Antidopingový výbor ČR
Czech Anti-Doping Committee

STRUČNÁ METODIKA

K DOSAŽENÍ SHODY S OBECNÝM NAŘÍZENÍM O OCHRANĚ OSOBNÍCH ÚDAJŮ

GENERAL DATA PROTECTION REGULATION (GDPR)

OBSAH:

1. STRUČNÉ SHRNUTÍ

1.1 Právní úprava ochrany osobních údajů se od 25.5.2018 řídí zejména (obecným) nařízením Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně osobních údajů (GDPR), směrnicí Evropského parlamentu a Rady (EU) č. 2016/680, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a zákonem č. 101/2000 Sb., o ochraně osobních údajů.

1.2 Nová úprava ochrany osobních údajů uvádí, že si klade za cíl zvýšit úroveň ochrany osobních údajů a zodpovědné zacházení s nimi.

1.3 Nové obecné povinnosti jsou:

a) důslednější úprava souhlasu se zpracováním osobních údajů
b) vznik pozice pověřence (pro rozsáhlé zpracovávání osobních údajů)
c) vedení záznamů o činnostech zpracování
d) sebeposouzení okolností při rizikovém zpracovávání osobních údajů
e) ohlašovací povinnost v případě porušení ochrany údajů

1.4 Relevantní otázky jsou:

a) jaké osobní údaje shromažďujeme
b) jaké osoby k nim mají přístup

c) jak kontrolujeme oprávnění pro přístup k osobním údajům
d) jak jsou likvidovány nebo skartovány osobní údaje
e) jak chráníme osobní údaje proti zneužití

2. VYMEZENÍ POJMŮ

2.1 **Osobní údaj** je téměř jakákoliv informace týkající se fyzické osoby (subjektu údajů). Příklady: Jméno, příjmení, datum narození, bydliště, rodné číslo, identifikační a daňové číslo, telefonní číslo, e-mail, výška, váha, velikosti, údaje z fotografií či videa, věk, pohlaví, rodinný stav, vzdělání, zaměstnání, příjmy a výdaje, jeho příbuzenstvo, údaje o chování či osobních preferencích či jiný identifikátor osoby.

2.2 **Zvláštní kategorie osobních údajů** (dříve citlivé osobní údaje) obsahuje například údaje o zdravotním stavu, rasovém původu či etnicitě, názorech (politických, náboženských, filosofických), biometrické a genetické údaje.

2.3 **Subjekt údajů** je každá fyzická osoba, jejíž osobní údaje jsou zpracovávány.

2.4 **Zpracování** je jakékoli nakládání s osobními údaji.

2.5 **Správce** je jakákoli fyzická nebo právnická osoba, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

2.6 **Zpracovatel** je fyzická nebo právnická osoba zpracovávající osobní údaje pro správce k jeho pokynu. Jedna osoba může být správcem (např. vůči svým zaměstnancům) i zpracovatelem (ve vztahu k jinému správci).

2.7 **Společní správci** společně stanoví účely a prostředky zpracování osobních údajů.

2.8 **Příjemce** je jakýkoli subjekt, kterému jsou osobní údaje poskytnuty. V některých případech nemusí být příjemcem orgán veřejné moci (ADV ČR).

2.9 **Právo vznést námitku** proti zpracování osobních údajů na základě oprávněného zájmu správce, ve veřejném zájmu (ADV ČR) nebo při výkonu veřejné moci, má kterýkoliv subjekt údajů. V případě námitky vůči zpracování pro účely přímého marketingu má správce povinnost zpracování ukončit.

2.10 **Úřad pro ochranu osobních údajů** (ÚOOÚ) je kontrolní a dozorový úřad pro ČR.

2.11 **Záznamy o činnostech zpracování** je povinen vést každý správce osobních údajů. GDPR předepisuje formální vedení záznamů o činnostech zpracování především pro velké organizace nad 250 zaměstnanců, nebo bez ohledu na počet zaměstnanců, pokud a) prováděné zpracování osobních údajů pravděpodobně představuje riziko pro práva a svobody subjektů údajů, b) zpracování osobních údajů není příležitostné, nebo c) zpracování zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů - platí blíže nespecifikovaná zásada, že čím větší zpracovatel, tím je třeba vést podrobnější záznamy.

2.12 **Pověřenec pro ochranu osobních údajů** (Data Protection Officer, DPO) je interním auditorem zpracování a ochrany osobních údajů.

