

Bezpečnostní směrnice nakládání s osobními údaji TJ STAR PRAHA z.s.

vypracovaná v souladu s Nařízením 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)

Datum poslední aktualizace: 9. 9. 2018

1	ÚVOD DO PROBLEMATIKY OCHRANY OSOBNÍCH ÚDAJŮ	3
2	ZÁKLADNÍ POJMY	4
3	OBECNĚ K POVINNOSTI ZAJIŠTĚNÍ BEZPEČNOSTI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	6
4	ZÁKLADNÍ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	7
5	NAKLÁDÁNÍ S DOKUMENTY	9
5.1	DOKUMENTY V ELEKTRONICKÉ PODOBĚ	9
5.2	DOKUMENTY V PAPIROVÉ PODOBĚ	11
5.3	PORUŠENÍ OCHRANY DAT	11
5.4	LIKVIDACE OSOBNÍCH ÚDAJŮ	12
6	PRAVIDLA VYUŽÍVÁNÍ SÍTĚ INTERNET	13
6.1	ZÁKAZY PRO UŽIVATELE	13
7	VSTUPY DO BUDOV A KANCELÁŘÍ	14
8	BEZPEČNOSTNÍ INCIDENTY	15
8.1	POSTUP PŘI VZNIKU BEZPEČNOSTNÍCH INCIDENTŮ	15
9	JEDNOTLIVÉ AGENDY SPRÁVCE	16
9.1	ÚČETNÍ A MZDOVÁ AGENDA	16
9.2	REGISTRACE ČLENŮ	16
9.3	KLUBOVÝ WEB A SOCIÁLNÍ SÍTĚ	17
9.4	KONKRÉTNĚ K ZABEZPEČENÍ BUDOV, MÍSTNOSTÍ A PC	17

1 Úvod do problematiky ochrany osobních údajů

Dne 27. 4. 2016 bylo přijato 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), v anglickém jazyce General Data Protection Regulation – GDPR) (dále jen „**Nařízení**“ nebo „**GDPR**“).

GDPR představuje nový právní rámec ochrany osobních údajů a má za úkol maximálně chránit práva občanů EU proti neoprávněnému nakládání s jejich osobními údaji. Toto Nařízení bylo přijato formou evropského nařízení, znamená to tedy, že je jednotně platné napříč všemi státy EU, a je přímo účinné v celém evropském prostoru dne 25. 5. 2018.

Řadu pravidel oblasti osobních údajů již známe z předchozí právní úpravy, GDPR však zavádí celou řadu pravidel nových. Mezi taková práva patří např. právo na výmaz a také právo „být zapomenut“. Jejich platnost a dodržování musí každý správce osobních údajů (takže nepochybně i **TJ STAR PRAHA z.s.**) zajistit a musí být také schopen doložit, že k zákonnému zpracování osobních údajů opravdu dochází.

GDPR poskytuje lidem, kterým údaje patří (tj. subjektům údajů - např. zaměstnancům, hráčům, rozhodčím a dalším členům) nové možnosti, jak mít o nakládání se svými osobními údaji přehled. Kromě toho došlo k rozšíření pojmu „osobní údaje“ – nově sem patří i e-mail, IP adresa, cookies v zařízení uživatele, či genetické a biometrické údaje. Právě poslední jmenované budou podléhat přísnějšímu režimu.

Nově je zavedena také oznamovací povinnost v případě narušení zabezpečení ochrany osobních údajů. Správce musí nahlásit únik či ohrožení osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o tom dozvěděl, Úřadu pro ochranu osobních údajů.

2 Základní pojmy

1. Co je to GDPR?

Obecné nařízení EU, podle kterého se řídí ochrana osobních údajů.

