



Kodex ochrany osobních údajů

1 ÚVOD

Hlavním cílem tohoto Kodexu je jednotným způsobem zajistit vysokou ochranu osobních údajů v organizace Zdravotnická záchranná služba Jihočeského kraje (dále jen „organizace“).

Z důvodu narůstající výměny informací a rostoucího propojování komunikačních systémů je v centru zájmu organizace ochrana osobních údajů pacientů, zaměstnanců, obchodních partnerů a dalších subjektů.

Organizace si je vědoma významu důvěryhodného a bezpečného nakládání s osobními údaji.

2 ROZSAH A PLATNOST

2.1 Právní povaha Kodexu

Tento Kodex je přílohou vnitřního předpisu SM01.25_Ochrana osobních údajů. Vztahuje se na nakládání s veškerými osobními údaji fyzických osob, zejména pak s údaji pacientů, zaměstnanců a dalších třetích stran, smluvních stran či obchodních partnerů.

Tento Kodex byl zpracován na základě Nařízení Evropského parlamentu a rady 2106/79, GDPR.

2.2 Právní předpisy upravující nakládání s osobními údaji

Níže uvedené principy mají za cíl zajistit vysoký stupeň ochrany údajů. Nenahrazují však požadované a případně zákonné podmínky, které musí být za účelem řádného nakládání s osobními údaji splněny.

Údaje shromážděné v Evropě musí být zpracovávány v souladu s právními předpisy země, v níž byly shromážděny, a to i v případě jejich předávání do zahraničí.

Shromažďování osobních údajů a jejich předávání orgánům veřejné správy bude vždy prováděno v souladu se závaznými právními předpisy ČR.

Tento Kodex se řídí právem ČR.



2.3 Ukončení platnosti Kodexu

Uplynutí doby trvání či ukončení platnosti tohoto Kodexu, bez ohledu na datum, okolnosti či důvody takového uplynutí či ukončení platnosti, nezabývá organizaci závazků či povinností obsažených v tomto Kodexu v souvislosti se zpracováním již předaných údajů.

3 PRINCIPY

3.1 Transparentnost zpracování údajů

3.1.1 Informační povinnost

Subjektům údajů musí být umožněn snadný přístup k informacím týkajícím se náležitého nakládání s jejich osobními údaji, např. prostřednictvím publikace tohoto Kodexu na internetových stránkách organizace.

3.1.2 Obsah a forma informací

Subjektům údajů musí být adekvátním způsobem poskytnuty následující informace:

- a) informace o identitě správce (správců) údajů a kontakt na něj (ně);
- b) informace o zamýšleném rozsahu a účelu shromažďování, zpracování a případně použití osobních údajů; tyto informace by měly zahrnovat bližší určení toho, jaké údaje se zaznamenávají, příp. zpracovávají/používají, proč, za jakým účelem a na jakou dobu;
- c) informace o příjemci, rozsahu a účelu (účelech) předání v případě, že jsou osobní údaje předávány třetím stranám;
- d) informace o způsobu zpracování, příp. použití údajů;
- e) informace o zákonných právech subjektů údajů.

Bez ohledu na zvolené médium by měly být tyto informace subjektům údajů poskytnuty v jasné a snadno srozumitelné formě.

3.1.3 Dostupnost informací

Výše uvedené informace musí být subjektům údajů poskytnuty při jejich prvním shromáždění a následně při každém dalším vyžádání.



3.1.4 Souhlas

Není-li shromáždění, zpracování či použití údajů nutné pro účely zahájení či plnění smluvního vztahu či neexistuje-li k tomu žádné jiné oprávnění ze zákona, je nutné získat souhlas subjektu údajů, a to nejpozději při zahájení shromažďování, zpracování či používání údajů.

Kromě výše uvedených informačních povinností je třeba dodržovat následující požadavky na souhlas subjektů údajů:

- **Souhlas** - musí jít o souhlas výslovný, dobrovolný a informovaný, tak, aby bylo subjektu údajů zejména zřejmé, v jakém rozsahu souhlas poskytuje a jaké jsou důsledky jeho neposkytnutí. Znění prohlášení o souhlasu musí být dostatečně přesné a musí subjekt údajů informovat o jeho právu vzít tento souhlas kdykoli zpět.
- **Forma** - souhlas musí být získán v podobě adekvátní okolnostem (obvykle v podobě písemné či elektronické). Ve výjimečných případech může jít o souhlas ústní, pokud je dostatečně doloženo jeho poskytnutí a okolnosti, z nichž vyplývá, že ústní souhlas je postačující.

