EU, by měl DPO ovládat minimálně jeden z úředních jazyků EU na takové úrovni, aby mohl v případě potřeby komunikovat s těmito zahraničními dozorovými úřady,[29] příp. s nově zřízeným Evropským sborem pro ochranu osobních údajů.

DPO bude hrát klíčovou roli v procesech ochrany osobních údajů, a proto musí mít odpovídající schopnosti, mimo jiné osobnostní, aby byl schopen veškeré úkoly naplnit. Funkci pověřence může vykonávat interní zaměstnanec Správce či zpracovatele nebo externí subjekt na základě smlouvy o poskytování služeb. V obou případech musí Pověřenec splňovat všechny požadavky na něho kladené a zároveň musí být chráněn proti nezákonnému ukončení smlouvy o poskytování služeb nebo nezákonnému propuštění ze zaměstnání, pokud se jedná o zaměstnance Správce. DPO se zejména nesmí v souvislosti se svou činností dostat do střetu zájmů. Kvůli hrozbě střetu zájmů nesmí Pověřenec v organizaci určovat účely a prostředky zpracování osobních údajů (nemělo by se jednat např. o zaměstnance, který pro Správce spravuje pracovněprávní vztahy). Ke střetu zájmů může dojít i v případě, kdy by měl Pověřenec zastupovat Správce nebo zpracovatele v soudním či obdobném řízení v případech týkajících se ochrany osobních údajů. S touto podmínkou úzce souvisí ustanovení článku 38 odst. 3 GDPR, dle kterého Pověřenec vykonává svou činnost nezávisle a s dostatečnou mírou samostatnosti. Za tímto účelem zejména nesmí dostávat pokyny týkající se výkonu svých úkolů, bez ohledu na to, zda se jedná o zaměstnance či externí osobu. Správce nebo zpracovatel jsou povinni zveřejnit kontaktní údaje pověřence a tím zajistit, aby měly subjekty údajů a dozorové orgány možnost přímo kontaktovat Pověřence bez potřeby dalšího zprostředkování.

9.2 PLNĚNÍ ÚKOLŮ

Hlavním úkolem pověřence je monitorování souladu činností zpracování osobních údajů s Nařízením. Za tímto účelem by měl Pověřenec se Správcem či zpracovatelem spolupracovat při zavádění vhodných technických a organizačních opatření k zajištění souladu a v souvislosti s tím poskytovat poradenství a doporučení. Spolupráce s dozorovými úřady bude klíčová, neboť znalosti v oblasti ochrany osobních údajů by měly přispět k zefektivnění vzájemné komunikace. Úřad by měl pověřence v problematice ochrany údajů považovat za své „rovnocenné partnery“. DPO bude dle Nařízení působit jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování údajů. Veškeré interní předpisy, postupy by měly být vyhotoveny nebo připomínkovány právě Pověřencem.

DPO bude mít důležité postavení při plnění nových povinností dle GDPR – *např. hodnocení posouzení vlivu na ochranu osobních údajů (článek 35 Nařízení)*. Správce by si měl vyžádat stanovisko pověřence k otázkám týkajícím se posouzení vlivu na ochranu osobních údajů, a to zejména v otázce, zda v konkrétním případě posouzení vlivu provést, jakou metodologii při provádění použít, jaké prostředky ochrany ke snížení rizika porušení práv subjektů údajů implementovat, zda bylo posouzení řádně provedeno anebo zda jsou závěry posouzení v souladu s požadavky Nařízení. Vzhledem ke komplexnosti témat, které má DPO řešit, je jeho vysoká odbornost žádoucí.