2.13 **Analýza rizik** slouží k jako přehled systematiky zpracování osobních údajů se zaměřením na potenciální rizika související se zpracováním. Součástí je návrh řešení známých rizik a postup vyřešení nebo minimalizace.

2.14 **Posouzení vlivu na ochranu osobních údajů** (Data Protection Impact Assessment, DPIA) je formalizovaná analýza rizik směřující k přijetí opatření snižujících vysoká rizika při zpracování osobních údajů na přijatelnou úroveň.

2.15 **Hlášení bezpečnostních incidentů** je povinnost správce při porušení zabezpečení, integrity nebo ztrátě osobních údajů. Je povinen informovat (1) dotčené subjekty údajů, existuje-li riziko pro narušení práv a svobod fyzických osob, a (2) Úřad pro ochranu osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o narušení správce dozvěděl - z této povinnosti jsou vyloučeny pouze incidenty s nízkou rizikovostí.

3. POŽADAVKY NA SHODU S GDPR

3.1 Dokumentace osvědčující naplnění zásad zpracování, ochrany a zabezpečení osobních údajů a revize dosavadní (i smluvní) dokumentace a interních předpisů, a to včetně dokumentace o zabezpečení informačních technologií.

3.2 Zavedení a popis standardizovaného procesu komunikace se subjekty údajů (standardizované odpovědi nebo formuláře) včetně standardizovaného poučování subjektu údajů o právech a povinnostech.

3.3 Zavedení standardizovaného procesu zjištění, hlášení a řešení bezpečnostních incidentů v rámci zpracování osobních údajů.

3.4 Systém sběru, evidence a zpracování souhlasů se zpracováním osobních údajů.

4. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A PRÁVA

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

4.2 **Zásada zákonnosti** vyžaduje, aby osobní údaje byly zpracovávány na základě právem stanovených legitimních důvodů (právních titulů), jimiž jsou nezbytnost:

(1) dodržení zákonné povinnosti,

(2) pro splnění úkolů správce prováděných ve veřejném zájmu (ADV ČR),

(3) při výkonu veřejné moci,

(4) pro plnění smlouvy, jejíž stranou je subjekt údajů,

(5) za účelem přijetí opatření na žádost subjektu údajů před uzavřením smlouvy,

(6) pro účely oprávněných zájmů nebo zpracování založené na souhlasu subjektu údajů.

4.3 **Zásada transparentnosti** souvisí s plněním informačních povinností vůči dotčeným subjektům údajů například prostřednictvím webových stránek nebo

se standardizovaným poučením obsaženým na formulářích s celosvětovou působností (formuláře dopingové kontroly).

4.4 **Zásada účelového omezení** znamená ohraničení svým zákonným účelem, tj. omezení pro účely své činnosti vyplývající v případě ADV ČR zejména ze Zřizovací listiny ADV ČR v návaznosti na mezinárodní smlouvy a školský zákon. Účel zpracování se považuje za výslovně vyjádřený, byl-li sdělen subjektům údajů. Legitimita účelu znamená, že je účel zpracování v souladu s právním řádem jako celkem.

4.5 **Zásada minimalizace údajů** znamená, že je možné zpracovávat pouze ty osobní údaje, které jsou pro činnost ADV ČR nezbytně nutné.

4.6 **Zásada přesnosti** znamená povinnost zpracovávat pouze přesná, správná a aktuální data. Postačuje zachovat povinnosti uložené mezinárodními standardy WADA (ISPPPI), popřípadě jednou za určitý časový úsek kontrolovat aktuálnost vedených údajů (žádost o potvrzení správnosti vedených údajů). Pravidelnost ověřování přesnosti a aktualizace osobních údajů by měla odpovídat potenciálnímu riziku vzniku újmy (aktivní nebo pasivní nakládání s údaji).

4.7 **Zásada integrity a důvěrnosti** je povinnost zajistit bezpečné zpracování osobních údajů, např. šifrováním, zálohováním, způsobem spolehlivého smazání údajů (zda běžný způsob smazání vede k uložení na sběrnicích informačních technologií a je obnovitelný a jak) a pravidelným testováním systému.

4.8 **Právo na informace nebo potvrzení** má subjekt údajů vůči správci informací, zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

a) účely zpracování,
b) kategorie dotčených osobních údajů,
c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
d) plánovaná doba, po kterou budou osobní údaje uloženy,
e) že má právo požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
f) že má právo podat stížnost u dozorového úřadu a který to je,
g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
h) o skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování (např. by mohlo odpovídat procesům v systému ADAMS).