2. Co je to osobní údaj?

Jedná se o **jakoukoli informaci** o fyzické osobě, která napomůže k její identifikaci. Např. pokud o někom víme, že je to volejbalista Motoru České Budějovice, nejedná se samo o sobě o osobní údaj, neboť osobu na základě této informace neidentifikujeme. Jestliže ale víme, že nosí číslo 10 a jmenuje se Jiří, lze už snadno dohledat konkrétní osobu. Proto už by se o osobní údaje jednalo.

Osobními údaji jsou zejména jméno, příjmení, pohlaví, věk a datum narození, osobní stav, fotografie, ale také např. i IP adresa.

3. Co to je zpracování osobních údajů?

Jakákoliv činnost, která je prováděna s osobními údaji. Např. pokud jsou zapisovány, vyplňovány nebo je někdo focen např. na registrační kartu (tzv. „registračku“). Taková činnost vždy podléhá pravidlům GDPR.

4. Kdo je to Správce a Zpracovatel osobních údajů?

Správce je subjekt, který rozhoduje o účelu a způsobu zpracování osobních údajů (např. klub **TJ STAR PRAHA z.s.** ve vztahu k zaměstnancům, členům, hráčům, rozhodčím atp.). Zpracovatelem se rozumí ten, kdo pro něj osobní údaje zpracovává (např. účetní firma).

5. Kdo je to Subjekt osobních údajů?

Fyzická osoba, jejíž osobní údaje jsou zpracovávány.

6. Kdo je to třetí strana?

Kdokoli mimo klub, komu jsou předávány osobní údaje.

7. Co je to bezpečnostní incident?

Jakákoliv situace, v jejímž rámci dojde k úniku, zničení nebo ztrátě osobních údajů.

8. Co jsou to „osobní údaje dostupné z veřejných rejstříků“?

Jedná se o osobní údaje, které je teoreticky možné volně získat z veřejně dostupných seznamů (například z obchodního rejstříku).

9. Co jsou to citlivé osobní údaje (zvláštní kategorie osobních údajů)?

Jedná se o osobní údaje, jejichž znalost může subjektu osobních údajů způsobit újmu. Jedná se např. o údaje vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuální orientaci subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů.

3 Obecně k povinnosti zajištění bezpečnosti zpracování osobních údajů

Každý sportovní klub by měl zabezpečit osobní údaje po technické a organizační stránce, tj. organizačně v dokumentech určit např. přístupové role a stanovit technické prostředky k jejich zabezpečení, např.:

1. používat odpovídající technické zařízení a programové vybavení způsobem, který vyloučí neoprávněný či nahodilý přístup k osobním údajům ze strany jiných osob,
2. údaje v elektronické podobě uchovávat na zabezpečených serverech nebo na nosičích dat, ke kterým mají přístup pouze pověřené osoby na základě přístupových kódů či hesel,
3. zajistit dálkový přenos údajů buď pouze prostřednictvím veřejně nepřístupné sítě, nebo prostřednictvím zabezpečeného přenosu po veřejných sítích,
4. **písemné dokumenty obsahující osobní údaje uchovávat na zabezpečeném místě** (uzamykatelná skříň, místnost atd.) a zároveň vést řádnou evidenci o pohybu takových písemných dokumentů, dohlédnout na nemožnost nahrávat data na soukromé USB klíče, apod.,
5. stanovit pravidla pro přístup k datům (hesla a role), zajistit logování tak, aby měl každý člen individuální přístup.