9.3 ODPOVĚDNOST

[29] http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

Pověřenec není přímo z Nařízení odpovědný za nesoulad zpracování osobních údajů subjektem, který jej pověřil. Nařízení jednoznačně stanoví, že uvedení a udržení činností zpracování v souladu s Nařízením je odpovědností Správce, resp. zpracovatele, který musí být také schopný tento soulad doložit. V případě, že Správce přijímá rozhodnutí v rozporu s Nařízením a posudkem pověřence, by Pověřenec měl mít možnost vysvětlit své odlišné stanovisko vrcholovému managementu Správce, resp. zpracovatele. V tomto ohledu je Pověřenec vrcholovým řídícím pracovníkům přímo podřízen, a proto Nařízení předpokládá, že pověřenci by „*v souvislosti s plněním svých úkolů neměli být správcem nebo zpracovatelem propuštěni ani sankcionováni*“. Toto ustanovení zajišťuje, že Pověřenec bude schopen plnit své úkoly nezávisle a současně bude chráněn před sankcemi, kterým by mohl být vystaven v důsledku řádného plnění svých povinností. Pověřenec však může být v souladu s vnitrostátním právem oprávněně propuštěn z jiných důvodů, které nesouvisí s prováděním jeho úkolů podle Nařízení.

10. MIMOŘÁDNÉ A KRIZOVÉ SITUACE

Porušení zabezpečení osobních údajů, zejména ztrátu, odcizení, poškození či zničení osobních údajů je každá osoba, která se o takové skutečnosti dozví, povinna neprodleně oznámit Správci.

10.1 OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ DOZOROVÉMU ÚŘADU

Správce je povinen porušení zabezpečení osobních údajů ohlásit Úřadu pro ochranu osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Správce není povinen porušení zabezpečení ohlásit, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.[30]

Ohlášení obsahuje zejména tyto informace:

(a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
(b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
(c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
(d) popis opatření, která Správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Osoba plnící ohlašovací povinnost za/jménem Správce ověří na webových stránkách www.uoou.cz dostupnost případného vzorového formuláře k plnění této povinnosti a je-li formulář dostupný, vyplní údaje v požadovaném (předepsaném) rozsahu. O dalších opatřeních v souvislosti s porušením bezpečnosti rozhodne Správce bez zbytečného odkladu poté, co se dozvěděl o skutečnostech týkajících se porušení zabezpečení osobních údajů.

[30] *Příkladem porušení, které nevyžaduje ohlášení, je ztráta bezpečně zašifrovaného mobilního zařízení používaného Správcem a jeho zaměstnanci. Za podmínky, že šifrovací klíč zůstal v bezpečném držení Správce a nejde o jedinou kopii osobních údajů, jsou osobní údaje pro útočníka nedostupné. Znamená to, že případ porušení pravděpodobně nevyústí v riziko pro práva a svobody dotčených subjektů údajů.*

10.2 OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ SUBJEKTU ÚDAJŮ

Správce je povinen porušení zabezpečení osobních údajů oznámit subjektu údajů, pokud je pravděpodobné, že porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

Oznámení je subjektu údajů poskytováno za použití jasných a jednoduchých jazykových prostředků[31] a obsahuje zejména tyto informace:

(a) jméno a kontaktní údaje kontaktního místa Správce, které může poskytnout bližší informace;
(b) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
(c) popis opatření, která Správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Oznamovací povinnost není Správce povinen plnit v případě, že:

(a) zajistí, že zasažené údaje jsou nečitelné nebo nejsou přiřaditelné ke konkrétním osobám, např. fyzické osoby nejsou identifikovatelné díky provedení pseudonymizace nebo osobní údaje nejsou čitelné díky použitému šifrování apod.,
(b) přijal následná opatření, která zajistí, že vysoké riziko se již pravděpodobně neprojeví, např. osobní údaje nejsou v držení třetí osoby, a/nebo
(c) by oznámení vyžadovalo nepřiměřené úsilí. V takovémto případě Správce přistoupí místo toho k veřejnému oznámení nebo podobnému opatření, s jehož pomocí budou subjekty údajů o porušení informovány stejně účinným způsobem.

11. PŘÍLOHY

11.1 PŘÍLOHA – ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

Záznamy o činnostech zpracovár

11.2 PŘÍLOHA – INFORMAČNÍ POVINNOST A SOUHLAS

Souhlas se zpracováním osobních

[31] *Příklady způsobu transparentní komunikace zahrnují přímé textování (např. e-mail, SMS, přímá zpráva), výrazné bannery nebo oznámení na webových stránkách, komunikace poštou a nápadné reklamy v tištěných médiích.*