



**KODEX POSKYTOVATELŮ DOMÁCÍ PÉČE
PRO OCHRANU OSOBNÍCH ÚDAJŮ**
garantovaný Grémiem managerů agentur domácí péče, z.s.

Článek 1

Preamble

1. Kodex poskytovatelů domácí péče pro ochranu osobních údajů (dále jen Kodex) je vypracován v souladu s požadavky 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), (dále jen GDPR).
2. Kodex přispívá k řádnému uplatňování GDPR s ohledem na konkrétní povahu a konkrétní potřeby poskytovatelů domácí péče, kteří zpracovávají osobní údaje obdobných kategorií a rozsahu u obdobných kategorií subjektů údajů (dále jen fyzických osob) a na technický a procesní způsob jejich zabezpečení jsou kladeny podobné nároky.
3. Kodex přispívá k řádnému uplatňování GDPR při ochraně fyzických osob v souvislosti se zpracováním osobních údajů poskytovateli domácí péče, s ohledem na odchylnou či zpřesňující úpravu právními předpisy.
4. Kodex je garantován profesním sdružením Grémium managerů agentur domácí péče, z.s. (dále jen Grémium), které zastupuje poskytovatele domácí péče.

Článek 2

Kodex

2. 1 Působnost Kodexu

1. Kodex je soubor konkrétních a praktických pravidel pro zpracování a ochranu osobních údajů správcem, fyzickou nebo právnickou osobou, která má oprávnění k poskytování domácí péče podle zákona o sociálních službách a poskytuje příslušné sociální služby v České republice (dále jen poskytovatel).
2. Kodex se vztahuje na zpracování osobních údajů fyzických osob, které poskytovatel zpracovává v rámci své hlavní činnosti, poskytování domácí péče podle zákona o sociálních službách, případně zdravotních služeb podle zákona o zdravotních službách¹ a při dalších souvisejících činnostech.
3. Kodex neobsahuje pravidla pro zpracování osobních údajů fyzických osob zpracovávaných poskytovatelem v rámci případné další hlavní činnosti.
4. Každý poskytovatel použije Kodex přiměřeně s ohledem na svou činnost, kategorie fyzických osob a zpracovávané kategorie osobních údajů, účel a prostředky zpracování osobních údajů.

¹ Zákon č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)



2. 2 Příloha Kodexu a pokyny k uplatňování Kodexu

1. Přílohou Kodexu je Slovník pojmů, který obsahuje definice a výklad základních pojmů používaných v Kodexu.
2. Kodex může být doplněn pokyny k uplatňování Kodexu, které rozvádějí a upřesňují vybraná ustanovení Kodexu. U poskytovatele, kterého se konkrétní ustanovení týká, se příslušný pokyn stává součástí vnitřní dokumentace.

Článek 3

Kategorie fyzických osob

3. 1 Vymezení kategorie fyzických osob

1. Poskytovatelé v rámci své hlavní činnosti a při dalších činnostech s ní souvisejících zpracovávají osobní údaje dále uvedených kategorií fyzických osob.
2. Každý poskytovatel vybere konkrétní kategorii fyzických osob, jejichž osobní údaje zpracovává a uvede ji v záznamech o činnostech dle článku 13. 2.
3. Pokud poskytovatel zpracovává osobní údaje fyzické osoby či osob, které nejsou v tomto článku vyjmenovány, uvede je v rovněž v záznamech o činnostech zpracování.

3.2 Klient a osoby s ním spjaté

1. Žadatel, se kterým nemohl poskytovatel uzavřít smlouvu o poskytnutí domácí péče podle zákona o sociálních službách.
2. Fyzická osoba, které je poskytována domácí péče služby podle zákona o sociálních službách a případně zdravotní služby podle zákona o zdravotních službách (dále jen klient).
3. Fyzické osoby s klientem spjaté, zejména:
 - a) zákonný zástupce a opatrovník,
 - b) pěstoun a poručník u nezletilých osob,
 - c) rodinní příslušníci,
 - d) osoby určených klientem (pacientem), zákonným zástupcem, opatrovníkem, k nahlížení do zdravotnické dokumentace klienta podle zákona o zdravotních službách,
 - e) fyzická osoba podílející se na úhradě poskytovaných sociálních služeb poskytovaných klientovi,
 - f) osoby blízké zemřelému klientovi ve smyslu zákona o zdravotních službách, které mají právo na informace o zdravotním stavu klienta, případně osoby, jimž klient vyslovil zákaz sdělování těchto informací.



3.3 Zaměstnanec a fyzické osoby v obdobném postavení

1. Uchazeč o zaměstnání.
2. Zaměstnanec.
3. Osoba připravující se u poskytovatele na výkon povolání (dále jen praktikant) nebo stážující v rámci celoživotního vzdělávání (dále jen stážista).
4. Osoba vykonávající dobrovolnickou činnost (dále jen dobrovolník).

3.4 Další fyzická osoba

1. Fyzické osoby - dodavatelé služeb, nebo jejich zaměstnanci, včetně zpracovatelů osobních údajů fyzických osob dle GDPR.
2. Zákonní zástupci a členové orgánů poskytovatele a další fyzické osoby, jejichž osobní údaje jsou na dokumentech podle zákona o archivnictví a spisové službě.
3. Fyzické osoby provádějící kontrolní činnost dle právních předpisů.
4. Fyzické osoby, které udělily souhlas se zpracováním svých osobních údajů.
5. Fyzické osoby, jejichž osobní údaje jsou zpracovávány v rámci sledování fyzických osob prováděného poskytovatelem, zejména prostřednictvím kamer a GPS v automobilech.

Článek 4

Kategorie osobních údajů

4.1 Vymezení kategorií osobních údajů

1. Poskytovatelé v rámci své hlavní činnosti a při dalších činnostech s ní souvisejících zpracovávají u jednotlivých kategorií fyzických osob dále uvedené kategorie osobních údajů.
2. Každý poskytovatel uvede v záznamech o činnostech zpracování u každé zde uvedené kategorie fyzických osob kategorie osobních údajů, které konkrétně zpracovává.
3. Pokud poskytovatel u fyzické osoby zpracovává i jiné kategorie osobních údajů, které nejsou v tomto článku uvedeny, uvede je u této kategorie fyzických osob v záznamech o činnostech zpracování.

