Český olympijský výbor

Obecná směrnice o zpracování osobních údajů

SHRNUTÍ

Účelem této Obecné směrnice o zpracování osobních údajů („**Směrnice**") je stanovení rámcových pravidel pro nakládání s osobními údaji a s dokumenty obsahujícími tyto osobní údaje. Součástí Směrnice je také obecný návod, jak jednat v souladu s organizačně-technickými a dalšími opatřeními směřujícími k dodržení platných a účinných právních předpisů na ochranu osobních údajů zavedenými v Českém olympijském výboru („**ČOV**") a spřízněných entitách v rámci českého olympijského hnutí.

Směrnice mezi jinými obecně určuje účel a rozsah shromažďování a zpracování osobních údajů, prostředky a způsob jejich zpracování, jakož i práva a povinnosti osob ve vztahu k těmto údajům a zacházení s nimi. Chránit osobní údaje je povinností jak ČOV, tak i každého jeho pracovníka, zaměstnance či jiné osoby vykonávající úkoly pro ČOV („**pracovníci**"). Konkrétní pravidla související s dílčími druhy zpracování osobních údajů (jako zpracování zaměstnaneckých dat, dat členů Českého olympijského týmu, dat sportovců z řad veřejnosti, zpracování prostřednictvím kamerového systému apod.) obsahují dílčí vnitřní dokumenty ČOV, na které tato Směrnice odkazuje.

ZÁKLADNÍ PRINCIPY

ČOV a všichni jeho pracovníci jsou při nakládání s osobními údaji povinni dodržovat obecné nařízení o ochraně osobních údajů (EU) 2016/679 a související právní předpisy upravující zpracování osobních údajů. Tyto právní předpisy stanoví hlavní pravidla a zásady, kterými je potřeba se při zpracování osobních údajů řídit, a ČOV tyto zásady přebírá.

ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. **Zákonnost, korektnost a transparentnost**: Veškeré osobní údaje zpracovávané ČOV musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem;
2. **Účelové omezení:** Osobní údaje lze shromažďovat pouze pro určité, výslovně vyjádřené a legitimní účely a tyto údaje nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný;
3. **Minimalizace údajů**: Osobní údaje lze zpracovávat pouze v rozsahu nezbytném pro naplnění stanoveného účelu;
4. **Přesnost:** Zpracovávat lze pouze přesné a v případě potřeby aktualizované osobní údaje; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny;
5. **Omezení uložení:** Uchovávat osobní údaje ve formě umožňující identifikaci subjektů údajů lze pouze po dobu ne delší, než je nezbytné pro účely zpracování;
6. **Integrita a důvěrnost:** Osobní údaje lze zpracovávat pouze způsobem, který zajistí náležitou ochranu osobních údajů pomocí vhodných technických nebo organizačních opatření, a to před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením;
7. **Odpovědnost:** Dodržení výše uvedených zásad včetně souladu s platnými a účinnými právními předpisy na ochranu osobních údajů musí být ČOV schopen doložit;
8. **Přístup založený na míře rizika** (tzv. Risk Based Approach): Čím větší je riziko, že daný druh zpracování prováděný ČOV může zasahovat do zájmů či základních práv a svobod subjektu údajů, tím vyšší opatření vedoucí k transparentnosti a bezpečnosti daného zpracování je třeba přijmout.

Není-li si daný pracovník, který nakládá s osobními údaji, jistý, jaké riziko je s daným zpracováním spojeno, či jaké konkrétní povinnosti se na něj v souvislosti se zpracováním osobních údajů vztahují, obrátí se na osobu odpovědnou za zpracování osobních údajů v rámci ČOV.

KONKRÉTNÍ PRAVIDLA

1. PŮSOBNOST

1.1 Směrnice je interním normativním předpisem, který zavazuje všechny pracovníky i osoby spolupracující s ČOV, jakož i další osoby, jež podléhají interním předpisům ČOV, stejně jako osoby, jež se k dodržování této Směrnice zavázaly v rámci smluvního vztahu s ČOV, nebo se zpracovatelem.

1.2 Směrnice je také závazná pro všechny pracovníky entit v rámci českého olympijského hnutí spřízněných s ČOV, zejména pak pro pracovníky společností Česká olympijská a.s., Olympic Festival s.r.o. a dalších osob, které ji přijmou jako svou interní směrnici kdykoliv v budoucnu („**Spřízněné osoby**"). ČOV zajistí, že Spřízněné osoby Směrnici přijmou k tomu oprávněnými orgány a s jejím zněním seznámí své pracovníky.

