
V souladu s ustanovením článku 3 odst. 18 stanov Českého svazu kanoistů, z.s. (ČSK) schválilo předsednictvo tuto

Bezpečnostní směrnici ČSK

Čl. I.

Úvodní ustanovení

1. Dne 27.4.2016 bylo přijato Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů-GDPR). Problematiky ochrany osobních údajů se dále dotýkají i jiné účinné právní předpisy, zejména zákon č. 110/2019Sb., o zpracování osobních údajů.
2. V rámci plnění povinností vyplývajících z právních předpisů uvedených v předchozím odstavci a v souladu s nimi byl pověřencem pro ochranu osobních údajů ČSK, společností GDPR Solutions, a.s. vypracován dokument obsahující bezpečnostní pravidla vztahující se k ochraně osobních údajů, tzv. bezpečnostní směrnice.

Čl. II.

Bezpečnostní směrnice

1. S odkazem na shora uvedené vydává předsednictvo ČSK Bezpečnostní směrnici nakládání s osobními údaji Českého svazu kanoistů, která tvoří přílohu tohoto vnitřního předpisu.
2. Bezpečnostní směrnice se vztahuje na zpracování osobních údajů v rámci veškeré činnosti ČSK a jeho jednotlivých sekcí a sportovních odvětví.

Čl. III.

Závěrečná ustanovení

Tato směrnice nabývá účinnosti dnem 16.4.2024 a v plném rozsahu nahrazuje veškeré předchozí vnitřní předpisy upravující problematiku, která je obsahem této směrnice.

Ing. Stanislav Ježek
předseda ČSK

Bezpečnostní směrnice nakládání s osobními údaji Českého svazu kanoistů
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)

1 ÚVOD DO PROBLEMATIKY OCHRANY OSOBNÍCH ÚDAJŮ	3
2 ZÁKLADNÍ POJMY	4
3 OBECNĚ K POVINNOSTI ZAJIŠTĚNÍ BEZPEČNOSTI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	5
4 ZÁKLADNÍ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	6
5 NAKLÁDÁNÍ S DOKUMENTY	7
5.1 DOKUMENTY V ELEKTRONICKÉ PODOBĚ	7
5.2 DOKUMENTY V PAPIROVÉ PODOBĚ	9
5.3 PORUŠENÍ OCHRANY DAT	9
5.4 LIKVIDACE OSOBNÍCH ÚDAJŮ	10
6 PRAVIDLA VYUŽÍVÁNÍ SÍTĚ INTERNET	10
6.1 ZÁKAZY PRO UŽIVATELE	10
7 VSTUPY DO BUDOV A KANCELÁŘÍ	10
8 BEZPEČNOSTNÍ INCIDENTY	11
8.1 POSTUP PŘI VZNIKU BEZPEČNOSTNÍCH INCIDENTŮ	11
9 JEDNOTLIVÉ AGENDY SPRÁVCE	11
9.1 ÚČETNÍ A MZDOVÁ AGENDA	11
9.2 ČLENOVÉ SVAZU A FYZICKÉ OSOBY	12
9.3 WEB A SOCIÁLNÍ SÍTĚ	13
9.4 KONKRÉTNĚ K ZABEZPEČENÍ BUDOV, MÍSTNOSTÍ A PC	13

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**“).

Nařízení 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, Nařízení 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 **Český svaz kanoistů**) zajistit a musí být také schopen doložit, že k zákonnému zpracování osobních údajů opravdu dochází.

Nařízení poskytuje lidem, kterým údaje patří (tj. subjektům údajů - např. zaměstnancům, závodníkům, 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.

Základní pojmy

1. Co je to Nařízení 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 kanoistou KK Slavia Praha, nejedná se o osobní údaj, neboť jej na základě této informace neidentifikujeme. Pokud ale známe jeho sportovní výsledky spolu s klubem, za který dotyčný závodí, lze kontrolou webového prohlížeče dohledat, o kterou osobu se konkrétně jedná. 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 Nařízení.