4.2 Klient a osoby s ním spjaté

1. Poskytovatel zpracovává identifikační a kontaktní údaje žadatelů o sociální služby, se kterými nemohl uzavřít smlouvu v souladu se zákonem o sociálních službách.
 - a) Poskytovatel vede a uchovává osobní údaje klienta, které slouží k plnění smlouvy o poskytování sociální služby a povinností stanovených právními předpisy. Identifikační údaje, kterými jsou jméno, případně jména, příjmení, datum narození, rodné číslo, je-li přiděleno a jeho zpracování



je stanoveno právními předpisy, např. zákonem o zdravotních službách, pohlaví, státní příslušnost, stav.

- b) Kontaktní údaje, adresu místa trvalého pobytu na území České republiky, případně adresu jiného místa, kde se zdržuje, jde-li o cizince, místo hlášeného pobytu na území České republiky a v případě osoby bez trvalého pobytu na území České republiky adresu bydliště v zahraničí.
- c) Osobní údaje vypovídající o stupni závislosti, na jejichž základě se rozhoduje o míře poskytnutí pomoci a výši příspěvku na péči.
- d) Údaje zjištěné z rodinné, osobní, pracovní a sociální anamnézy,
- e) Informace o zdravotním stavu, o průběhu a výsledku poskytovaných zdravotních služeb a dalších významných okolnostech souvisejících se zdravotním stavem klienta a postupem při poskytování zdravotních služeb, včetně fotodokumentace částí těla pro potřeby zdravotnického personálu.
- f) Další údaje podle zákona o zdravotních službách nebo jiných právních předpisů upravujících zdravotní služby nebo poskytování zdravotní péče.

- 2. Ve zdravotnické dokumentaci mohou být v rámci rodinné anamnézy uvedeny i osobní údaje o zdravotním stavu rodinných příslušníků.
- 3. Na žádost klienta mohou být ve zdravotnické dokumentaci uvedeny i identifikační a kontaktní údaje fyzické osoby, které může poskytovatel poskytnout osobní údaje o zdravotním stavu pacienta v klientem určeném rozsahu, nebo fyzické osoby, které klient poskytnutí těchto informací omezil či zakázal.
- 4. Zdravotnická dokumentace obsahuje také identifikační údaje a podpis zdravotnického nebo jiného odborného pracovníka, který provedl záznam do karty pacienta, a identifikační údaje osob, které mohou mít ke zdravotnické dokumentaci přístup podle zákona o zdravotních službách a identifikační a kontaktní údaje zdravotnických pracovníků poskytujících externí zdravotní péči.
- 5. Poskytovatel vede a uchovává v evidenci klienta, případně ve zdravotnické dokumentaci osobní údaje zákonných (případně i jiných) zástupců nezletilých i zletilých pacientů v rozsahu přiměřeném postupu při poskytování zdravotních služeb, zejména identifikační údaje zákonného zástupce, jméno, příjmení, titul, číslo průkazu totožnosti, občanského průkazu, pasu nebo jiného obdobného dokumentu, případně kopie příslušných dokladů potvrzujících legitimitu zákonného zástupce, a nezbytné kontaktní údaje, korespondenční adresu, číslo telefonu nebo e-mail.

4.3 Zaměstnanec a fyzické osoby v obdobném postavení

- 1. Poskytovatel, zaměstnavatel, zpracovává osobní údaje uchazeče o zaměstnání, zaměstnance, praktikanta, stážisty a dobrovolníka, které slouží k plnění smlouvy a povinností stanovených právními předpisy:
 - a) osobní údaje sloužící k jednoznačné identifikaci uchazeče o zaměstnání, zaměstnance, stážisty a dobrovolníka a nezbytné kontaktní údaje dle zákona zákoník práce²,
 - b) u zahraniční fyzické osoby kopie dokladů o povolení k zaměstnání a povolení k pobytu dle zákona o zaměstnanosti³,

² Zákon č. 262/2006 Sb., Zákon zákoník práce



- c) lékařské posudky, vstupní a periodické prohlídky podle kategorie práce a podle rizika ohrožení zdraví dle zákona o ochraně veřejného zdraví⁴ a vyhlášky o specifických zdravotních službách⁵, záznamy o úrazech,
- d) u sociálních pracovníků, pracovníků v sociálních službách a zdravotnických pracovníků kopie dokladu o způsobilosti k výkonu povolání a doklad o bezúhonnosti, výpis z rejstříku trestů, dle zákona o sociálních službách a zákona o zdravotních službách,
- e) další osobní údaje nutné ke splnění právní povinnosti dle právních předpisů,
- f) další osobní údaje nutné ke splnění smlouvy.

4.4 Další fyzická osoba

- 1. Poskytovatel zpracovává osobní údaje dalších fyzických osob, zejména:
 - a) identifikační a kontaktní údaje dodavatele služeb, zpracovatele,
 - b) identifikační a kontaktní údaje statutárních zástupců a členů orgánů poskytovatele a dalších fyzických osob dle odst. 2 čl. 3. 4,
 - c) identifikační údaje fyzické osoby provádějící kontrolu dle právních předpisů,
 - d) identifikační a kontaktní, případně další osobní údaje fyzické osoby, které jsou zpracovávány na základě souhlasu,
 - e) osobní údaje získané prostřednictvím zařízení umožňujících sledování fyzických osob, zejména kamerových systémů, GPS v automobilech a zabezpečovacích systémů.

Článek 5

Evidence osobních údajů

- 1. Poskytovatel v rámci své hlavní činnosti, poskytování domácí péče a případně zdravotních služeb, a při souvisejících činnostech, zpracovává manuálně nebo automatizovaně osobní údaje fyzických osob, které jsou obsaženy v samostatné evidenci, nebo do ní mají být zařazeny, dle jednotlivých kategorií fyzických osob a účelu zpracování:
 - a) Osobní údaje žadatelů o domácí péči jsou vedeny v samostatné evidenci dle zákona o sociálních službách.
 - b) Osobní údaje klientů, kterým je poskytována domácí péče, případně jejich zákonných zástupců a rodinných příslušníků a dalších fyzických osob s nimi spjatých jsou vedeny v sociální dokumentaci klientů.
 - c) Osobní údaje klientů o jejich zdravotním stavu a poskytnutých zdravotních službách, případně jejich zákonných zástupců, rodinných příslušníků a dalších osob dle zákona o zdravotních službách, jsou vedeny ve zdravotnické dokumentaci.