3.2 Použití pro konkrétní účel

Osobní údaje nesmí být použity za jiným účelem než za účelem, k němuž byly původně poskytnuty.

Použití služeb či získání produktů, popř. služeb nesmí být podmíněno souhlasem subjektů údajů s použitím jejich údajů pro jiné účely, než je zahájení či plnění smluvního vztahu. To platí pouze tehdy, nemohou-li, či nemohou-li z rozumného hlediska, subjekty údajů využívat srovnatelné služby či srovnatelné produkty.

3.3 Zvláštní případy zpracování údajů

Nařízení definuje zvláštní případy zpracování osobních údajů:

- a) Přímý marketing
- b) Automatizované individuální rozhodnutí
- c) Zpracování zvláštní kategorie osobních údajů

Organizace nezpracovává zvláštní kategorie údajů dle písmena a) a b), zpracovává pouze zvláštní kategorie osobních údajů dle písmena c).



3.3.1 Zvláštní kategorie osobních údajů

Pro nakládání s osobními údaji zvláštní kategorie je nutné výslovné oprávnění na právním základě či předchozí souhlas subjektu údajů. Nakládání s osobními údaji zvláštní kategorie je rovněž dovoleno, je-li nutné pro zpracování údajů za účelem naplnění práv a splnění povinností příslušného subjektu v oblasti pracovního práva, dovoluje-li to právo daného státu poskytující příslušné záruky.

Před zahájením shromažďování, zpracovávání či využívání takovýchto údajů je ve všech potřebných případech nutná konzultace se zaměstnancem organizace odpovědným za ochranu údajů, popř. DPO. Měla by být řádně zohledněna povaha, rozsah, účel, nutnost a právní podklad použití údajů.

3.4 Kvalita a přiměřenost údajů, zpracování údajů pouze v nutných případech

3.4.1 Kvalita údajů

Osobní údaje musí být vždy správné a v potřebných případech musejí být průběžně aktualizovány (kvalita údajů).

S ohledem na účel (účely), za nímž jsou údaje shromažďovány, zpracovávány či využívány, jsou přijímána náležitá opatření, aby bylo zajištěno vymazání či případně oprava jakýchkoli nesprávných či neúplných informací.

3.4.2 Přiměřenost, zpracování údajů pouze v nutných případech, anonymizace a využití pseudonymů

Osobní údaje musí být s ohledem na jejich použití pro konkrétní účel přiměřené, relevantní a musí mít odpovídající rozsah (přiměřenost). V rámci konkrétního využití smí být údaje zpracovávány pouze tehdy, je-li to nutné (zpracování údajů pouze v nutných případech).

V případech, kdy je to možné a ekonomické, je třeba aplikovat procesy pro vymazání identifikačních znaků subjektů údajů (anonymizace) či jejich nahrazení jinými charakteristikami (využití pseudonymů). Při anonymizaci a využití pseudonymů je třeba postupovat tak, aby nebylo možné zjistit původní identitu subjektů údajů anebo aby to bylo možné pouze při vynaložení neúměrně velkého úsilí.



3.4.3 Profilace, statistické analýzy

Na základě příslušných nejmodernějších koncepcí či technologií jsou aplikována organizační a technická opatření s cílem zamezit zjištění profilů (např. profily pohybu, uživatelské profily, profily spotřeby). Výjimku tvoří případy, kdy to výslovně dovolují právní předpisy či kdy k tomu subjekt údajů poskytl předchozí souhlas.

Tento požadavek se nevztahuje na čistě statistické analýzy či studie na základě anonymizovaných údajů či údajů s využitím pseudonymů.

3.4.4 Archivace údajů

Při vytváření pravidel pro archivaci údajů jsou zohledněny principy zpracování údajů, zejména pak princip přiměřenosti a princip zpracování údajů pouze v nutných případech. Osobní údaje nelze archivovat bez výslovného souhlasu subjektu údajů, s výjimkou případů, kdy je to nutné z provozních důvodů či je to požadováno zákonem.

3.5 Omezení dalšího předávání

3.5.1 Předávání údajů třetím stranám

Předávání osobních údajů třetím stranám je možné pouze na právním základě, například v případech, kdy je to nutné pro splnění smluvního požadavku vůči subjektu údajů či kdy k tomu subjekt údajů poskytl svůj souhlas.