Pokud správce o fyzické osobě žádné údaje nezpracovává, poskytuje se informace, že osobní údaje tazatele nejsou předmětem zpracování osobních údajů ze strany správce. Doporučuje se vstřícnost s ohledem na možné následné kontroly ze strany ÚOOÚ.

4.9 **Právo na výmaz** představuje povinnost správce zlikvidovat osobní údaje, které o žadateli zpracovává, pokud je splněna alespoň jedna podmínka:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,

b) subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
d) osobní údaje byly zpracovávány protiprávně,
e) osobní údaje musí být vymazány ke splnění právní povinnosti,
f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti (zpravidla marketing),

Výše uvedené podmínky se neuplatní, pokud je zpracování osobních údajů nezbytné:

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

4.10 **Právo na přenositelnost** představuje právo subjektu údajů získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, a to v případě, že zpracování osobních údajů je založeno na souhlasu nebo na smlouvě a zpracování se provádí elektronicky (kumulativní podmínky). Při výkonu svého práva na přenositelnost má žadatel – subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné. **Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu** (ADV ČR) nebo při výkonu veřejné moci, kterým je správce pověřen.

4.11 **Právo na opravu nebo doplnění** má subjekt údajů tak, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se subjektu týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů. Pokud se správce domnívá, že zpracovávané osobní údaje jsou přesné, informuje o tom žadatele s odůvodněním.

4.12 **Další práva** jsou **právo na omezení zpracování, právo podat námitku proti automatizovanému rozhodování**.

5. INTERNÍ DOKUMENTACE

5.1 Záznam o činnostech zpracování

	Kategorie a charakteristiky zpracování osobních údajů	**Komentáře pro vyplnění**
1	Jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro	Uveďte jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů.

	ochranu osobních údajů	
2	Identifikace zpracovávaných osobních údajů.	Uveďte seznam všech zpracování osobních údajů, které provádíte, podle hlavních kategorií: (a) programová agenda (programový úsek); (b) zaměstnanci a spolupracovníci; (c) provoz ADV ČR, daně a účetnictví (dodavatelé) (správní úsek); (d) obchod a marketing, komunikace online; (e) ostatní.
3	Proč (za jakým účelem) a na základě jakého právního titulu se osobní údaje v rámci zpracovávání zpracovávají?	Uveďte pro každé zpracování osobních údajů účel (cíl, smysl zpracování) a rovněž právní titul zpracování (půjde zejména o plnění smlouvy se subjektem a plnění zákonných povinností; v případě právní povinnosti odkaz na příslušný právní základ). Tuto část lze sloučit s předchozím bodem ve formátu: Zpracování – Účel – Právní titul.
4	Jaké osobní údaje jsou zpracovávány?	Pro každé zpracování uveďte všechny kategorie osobních údajů, které zpracováváte.
5	Z jakých zdrojů jsou osobní údaje získány?	Uveďte všechny subjekty, od nichž získáváte osobní údaje, které v rámci své činnosti zpracováváte. Půjde jak o subjekty údajů (sportovci, zaměstnanci, aj.), tak o třetí strany (smluvní strany, aj.).
6	Kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích:	Uveďte všechny kategorie osob a organizací, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích (WADA, za určitých omezení i zahraniční antidopingové organizace atp.).
7	V jakém termínu a jak se osobní údaje likvidují?	Uveďte pro každé zpracování osobních údajů archivační a skartační lhůtu. Má-li ADV ČR interní předpis, lze na něj odkázat.
8	Jakým způsobem se osobní údaje aktualizují?	Uveďte způsob aktualizace osobních údajů (např. obdržením informace od sportovce o změně kontaktních údajů skrze ADAMS atp.). Lze odkázat na interní předpis.
9	Které listinné a elektronické evidence (spisovny, archivy, IT systémy, datová úložiště) provádějí zpracování?	Uveďte podrobně, jaké listinné evidence a IT systémy využíváte pro svou činnost a jejich vazbu na konkrétní zpracování (ADAMS a vlastní IT systém). Lze odkázat na interní předpis nebo dokumentaci informačního prostředí (např. spisový plán, popis IT systémů, směrnici o zpracování osobních údajů).
10	Je prostředí ADV ČR pravidelně bezpečnostně testováno (zejm. IT systémy) a interně nebo	V závislosti na objemu zpracovávaných osobních údajů je třeba zvolit délku časového období mezi dvěma testy. Opět