³ Zákon č. 435/2004 Sb., Zákon o zaměstnanosti

⁴ Zákon č. 258/2000 Sb., Zákon o ochraně veřejného zdraví a o změně některých souvisejících zákonů

⁵ Vyhláška č. 79/2013 Sb., Vyhláška o provedení některých ustanovení zákona č. 373/2011 Sb., o specifických zdravotních službách, (vyhláška o pracovně lékařských službách a některých druzích posudkové péče)



- d) Osobní údaje uchazečů o zaměstnání a zaměstnanců jsou vedeny v personální a mzdové evidenci.
- e) Osobní údaje praktikantů, stážistů a dobrovolníků jsou vedeny v provozní evidenci.
- f) Osobní údaje dalších fyzických osob, zejména dodavatelů služeb, včetně zpracovatelů osobních údajů, zástupců a členů orgánů poskytovatele a fyzických osob provádějících kontrolu dle právních předpisů, jsou vedeny převážně v provozní evidenci.
- g) Osobní údaje dalších osob, které nahlížely v souladu se zákonem o zdravotních službách do zdravotnické dokumentace klienta, jsou do ní zaznamenány.
- h) Osobní údaje fyzických osob zpracovávané na základě souhlasu jsou vedeny v samostatné evidenci.
- i) Osobní údaje fyzických osob sledovaných prostřednictvím zařízení dle článku 3. 4, které jsou ukládány, jsou vedeny v samostatné evidenci.

Článek 6

Zpracování zvláštní kategorie osobních údajů

1. Poskytovatel zpracovává údaje o zdravotním stavu klienta, které spadají do zvláštní kategorie osobních údajů (citlivé údaje). Jejich zpracování je nezbytné pro účely poskytování zdravotní péče a dle článku 9 GDPR je v souladu s tímto nařízením.
2. Zpracováním zvláštní kategorie osobních údajů je rovněž zpracování osobních údajů uchazeče o zaměstnání a zaměstnance týkajících se jejich zdravotní způsobilosti k výkonu povolání a zdravotního stavu dle kategorie vykonávané práce a rizika ohrožení zdraví, kniha úrazů a průkazy práce neschopného pojištěnce. Jejich zpracování je nezbytné pro účely preventivního a pracovního lékařství a pro posouzení pracovní schopnosti zaměstnance a je upraveno právními předpisy.
3. Zpracování osobních údajů o zdravotním stavu klienta za účelem odborného sdělení, publikace, případně vědeckého výzkumu je v souladu s GDPR jen tehdy, pokud poskytovatel zajistí před jejich zpracováním písemný souhlas klienta, případně zákonného zástupce, se zpracováním těchto osobních údajů pro každý stanovený účel.
4. Zpracování zvláštní kategorie osobních údajů, údajů o zdravotním stavu klienta, osobních údajů zaměstnanců je v souladu s GDPR, pokud slouží pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednájí v rámci svých soudních pravomocí.
5. Osobní údaje zvláštní kategorie uvedené v odstavci 1. a 2. jsou vždy zpracovávány pouze pracovníkem poskytovatele, osobou vázanou mlčenlivostí, nebo jinou osobou, na niž se vztahuje povinnost mlčenlivosti, například zpracovatelem, účetní organizací, IT organizací. Evidence osob, které zpracovávají zvláštní kategorie osobních údajů, je vedena ve vnitřní dokumentaci GDPR.



Článek 7

Zásady zpracování osobních údajů

1. Poskytovatel shromažďuje a zpracovává osobní údaje ve vztahu k fyzické osobě korektně a zákonným a transparentním způsobem. Každé fyzické osobě poskytne jasné a srozumitelné informace o jejích zpracovávaných osobních údajích a právech způsobem uvedeným v článku 10. 1.
2. Poskytovatel shromažďuje osobní údaje za účelem:
 - a) poskytování sociálních, případně zdravotních služeb, a ostatních služeb s touto péčí souvisejících, dle zákona o sociálních službách a zákona o zdravotních službách,
 - b) plnění pracovněprávních vztahů podle zákona zákoník práce,
 - c) plnění smluvních vztahů vyplývajících z příslušné smlouvy,
 - d) plnění požadavků dozorových a jiných státních orgánů a zákonných povinností vyplývajících z dalších právních předpisů,
 - e) odborné prezentace, publikace, případně vědeckého výzkumu,
 - f) ochrany oprávněného zájmu poskytovatele prostřednictvím sledovacích zařízení dle článku 8.
 - g) marketingu a přímého marketingu.
3. Rozsah zpracovávaných osobních údajů je přiměřený, relevantní a omezený ve vztahu k účelu zpracování:
 - a) Osobní údaje žadatele o domácí péči jsou vedeny v souladu se zákonem o sociálních službách.
 - b) Osobní údaje klienta, zákonného zástupce a případně fyzických osob s klientem spjatých, jsou vedeny v sociální dokumentaci klienta podle zákona o sociálních službách, či ve zdravotnické dokumentaci v souladu se zákonem o zdravotních službách a vyhláškou o zdravotnické dokumentaci. Jejich rozsah je přiměřený potřebám poskytované domácí, případně zdravotní péče.
 - c) Osobní údaje uchazeče o zaměstnání jsou zpracovány v přiměřeném rozsahu vzhledem k časovému průběhu navazování pracovněprávního vztahu a vyžadovány jsou jen takové osobní údaje, které jsou přiměřené vzhledem ke konkrétní pracovní pozici.
 - d) Osobní údaje zaměstnance, praktikanta a stážisty, nezbytné pro plnění smlouvy a zákonné povinnosti, jsou zpracovány v rozsahu, který je v souladu se zákonem zákoník práce, zákonem o daních z příjmu⁶, zákonem o pojistné na sociální zabezpečení⁷, zákonem o zdravotních službách a dalšími právními předpisy.
 - e) Osobní údaje dobrovolníka jsou vedeny obdobně, jako u fyzických osob dle odstavce 3b).
 - f) Osobní údaje dalších osob, zejména dodavatelů a zpracovatelů, zástupců a členů orgánů poskytovatele, jsou zpracovávány v rozsahu omezeném pro potřeby smluvních vztahů a právních předpisů.
 - g) Osobní údaje fyzických osob, které udělily souhlas se zpracováním svých osobních údajů, jsou zpracovány v rozsahu, který umožňuje jejich jednoznačnou identifikaci.