4 Základní zásady zpracování osobních údajů

1. U každého osobního údaje je nezbytné jasně **stanovit účel jeho zpracování**, který není v rozporu s právními předpisy nebo oprávněnými zájmy subjektů údajů (měnit účel v průběhu zpracování principiálně lze, ale pouze ve značně omezeném rozsahu).
2. Každý osobní údaj musí být pro daný účel zpracován na základě platného právního titulu/důvodu, tj. zákonné zmocnění, oprávněný zájem, veřejný zájem, životně důležitý zájem, smlouva, výjimečně pak souhlas subjektu údajů.
3. Skutečnosti v bodech 1 a 2 této kapitoly jsou stanoveny v záznamech o činnosti zpracování, kterými klub také disponuje a které by měl pravidelně aktualizovat.
4. Zpracovávat je možné pouze osobní údaje v nejmenším možném rozsahu, který ještě postačuje ke splnění účelu zpracování (zásada minimalizace). Tzn. není třeba zpracovávat všechny osobní údaje svého člena, jelikož například náboženské vyznání hráče není pro klub důležité. Klub by proto „zbytečné“ osobní údaje neměl zpracovávat.
5. Je-li právním důvodem pro zpracování osobních údajů souhlas subjektu údajů, musí splňovat náležitosti dle GDPR (před udělením souhlasu náležitě informování a poučení mimo jiné i o možnosti odvolání souhlasu). To, že byl souhlas udělen musí být klub **TJ STAR PRAHA z.s.** jakožto správce schopen kdykoliv prokázat (čl. 7 GDPR).
6. V každém případě zpracování osobních údajů musí být subjekt údajů ze strany správce náležitě **informován** o podmínkách zpracování osobních údajů a o svých právech. V některých případech může být informační povinnost splněna i zveřejněním informací na webových stránkách a nástěnce klubu.
7. Je nezbytné zajistit právní titul k případnému předání osobních údajů mimo EU/EHS (např. konání soutěže v nečlenském státu).
8. Je nezbytné zajistit, aby osoby, které přistupují k osobním údajům, či je dále zpracovávají, dodržovaly tento vnitřní předpis.
9. Ve větších klubech je třeba náležitě vyškolit zaměstnance, kteří s osobními údaji nakládají.
10. V případě jakýchkoliv pochybností při konkrétních zpracováních je třeba se vždy poradit s odborníky.
11. Ve smlouvách s obchodními partnery musí být stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie osobních údajů. Zejména by měla být se zpracovatelem smluvně ošetřena součinnost při výkonu práv subjektů údajů, oznamování a řešení bezpečnostních incidentů.
12. Je třeba prověřit z pohledu správce, zda zpracovatelé, které využívá, splňují uvedené požadavky a následně je nutné toto pravidelně prověřovat. Současně je třeba monitorovat

smlouvy, které jsou uzavřeny se zpracovateli, a případně je doplnit či upravit.

5 Nakládání s dokumenty

5.1 Dokumenty v elektronické podobě

Elektronické dokumenty se nachází v paměti výpočetní techniky, tj. telefonů, tabletů, či počítačů. Je proto nutné, aby byla dodržována určitá pravidla při manipulaci s touto technikou:

1. Při ovládání PC je třeba zejména:
 - i. Dodržovat následující nastavení zásad hesla a politiky konta:
 - nezobrazovat jméno posledně přihlášeného uživatele,
 - ochrana heslem:
 - vynutit použití historie hesel – počet hesel, které si systém pamatuje: obvykle 10,
 - maximální doba platnosti hesla – počet dní: obvykle 180
 - minimální doba platnosti hesla – počet dní: obvykle 1,
 - minimální délka hesla – počet znaků: obvykle 8,
 - hraniční hodnota uzamčení účtu – počet povolených pokusů o přihlášení: obvykle 3,
 - trvání uzamčení účtu: Uzamčení dočasné – obvykle 20 minut,
 - vynulování počítačového uzamčení účtu po čase: obvykle 20 minut. (Tedy po uplynutí 20 minut dojde k vynulování počítačového uzamčení účtu a uživatel má opět 3 pokusy pro přihlášení.).
 - uzamknutí počítače obvykle při neaktivitě delší než 30 minut.
 - ii. Dodržovat bezpečnost poskytovanou systémem správy hesel. Heslo je citlivé na jeho kompromitaci vždy, když je použito, uloženo nebo jinak zaznamenáno. Pro zajištění bezpečnosti musí být hesla zadávána s opatrností. Následující doporučení pomáhají hesla chránit.
 - Nikdy nezapisovat heslo.
 - Nikdy s nikým nesdílet heslo.
 - Nikdy nepoužívat heslo pro přihlášení se do sítě pro jiné účely.
 - Používat rozdílná hesla pro přihlášení se do sítě a pro účet Administrátor na počítači.
 - Měnit své heslo do sítě každých 180 dní nebo dle požadavků vynucených lokálními politikami zabezpečení.
 - Měnit heslo okamžitě, pokud existuje podezření, že by mohlo být kompromitováno.
 - Aby heslo bylo silné, musí splňovat následující požadavky:
 - musí být nejméně 8 znaků dlouhé,
 - musí obsahovat znaky ze dvou z následujících tří skupin:

Popis	Příklady
Velká a malá písmena	A, B, C ... a, b, c, ...
Číslice	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symboly	` ~ ! @ # \$ % ^ & * () _ + - = { } [] \ : " ; ' < > ? , . /

- musí být signifikantně odlišné od předchozího,
 - nesmí obsahovat jméno nebo uživatelské jméno,
 - nesmí ho tvořit běžné slovo nebo jméno,
 - nesmí být snadno uhodnutelné (např. Jméno + datum narození...).
- Hesla administrátorů musí být po každé změně uložena do trezoru v zapečetěné obálce.
- iii. Při krátkodobém opuštění PC aktivovat spořič obrazovky s heslem.
2. Pracovníci/členové klubu **TJ STAR PRAHA z.s.** mají právo nahlížet do souborů obsahujících osobní údaje jen za předpokladu, že je to nezbytné k výkonu jejich pracovního zařazení.
 3. Pracovníci/členové mají právo **zpřístupňovat** dokumenty obsahující osobní údaje **třetím osobám** či subjektům jen za předpokladu, že mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, předpisem sportovního svazu, předpisem klubu TJ STAR PRAHA z.s.**, případně uloží-li jim takovou **povinnost vedoucí pracovník/předseda spolku.**
 4. Pracovníci/členové klubu **TJ STAR PRAHA z.s.** mají zakázáno ukládat osobní údaje do veřejně přístupných rozhraní, prohlížečů a databází, ledaže mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, předpisem sportovního svazu, předpisem klubu TJ STAR PRAHA z.s.**, případně uloží-li jim takovou **povinnost vedoucí pracovník/předseda spolku.**
 5. Osobní údaje je možné vkládat do předem připravených databází, které jsou k tomu určeny nebo do vlastních (nesdílených) dokumentů, do kterých mají přístup jen sami pracovníci/členové.
 6. Pracovníci/členové nemají bez výslovného povolení vedoucího pracovníka/předsedy spolku právo tisknout osobní údaje obsažené ve sdílených databázích.
 7. Je **zakázáno** pořizovat **skeny občanských průkazů** vyjma situací, kdy je to pořizovaná stanoveno jako zákonná povinnost nebo kdy k tomu subjekt osobních údajů předá výslovný a svobodný souhlas se všemi zákonnými náležitostmi.