	externě (externí dodavatel IT řešení)? Jak?	lze odkázat na interní předpis (např. bezpečnostní normu).
11	Jak je zajištěna bezpečnost šifrování dat při komunikaci?	Uveďte, jak řešíte komunikaci citlivých informací (skrze ADAMS, nastavení kancelářského balíku, serveru atp.) a dále např. jak zabezpečujete předání údajů o zaměstnancích externím např. účetním. Je-li vydán, postačí odkaz na vnitřní předpis.
12	Jak je zajištěna bezpečnost sdílení dat s externími subjekty? Mají všichni externí dodavatelé, zpracovávající osobní údaje, uzavřené smlouvy o zpracování osobních údajů, poskytující odpovídající záruky ochrany?	Uveďte, zda vaši dodavatelé, kteří mohou mít přístup ke zpracovávaným osobním údajům (např. účetní nebo správce webu ADV ČR) mají uzavřeny smlouvy o zpracování osobních údajů. Je-li vydán, postačí odkaz na vnitřní předpis.
13	Je zajištěna nevratná likvidace dat v rámci databázového systému?	Uveďte, zda na konci životního cyklu příslušného zpracování osobních údajů je váš IT systém schopný nevratně osobní údaje vymazat (s ohledem na existenci záloh systému, zabezpečení proti nechtěnému vymazání atp.).
14	Je k dispozici procedura k určení práv subjektů údajů a jejich výkon s ohledem na jejich zpracovávané údaje?	Uveďte, zda máte zaveden interní proces vyřizování žádostí subjektů údajů a jakou formou postupujete (např. odkaz na formuláře na vašem webu nebo v listinné podobě). Rovněž je potřeba vymezit, v jakých situacích jsou práva subjektů omezována a z jakých titulů (např. nevydání informací protistraně apod.).
15	Poskytují se oprávněným subjektům údajů předepsané informace, zejména o: - rozsahu a účelu zpracování, - způsobu zpracování osobních dat, komu mohou být osobní údaje zpřístupněny?	Uveďte, kde a jakou formou poskytujete předepsané informace pro subjekty údajů.
16	Zabraňují nasazené technické prostředky a uplatňovaná organizační opatření nahodilému anebo neoprávněnému přístupu k osobním údajům, jejich změně, zcizení, zneužití, zničení nebo ztrátě?	Uveďte, jaká bezpečnostní opatření používáte pro zajištění bezpečnosti zpracovávaných osobních údajů (provozní opatření, IT opatření, logování v IT systému). Opět lze odkázat na vnitřní předpis, je-li vydán.
17	Jsou zpracovávané osobní údaje přenášeny do zahraničí nebo jsou přístupné ze zahraničí?	Uveďte, zda jsou vámi zpracovávané osobní údaje přenášeny do zahraničí nebo přístupné ze zahraničí (např. ADAMS).
18	Jsou pracovníci, mající přístup k osobním údajům v rámci zpracování osobních údajů, proškoleni? Mají tito pracovníci ve svých smlouvách sjednánu	Uveďte, zda jsou pracovníci ADV ČR (zaměstnanci i jinak smluvně zavázané osoby k výkonu činnosti pro ADV ČR) proškoleni o GDPR a zásadách ochrany osobních údajů. Uveďte, zda pokud nemá

	povinnost mlčenlivosti ve vztahu ke zpracovávaným osobním údajům?	externí spolupracovník ADV ČR zákonnou povinnost mlčenlivosti, je k mlčenlivosti ve vztahu ke zpracovávaným osobním údajům smluvně zavázán?