1.3 ČOV je povinen zajistit, aby se osoby, které zpracovávají osobní údaje na základě smlouvy s ČOV, zavázaly dodržovat ustanovení této Směrnice.

2. ZÁKLADNÍ POJMY

Osoby nakládající s osobními údaji a subjekt údajů

(a) **Správce:** Subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů nebo kterému povinnost zpracovávat osobní údaje ukládají platné a účinné právní předpisy; za správce se pro účely této Směrnice považuje ČOV;

(b) **Zpracovatel:** Osoba (fyzická nebo právnická), která zpracovává osobní údaje pro správce;

(c) **Subjekt údajů:** Identifikovaná nebo identifikovatelná fyzická osoba (nikoliv osoba právnická – společnost nebo organizace).

Osobní údaje a jejich druhy

(d) **Osobní údaje:** Veškeré informace o fyzické osobě (subjekt údajů), kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, datum narození, identifikační číslo, adresné a kontaktní údaje, lokační údaje nebo síťový identifikátor. Za osobní údaje se považují i data, která se sama o sobě netýkají fyzické osoby, ale ve spojení s jinými informacemi by již bylo možné tato data přiřadit (i jen potenciálně) ke konkrétní fyzické osobě;

(e) **Zvláštní kategorie osobních údajů:** Osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby; zvláštní ochrany požívají údaje týkající se odsouzení za trestné činy;

(f) **Biometrické údaje:** Osobní údaje vyplývající z fyzických či fyziologických znaků člověka jako např. zobrazení obličeje, údaje o otiscích prstů apod.;

(g) **Anonymní údaj:** Takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů – nejedná se tedy o osobní údaj.

Zpracování osobních údajů

(h) **Zpracování osobních údajů:** Jakákoliv operace s osobními údaji jako např. shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, seřazení, zpřístupnění, ale i výmaz nebo zničení;

(i) **Shromažďování osobních údajů:** Systematický postup, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování;

(j) **Uchovávání osobních údajů:** Udržování údajů v takové podobě, která je umožňuje dále zpracovávat;

(k) **Likvidace osobních údajů:** Fyzické zničení jejich nosiče, jejich fyzické vymazání nebo trvalé vyloučení z dalších zpracování; formou likvidace osobních údajů je i **anonymizace**;

(l) **Anonymizace:** Činnost, při které dojde k trvalému smazání či rozpojení identifikátorů, pomocí kterých je možné ztotožnit konkrétní fyzickou osobu;

(m) **Pseudonymizace:** Zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně; po opětovném přiřazení dodatečných informací je možné konkrétní fyzickou osobu opětovně identifikovat;

(n) **Profilování:** Automatizované zpracování spočívající v použití osobních údajů k hodnocení, rozboru či odhadu některých osobních aspektů fyzické osoby týkajících se např. pracovního výkonu, ekonomické situace, osobních preferencí, zájmů, chování, místa, kde se nachází apod.

Další

(o) **Nařízení, nebo GDPR:** 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);

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

3. ODPOVĚDNÁ OSOBA

3.1 ČOV nejmenoval pověřence pro ochranu osobních údajů, neboť neprovádí zpracování, jehož hlavní činnost spočívá v operacích, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé, pravidelné a systematické monitorování subjektů údajů anebo v operacích spočívajících v rozsáhlém zpracování zvláštních kategorií osobních údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

3.2 Osobou odpovědnou za dohled nad dodržováním ochrany osobních údajů dle platných a účinných právních předpisů a dle této Směrnice je pracovník na pozici Právník ČOV („**Odpovědná osoba**").

3.3 Odpovědná osoba je hlavním garantem dodržování Nařízení a této Směrnice ze strany pracovníků ČOV, jakož i dalších osob uvedených v *článku 1.1*.

3.4 Odpovědná osoba musí být vedením Správce, jakož i pracovníky Správce konzultována ve všech zásadních otázkách týkajících se zpracování a/nebo ochrany osobních údajů.

3.5 Odpovědná osoba komunikuje a spolupracuje jménem ČOV s Úřadem pro ochranu osobních údajů („**Úřad**") a zejména zajišťuje jménem ČOV veškerá příslušná podání k tomuto Úřadu. Především se jedná o předchozí konzultaci dle čl. 36 Nařízení a předávání osobních údajů do zahraničí podle čl. 44 a násl. Nařízení.