5.2 Dokumenty v papírové podobě

1. Listiny obsahující jakékoli osobní údaje (např. zápisy o utkání, faktury) nesmí být ponechány nechráněny na volně dostupném místě. Ideální variantou je tyto listiny ukládat do uzamykatelných skříní, nicméně v místnostech přístupných pouze pro zaměstnance mohou být uloženy **i v neuzamykatelných skříních**.
2. Pracovníci/členové, kteří mají uložené listiny s osobními údaji v neuzamčené skříní dle bodu 1. jsou povinni uzamykat kancelář pokaždé, když ji opouští.
3. Žádné dokumenty nebudou ponechávány bez dozoru na pracovní ploše stolu, při odchodu z práce, příp. opuštění kanceláře (jednání, přestávka na oběd atd.) budou dokumenty obsahující osobní údaje uklizeny v šuplících.
4. Listiny obsahující **citlivé osobní údaje** (karta zaměstnance, dotazník zaměstnance, jakékoli informace o zdravotním stavu) mohou být uloženy jen v **uzamčených** skříních, a to jak na místech veřejně přístupných, tak i na místech přístupných pouze zaměstnancům.
5. Pracovníci/členové mají právo **nahlížet** do dokumentů obsahujících osobní údaje jen za předpokladu, že je to **nezbytné** k výkonu jejich pracovního zařazení.
6. Pracovníci/členové mají právo **zpřístupňovat** dokumenty obsahující osobní údaje **třetím osobám** či subjektům jen za předpokladu, že mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, předpisem sportovního svazu, předpisem klubu**, případně uloží-li jim takovou **povinnost vedoucí pracovník/předseda spolku**.
7. Je **zakázáno** pořizovat **kopie občanských průkazů** vyjma situací, kdy je toto pořizování stanoveno jako zákonná povinnost nebo kdy k tomu subjekt osobních údajů předá výslovný a svobodný souhlas se všemi zákonnými náležitostmi.

5.3 Porušení ochrany dat

1. Každý klub je povinen ohlásit únik či ohrožení zabezpečení osobních dat Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o incidentu dozvěděl.

Ohlášení musí obsahovat minimálně:

- i. popis povahy daného případu porušení zabezpečení osobních údajů,
- ii. popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- iii. popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení,
- iv. zabezpečení osobních údajů.

2. Každý pracovník/členové klubu **TJ STAR PRAHA z.s.** je povinen o jakémkoli podezření o úniku osobních údajů informovat tajemníka spolku.

5.4 Likvidace osobních údajů

1. Ve chvíli, kdy opadne poslední oprávněný zájem pro zpracovávání osobních údajů, je nutné tyto údaje zlikvidovat. V případě přepisovatelných medií lze údaj vymazat, v případě nepřepisovatelných medií či papírové podoby musí dojít k fyzickému zničení v podobě:
 - i. rozdrcení (diskety, disky),
 - ii. skartování (papír)
 - iii. formátování či přepsání (elektronické přepisovatelné disky),
 - iv. demagnetizace (diskety).
2. Konkrétně je třeba dodržovat zásady a postupy, které ohledně likvidace osobních údajů stanovuje spisový a skartační řád.

6 Pravidla využívání sítě Internet

1. Zaměstnanci a členové klubu budou používat síť Internet tak, aby se minimalizovala možná rizika vyplývající z jeho používání. Nesprávné používání a zneužití služeb Internetu představuje hrozbu pro informační systém.
2. Zaměstnanci mají zakázáno navštěvovat stránky s neznámým obsahem.

6.1 Zákazy pro uživatele

Je zejména zakázáno:

1. používat informační prostředky pro zobrazování, ukládání, zpracování nebo šíření materiálů, které omezují lidská práva a práva menšin, jsou rasistické, sexuálně zaměřené, nebo jiným způsobem nezákonné,
2. poskytnout služební identifikační prostředky využívané při práci s informačními technologiemi prostřednictvím Internetu (např. heslo) cizí osobě,
3. stahovat z Internetu nelegální software,
4. svévolně instalovat jakýkoli software, včetně různých plug-in modulů na pracovní stanici uživatele,
5. svévolně měnit nastavení programů umožňujících komunikaci s Internetem,
6. poskytnout neautorizovanému subjektu přístup ke službám Internetu ze služebních počítačů,
7. posílat informace s osobními údaji v otevřeném tvaru elektronickou poštou,
8. připojovat se z pracovních stanic na privátní internetové účty,
9. jakýmkoli způsobem provádět vyhledávání, monitorování a zjišťování stavu portů na serverech klubového informačního systému.