⁶ Zákon č. 586/1992 Sb., Zákon České národní rady o daních z příjmů

⁷ Zákon č. 589/1992 Sb., Zákon České národní rady o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti



- h) Osobní údaje fyzických osob získané prostřednictvím zařízení umožňujících sledování fyzických osob jsou vedeny výhradně za účelem oprávněných zájmů poskytovatele, v minimálním rozsahu a jen po dobu nezbytně nutnou.
4. Poskytovatel se řídí následujícími opatřeními, zajišťujícími, aby osobní údaje, které jsou nepřesné, byly bezodkladně opraveny nebo vymazány, s přihlédnutím ke specifičnosti účelu, pro které jsou zpracovány:
- a) Osobní údaje klienta uvedené ve smlouvě o poskytování domácí péče jsou opraveny prostřednictvím dodatku smlouvy. Nepřesné nebo neaktuální osobní údaje vedené v sociální dokumentaci klienta podle zákona o sociálních službách jsou bezodkladně opraveny.
 - b) Osobní údaje klienta vedené ve zdravotnické dokumentaci jsou vzhledem k vysokým nárokům kladeným na poskytování zdravotní péče lege artis plně aktualizované při každé návštěvě klienta.
 - c) Opravy nepřesných nebo neaktuálních osobních údajů klienta ve zdravotnické dokumentaci jsou v souladu se zákonem o zdravotních službách prováděny bezodkladně po jejich zjištění novým zápisem ve zdravotnické dokumentaci. Okamžitý výmaz jednotlivých, byť nepřesných osobních údajů, není možný z důvodu nesouladu s požadavky tohoto zákona.
 - d) Osobní údaje zákonného zástupce klienta a fyzických osob s klientem spjatých jsou nedílnou součástí sociální dokumentace klienta či zdravotnické dokumentace, nejsou vedeny v samostatné evidenci. Opravy a aktualizace jsou prováděny po jejich zjištění novým zápisem v sociální či zdravotnické dokumentaci, okamžitý výmaz není v souladu se zákonem o sociálních službách, zákonem o zdravotních službách a vyhláškou o zdravotnické dokumentaci.
 - e) Opravy a aktualizace osobních údajů zaměstnance, praktikanta, stážisty a dobrovolníka, uvedených ve smlouvě jsou prováděny dodatkem smlouvy, výmaz původně uvedených osobních údajů není v souladu s právními předpisy.
 - f) Osobní údaje zaměstnance, praktikanta, stážisty a dobrovolníka, nezbytné pro plnění právní povinnosti, jsou aktualizovány zařazením aktuálních osobních údajů do příslušného osobního spisu.
 - g) Ostatní osobní údaje zaměstnance, praktikanta, stážisty a dobrovolníka, vedené v osobním spisu, které nejsou součástí smlouvy a neslouží pro plnění právní povinnosti, jsou bezodkladně opraveny. Nepřesné osobní údaje jsou vymazány nebo skartovány.
 - h) Osobní údaje dalších fyzických osob, zejména dodavatelů a zpracovatelů, zpracovávané na základě smlouvy, jsou opravovány a aktualizovány dodatkem smlouvy.
 - i) Osobní údaje zástupců a členů orgánů, osob uvedené ve smlouvě jsou opravovány a aktualizovány v souladu s právními předpisy.
 - j) Osobní údaje fyzických osob, které udělily souhlas se zpracováním osobních údajů, jsou opravovány a aktualizovány prostřednictvím udělení nového souhlasu.
5. Poskytovatel ukládá a zpracovává osobní údaje zpravidla ve formě listinné, elektronické, grafické (např. fotografie). Osobní údaje na všech typech nosičů jsou vždy označeny tak, tak aby byla umožněna jednoznačná identifikace fyzické osoby a to pouze po dobu, po kterou jsou ukládány:
- a) Osobní údaje klienta vedené v sociální dokumentaci jsou uloženy po dobu 5 let od skončení platnosti smlouvy o poskytování sociálních služeb.



- b) Osobní údaje klienta, zákonného zástupce a dalších osob, vedené ve zdravotnické dokumentaci jsou uloženy po dobu, která je v souladu se zdravotnickou legislativou. Výmaz je možný až po uplynutí lhůt stanovených vyhláškou o zdravotnické dokumentaci.
 - c) Osobní údaje uchazeče o zaměstnání, který neuzavřel pracovněprávní vztah, jsou bezodkladně vymazány (v elektronické podobě) nebo skartovány (v listinné podobě). Další uchování osobních údajů, například pro obsazení uvolněné pracovní pozice, je možné jen se souhlasem fyzické osoby.
 - d) Osobní údaje zaměstnance nezbytné pro plnění smlouvy nebo právní povinnosti jsou uloženy a výmaz je prováděn v souladu s právními předpisy. Konkrétní doba uložení a způsob výmazu jednotlivých osobních dokladů jsou uvedeny v záznamech o činnosti zpracování.
 - e) Osobní údaje praktikanta, stážisty a dobrovolníka jsou ukládány a skartovány obdobně, jako u zaměstnance.
 - f) Osobní údaje dodavatelů služeb a zpracovatelů jsou ukládány po dobu 5 let od skončení smlouvy. Výmaz je prováděn v souladu s právními předpisy.
 - g) Souhlasy jsou ukládány po dobu 5 let od ukončení souhlasu nebo pominutí účelu, pro které byly uděleny.
 - h) Doba, po kterou jsou ukládány konkrétní osobní údaje získané prostřednictvím kamer, či jiného způsobu sledování fyzických osob, je uvedena v záznamech o činnostech zpracování.
6. Poskytovatel zpracovává osobní údaje způsobem, který zajistí jejich náležité zabezpečení, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (integrita a důvěrnost), v souladu s článkem 12.
7. Poskytovatel odpovídá za dodržení zásad stanovených v článku 7 a soulad s tímto ustanovením dokládá:
- a) účastí na Kodexu dle článku 19,
 - b) prostřednictvím dalších dokumentů obsažených ve vnitřní dokumentaci GDPR dle článku 13,
 - c) doložením monitorovacích zpráv – Atestů vydaných oprávněnou organizací.

Článek 8

Zákonnost zpracování

1. Poskytovatel zpracovává osobní údaje vždy zákonným způsobem a v souladu s článkem 6 GDPR. V záznamech o činnostech zpracování je u každé kategorie osobních údajů, zpracovaných u jednotlivých kategorií fyzických osob, vždy uvedena nejméně jedna z právních podmínek. Základní pravidla jsou stanovena níže:
- a) Zpracování osobních údajů klienta vedených v sociální dokumentaci klienta, případně ve zdravotnické dokumentaci, je nezbytné pro splnění právní povinnosti, která se na poskytovatele vztahuje dle zákona o sociálních službách, zákona o zdravotních službách a vyhlášky o zdravotnické dokumentaci. Odpovídající rozsah je stanoven těmito právními předpisy a je přiměřený potřebám poskytované sociální či zdravotní péče.



