Desatero GDPR pro Kluby

Osobní údaj = každá informace o identifikované nebo identifikovatelné fyzické osobě (lze rozdělit do několika kategorií – *identifikační údaje, adresní údaje, kontaktní údaje, popisné údaje, finanční údaje* a *údaje o zdravotním stavu*) – („**OÚ**“)
Zpracování OÚ = jakákoliv operace s OÚ (např. zaznamenání, shromáždění, uložení, pozměnění, nahlédnutí, šíření, vymazání,…)
Správce = ten, kdo určuje účel a prostředky zpracování OÚ (zpravidla Klub)
Zpracovatel = ten kdo zpracovává OÚ pro správce dle jeho pokynů
Subjekt údajů = identifikovaná nebo identifikovatelná fyzická osoba (např. člen, zákonný zástupce, zákazník,…)
Souhlas = svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává své svolení ke zpracování svých osobních údajů
Porušení zabezpečení OÚ = jakýkoliv incident zejm. ztráta, odcizení, poškození, zničení či neoprávněný přístup k OÚ
Profilování = automatizované zpracování OÚ spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě
Odpovědná osoba = osoba odpovědná za otázky zpracování osobních údajů v Klubu

Základní pravidla pro zpracování osobních údajů

1) Právní základ – Pro každé zpracování OÚ musí existovat právní základ.
    a. Souhlas je pouze jeden z několika základů, dalšími jsou např. plnění smlouvy či plnění právní povinnosti Klubu – zejména na základě následujících předpisů
        i. *115/2001 Sb., o podpoře sportu;*
        ii. *373/2011 Sb., o specifických zdravotních službách;*
        iii. *391/2013 Sb., vyhláška o zdravotní způsobilosti k tělesné výchově a sportu.*
    b. Všechny právní základy mají stejnou váhu, může existovat více základů paralelně.
    c. Pokud přestane existovat poslední právní základ nelze OÚ nadále zpracovávat.
2) Transparentnost – subjekt údajů by měl mít vždy povědomí a možnost se seznámit s tím, jak a jaké OÚ Klub zpracovává (vč. toho komu je předává).
    a. Zpracování by nemělo být pro subjekt údajů zcela překvapivé.
    b. Subjekt údajů má právo být na počátku o zpracování informován a informace kdykoliv aktivně požadovat.
3) Účelové omezení – OÚ získané za jedním konkrétním účelem nesmějí být použity za jiným účelem.
    a. Účel musí být jasně a transparentně stanoven předem (např. registrace člena klubu, zveřejňování údajů členů v příslušné databázi/evidenci, marketingové účely,…)
    b. Způsoby (postupy a prostředky) zpracování musí odpovídat účelu, za kterým se OÚ zpracovávají.
4) Omezení uložení – doba zpracování nesmí přesáhnout dobu nezbytnou k naplnění účelu.
    a. Je třeba brát v potaz např. zákonné lhůty pro uchování některých OÚ.

5) Minimalizace osobních údajů – zpracovávat pouze OÚ, které jsou přiměřené, relevantní a nezbytné k dosažení stanoveného účelu.
    a. Aplikace principu *need-to-know* nikoliv *nice-to-have.*
    b. Rozsah OÚ by měl být minimální možný tak, aby Klub shromažďoval osobní údaje v nejmenším možném rozsahu, při kterém zamýšlené zpracování může dosáhnout stanoveného účelu.
6) Přesnost – zpracovávané OÚ musí být správné a přesné ve vztahu ke stanovenému účelu zpracování.
    a. Subjekt údajů má právo na opravu a doplnění nepřesných nebo neaktuálních OÚ.
7) Důvěrnost – zajištění vhodných opatření na ochranu OÚ.
8) Přístup založený na míře rizika – opatření na ochranu OÚ mají být přizpůsobená rizikovosti zpracovávaných OÚ (tzn. použít patřičná opatření, pokud jsou zpracovávány např. OÚ o zdravotním stavu či rodná čísla) = racionální přístup k ochraně osobních údajů.

Práva subjektů údajů

1) Právo na informace o zpracování a přístup ke svým OÚ – viz. bod 2) b výše.
2) Právo na opravu OÚ – viz. bod 6) a výše.
3) Právo na výmaz OÚ – subjekt údajů má právo požadovat výmaz OÚ, které se ho týkají **za podmínek**, že **a)** osobní údaje již nejsou potřebné pro stanovený účel **nebo b)** je odvolán souhlas a neexistuje jiný právní důvod **nebo c)** je podána námitka proti zpracování a neexistuje převažující oprávněný důvod pro zpracování **nebo d)** OÚ byly zpracovány protiprávně **nebo e)** výmaz přikazuje právní řád **nebo f)** jedná se o zpracování OÚ dítěte v souvislosti s nabídkou služeb informační společnosti (typicky elektronického obsahu).
4) Právo na omezení zpracování OÚ – do té míry, pokud jsou zpracovávány nepřesné OÚ, pokud jde o nezákonné zpracování OÚ, OÚ již nejsou potřebné ke stanovenému účelu, subjekt údajů vznesl námitku proti zpracování a prozatím nebylo rozhodnuto o její oprávněnosti.
    a. Obdobné podmínky jako pro výmaz, ale subjekt údajů žádá pouze omezení rozsahu nebo omezení způsobů zpracování (např. ponechání v databázi, ale další neoslovování), případně jako předběžné opatření, než je rozhodnuto správcem o námitce.
5) Právo vznést námitku proti zpracování – zejm. tam kde zpracování probíhá na základě oprávněného zájmu Klubu
    a. Námitku zaměstnanec v jednoduchých případech posoudí sám, ve složitých případech postoupí Odpovědné osobě.
    b. Posouzení námitky spočívá v poměřování zásahu do základních práv a svobod subjektu údajů a oprávněného zájmu Klubu (je zpracování způsobilé dosáhnout oprávněného zájmu? – kritérium vhodnosti; Jedná se o nejméně invazivní prostředek, jak oprávněného zájmu docílit? – kritérium nezbytnosti).
    c. Pokud jde o námitku proti zpracování OÚ za účelem přímého marketingu vyhoví se vždy bez dalšího.