Toto se nevztahuje na případy, kdy existují národní omezení, zejména z důvodů bezpečnosti státu, národní obrany, veřejného pořádku či prevence, vyšetřování, odhalování a stíhání trestných činů, požadující předávání osobních údajů pro tyto účely.

3.5.2 Odpovědnost

Při předávání údajů třetím stranám, které nepatří mezi orgány veřejné správy, je povinna zajistit zpracování či využívání údajů v souladu se zákonem společnost, která údaje původně shromáždila. Stejně tak je před předáním údajů potřeba s příjemcem projednat a odsouhlasit příslušná opatření pro zajištění ochrany a bezpečnosti údajů. V případě, kdy jsou uzavírány smlouvy se subjekty v zemích bez adekvátní úrovně ochrany údajů, je nutné zajistit dostatečné záruky s ohledem na ochranu práva na soukromí jednotlivce a výkon práv s tím spojených.



V souladu se všeobecně akceptovanými standardy jsou přijímána příslušná technická a organizační opatření pro zajištění integrity a bezpečnosti údajů během jejich předávání třetí straně.

3.5.3 Zpracování údajů subdodavatelí

V případě využití služeb subdodavatele musí smlouva kromě ujednání specifikující práci, kterou má subdodavatel vykonat, rovněž obsahovat povinnosti subdodavatele jakožto zpracovatele údajů. Tyto povinnosti obsahují pokyny organizace (správce údajů) v souvislosti s druhem a způsobem zpracování osobních údajů, účelem jejich zpracování a technickými a organizačními opatřeními potřebnými pro jejich ochranu.

Subdodavatel není bez předchozího souhlasu správce údajů oprávněn využít osobní údaje pro vlastní zpracovatelské účely či zpracovatelské účely třetích stran. V druhém uvedeném případě je třeba se s takovýmto subdodavatelem (subdodavatelí) rovněž dohodnout na výše uvedených pravidlech.

Subdodavatelé budou vybíráni podle schopnosti splnit výše uvedené požadavky.

3.6 Ochrana údajů, organizace a bezpečnost údajů

3.6.1 Osoby odpovědné za ochranu údajů

Organizace jmenuje osobu odpovědnou za ochranu údajů (Data Protection Officer), jejímž úkolem je zajistit poučení zaměstnanců o zákonných požadavcích a/nebo interních požadavcích a o strategii ochrany údajů a soukromí. Mezi další povinnosti patří komunikace se subjekty údajů a s dozorovým úřadem, zvyšování kultury ochrany osobních údajů v organizaci a zejména spolupráce s vedením organizace na ochraně osobních údajů.

3.6.2 Kontrola úrovně ochrany údajů

V pravidelných intervalech probíhá kontrola úrovně ochrany údajů (např. prostřednictvím auditu ochrany informací) za účelem přezkoumání efektivity a úspěšnosti implementovaných technických a organizačních opatření pro ochranu údajů. Takovéto audity může interně provádět osoba odpovědná za ochranu údajů a DPO. Jinou alternativou je provádění těchto auditů externí třetí stranou schválenou správcem údajů. Základem pro stanovení úrovně ochrany údajů jsou požadavky právních předpisů a firemní strategie ochrany údajů vztahující se na příslušnou organizační jednotku a požadavky tohoto Kodexu.



3.6.3 Technická a organizační opatření, opatření ve vztahu k zaměstnancům

Při zahájení pracovně-právního vztahu musí být se zaměstnanci písemně sjednány závazky související se zachováním mlčenlivosti. Kromě toho musí být stanovena příslušná technická a organizační opatření pro nakládání s údaji v souvislosti s firemními procesy a IT systémy. V rámci takovýchto opatření je nutné:

- a) zamezit přístupu neoprávněných osob k systémům pro zpracování údajů, v rámci nichž jsou zpracovávány či využívány osobní údaje (regulace fyzického přístupu);
- b) zajistit, aby neoprávněné osoby nemohly systémy pro zpracování údajů používat (regulace používání datových systémů);
- c) zajistit, aby osoby oprávněné k používání systému pro zpracování údajů měly přístup výhradně k údajům, k nimž jsou oprávněny přistupovat, a aby neoprávněné osoby nemohly osobní údaje během zpracovávání či používání či po jejich zaznamenání číst, kopírovat měnit ani mazat (regulace přístupu k údajům);
- d) zajistit, aby v průběhu elektronického přenosu či předávání či nahrávání údajů na datový nosič nemohly neoprávněné osoby osobní údaje číst, kopírovat, měnit ani mazat a aby bylo možné prozkoumat a stanovit, v jakých případech mají být údaje přenášeny prostředky pro přenos dat (regulace přenosu dat);
- e) zajistit, aby bylo možné zpětně přezkoumat a zjistit, zda a kým byly osobní údaje do systémů pro zpracovávání údajů zadány, v těchto systémech změněny či z nich odstraněny (kontrola zadávání údajů);
- f) zajistit, aby osobní údaje zpracovávané subdodavateli byly zpracovávány pouze v souladu s pokyny objednatele (kontrola subdodavatele);
- g) zajistit ochranu osobních údajů proti náhodnému zničení či ztrátě (zajištění dostupnosti údajů);
- h) zajistit, aby údaje shromážděné pro různé účely byly zpracovávány odděleně (pravidlo odděleného zpracování údajů).

3.7 Práva subjektů údajů

3.7.1 Právo na dotazy a stížnosti

Každý subjekt údajů je oprávněn kontaktovat zaměstnance organizace odpovědného za ochranu údajů s dotazy a stížnostmi v souvislosti s aplikací tohoto Kodexu.

Pro zjednodušení kontaktu je určeno 1 kontaktní místo: gdprou@zsjk.cz.

Organizace zajistí zachování práv subjektu údajů.



3.7.2 Právo na informace

Každý subjekt údajů je oprávněn si kdykoli od organizace vyžádat informace týkající se:

- a) osobních údajů u ní uložených, včetně jejich původu a příjemce (příjemců);
- b) účelu jejich zpracování či použití;
- c) osob a oddělení, kterým jsou jeho údaje standardně předávány, zejména v případě jejich předávání do zahraničí;
- d) ustanovení tohoto Kodexu.

Tyto informace musí být příslušnému subjektu údajů, který o ně projeví zájem, sděleny ve srozumitelné podobě a v přiměřené časové lhůtě a měly by mu být poskytnuty v písemné či elektronické podobě.

V případech, kdy to příslušný národní zákon dovoluje, si může organizace za poskytnutí příslušné informace účtovat poplatek.

3.7.3 Právo na vznesení námítky/výmaz údajů/blokování údajů

Pokud je k tomu oprávněn, může příslušný subjekt údajů vznést vůči organizaci námitku proti použití jeho údajů.

Toto právo na vznesení námítky se vztahuje i na případy, kdy subjekt údajů s použitím svých údajů dříve souhlasil.

Oprávněné žádosti o výmaz či blokování údajů budou bez zbytečného odkladu kladně vyřízeny. Takovéto žádosti jsou oprávněné zejména tehdy, pominou-li právní důvody pro použití údajů. Má-li subjekt údajů na výmaz údajů právo, ale není-li výmaz možný nebo není možný při vynaložení přiměřeného úsilí, budou údaje chráněny proti nepovolenému užití blokováním. Zákonné lhůty pro uchování údajů budou dodržovány.

3.7.4 Právo na opravu

Subjekt údajů může kdykoli požádat, aby organizace opravila jeho osobní údaje zaznamenané organizací v případě, že tyto údaje jsou neúplné a/nebo nesprávné.



3.7.5 Právo na vysvětlení a komentář

V případě tvrzení subjektu údajů, že byla porušena jeho práva v důsledku nezákonného zpracování údajů, zejména pak v případě porušení tohoto Kodexu, objasní organizace bez zbytečného odkladu okolnosti případu.

Zaměstnanec organizace odpovědný za ochranu údajů popř. ve spolupráci s DPO koordinuje veškerou příslušnou korespondenci se subjektem údajů.

3.7.6 Výkon práv subjektů údajů

Subjekty údajů nebudou z důvodu využití těchto práv znevýhodněny. Způsob komunikace se subjektem údajů, např. telefonický, elektronický či písemný kontakt, by měl v příslušných případech brát ohled na požadavek subjektu údajů.

3.8 Řízení procesu ochrany údajů/Odpovědnost za ochranu údajů

3.8.1 Odpovědnost za zpracování údajů

Organizace má ve své funkci správce údajů povinnost zajišťovat dodržování požadavků na ochranu údajů a ustanovení tohoto Kodexu, a to zejména ve vztahu k subjektům údajů.

Zaměstnanec organizace odpovědný za ochranu údajů a popř. DPO bude bezodkladně informována o jakémkoli porušení (včetně podezření) předpisů o ochraně údajů a ustanovení tohoto Kodexu.