- b) Zpracování osobních údajů zákonného zástupce klienta a osob s klientem spjatých je nezbytné pro splnění právní povinnosti, dodržení zákonného postupu při poskytování sociálních či zdravotních služeb, dle zákona o sociálních službách a zákona o zdravotních službách. Rozsah osobních údajů je minimalizován na nezbytné identifikační a kontaktní údaje a údaje dokládající jejich právní status.
- c) Osobní údaje fyzické osoby – uchazeče o zaměstnání, zaměstnance, praktikanta, stážisty a dobrovolníka, jsou zpracovávány za účelem navázání nebo plnění smlouvy, případně pro provedení opatření přijatých před uzavřením smlouvy na žádost fyzické osoby. Smluvní stranou je uchazeč o zaměstnání, zaměstnanec, praktikant, stážista, dobrovolník nebo organizace dobrovolníka vysílající. Zpracování osobních údajů zaměstnance je rovněž nezbytné z důvodu splnění právní povinnosti a rozsah zpracování osobních údajů je stanoven právními předpisy^{8,9,10,11,12,13,14,15}.
- d) Osobní údaje dodavatele služeb, zpracovatele a další fyzické osoby jsou zpracovávány zejména za účelem plnění smlouvy.
- e) Osobní údaje zákonných zástupců a členů orgánů poskytovatele jsou zpracovány zejména na základě právních předpisů, které upravují jejich právní formu^{16,17,18,19,20} a zákona o archivnictví²¹.
- f) Za zákonný způsob je považováno i zpracování osobních údajů na základě udělení souhlasu fyzické osoby dle článku 9.
- g) Zpracování osobních údajů získaných sledováním fyzických osob prostřednictvím kamerových a zabezpečovacích systémů, GPS, je v přiměřeném rozsahu nezbytné pro účely oprávněných zájmů poskytovatele, zejména ochrany majetku.

Článek 9

Podmínky vyjádření souhlasu

1. Poskytovatel souhlas fyzické osoby se zpracováním osobních údajů nevyžaduje a nesmí vyžadovat, pokud je zpracování zákonné z jiných právních důvodů uvedených v článku 6 GDPR, zejména:
 - a) při zpracování osobních údajů klienta, jeho zákonného zástupce či osoby s klientem spjaté, za účelem poskytování sociální či zdravotní péče a plnění povinností poskytovatele upravených

⁸ Zákon č. 262/2006 Sb., Zákon zákoník práce

⁹ Zákon č. 187/2006 Sb., Zákon o nemocenském pojištění

¹⁰ Zákon č. 435/2004 Sb., Zákon o zaměstnanosti

¹¹ Zákon č. 155/1995 Sb., Zákon o důchodovém pojištění

¹² Zákon č. 89/2012 Sb., Zákon občanský zákoník

¹³ Zákon č. 48/1997 Sb., Zákon o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů

¹⁴ Zákon č. 586/1992 Sb., Zákon České národní rady o daních z příjmů

¹⁵ Zákon č. 589/1992 Sb., Zákon České národní rady o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti

¹⁶ Zákon č. 40/1964 Sb., Občanský zákoník

¹⁷ Zákon č. 90/2012 Sb., Zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích)

¹⁸ Zákon č. 3/2002 Sb., Zákon o svobodě náboženského vyznání a postavení církví a náboženských společností a o změně některých zákonů (zákon o církvích a náboženských společnostech)

¹⁹ Zákon č. 227/1997 Sb., Zákon o nadacích a nadačních fondech a o změně a doplnění některých souvisejících zákonů (zákon o nadacích a nadačních fondech)

²⁰ Zákon č. 128/2000 Sb., Zákon o obcích (obecní zřízení)

²¹ Zákon č. 499/2004 Sb., Zákon o archivnictví a spisové službě a o změně některých zákonů



zákonem o sociálních službách a zákonem o zdravotních službách, které není založeno na souhlasu fyzické osoby, ale je nezbytné pro splnění právní povinnosti poskytovatele,

- b) při zpracování osobních údajů uchazeče o zaměstnání a zaměstnance za účelem navázání nebo plnění pracovněprávního vztahu, které není založeno na souhlasu fyzické osoby, ale je nezbytné pro plnění uzavřené smlouvy a právní povinnosti poskytovatele dle právních předpisů,
- c) při zpracování osobních údajů praktikanta, stážisty, dobrovolníka, které není založeno na souhlasu fyzické osoby, ale je nezbytné pro plnění příslušné smlouvy.

2. Poskytovatel souhlas se zpracováním osobních údajů fyzické osoby vždy vyžaduje:

- a) při zpracování osobních údajů klienta, případně jiné fyzické osoby, pro účely odborné prezentace, publikace, případně vědeckého výzkumu, pokud by zveřejnění fotografie a dalších osobních údajů mohlo vést k identifikaci fyzické osoby,
- b) při uvedení fotografie klienta na nástěnkách, webových stránkách, sociálních sítích a podobně, pokud by zveřejnění fotografie nebo fotografie s dalšími osobními údaji mohlo vést k jeho identifikaci.
- c) při uvedení fotografie, případně dalších osobních údajů zaměstnance na webových stránkách poskytovatele, letáčích, plakátech a dalších prezentačních materiálech,
- d) při použití osobních údajů fyzické osoby v rámci marketingu a k přímému marketingu,
- e) při zpracování osobních údajů fyzické osoby za účelem, který nesplňuje ani jednu z dalších zákonných podmínek uvedených v článku 6 GDPR.

3. Žádost o vyjádření souhlasu musí být vždy předložena způsobem, který je od jiných skutečností jasně odlišitelný, srozumitelný a snadno přístupný za použití jasných a srozumitelných jazykových prostředků.

4. Před udělením souhlasu poskytovatel fyzickou osobu informuje o jejím právu svůj souhlas kdykoliv odvolat, dále o skutečnosti, že odvoláním souhlasu nemůže být zpochybněna zákonnost zpracování, které poskytovatel provedl před jeho odvoláním.

5. Před udělením souhlasu se zpracováním osobních údajů k přímému marketingu musí být fyzická osoba výslovně upozorněna na právo vznést námitku proti tomuto způsobu zpracování.

6. Souhlas se zpracováním osobních údajů dítěte do dovršení 15 let, dle občanskoprávní úpravy, uděluje jeho zákonný zástupce.