3.6 Odpovědná osoba je odpovědná za aktuálnost a správnost záznamů o zpracování osobních údajů tvořících *přílohu č. 3* této Směrnice a za dodržování a aktualizaci Zásad zabezpečení osobních údajů tvořících *přílohu č. 1* této Směrnice, které připravuje vždy s ohledem na posouzení rizik souvisejících se zpracováním osobních údajů podle čl. 32 Nařízení.

3.7 Osoby vázané touto Směrnicí jsou povinny Odpovědnou osobu informovat o veškerých skutečnostech, které mohou být významné pro ochranu osobních údajů ze strany ČOV.

3.8 Odpovědná osoba plní i další povinnosti stanovené jí touto Směrnicí.

4. ÚČEL A ROZSAH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

4.1 Osoby vázané touto Směrnicí jsou oprávněny shromažďovat a zpracovávat osobní údaje či tyto osobní údaje předat dalším osobám pouze za účelem a způsobem stanoveným ve vnitřních dokumentech ČOV nebo dle pokynu či upřesnění Odpovědné osoby.

4.2 Osobní údaje smí být předány pouze těm dalším osobám, které zmiňují vnitřní dokumenty ČOV, nebo pokud předání těmto osobám bylo povoleno Odpovědnou osobou (s výjimkou předání nebo zpřístupnění příslušným státním orgánům a dalším osobám, jež upravují zvláštní právní předpisy – např. Policie ČR). Totéž platí i pro předání osobních údajů do zahraničí.

4.3 Osoby vázané touto Směrnicí se řídí platným retenčním plánem, který tvoří *přílohu č. 4* této Směrnice a neuchovávají osobní údaje v rozporu s tímto retenčním plánem nebo v rozporu s principem omezení uložení či touto Směrnicí. Po uplynutí doby stanovené v retenčním plánu či po zániku účelu, pro který byla osobní data uchovávána, je třeba provést likvidaci osobních údajů v souladu s vnitřními dokumenty ČOV či pokyny Odpovědné osoby.

5. PROSTŘEDKY A ZPŮSOB ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

5.1 Při zpracování osobních údajů je třeba volit prostředky, které jsou přiměřené z hlediska účelu zpracování. Je nutné postupovat tak, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také je třeba dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

5.2 Vnitřní dokument ČOV (např. Zásady zpracování osobních údajů) stanoví, zda mohou pracovníci zpracovávat osobní údaje subjektů údajů bez souhlasu těchto subjektů údajů, či pouze na základě jejich souhlasu.

5.3 V případech, kdy je možné zpracovávat osobní údaje pouze na základě souhlasu subjektů údajů, vnitřní dokument ČOV či Odpovědná osoba stanoví text souhlasu, který bude poskytován subjektům údajů před získáním osobních údajů či jiným zahájením jejich zpracování.

5.4 V případech, kdy je možné zpracovávat osobní údaje i bez souhlasu subjektů údajů, vnitřní dokument ČOV či Odpovědná osoba stanoví, jaké informace a poučení musí být subjektům údajů poskytnuty (buďto formou písemného dokumentu, informace podané elektronickou formou, nebo ústně) před získáním osobních údajů či jiným zahájením jejich zpracování.

5.5 Osoby vázané touto Směrnicí smí zpracovávat osobní údaje pouze ve formě stanovené vnitřními dokumenty ČOV či dle pokynu Odpovědné osoby. Fyzické dokumenty obsahující osobní údaje smí být uchovávány a zpracovávány pouze v rámci prostor ČOV nebo akcí organizovaných ČOV, a to na předem určených místech pro jejich uchování či manipulaci. Elektronické dokumenty smí být zpracovávány pouze prostřednictvím předem určených systémů, přičemž manipulace s osobními údaji v rámci systémů je ze strany ČOV logována, což umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány.

5.6 Veškeré osobní údaje či dokumenty obsahující osobní údaje musí být zpracovávány v souladu se Zásadami zabezpečení osobních údajů uvedenými v *příloze č. 1*, nebo ve zvláštních vnitřních dokumentech ČOV.