4. Kdo je to Správce a Zpracovatel osobních údajů?

Správce je subjekt, který rozhoduje o účelu a způsobu zpracování osobních údajů (např. **Český svaz kanoistů** ve vztahu k zaměstnancům, členům, závodníkům, 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 svaz, komu jsou předávány osobní údaje.

7. Co je to bezpečnostní incident?

Jakákoli 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.

Obecně k povinnosti zajištění bezpečnosti zpracování osobních údajů

Český svaz kanoistů (dále také „**svaz**“) musí zabezpečit osobní údaje po technické a organizační stránce, tj. organizačně v dokumentech určit např. přístupové role a stanovit technické prostředky k jejich zabezpečení, např.:

používat odpovídající technické zařízení a programové vybavení způsobem, který vyloučí neoprávněný či nahodilý přístup k osobním údajům ze strany jiných osob,

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,

zajistit dálkový přenos údajů buď pouze prostřednictvím veřejně nepřístupné sítě, nebo prostřednictvím zabezpečeného přenosu po veřejných sítích,

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.,

stanovit pravidla pro přístup k datům (hesla a role), zajistit logování tak, aby měl každý člen individuální přístup,

stanovit transparentní ujednání mezi svazem a jednotlivými sportovními kluby týkající se zpracování osobních údajů, stejně jako spolupracovat se zastřešující organizací co se týče ochrany osobních údajů (tedy např. s Českou unií sportu, z.s., dále také „**ČUS**“). K tomuto účelu svaz přijme novou směrnici o evidenci členské základny.

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).

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.

Skutečnosti v bodech 1 a 2 této kapitoly jsou stanoveny v záznamech o činnosti zpracování, kterými svaz také disponuje a které by měl pravidelně aktualizovat.

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 sportovce není pro svaz důležité. Svaz by proto „zbytečné“ osobní údaje neměl zpracovávat.

Je-li právním důvodem pro zpracování osobních údajů souhlas subjektu údajů, musí splňovat náležitosti dle Nařízení (před udělením souhlasu náležité informování a poučení mimo jiné i o možnosti odvolání souhlasu). To, že byl souhlas udělen musí být **Český svaz kanoistů** jakožto správce schopen kdykoliv prokázat (čl. 7 Nařízení).

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 je informační povinnost možné splnit prostřednictvím zveřejnění deklarace na webových stránkách nebo nástěnce svazu.

Je nezbytné zajistit právní titul k případnému předání osobních údajů mimo EU/EHS (např. konání soutěže v nečlenském státu).

Je nezbytné zajistit, aby osoby, které přistupují k osobním údajům, či je dále zpracovávají, dodržovaly tento vnitřní předpis.

Je třeba náležitě vyškolit zaměstnance svazu, kteří s osobními údaji nakládají.

V případě jakýchkoliv pochybností při konkrétních zpracováních je třeba se vždy poradit s odborníky.

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.

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.

Nakládání s dokumenty

Dokumenty v elektronické podobě

Elektronické dokumenty se nachází v paměti výpočetní techniky, tj. telefonů, tabletů, či počítačů, kterými svaz disponuje. 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
Symbody	` ~ ! @ # \$ % ^ & * () _ + - = { } [] \ : " ; ' < > ? , . /

- 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 by měla být po každé změně uložena do trezoru v zapečetěné obálce.

iii. Při krátkodobém opuštění PC aktivovat spořič obrazovky s heslem.

Zaměstnanci spolku **Českého svazu kanoistů** mají právo nahlížet do souborů obsahujících osobní údaje jen za předpokladu, že je to nezbytné k výkonu jejich pracovního zařazení.

Zaměstnanci mají právo **zpřístupňovat** dokumenty obsahující osobní údaje **třetím osobám** či subjektům jen za předpokladu, že mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, vnitřním předpisem svazu**, případně uloží-li jim takovou **povinnost vedoucí pracovník**.

Zaměstnanci **svazu** mají zakázáno ukládat osobní údaje do veřejně přístupných rozhraní, prohlížečů a databází, ledaže mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, vnitřním předpisem svazu**, případně uloží-li jim takovou **povinnost vedoucí pracovník**.