Článek 10

Práva fyzické osoby

10.1 Právo na transparentní informace, sdělení a postupy při výkonu práv

- 1. Poskytovatel přijme vhodná opatření, aby fyzické osobě poskytl srozumitelně a přístupným způsobem veškeré informace uvedené v článcích 13 a 14 GDPR a učinil veškerá sdělení uvedená v článcích 15 až 22 a 34 GDPR. Standardní formy sdělení, které poskytovatel používá pro jednotlivé



kategorie fyzických osob, jsou uvedeny níže. Dokumenty obsahující potřebné informace jsou součástí záznamů o činnostech zpracování.

2. Klientovi, zákonnému zástupci a dalším osobám, jejichž osobní údaje jsou vedeny v sociální dokumentaci či zdravotnické dokumentaci klienta, jsou poskytnuty informace a sdělení následujícím způsobem:
 - a) v dokumentu o právech klientů, který obsahuje veškeré informace a sdělení dle odstavce 1. včetně informace o účasti poskytovatele na Kodexu, dostupném zájemci o poskytování sociálních služeb, žadateli a klientovi, případně jeho zákonnému zástupci prostřednictvím webových stránek poskytovatele či jiným způsobem,
 - b) ústně, pokud si to klient, případně zákonný zástupce či další oprávněné osoby vyžádají. Poskytovatel pro tyto účely určí odpovědnou osobu, případně pověřence, jejíž jméno a kontakt jsou uvedeny v dokumentu o právech klientů a na webových stránkách, pokud jsou založeny.
3. Uchazeči o zaměstnání, zaměstnanci a stážistovi jsou jejich práva zajištěna:
 - a) poskytnutím příslušného dokumentu o právech klientů a vnitřní dokumentace v přiměřeném rozsahu, v listinné podobě nebo elektronicky,
 - b) ústně, pokud si to fyzická osoba vyžádá, odpovědnou osobou, případně pověřencem.
4. Způsob poskytnutí informací další fyzické osobě, pokud její osobní informace zpracovává, stanoví poskytovatel ve vnitřní dokumentaci GDPR.
5. Pokud poskytovatel získává osobní údaje přímo od fyzické osoby, splní povinnost poskytnout informace uvedené v článku 13 GDPR odstavce 1. v okamžiku jejich získání způsobem uvedeným v odstavcích 2. a 3. tohoto článku. Tyto informace nemusí poskytovat v případech:
 - a) kdy se jedná o záchranu lidského života,
 - b) pokud již fyzická osoba uvedené informace má, a to do té míry, v níž je má.
6. Jestliže osobní údaje nebyly získány od fyzické osoby, splní poskytovatel povinnost poskytnout fyzické osobě informace uvedené v článku 14 GDPR způsobem uvedeným v odstavcích 2. a 3. tohoto článku.
7. Poskytovatel poskytne tyto informace:
 - a) v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovány,
 - b) nejpozději v okamžiku, kdy poprvé dojde ke komunikaci s fyzickou osobou, mají-li být osobní údaje použity pro účely této komunikace, nebo
 - c) nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.
8. Při získání osobních údajů dle odstavce 6. nemusí poskytovatel informovat:
 - a) fyzickou osobu, která již uvedené informace má, například uchazeče o zaměstnání, zaměstnance, praktikanta, stážistu, dobrovolníka, který byl prokazatelně seznámen s vnitřní dokumentací v přiměřeném rozsahu, kde jsou všechny tyto informace uvedeny,



- b) klienta, neboť získávání osobních údajů klientů (pacientů) od jiných zdravotnických zařízení je upraveno zákonem o zdravotních službách a zákonem o sociálních službách, kde jsou stanovena vhodná opatření na ochranu jeho oprávněných zájmů,
- c) pokud se ukáže, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí; to platí zejména v případě zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely s výhradou podmínek a záruk uvedených v čl. 89 odst. 1. GDPR, nebo pokud je pravděpodobné, že uplatnění povinnosti uvedené v odstavci 1. tohoto článku by znemožnilo nebo výrazně ztížilo dosažení cílů uvedeného zpracování. V takových případech přijme poskytovatel vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů, včetně zpřístupnění daných informací veřejnosti,
- d) osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu, včetně zákonné povinnosti mlčenlivosti.

10. 2 Právo na přístup k osobním údajům

1. Poskytovatel vydá fyzické osobě na její žádost potvrzení, zda zpracovává, nebo nezpracovává osobní údaje, které se jí týkají. Pokud jsou osobní údaje zpracovávány, umožní fyzické osobě přístup k těmto osobním údajům:
 - a) V případě zdravotnické dokumentace vedené o klientovi je nahlížení, pořizování jejich výpisů nebo kopií a požadování úhrady upraveno příslušným ustanovením zákona o sociálních službách²², kterým se poskytovatel řídí.
 - b) Poskytovatel poskytne na základě žádosti uchazeči o zaměstnání, zaměstnanci, praktikantovi, stážistovi, dobrovolníkovi a případně další fyzické osobě přístup a případně kopii zpracovávaných osobních údajů.
 - c) Za další kopie na žádost výše uvedené fyzické osoby může poskytovatel účtovat přiměřený poplatek na základě administrativních nákladů.
 - d) Jestliže fyzická osoba podá žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud fyzická osoba údajů nepožádá o jiný způsob. Při poskytnutí osobních údajů, zejména zvláštní kategorie, v elektronické formě musí být zajištěn bezpečný přenos.
 - e) Poskytovatel musí fyzickou osobu žádající o přístup k osobním údajům prokazatelně identifikovat. Pokud o totožnosti osoby pochybuje, může požádat o poskytnutí dodatečných informací nezbytných k prokázání totožnosti. Při neprokázání totožnosti požadované osobní údaje neposkytne.
 - f) Právem získat kopii nesmějí být nepříznivě dotčena práva a svobody jiných osob.
2. Poskytovatel zajistí rovněž fyzické osobě přístup k následujícím informacím dle článku 15 GDPR:
 - a) jaká kategorie osobních údajů je zpracovávána,
 - b) jaký je účel zpracování,
 - c) jakému příjemci nebo kategorii příjemců budou osobní údaje zpřístupněny,

²² § 65, Zákon č. 108/2006 Sb., Zákon o sociálních službách



- d) jaká bude doba uložení osobních údajů nebo na základě čeho se tato doba určuje,
 - e) jaká jsou práva fyzické osoby na opravu, výmaz, omezení zpracování osobních údajů nebo právo vznést námitku proti konkrétnímu zpracování osobních údajů,
 - f) informaci o právu stěžovat si u Úřadu pro ochranu osobních údajů,
 - g) jaké jsou zdroje, ze kterých poskytovatel čerpal osobní údaje fyzické osoby,
 - h) informace o případném automatizovaném zpracování osobních údajů, včetně profilování.
3. Přístup k informacím je u jednotlivých kategorií fyzických osob zajištěn poskytovatelem následovně:
- a) klientům jejich zákonným zástupcům a dalším osobám, jejichž osobní údaje jsou vedeny ve zdravotnické dokumentaci, jsou veškeré informace zpřístupněny v dokumentu o právech klientů a dalšími způsoby v článku 10. 1 odstavci 2.,
 - b) uchazeči o zaměstnání, současnému či bývalému zaměstnanci, praktikantovi, stážistovi, dobrovolníkovi a další fyzické osobě zpřístupněním vnitřní dokumentace v přiměřeném rozsahu,
 - c) dalším osobám zpřístupněním vnitřní dokumentace v přiměřeném rozsahu.