5.2 **Žádosti a stížnosti subjektů údajů**. To lze zajistit buď skrze web (online formuláře) nebo v listinné podobě (ke stažení z webu, na sekretariátu ADV ČR). Vzhledem ke zkušenostem s předchozími stížnostmi a žádostmi lze tento formát včetně typové odpovědi povýšit na pravidelný standard a nikoliv ad hoc potřebu (podle předpisů se žádosti a stížnosti považují za běžný institut a nikoliv výjimečný, jak fakticky bylo v ADV ČR známo doposud. U všech žádostí je nutné ověřit, že příslušné podání podal ten, kdo je k němu oprávněn a podepsán, tedy vždy je třeba ověřit identitu, aby nedošlo k úniku dat jejich poskytnutím neoprávněné osobě. S ohledem na maximální opatrnost se jeví jako nejbezpečnější způsoby (1) písemné žádosti s úředně ověřeným podpisem v originálním vyhotovení, (2) osobní návštěva s prokázáním se platným dokladem prokazujícím totožnost (občanský průkaz, pas, řidičský, zbrojní či služební průkaz s podobiznou). V případě absence datové schránky (kde se odesílatel považuje za ztotožněného) lze využít online řešení s požadavkem na zadání elektronického podpisu vydaného certifikační autoritou, která zajišťuje při poskytnutí elektronického podpisu ztotožnění (I.CA, Postsignum). Rovněž lze využít emailové komunikace, kde tazatel nebo stěžovatel využije elektronického podpisu, který by měl splňovat standard dle zákona o elektronických komunikacích. Prostě podepsané žádosti či stížnosti se optikou GDPR nejeví jako dostatečně průkazné ohledně totožnosti. **Lhůta** se považuje za v zásadě "bezodkladnou" pro vyřízení podání, nejpozději do 1 měsíce od obdržení žádosti. Řízení je **bezplatné**, leda by se jednalo o zjevně šikanózní nebo nepřiměřené požadavky, lze vyřídit podání odmítnutím nebo přiměřeným zpoplatněním s ohledem na povahu požadavku a s náležitým zdůvodněním.

6. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

6.1 ADV ČR do jisté míry je orgánem veřejné moci, resp. vykonává výsek veřejné moci ve veřejném zájmu, přičemž takový veřejný subjekt nebo orgán veřejné moci s výjimkou soudů je povinen jmenovat pověřence vždy. Rovněž je vždy povinnost jmenovat správce v případě takových operací ve zpracování údajů, které kvůli své povaze, rozsahu nebo účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, což by mohlo odpovídat činnosti sledování míst pobytu sportovců a plánování a realizace dopingových kontrol.

6.2 Vzhledem k tomu, že ADV ČR spíše je povinen jmenovat pověřence, než není, lze doporučit se obrátit na MŠMT s požadavkem na sdílení pověřence metodicky nejbližšího k předmětu činnosti ADV ČR. Rovněž z konzultace s ÚOOÚ vyplynulo, že ADV ČR považuje za takový povinný veřejný subjekt. V případě absence vhodného pověřence lze zvážit delegaci na osobu, která již vykonává činnosti dle čl. 2.17 organizačního řádu ADV ČR týkající se kontrolora kvality pro příbuznost činnosti. Aktuální náležitosti a kvalifikace pověřence není součástí této metodiky.

6.3 Pověřenec pro ochranu osobních údajů vykonává alespoň tyto úkoly:
a) poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle

tohoto nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany údajů,

b) monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů,
c) poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování,
d) spolupráce s dozorovým úřadem, a
e) působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace, a případně vedení konzultací v jakékoli jiné věci.

6.4 Soulad postupů a procesů podle GDPR v rámci činnosti správce není odpovědností pověřence, nýbrž je povinností a odpovědností správce (zpracovatele osobních údajů). Pověřenec nesmí určovat nebo závazně schvalovat účely nebo prostředky zpracování osobních údajů. V takovém případě může činnost pověřence směřovat ke kontrole vlastní činnosti, čímž dochází k výraznému střetu zájmů. Správce je proto vždy povinen zajistit, aby byla agenda (administrativní činnosti) související s vyřizováním záležitostí regulovaných GDPR svěřena konkrétní osobě odlišné od pověřence.

V rámci ADV ČR tak přichází v úvahu jmenování pověřencem, v případě výběru z vlastních (kmenových) zaměstnanců, toliko zaměstnance zařazeného do správního úseku, protože nevykonává podstatnou (programovou) činnost ADV ČR.

7. SOUHLASY SUBJEKTŮ ÚDAJŮ SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

7.1 Vzhledem k tomu, že ADV ČR zpracovává osobní údaje ve veřejném zájmu, jehož součástí je celosvětový standardizovaný formát souhlasu zejména ve formuláři dopingové kontroly, a nejde v návaznosti na konzultaci s ÚOOÚ o vynucený souhlas s poskytnutím osobních údajů (veřejný zájem na zpracování), **není v tuto chvíli nutné měnit stávající formát souhlasů, ale do budoucna, tj. pro všechny další poskytované souhlasy např. při zahájení závodní činnosti, se doporučuje (nejde-li o standardizovaný formulář s celosvětovou působností) vyžadovat souhlas ve formátu přiblíženém požadavkům GDPR.**