Osobní údaje je možné vkládat do předem připravených databází, které jsou k tomu určené nebo do vlastních (nesdílených) dokumentů, do kterých mají přístup jen sami pracovníci.

Zaměstnanci nemají bez výslovného povolení vedoucího pracovníka právo tisknout osobní údaje obsažené ve sdílených databázích.

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.

Registrační a jiné informační systémy, které svaz spravuje a do kterých mají přístup fyzické osoby, nebo jednotliví členové svazu (sportovní kluby) musí být spravovány s nejvyšším zřetelem na ochranu osobních údajů v nich obsažených.

Dokumenty v papírové podobě

1. Listiny obsahující jakékoli osobní údaje (např. zápisy o závodu, 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**.

Zaměstnanci, kteří mají uložené listiny s osobními údaji v neuzamčené skříně dle bodu 1. jsou povinni uzamykat kancelář pokaždé, když ji opouští.

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.

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.

Zaměstnanci mají právo **nahlížet** do dokumentů obsahujících osobní údaje jen za předpokladu, že je to **nezbytné** k výkonu jejich pracovního zařazení.

Zaměstnanci mají právo **zpřístupňovat** dokumenty obsahující osobní údaje **třetím osobám** či subjektům jen za předpokladu, že mají takovou povinnost uloženou **právním předpisem, rozhodnutím příslušného orgánu, vnitřním předpisem svazu**, případně uloží-li jim takovou **povinnost vedoucí pracovník**.

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.

Porušení ochrany dat

1. **Český svaz kanoistů** 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.

Každý zaměstnanec **svazu** je povinen o jakémkoli podezření o úniku osobních údajů informovat pověřence GDPR (kontakt: kmare@gdprolutions.cz, tel. 608 311 933).

Likvidace osobních údajů

Ve chvíli, kdy opadne poslední oprávněný zájem pro zpracovávání osobních údajů, je nutné tyto údaje zlikvidovat. V případě přepisovatelných médií lze údaj vymazat, v případě nepřepisovatelných médií 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).

Pravidla využívání sítě Internet

1. Zaměstnanci a členové svazu 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.

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,
poskytnout služební identifikační prostředky využívané při práci s informačními technologiemi prostřednictvím Internetu (např. heslo) cizí osobě,
stahovat z Internetu nelegální software,
svévolně instalovat jakýkoli software, včetně různých plug-in modulů na pracovní stanici uživatele,
svévolně měnit nastavení programů umožňujících komunikaci s Internetem,
poskytnout neautorizovanému subjektu přístup ke službám Internetu ze služebních počítačů,
posílat informace s osobními údaji v otevřeném tvaru elektronickou poštou,
posílat informace s osobními údaji osobní elektronickou poštou,
připojovat se z pracovních stanic na privátní internetové účty,
jakýmkoli způsobem provádět vyhledávání, monitorování a zjišťování stavu portů na serverech svazového informačního systému.

Vstupy do budov a kanceláří

1. Zaměstnanec nemá povoleno umožnit vstup do budovy (resp. prostoru využívaném **svazem**) 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.

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.:
neoprávněný přístup do informačních systémů a úložišť,
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 Pověřenci pro ochranu osobních údajů na emailové adrese kmares@gdpr solutions.cz

Postup při vzniku bezpečnostních incidentů

1. Po zjištění vzniku bezpečnostního incidentu zaměstnanec informuje Pověřence pro ochranu osobních údajů na emailové adrese kmares@gdpr solutions.cz. 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 Pověřence pro ochranu osobních údajů na emailové adrese kmares@gdpr solutions.cz, případně do 72 hodin i dozorový úřad.