7 Vstupy do budov a kanceláří

1. Zaměstnanec nemá povoleno umožnit vstup do budovy (resp. prostoru využívaném klubem **TJ STAR PRAHA z.s.**) za jiným než pracovním/spolkovým účelem.
2. V případě, že zaměstnanci nejsou přítomni na pracovišti, jsou zodpovědní za zamykání a jiné zabezpečení svých kanceláří, jakož i uložení dokumentů obsahujících osobní údaje do míst dle této směrnice.

8 Bezpečnostní incidenty

1. Může se stát, že dojde k tzv. bezpečnostnímu incidentu. To je situace, ve které dochází k narušení bezpečí osobních údajů. Za takový incident považujeme např.:
 - i. neoprávněný přístup do informačních systémů a úložišť,
 - ii. pokus o neoprávněný přístup do informačních systémů a úložišť.
2. Tento přístup nebo pokus o něj může být jak fyzický, tak elektronický (např. cílené zaslání e-mailu „infikovaného“ virem, ...).
3. V případě, že zaměstnanec zjistí, že došlo k narušení bezpečí osobních údajů, neprodleně tuto skutečnost nahlásí tajemníkovi spolku.

8.1 Postup při vzniku bezpečnostních incidentů

1. Po zjištění vzniku bezpečnostního incidentu zaměstnanec informuje tajemníka spolku. Vedoucí zásadou při vzniku bezpečnostního incidentu je, že zaměstnanec bude vždy nápomocen k tomu, aby došlo k bezodkladnému napravení porušení a k rychlému prošetření incidentu.
2. V závislosti na typu incidentu je třeba přijmout adekvátní bezpečnostní opatření, která minimalizují škody a vznik dalších rizik.
3. Pokud incident jakýmkoli způsobem ohrozí osobní údaje, je třeba neprodleně informovat tajemníka spolku, případně do 72 hodin i dozorový úřad.

9 Jednotlivé agendy správce

9.1 Účetní a mzdová agenda

1. Klub **TJ STAR PRAHA z.s.** uznává, že rozsah osobních údajů potřebný k řádnému vedení účetní a mzdové agendy je značný, a proto bere zvláštní zřetel na ochranu těchto osobních údajů.
2. Účetní a mzdová agenda může být v rámci klubu řešena dvojím způsobem:
 - i. samotným klubem,
 - ii. externím subjektem.
3. V případě, že je účetní a mzdová agenda vykonávána samotným klubem, je třeba zajistit, aby všichni zaměstnanci přicházející do styku s osobními údaji byli řádně proškoleni a informováni o povinnosti zachovávat mlčenlivost a řádně s těmito osobními údaji nakládat.
4. V případě, že je účetní a mzdová agenda vykonávána externím subjektem, je třeba s tímto subjektem zvláště smluvně upravit povinnost při zpracování těchto údajů dodržovat požadavky Nařízení.
5. Účetní dokumentaci v listinné podobě je třeba zabezpečit dvojitou linií zabezpečení, tzn. uchovávat dokumenty v uzamykatelném prostoru v uzamykatelné místnosti.
6. Je nutné, aby jednotlivé účetní dokumenty byly zpracovávány (uloženy) jen po dobu nezbytně nutnou, tzn. po dobu stanovenou speciálními právními předpisy (např. zákon o účetnictví, daňové předpisy), a po uplynutí této doby byly skartovány.
7. Účetní dokumentaci v elektronické podobě je třeba chránit heslem a ukládat ji v rámci bezpečných programů na bezpečných serverech. Je třeba zajistit, aby heslo do těchto programů splňovalo požadavky dle této směrnice.
8. Je nezbytně nutné, aby jednotlivé účetní dokumenty byly v programu elektronicky zpracovávány jen po dobu nezbytně nutnou, tzn. po dobu stanovenou speciálními právními předpisy (např. zákon o účetnictví), a po uplynutí této doby byly z programu smazány.
9. K náboru nových zaměstnanců je možné využít externí subjekt (např. agenturu práce), je však nutné uzavřít s tímto externím subjektem smlouvu tak, aby pokrývala všechny požadavky, které na ochranu a nakládání s osobními údaji stanovuje Nařízení.
10. Při náboru nových zaměstnanců je třeba bez souhlasu neuchovávat životopisy nebo jiné dokumenty těch uchazečů, kteří nebyli přijati do pracovního či obdobného poměru (například je třeba smazat životopis neúspěšného kandidáta).
11. Osobní složka, či archivovaná pracovní smlouva či dohoda o provedení práce nebo licence (např. trenérská), musí být řádně zabezpečena alespoň dvěma liniemi zabezpečení, tzn. uchovávat dokumenty v uzamykatelném prostoru v uzamykatelné místnosti.
12. Klub **TJ STAR PRAHA z.s.** zpracovává osobní údaje související s účetní a mzdovou agendou po dobu, kterou stanovují právní předpisy, potom je třeba osobní údaje smazat a již dále nezpracovávat.