3.8.2 Povinnost dozoru a konzultací

Osoba odpovědná za ochranu údajů je povinna sledovat, zda jsou dodržovány národní a mezinárodní předpisy upravující ochranu údajů a tento Kodex. V tomto ohledu jsou vedoucí pracovníci organizace povinni informovat příslušnou osobu odpovědnou za ochranu údajů o příslušném vývoji a plánech do budoucna.

Nebudou-li tomu bránit právní překážky, je osoba odpovědná za ochranu údajů oprávněna přímo na místě přezkoumat veškeré techniky pro zpracování dat, při nichž jsou využívány osobní údaje.

Ve vhodných případech a v rámci svých povinností přezkumu bude zaměstnanec organizace odpovědný za ochranu údajů popř. DPO využívat jednotné mechanismy např. v podobě společných auditů ochrany údajů.



3.8.3 Proškolení zaměstnanců

Zaměstnanci organizace budou dostatečně proškoleni ve znalosti předpisů na ochranu údajů a aplikaci tohoto Kodexu.

Ve spolupráci se zaměstnancem organizace odpovědným za ochranu údajů popř. s DPO zajistí organizace pro takovéto školení vhodné materiály.

3.8.4 Spolupráce s příslušnými orgány veřejné správy

Organizace se zavazuje, že v přiměřené časové lhůtě a přiměřeném rozsahu zodpoví dotazy příslušnému orgánu veřejné správy, který je za ně odpovědný či který je případně odpovědný za organizaci předávající údaje, a že se bude řídit doporučeními tohoto orgánu.

V případě změny legislativy vztahující se na organizaci, jež by mohla mít zásadně negativní vliv na záruky poskytované tímto Kodexem, oznámí organizace změnu příslušnému orgánu veřejné správy.

4 DEFINICE POJMŮ

Automatizovaná individuální rozhodnutí jsou rozhodnutí, jež mají pro subjekt údajů právní důsledky či na něj mají významný vliv a jež jsou založena výhradně na automatizovaném zpracování údajů, jehož cílem je vyhodnocení určitých osobních aspektů subjektu údajů, např. jeho pracovní výkon, úvěrová způsobilost, spolehlivost, chování apod.

Kodex je tento Kodex ochrany osobních údajů.

Nakládání s osobními údaji je jakákoli operace či soubor operací prováděných s osobními údaji, jako je jejich shromažďování, zaznamenávání, organizace, ukládání, úpravy či změny, vyhledávání, konzultace, použití, zpřístupňování přenosem, šíření či poskytování jiným způsobem, seřazování či kombinování, blokování, mazání či likvidace. To zahrnuje i ruční zpracování osobních údajů ve strukturovaných složkách.

Osobní údaje jsou veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě (subjektu údajů); identifikovatelná osoba znamená osobu, kterou lze přímo či nepřímo identifikovat, zejména pak pomocí identifikačního čísla či jednoho či více faktorů specifických pro její fyzickou, fyziologickou, mentální, ekonomickou, kulturní či sociální identitu.

Příjemce je jakákoli fyzická či právnická osoba, orgán veřejné správy, agentura či jakýkoli jiný subjekt, jemuž jsou údaje zpřístupněny, ať již jde o třetí stranu či nikoli. Orgány veřejné správy,



kteří mohou údaje případně obdržet v rámci jednotlivého dotazu, však nejsou za příjemce považovány.

Společnost je každá společnost, která se řídí tímto Kodexem.

Správce údajů je společnost, která sama či společně s dalšími společnostmi určuje účel a prostředky zpracování osobních údajů.

Subjekt údajů je jakákoli fyzická osoba, s jejímiž osobními údaji Společnost nakládá.

Zpracovatel údajů je jakákoli fyzická či právnická osoba, orgán veřejné správy, agentura či jakýkoli jiný subjekt zpracovávající osobní údaje jménem správce údajů (zpracování údajů prostřednictvím subdodavatele).

Zvláštní kategorie údajů jsou údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském či filozofickém přesvědčení, členství v odborech nebo o zdraví či sexuálním životě.

Třetí strana je jiná osoba či subjekt, než je správce údajů. Mezi třetí strany nepatří subjekty údajů ani osoby či subjekty, které mají povinnost shromažďovat, zpracovávat či využívat osobní údaje v ČR, jiném členském státu Evropské unie či jiném státu, jenž uzavřel Dohodu o evropském hospodářském prostoru.