6. PRÁVA SUBJEKTŮ ÚDAJŮ

6.1 Podle GDPR mají subjekty údajů možnost využít svého práva požadovat po ČOV:

(i) přístup ke svým osobním údajům;

(ii) opravu osobních údajů;

(iii) výmaz osobních údajů;

(iv) omezení zpracování údajů týkajících se subjektu údajů;

(v) právo vznést námitku proti zpracování; a

(vi) právo na přenositelnost údajů.

6.2 Pokud kterákoliv osoba vázána touto Směrnicí obdrží žádost související s uplatněním práva subjektů údajů podle článku 6.1(i), bude postupovat podle článku 7; v ostatních případech postoupí žádost Odpovědné osobě.

7. POUČOVACÍ A INFORMAČNÍ POVINNOST, PRÁVO NA PŘÍSTUP K ÚDAJŮM

7.1 V případě, kdy ČOV získal osobní údaje od subjektu údajů, je povinen jej poučit ve smyslu čl. 13 GDPR. Za tím účelem zajistí, aby se subjekt údajů řádně seznámil s obsahem poučení a aby subjekt údajů tuto skutečnost stvrdil svým podpisem či jiným prokazatelným projevem vůle.

7.2 V případě, že osobní údaje nebyly získány od subjektu údajů, je ČOV povinen jej poučit ve smyslu čl. 14 GDPR. Za tímto účelem zajistí, aby se subjekt údajů řádně seznámil s obsahem poučení a aby subjekt údajů tuto skutečnost stvrdil svým podpisem či jiným prokazatelným projevem vůle.

7.3 Informace uvedené v *článku 7.1* poskytne Správce subjektu údajů nejpozději v okamžiku získání osobních údajů a informace uvedené v *článku 7.2* poskytne ČOV subjektu údajů v přiměřené lhůtě po získání osobních údajů, ale nejpozději do 30 dnů. V případech, kdy mají být osobní údaje použity pro účely komunikace, poskytne tyto informace v okamžiku, kdy poprvé dojde k této komunikaci, anebo pokud mají být osobní údaje zpřístupněny jinému příjemci, poskytne ČOV informace při prvním zpřístupnění osobních údajů.

7.4 Uplatní-li subjekt údajů právo na přístup ke svým osobním údajům dle čl. 15 GDPR, je mu ČOV povinen tuto informaci předat bez zbytečného odkladu, ale nejpozději do 30 dnů ode dne doručení žádosti. Informace jsou poskytnuty zásadně ve formě, ve které subjekt údajů uplatňuje své právo.

7.5 ČOV je povinen před sdělením informací o zpracování v rámci uplatněného práva na přístup ze strany subjektu údajů ověřit identitu dotazujícího se subjektu údajů. K ověření identity subjektu údajů, který žádá o přístup k osobním údajům, využije ČOV všech vhodných opatření. Není-li ČOV schopen dostatečně identifikovat subjekt údajů, informuje ho o této skutečnosti, pokud je to možné. Ověřování identity není zneužíváno k získávání dalších údajů a k jejich uchování za jinými účely než je reakce na konkrétní žádost subjektu údajů.

7.6 Obsahem informace uvedené v *článku 7.4* je sdělení o:

(a) účelu zpracování osobních údajů,

(b) osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování,

(c) příjemci, případně kategoriích příjemců,

(d) době, po kterou budou osobní údaje uloženy,

(e) existenci práva požadovat od ČOV opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování,

(f) právu podat stížnost u Úřadu pro ochranu osobních údajů,

(g) veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány

od subjektu údajů, a

(h) skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování a v těchto případech smysluplné informace týkající se použitého postupu, jakož i sdělení o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů.

7.7 Informace dle článku 7.6 je poskytována v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

8. ZAPOJENÍ ZPRACOVATELE OSOBNÍCH ÚDAJŮ

8.1 ČOV může zpracováním osobních údajů pověřit třetí osobu (zpracovatele), která poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření, aby byla zajištěna ochrana práv subjektů údajů.

8.2 Pověření dle předchozího odstavce lze udělit pouze v rámci smlouvy o zpracování osobních údajů, která musí mít písemnou formu.

8.3 Vzor smlouvy o zpracování osobních údajů je uveden v *příloze č. 2*. Jakékoliv odchylky od přiložené vzorové smlouvy musí být před podpisem takové smlouvy konzultovány s Odpovědnou osobou.

9. OPRÁVNĚNÉ OSOBY A ROZSAH OPRÁVNĚNÍ

9.1 Konkrétním pracovníkům jsou přiděleny role, v rámci kterých smí tito pracovníci přistupovat a nakládat s konkrétními osobními údaji pro konkrétní účely.