Jednotlivé agendy správce

Účetní a mzdová agenda

1. **Český svaz kanoistů** 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 řeší **Český svaz kanoistů** externě, konkrétně ji zajišťuje Česká unie sportu. Je nutné, aby byly dotčené subjekty údajů dostatečně obeznámeny, že jsou jejich osobní údaje předávány zpracovateli a že jsou zajištěny veškeré bezpečnostní náležitosti.
3. Při předávání osobních údajů subjektu externímu subjektu je třeba, aby předání probíhalo přes důvěryhodný kanál (například internetovou aplikaci apod.).
4. K náboru nových zaměstnanců je možné využít externí subjekt (např. agenturu práce), je však nutné uzavřít s tímto externím subjektem takovou smlouvu, aby pokrývala všechny požadavky, které na ochranu a nakládání s osobními údaji stanovuje Nařízení.
5. Při náboru nových zaměstnanců je třeba bez souhlasu **ne** uchovávat životopisy nebo jiné dokumenty těch uchazečů, kteří nebyli přijati do pracovního či obdobného poměru (tedy je třeba smazat životopis neúspěšného kandidáta).
6. 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.

Členové svazu a fyzické osoby

1. **Český svaz kanoistů** registruje své členy na základě přihlášky podané příslušným oddílem. Není tedy možné, aby se členem stala fyzická osoba, který zároveň není registrována v některém z oddílů. Svaz v rámci přihlášky požaduje pouze ty osobní údaje, které jsou nezbytné k výkonu činnosti svazu a které si svaz dopředu stanovil spolu s účely pro jejich zpracování. Účely, pro které jsou svazu předávány osobní údaje fyzických osob jsou zejména: účetní, personální a mzdová agenda, registrace členů, přihlašování na závody a výsledkový servis, zajištění pojištění, žádosti o dotace, činnost Sportovních center mládeže a Sportovních středisek mládeže, informování veřejnosti o činnosti svazu a propagace svazu.
2. V rámci rozdělení svazu na jednotlivé sekce je postup při registraci nových členů svazu a přihlašování členů na závody, resp. vyhlášení výsledku, odlišný.
3. V sekci divoká voda je využíván Registrační výsledkový portál (dále také jako „RVP“), který spravuje externí společnost na základě smlouvy. Jednotlivé členy zde registrují samotné oddíly, bez nutnosti zásahu svazu, a to pouze skrze RVP v elektronické podobě. Zde je nutné zmínit, že pouze dva pověření zaměstnanci svazu mají možnost vidět veškeré údaje vložené do RVP. Jednotliví závodníci a kluby vidí pouze jméno, příjmení, datum narození a oddíl ostatních sportovců. Přihlašování sportovců na mezinárodní závody pak už probíhá přes svaz, kdy je nutné vyplnit tzv. evidenční list člena reprezentačního družstva. Výsledky z jednotlivých soutěží jsou zveřejněny na RVP a webových stránkách svazu, potažmo na sociálních sítích.
4. V rámci sekce rychlostní kanoistika a vodní turistika je používán jiný registrační systém, který je také vytvořen a spravován externím subjektem. Registrace vztahující se k sekci rychlostní kanoistika mají na starost dvě osoby, zatímco registraci nových členů u vodní turistiky má v gesci pouze jedna. Je nutné, aby tyto osoby byly dostatečně obeznámeny s bezpečnostními opatřeními, které se pojí k práci s osobními údaji. Registrace se uskutečňují na základě písemných dokumentů zaslaných jednotlivými oddíly. Informace v nich obsažené poté pracovníci svazu zadají do registračního systému. Přístup třetím osobám do tohoto rozhraní je podmíněn souhlasem odpovědných pracovníků svazu. Při prvotním přihlášení se členům zobrazí mj. i zaškrťovací políčko se souhlasem o zpracování osobních údajů. Odlišný je také přihlašovací a výsledkový systém, kdy sekce rychlostní kanoistiky spolupracuje s externím subjektem, který systém spravuje a skrze který se výsledky také zveřejňují. U vodní turistiky zajišťuje obě činnosti pořadatelé závodů, a to vždy prostřednictvím totožného softwaru.
5. Informační povinnost fyzickým osobám je realizována před podáním přihlášky. Svaz ale musí být připraven v případě potřeby fyzické osobě také na její žádost poskytnout informace o zpracování jejich osobních údajů i při již probíhajícím zpracování.
6. Informace o fyzických osobách je třeba uchovávat tak, aby byly chráněny dvěma liniemi zabezpečení, tzn. uchovávat dokumenty v uzamykatelném prostoru v uzamykatelné místnosti.
7. Informace o fyzických osobách v elektronické podobě je třeba dostatečně chránit tak, aby k nim neměla přístup nepověřená osoba.