10. 3 Právo fyzické osoby na opravu, výmaz

- 1. Poskytovatel zpracovává standardně osobní údaje fyzických osob, u nichž provedení opravy a výmazu klienta stanovuje zejména zákon o zdravotních službách a právo fyzických osob je v tomto případě omezeno.
- 2. Pokud fyzická osoba odvolá souhlas, na jehož základě byly osobní informace zpracovány, má právo na to, aby poskytovatel bez zbytečného odkladu tyto osobní údaje vymazala z evidence, v níž jsou vedeny pro účel, na který byl souhlas poskytnut.
- 3. Pokud poskytovatel zpřístupnil nepřesné osobní údaje fyzické osoby příjemcům, například jiným zdravotnickým zařízením, zdravotním pojišťovnám, orgánům státní správy, a musí je opravit, oznámí tuto skutečnost příjemcům a zpřístupní jim opravené osobní údaje, pokud je to možné nebo to nevyžaduje nepřiměřené úsilí.

10. 4 Právo na omezení zpracování

- 1. Fyzická osoba má právo na to, aby poskytovatel omezil zpracování jejích osobních údajů ve stanovených případech. Osobní údaje, jichž se toto právo týká, jsou označeny a jejich zpracování je omezeno. Omezením zpracování se netýká jejich uložení a plnění důležitého veřejného zájmu, povinností stanovených právními předpisy.
- 2. Právní důvody pro omezení zpracování:
 - a) fyzická osoba popírá přesnost osobních údajů, omezení trvá po dobu potřebnou k ověření přesnosti osobních údajů,
 - b) zpracování je protiprávní, fyzická osoba odmítá výmaz osobních údajů a žádá omezení jejich použití,



- c) poskytovatel již osobní údaje nepotřebuje, ale fyzická osoba je požaduje pro určení, výkon nebo obhajobu právních nároků.

10. 5 Právo na přenositelnost údajů

1. Poskytovatel, který zpracovává osobní údaje fyzické osoby na základě souhlasu dle článku 9 nebo smlouvy (zejména pracovně právní, dodavatelsko-odběratelské, zpracovatelské) a zároveň automatizovaně (elektronicky), má povinnost předat osobní údaje:
 - a) ve strukturovaném, běžně používaném a strojově čitelném formátu této fyzické osobě,
 - b) nebo přímo jinému správci, je-li to technicky proveditelné.

10. 6 Právo vznést námitku

1. Poskytovatel zpracovává osobní údaje především na základě plnění právní povinnosti nebo smlouvy. Právo fyzické osoby podat námitku podle článku 21 odstavce 1. GDPR v těchto případech nelze uplatnit.
2. Pokud poskytovatel zpracovává osobní údaje na základě oprávněného zájmu, prostřednictvím bezpečnostního či kamerového sledování, má fyzická osoba, které se sledování týká, právo vznést námitku. Poskytovatel nesmí dále osobní údaje zpracovávat, pokud neprokáže závažné důvody, které převažují nad zájmy nebo právy a svobodami fyzické osoby. Na toto právo musí být fyzická osoba výslovně upozorněna nejpozději v okamžiku první komunikace.
3. Pokud poskytovatel na základě souhlasu zpracovává osobní údaje fyzické osoby pro účely přímého marketingu, může fyzická osoba vznést kdykoli námitku proti zpracování pro přímý marketing a na toto právo je při žádosti o souhlas výslovně upozorněna. V případě vznesené námítky nebudou osobní údaje již pro tento účel zpracovány a bude z přímého marketingu vyřazena.

Článek 11

Příjemce a zpracovatel

11. 1 Příjemce

1. Příjemcem je každá fyzická nebo právnická osoba, které jsou poskytnuty osobní údaje, s výjimkou orgánů veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu.
2. Poskytovatel uvede kategorie příjemců, kterým poskytuje osobní údaje fyzických osob v záznamech o činnostech zpracování dle článku 13. 2, včetně příjemců ve třetích zemích nebo v mezinárodních organizacích.
3. Poskytovatel poskytne fyzické osobě informace, jakému příjemci nebo kategorii příjemců, zejména ve třetích zemích nebo v mezinárodních organizacích, jeho osobní údaje poskytl nebo bude poskytovat, přístupným způsobem uvedeným v článku 10.1.



11. 2 Zpracovatel

1. Poskytovatel může využívat pro zpracování osobních údajů zpracovatele, zejména organizace zpracovávající účetnictví, daňové poradce, IT organizace. Povinností poskytovatele je využívat takové organizace, které poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření pro soulad s GDPR.
2. Poskytovatel je povinen uzavřít s každým zpracovatelem písemnou smlouvu nebo dodatek již uzavřené smlouvy, které zavazují zpracovatele vůči správci a zejména obsahují:
 - a) předmět a dobu trvání zpracování, povahu a účel zpracování, typ osobních údajů a kategorie fyzických osob, povinnosti a práva poskytovatele,
 - b) závazek zpracovatele zpracovávat osobní údaje pouze na základě doložených pokynů poskytovatele,
 - c) závazek zpracovatele nezapojit do zpracování žádného dalšího zpracovatele (jiného dodavatele informačních (IT) systémů, organizaci spravující úložiště dat a podobně) bez předchozího konkrétního nebo obecného písemného povolení poskytovatele a v tomto případě závazek informovat o zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení,
 - d) závazek zajistit uložení stejných povinností, které jsou ve smlouvě se zpracovatelem, i dalšímu zpracovateli,
 - e) povinnost zpracovatele zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
 - f) závazek zabezpečit zpracování osobních údajů dle článku 32 GDPR,
 - g) další ujednání dle článku 28 GDPR.
3. Poskytovatel zapojí do zpracování pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření pro soulad s GDPR.