9.2 Registrace členů

1. Klub **TJ STAR PRAHA z.s.** registruje své členy pouze na základě přihlášky a požaduje po nich pouze ty osobní údaje, které jsou nezbytné k výkonu činnosti klubu a které si klub dopředu stanovil spolu s účely pro jejich zpracování.
2. Před vyplněním a podpisem přihlášky je třeba potenciálního člena informovat o jeho právech a dalších podstatných informacích, které se týkají zpracování jeho osobních údajů. Informační povinnost v některých případech lze splnit i deklarací na webových stránkách či vyvěšením informací na nástěnce klubu. Klub však vždy musí být připraven poskytnout vyjasňující, či doplňující informace.
3. U osob mladších 16 let je třeba vyžádat si souhlas zákonného zástupce (rodiče přihlášku musí podepsat).

4. Přihlášky je třeba uchovávat tak, aby byly chráněny dvěma liniemi zabezpečení, tzn. uchovávat dokumenty v uzamykatelném prostoru v uzamykatelné místnosti.
5. Přihlášky v elektronické podobě je třeba dostatečně chránit tak, aby k nim neměla přístup nepověřená osoba.
6. Klub **TJ STAR PRAHA z.s.** předává osobní údaje subjektů osobních údajů příslušným sportovním Svazům, příslušným Okresním sdružením České unie sportu, SCS ČUS, výboru České unie sportu, z.s., se sídlem Zátopkova 100/2, Břevnov (Praha 6), 169 00, Praha a příslušným orgánům státní správy a samosprávy. O tomto faktu je třeba subjekt údajů informovat, např. deklarací na webových stránkách klubu.

9.3 Klubový web a sociální sítě

1. Klubový web je místo, na kterém se veřejnosti i členové klubu mohou dozvědět zásadní informace o činnosti klubu, včetně některých osobních údajů. Proto je třeba přistupovat obezřetně k obsahu, který bude (a je) na webových stránkách či sociálních sítích klubu zveřejňován.
2. Je třeba postavit najisto, kdo spravuje který nástroj klubové propagace v daném čase, to znamená, že klub si musí zejména:
 - i. ujednat s jednotlivými oddíly, kdo spravuje webové stránky, případně jejich části,
 - ii. stanovit kdo má přístup do administrátorské části webu či sociální sítě a může tak vkládat obsah, či jej měnit nebo mazat,
 - iii. stanovit odpovědnost za neautorizované vložení osobního údaje.
3. Před zveřejněním fotografií z akce klubu je třeba vždy posoudit, zda tyto fotografie spadají do tzv. zpravodajské licence. V pochybnostech je nutné zveřejnění fotografií konzultovat. Obecně je doporučeno nezveřejňovat:
 - i. detailní fotografie osob,
 - ii. přiblížené fotografie na obličej osoby,
 - iii. Fotografie, z nichž nevyplývá, že byly pořízeny v rámci zpravodajské licence (například nezávislý divák by nepoznal, že fotografie byla pořízena na utkání, jelikož zobrazuje jen vzdáleně související tematiku) apod.
4. Pokud klub některé fotografie použije pro svou vlastní propagaci a tato fotografie bude obsahovat osobní údaj (podobu) osoby, je třeba si před použitím takové fotografie vyžádat souhlas subjektu údajů.
5. Nedoporučuje se bez souhlasu pořizovat fotografie zaměstnanců a ty užívat k propagační činnosti. V případě, že by klub chtěl bez souhlasu využít fotky svých zaměstnanců k propagační činnosti, je nutné tuto praktiku konzultovat.
6. Je možné zveřejňovat kontaktní údaje zaměstnanců v přiměřeném rozsahu. A to pouze u těch zaměstnanců, u kterých je to nutné z důvodu styku s veřejností. U ostatních zaměstnanců je třeba si ke zveřejnění jejich osobních údajů vyžádat souhlas.