8. **Český svaz kanoistů** předává osobní údaje subjektů osobních údajů České unii sportu (zkráceně ČUS, Českému olympijskému výboru (zkráceně ČOV), Mezinárodní kanoistické federaci (dále také jako „ISF“) a příslušným orgánům státní správy a samosprávy. Při účasti na zahraničních soutěžích dochází k předání osobních údajů v nezbytné míře jejich organizátorům či ISF, v případě vízové povinnosti úřadům daných zemí a u zajištění pojištění pro členy výpravy dochází k předání informací jednotlivým pojišťovnám. O možném předávání osobních údajů je třeba subjekt údajů informovat, např. deklarací na webových stránkách svazu.

Web a sociální sítě

1. Svazový web je místo, na kterém se veřejnost i členové svazu a jednotlivé kluby mohou dozvědět zásadní informace o činnosti svazu, včetně některých osobních údajů. Proto je třeba přistupovat obezřetně k obsahu, který bude (a je) na webových stránkách či sociálních sítích svazu zveřejňován.
2. Je třeba postavit najisto, kdo spravuje který nástroj svazové propagace v daném čase, to znamená, že svaz si musí zejména:
 - i. ujasnit, 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 svazu 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. přibližné 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 svaz 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 svaz 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.

Konkrétně k zabezpečení budov, místností a PC

1. Svaz musí stále udržovat přehled o tom, jaké prostory, které spravuje, obsahují osobní údaje a kdo k těmto osobním údajům má přístup (tedy kdo má přístup do kanceláří svazu).
2. Je třeba, aby pověřený pracovník 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. 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. 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.
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 uzamykatelná místnost a uzamykatelná kartotéka).
6. Vstupy do místností a kanceláří musí být osazeny spolehlivými zámky vyšší úrovně zabezpečení (například veškeré dokumenty obsahující osobní údaje musí být umístěny v uzamčených skříních).
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 svazu 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.

Zásady zpracování osobních údajů v rámci ČSK

A) Obecná ustanovení:

1. Zásady zpracování osobních údajů v rámci ČSK (dále jen Zásady) zavazují všechny sportovní sekce ČSK, členské oddíly / kluby, rozhodčí, trenéry, funkcionáře, sportovce a další členy ČSK (dále společně jen „členové“).
2. Zásady se vztahují na chování během soutěží, závodů, výkonů funkcí, zaměstnaneckých poměrů a veškerého ostatního chování spojeného s činností ČSK.
3. Zásady jsou součástí Bezpečnostní směrnice nakládání s osobními údaji ČSK.
4. Osobním údajem se myslí jakýkoliv údaj, na jehož základě je samo o sobě nebo ve spojení s dalším údajem možné identifikovat konkrétní osobu.

B) Pravidla nakládání s osobními údaji pro členy ČSK:

Členové jsou v rámci činnosti ČSK povinni dodržovat zejména níže uvedené postupy:

- požadovat pouze osobní údaje v rozsahu nezbytném pro daný účel zpracování
- nepředávat a nezveřejňovat osobní údaje třetím osobám, jestliže k tomu nejsou zmocněni či to nevyplývá z povahy jejich činnosti
- pokud se některý z členů dozví o skutečnosti, která by mohla narušit bezpečnost osobních údajů, neprodleně ji nahlásí pověřenci GDPR (kontakt: kmares@gdprsolutions.cz, tel. 608 311 933)
- poskytovat ČSK pouze své aktuální osobní údaje hlásit změny
- neponechávat své doklady, které obsahují osobní údaje, bez dozoru na místech přístupných jiným členům či třetím osobám tak, aby zamezili jejich případnému odcizení či zneužití,
- pokud některý z členů nalezne dokument s osobními údaji, odevzdá jej odpovědné osobě; jestliže si vlastník dokumentu na výzvu tento nevyzvedne, bude tento dokument zničen