9.2 Nikdo nesmí nakládat s osobními údaji nad rámec svého oprávnění, jak je vymezeno v popisu jednotlivých rolí a zařazení konkrétních pracovníků k těmto jednotlivým rolím.

9.3 Individuální výjimky z výše uvedených pravidel může výslovně udělit Odpovědná osoba.

10. POVINNOST MLČENLIVOSTI

10.1 Všechny osoby, které zpracovávají osobní údaje pro Správce, jakož i další osoby, které přijdou do styku s osobními údaji u Správce nebo zpracovatele, jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních přijatých podle této Směrnice či jiných vnitřních dokumentů ČOV. Povinnost mlčenlivosti trvá i po skončení příslušných prací.

11. PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

11.1 Jakýkoliv případ porušení zabezpečení osobních údajů, zejména ztrátu, odcizení, poškození či zničení osobních údajů (bez ohledu na riziko zásahu do práv subjektů údajů související s konkrétním případem porušení zabezpečení osobních údajů) je každá osoba, která se o takové skutečnosti dozví, povinna neprodleně oznámit svému nadřízenému a současně i Odpovědné osobě.

11.2 Osoby vázané touto Směrnicí jsou povinny hlásit ve smyslu předchozího odstavce i potenciální hrozby porušení zabezpečení osobních údajů, pokud se o nich dozví.

11.3 V rámci tohoto hlášení uvede osoba, která se dozví o případu porušení zabezpečení osobních údajů nebo pouhé hrozbě, především:

(a) co nejúplnější a nejpřesnější popis povahy daného případu porušení zabezpečení osobních údajů nebo hrozby, včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

(b) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

(c) návrh možných opatření s cílem vyřešit dané porušení zabezpečení osobních údajů, příp. předejít dané hrozbě, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

11.4 Osoby vázané touto Směrnicí poskytnou veškerou svoji součinnost k usnadnění přijetí opatření, které zvolil ČOV v reakci na případ porušení zabezpečení osobních údajů nebo hrozbu.

12. SOUČINNOST

12.1 V případě, že bude nutné za účelem zajištění souladu s GDPR upravit některé stávající procesy či v současnosti prováděné operace a činnosti zahrnující shromažďování a zpracovávání osobních údajů nebo za účelem vypracování posouzení vlivu na ochranu osobních údajů, jsou osoby, na které se vztahuje tato Směrnice, povinny poskytnout nezbytnou součinnost a spolupracovat s Odpovědnou osobou.

13. SOUČINNOST

13.1 Tato Směrnice nabývá platnosti a účinnosti okamžikem schválení Výkonným výborem ČOV dne: 11. 12. 2018

Seznam příloh:

Příloha č. 1 – Zásady zabezpečení osobních údajů

Příloha č. 2 – Vzor smlouvy o zpracování osobních údajů

Příloha č. 3 – Datová mapa

Jiří Kejval

předseda ČOV

Příloha č. 1 - Zásady zabezpečení osobních údajů

A. Pravidla týkající se technického zabezpečení dat

i) Osobní údaje obsažené v elektronické formě na datovém nosiči informací musí být uloženy buď na samostatných datových nosičích umístěných v uzamykatelných skříních, a/nebo místnostech přístupných pouze osobám s patřičným pověřením anebo na serveru, k němuž mají fyzický přístup pouze tyto osoby. Tento server musí být umístěn v uzamykatelné skříni a zamykatelné místnosti.

ii) Pokud jsou osobní údaje uloženy na serverech poskytovatelů cloudových služeb (např. OneDrive, Disk Google apod.), považuje se takový poskytovatel cloudových služeb za zpracovatele osobních údajů.

iii) Server, na kterém jsou data obsahující osobní údaje uložena, musí být chráněn proti útoku z internetu firewallem a antivirovým systémem či obdobnými zabezpečovacími prostředky.

iv) Datové soubory musí být šifrovány zejména v následujících případech:

- při zpracování osobních údajů na přenosných zařízeních – notebook, mobil, tablet;
- v souvislosti s posíláním osobních údajů přes internet a zejména ve veřejné Wi-Fi síti;
- uchování dat na serveru.

v) Systém musí pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány.