9.4 Konkrétně k zabezpečení budov, místností a PC

1. Klub musí stále udržovat přehled o tom, jaké prostory, které spravuje, obsahují osobní údaje a kdo k těmto osobním údajům má přístup (tedy kdo má klíče například od kanceláře účetní).

2. Je třeba, aby pověřený pracovník (například tajemník spolku) vedl seznam držitelů klíčů od budov, místností a dalších prostor, kde se zpracovávají osobní údaje a tento seznam byl pravidelně aktualizován.
3. Náhradní klíč je nutné uložit bezpečným způsobem, zejména stanovit režim, kdy náhradní klíč může být vydán pouze na omezenou dobu předem stanovenému zaměstnanci (například paní účetní si zapomene doma klíče a pověřená osoba, například tajemník spolku, pouze jí vydá klíč od účtárny, a to na dobu jednoho dne, naopak pověřená osoba nevydá náhradní klíč například hráči, který by chtěl z nějakého důvodu vstoupit do účtárny apod.). Náhradní klíče je třeba uchovávat v zalepené a zapečetěné (např. podpisem přes lem obálky) obálce a v tomto stavu také musí být oprávněnou osobou navrácen (tedy paní účetní klíč od účtárny po tom, co získá své původní klíče, vloží do obálky, tu zalepí a pře její lem se podepíše, takto obálku předá oprávněné osobě). O každém vydání náhradního klíče a jeho navrácení je nutné vést záznam v k tomu určené knize, obsahující nejméně datum, čas, jméno oprávněné osoby a podpisy vydávajícího i přijímajícího.
4. Je třeba omezit přístup do prostor, kde se zpracovávají osobní údaje těm osobám, které tento přístup mít nemusí (například trenér nemusí mít klíč od kanceláře účetní).
5. Prostory, kde dochází ke zpracování osobních údajů, musí být zabezpečeny minimálně jednou linií zabezpečení (jeden zámek), některé osobní údaje musí být zabezpečeny dvěma liniemi ochrany (dva zámky – například místnost a kartotéka).
6. Vstupy do místností a kanceláří musí být osazeny spolehlivými zámky vyšší úrovně zabezpečení (tedy ne běžnými zámky od pochybných výrobců, ale například vyšší řadou zámků FAB).
7. Úklid v prostorách, kde dochází ke zpracování osobních údajů, musí být prováděn tak, aby byly osobní údaje co nejvíce chráněny (například pod dohledem zaměstnanců v pracovní době).
8. Počítače klubu musí být chráněny heslem splňujícím požadavky dle této směrnice, každý jednotlivý uživatel také musí mít své jedinečné uživatelské jméno. Je třeba nastavit parametry automatického odhlašování dle této směrnice. Do aplikací v rámci PC je třeba také stanovit jméno a heslo, které bude splňovat požadavky této směrnice.