7.2 V případě, že sportovec přihlášený k závodní činnosti odvolá souhlas se zpracováním osobních údajů, přicházejí v úvahu dvě řešení. Buď takové odvolání souhlasu odmítnout z důvodu výkonu činnosti ve veřejném zájmu, nebo odvolání souhlasu vyhovět s následkem odhlášky ze závodní činnosti s možným dopadem při pokračování závodní činnosti mimo režim dopingové kontroly na deliktní odpovědnost podle Směrnice pro kontrolu a postih dopingu ve sportu v České republice. Tato metodika neřeší konkrétní porušení Směrnice. Než bude tato otázka najisto vyřešena s např. Světovou antidopingovou agenturou, doporučuje se dát sportovci na výběr mezi těmito variantami, resp. jej požádat o upřesnění, zda odvoláním souhlasu končí či nikoliv závodní činnost, a pokud nikoliv, pak odvolání odmítnout z důvodu činnosti ve veřejném zájmu. Rovněž je nutné sportovce v tomto směru předem poučit.

8. BEZPEČNOSTNÍ INCIDENTY

8.1 Za bezpečnostní incident, který musí vyústit v patřičný úkon vyrozumění subjektu údajů a ÚOOÚ (obecně řečeno), se považuje přímý útok na zpracovávaný data zvenčí anebo zevnitř (např. úmyslné vynesení informací nebo nedbalostní jednání jako vymazání části údajů v IT systému omylem), ztráta kontroly nad daty (např. útok hackera, který převezme kontrolu nad IT systémem či webem), ztráta mobilního telefonu s kontakty na subjekty údajů nebo notebooku s osobními údaji subjektů. V případě, že je nepravděpodobné vytěžení údajů např. ze zašifrovaného nosiče dat, není hlášení nutné. Každý jednotlivý incident je třeba vyhodnotit individuálně a bližší návod zatím není k dispozici.

8.2 V případě všech incidentů, tj. těch, které je potřeba oznamovat, i těch, které oznamovat není nutné, se tyto zaznamenávají do evidence incidentů bez výjimky. Součástí toho je rovněž přijetí opatření, aby se incident neopakoval.

9. SDÍLENÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

9.1 V rámci Evropské unie, resp. Evropského hospodářského prostoru, není nutné přijímat žádné zvláštní postupy a považuje se jako by šlo o předávání údajů v rámci ČR.

9.2 V případě předávání mimo tento prostor je nutné provést kontrolu např. na webu ÚOOÚ, zda je s příslušnou zemí zaručena vzájemnost. V případě ADV ČR jde zejména o Kanadu (WADA) a Švýcarsko (CAS), které jsou považovány za vyhovující a požívají stejného režimu, jako při předávání údajů v ČR. V případě potřeby sdílet údaje např. s antidopingovou organizací mimo tyto země se zaručenou vzájemností je nutné využít smluvních doložek k dispozici ke stažení na webu ÚOOÚ.

10. KOLIZE PRÁVNÍCH ŘÁDŮ, KODEXU A DALŠÍCH PŘEDPISŮ

10.1 V návaznosti na konzultaci s ÚOOÚ lze mít za na jisto postavené, že v případě konfliktu se vychází z primárního interpretačního východiska, že kolizní úpravy **nejsou** v kolizi a hledá se vzájemně souladný výklad a řešení.

10.2 Pokud to možné není, ADV ČR je povinen se řídit primárně nad všechny kolidující jiné přepisy, GDPR nevyjímaje, Směrnicí, Kodexem a Standardy, leda samotné tyto předpisy stanoví, že se v případě větší přísnosti či jiné preference použije národní úprava. GDPR, resp. předpisy Evropské unie se považují za národní úpravu. Obecné (ústavní) pravidlo zní, že mezinárodní smlouvy (mezinárodní antidopingová úmluva) jsou nadřazené národním zákonům.

10.3 Má se za to, že Standard ISPPPI je v souladu s GDPR. Ve své preambuli odkazuje, že změní ISPPPI je v souladu s předcházející unijní úpravou, a to směrnicí 95/46/ES, která je nařízením GDPR zrušena a nahrazena. Odkazem na uplatnění přísnější úpravy, než té obsažené ve Standardu ISPPPI, resp. vůbec na úpravu týkající se styku právních řádů, se zaobírá zejména čl. 6 ISPPPI.

V Praze dne 30. dubna 2018
Zpracoval: Mgr. Ondřej Pecák