vi) Datové soubory obsahující osobní údaje, jejichž ztráta nebo změna by mohly mít negativní důsledky pro subjekty údajů, musejí být pravidelně, alespoň jednou za dva týdny, zálohovány, resp. zálohy se v pravidelných, maximálně dvoutýdenních, intervalech přepisují. ČOV může stanovit častější frekvenci zálohování v případech, kdy by ztráta nebo změna osobních údajů znamenala zvýšené riziko.

vii) Zálohy jsou šifrovány zejména v následujících případech:

- při uchování dat na serverech.

viii) Zálohy jsou testovány alespoň jednou za dva týdny.

ix) Pracovníci jsou zejména povinni:

(1) nezanechávat systémy, včetně přenosných zařízení obsahujících osobní údaje, bez dozoru, pokud nejsou zabezpečeny v uzamčené místnosti;

(2) používat příslušná bezpečná hesla pro přihlášení do systémů nebo databází obsahujících osobní údaje, zajistit, aby tato hesla zůstala důvěrná a tato hesla průběžně měnit;

(3) nesdělovat hesla a vstupní údaje jiným osobám nebo poskytnout přístup prostřednictvím svých přihlašovacích oprávnění do systému;

(4) dodržovat vždy standardní postupy pro odhlášení ze systémů. Nesprávným odhlášením může vzniknout příležitost ke zneužití pod identitou uživatele;

(5) nepoužívat sdílené účty.

x) Za účelem zajištění ochrany musí informační systémy používané v ČOV zajišťovat alespoň tyto bezpečnostní funkce:

(1) zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením. Zaznamenává se zejména použití identifikačních a autentizačních informací, pokusy o zkoumání přístupových práv, vytváření nebo rušení objektu informačního systému nebo činnost autorizovaných subjektů informačního systému ovlivňující bezpečnost informačního systému;

(2) možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele, bezpečnostního správce nebo správce informačního systému;

(3) ošetření paměťových objektů (médií) před jejich dalším použitím, zejména před přidělením jinému subjektu informačního systému, které znemožní zjistit jejich předchozí obsah;

(4) ochranu důvěrnosti dat během přenosu mezi zdrojem a cílem a jejich integritu;

(5) možnost šifrování osobních údajů

(6) schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; a

(7) možnost pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

xi) Za elektronickou ochranu osobních údajů odpovídá systémový administrátor, jehož pověřuje ČOV („**Systémový administrátor**").

xii) V případě opravy informačního systému je třeba zajistit, že osoby, které budou tuto opravu provádět, jsou důvěryhodné a budou vázány povinností mlčenlivosti ve smyslu článku 10, a to pod hrozbou smluvní pokuty.

xiii) Bezpečnost a funkcionalita všech systémů musí být průběžně testovány a vyhodnocovány. Aplikace napojené na internet musí být testovány alespoň v intervalu dvou týdnů.

B. Pravidla pro předávání souborů obsahujících osobní údaje mimo ČOV

Osobní údaje musí být při přenosu nebo při jejich uložení na přenosná zařízení šifrovány nebo pseudonymizovány.

C. Access Management

K přístupu k datovým souborům jsou oprávněny pouze osoby k tomu pověřené, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby, a to v rozsahu jejich oprávnění tam specifikovaných.

Do příslušných databází a systémů, včetně fyzických verzí, mají přístup jen ti uživatelé, kteří je při výkonu své práce potřebují, přičemž přístupová oprávnění jsou definována dle funkcí. Každý uživatel může do systémů přistupovat pouze pod svým unikátním ID a přístupové údaje nesmí sdílet s dalšími uživateli. O udělení přístupu jakýchkoli třetích osob do systémů ČOV rozhoduje příslušný vedoucí pracovník ČOV.

Přístupová oprávnění k příslušným databázím a systémům jsou pravidelně přezkoumávána tak, aby účty uživatelů byly včas přidány, upraveny a smazány, aby se snížilo riziko neoprávněného a nevhodného přístupu k osobním údajům.

D. Postup v případě odchodu zaměstnance

V případě odchodu zaměstnance je ČOV povinen bez zbytečného odkladu informovat Systémového administrátora, který zruší přístupy zaměstnance do jednotlivých systémů.

Příloha č. 2. – Vzor smlouvy o zpracování osobních údajů

ČOV_Vzorová
smlouva o zpracován

Příloha č. 3. – Datová mapa

DM_COV.docx

Příloha č. 4 – Retenční plán

ČOV_data record retention schedule_d