6) Právo na přenositelnost OÚ – právo subjektu údajů přenést všechny své osobní údaje ve strojově čitelné podobě k jinému správci (směřuje primárně na jiné typy správců – např. sociální sítě)

Co dělat v případě uplatnění práva subjektem údajů

A. Je žádost podána subjektem údajů? (nelze uplatňovat práva za jiného bez platného zmocnění)
B. Vzniklo v daném případě uplatňované právo? (např. „odvolání souhlasu" tam, kde se jedná o zpracování nezbytné pro splnění právní povinnosti Klubu, není možné)
C. Je možné snadno určit, zda se jedná o oprávněné uplatnění práva? (např. právo na omezení zpracování fotografie v důsledku odvolání souhlasu)
D. Provedení příslušných kroků k uspokojení práva nebo předání nadřízenému pracovníkovi s oprávněním tyto kroky provést.
E. V případě nemožnosti snadno určit, zda se jedná o oprávněné uplatnění práva postoupení požadavku nadřízenému pracovníkovi příp. Odpovědné osobě.
F. Vždy podat zprávu o uplatnění práva a řešení Odpovědné osobě.

Co dělat v případě podezření či zjištění porušení zabezpečení OÚ

A. Neprodleně oznámit nadřízenému pracovníkovi a současně Odpovědné osobě.
B. Poskytnout veškerou součinnost při řešení incidentu porušení zabezpečení OÚ.
C. Provést nápravná opatření pro zabránění opakování incidentu.

Klub má povinnost jakékoliv významné porušení zabezpečení osobních údajů nahlásit Úřadu pro ochranu osobních údajů do 72h od doby, kdy se o porušení dozvěděl – činí tak Odpovědná osoba.

Zpracovatelé – v případě angažování zpracovatele je vždy třeba uzavřít navíc také zpracovatelskou smlouvu.
Předávání OÚ do zemí, které neposkytují dostatečnou úroveň ochrany OÚ (mimo EU/EHP) – možné pouze s těmi partnery, se kterými byly uzavřeny standardní smluvní doložky.

Základní pravidla pro nakládání s OÚ

Každodenní dodržování základních principů → dodržování většiny pravidel GDPR

Mlčenlivost - všechny osoby, které zpracovávají osobní údaje pro klub, jsou povinny zachovávat mlčenlivost o těchto osobních údajích a o přijatých bezpečnostních opatřeních

Záznamy o zpracování - zpracování údajů Klubem není příležitostné a může představovat zásahy do práva a svobod subjektu údajů, Klub proto musí vést záznamy o kontaktních údajích Správce, účelech zpracování, kategoriích Subjektů údajů, příjemců, informacích o předávání údajů do zahraničí, plánovaných lhůtách pro výmaz a přijatých opatřeních

Kamerový systém – Klub stanoví účel zpracování (např. ochrana majetku a zdraví osob), dodržuje základní zásady zpracování OÚ, stanoví lhůtu pro uchování záznamů (doporučená 1 týden), informuje Subjekty údajů o existenci kamerového systému (např. pomocí informační tabule) a vyhotoví interní směrnici popisující oprávněnost pořizování záznamů.

Fotografie - 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

OÚ v papírové podobě:

- Systematizované vedení dokumentů umožňující spolehlivou orientaci a určení rozsahu zpracovávání OÚ
- Vedení systému umožňujícího doložit řádné získání kontaktních údajů
- Udržování dokumentů obsahujících OÚ mimo možnost volného nebo nahodilého přístupu (tzv. praxe čistého stolu)
- Průběžná skartace nepotřebných dokumentů
- Trvalé uzamykání či obdobná ochrana dokumentů obsahujících „citlivé" osobní údaje (např. o zdravotním stavu)
- Uzamykání prostorů či stolu/skříně s dokumenty obsahujícími OÚ při odchodu z práce

OÚ v elektronické podobě:

- Nastavení netriviálního hesla na osobním počítači a jeho pravidelná obměna
- Přístup do IT systémů obsahujících osobní údaje na základě hesla a dispozice oprávněními dle rolí
- Využívání sdílených disků k přístupu k dokumentům a jejich ukládání -> nevytváření dalších kopií OÚ na lokálních discích
- Udržování systému složek a podsložek a v nich řádně třízených dokumentů obsahujících OÚ
- Promazávání nepotřebných či neaktuálních souborů s OÚ
- Třízení elektronické pošty a zejména její pravidelné promazávání/archivace
- Zamykání obrazovky při odchodu od osobního počítače
- Při komunikaci s dodavateli zasílat větší objemy osobních údajů pouze v zašifrované podobě (jednotlivé údaje v nezašifrované podobě zasílat pouze výjimečně – např. při komunikaci s uchazečem o práci, zašle-li životopis apod.)
- Věnovat řádnou pozornost celému e-mailu (předmětu, odesílateli, tělu) před otevřením přílohy
- Nenavštěvovat neznámé či podezřelé odkazy v e-mailech nebo na webu