Článek 12

Zabezpečení osobních údajů

12. 1 Systém řízení ochrany osobních údajů

1. Poskytovatel vytvoří systém řízení ochrany osobních údajů (dále jen SOOÚ), aby zajistil stálou úroveň zabezpečení zpracovávaných osobních údajů.
2. Součástí SOOÚ je pravidelný vnitřní audit úrovně zabezpečení zpracovávaných osobních údajů, prováděný s ohledem na následující skutečnosti:
 - a) způsob vedení, ukládání a dostupnost evidence dle článku 3, zejména s ohledem na aktuální stav výpočetní techniky, která slouží ke zpracování osobních údajů nebo bezpečnost jejich zpracování ovlivňuje,



- b) prověření, zda jsou osobní údaje shromažďovány pouze pro legitimní účely a zda je jejich zpracování přiměřené, relevantní a omezené ve vztahu ke konkrétnímu účelu,
 - c) posouzení rozsahu zpracovávaných osobních údajů, zvláště osobních údajů zvláštní kategorie, který je rozhodující pro rozhodnutí o jmenování pověřence,
 - d) posouzení doby nezbytné pro uložení osobních údajů,
 - e) posouzení pravděpodobnosti a závažnosti rizik pro práva a svobody fyzických osob,
 - f) náklady potřebné k provedení.
3. Poskytovatel posuzuje závažnost rizik porušení zabezpečení osobních údajů, aby zajistil neustálou důvěrnost, integritu, dostupnost a odolnost systému řízení osobních údajů:
- a) pravidelně, v cyklech odpovídajících povinnému monitorování dodržování Kodexu.,
 - b) v případě technických nebo organizačních změn, zvláště při zavádění nových způsobů zpracování osobních údajů, které by mohly zvýšit rizika,
 - c) v případě, kdy by mohlo dojít nebo již došlo k bezpečnostnímu incidentu.
4. Poskytovatel na základě vnitřního auditu identifikuje slabá místa zabezpečení a provede vhodná technická a organizační opatření, aby zajistil takovou úroveň zabezpečení odpovídající danému riziku, která eliminuje rizika neoprávněného či protiprávního zpracování, neoprávněného přístupu, náhodné ztráty, pozměňování, zničení nebo poškození.

12. 2 Technická opatření

1. Osobní údaje v papírové i elektronické podobě, zvláště sociální dokumentace klienta a zdravotnická dokumentace a další údaje zvláštní kategorie, musí být uloženy tak, aby bylo zamezeno přístupu neoprávněných osob, byly chráněny před neoprávněným zásahem, dodatečnými modifikacemi, ztrátou, zničením či jejich zneužitím.
2. Poskytovatel zavede odpovídající technická opatření běžné nebo vyšší úrovně ochrany:
 - a) zabezpečí objekt poskytovatele, kde jsou vedeny a uloženy osobní údaje fyzických osob, minimálně bezpečnostním zámekem, případně elektronickým zabezpečovacím systémem, kamerami apod.,
 - b) zabezpečí každou kartotéku, kde je v listinné podobě vedena sociální dokumentace klienta a zdravotnická dokumentace a další evidence dle článku 5, zámekem, případně ji umístí v uzamykatelném prostoru, který je přístupný pouze oprávněným osobám,
 - c) při transportu nosičů s osobními údaji fyzických osob je zabezpečí tak, aby zamezil jejich ztrátě nebo odcizení,
 - d) omezí riziko odcizení přístrojů (hardware), které jsou používány pro elektronické zpracování zdravotnické dokumentace a dalších osobních údajů, vhodným zabezpečením proti odcizení,
 - e) zajistí bezpečné uložení technických nosičů dat s kopiemi datových souborů na jiném místě, než jsou přístroje (hardware).



3. Poskytovatel chrání elektronicky zpracovávané osobní údaje vhodným softwarem, který zajišťuje dvoufázové ověření identity:
 - a) při přihlášení do operačního systému používaných přístrojů (hardware) a datových nosičů,
 - b) při přihlášení do databází.
4. Vnitřní síť poskytovatele je chráněna před vnějším prostředím pomocí firewallu a přiměřenou antivirovou ochranou.
5. Vzdálený přístup k datům musí být zabezpečen.
6. Zálohování zdravotnické dokumentace je zajištěno v souladu se zákonem o zdravotních službách:
 - a) bezpečnostní kopie datových souborů jsou prováděny nejméně jednou za pracovní den nebo za den, kdy došlo ke změně osobních údajů, na vhodný softwarově zabezpečený nosič,
 - b) před uplynutím doby životnosti zápisů na technickém nosiči dat je zajištěn přenos na jiný technický nosič dat.
7. Poskytovatel zajistí čitelnost dat vedených ve zdravotnické dokumentaci nejméně po dobu, která je stanovená pro uchování zdravotnické dokumentace.
8. V případě, že má poskytovatel k dispozici wifi připojení pro klienty, je odděleno od vnitřní sítě.

12. 3 Organizační opatření

1. Osobní údaje fyzických osob, jsou vždy zpracovávány pouze osobou, která je k tomu v příslušném rozsahu oprávněná. Všechny tyto osoby mají definován rozsah odpovědnosti a povinností, včetně mlčenlivosti:
 - a) zaměstnanci, praktikanti, stážisti a dobrovolníci ve vnitřní dokumentaci nebo písemnou smlouvou,
 - b) zpracovatelé (účetní organizace, IT organizace) vždy písemnou smlouvou,
 - c) další osoby v rozsahu zmocnění právními předpisy.
2. Nahlížení do zdravotnické dokumentace, pořizování jejích výpisů nebo kopií jinými osobami než je klient (pacient), dle příslušného ustanovení zákona o zdravotních službách²³, a předávání osobních údajů pro zpracování v Národním zdravotnickém informačním systému dle § 70 téhož zákona je v souladu s GDPR. Tento zákonný způsob zpracování nevyžaduje souhlas klienta.
3. Poskytovatel zajistí v případě zániku oprávnění k poskytování sociálních či zdravotních služeb zdravotnickou dokumentaci v souladu s § 57 zákona o zdravotních službách.
4. Poskytovatel stanoví ve vnitřní dokumentaci pravidla pro manipulaci se všemi nosiči osobních údajů, zejména s listinami, PC, notebooky, tablety, chytrými telefony a technickými nosiči dat, a to jak uvnitř zařízení sociální péče, či jiných prostor, tak především mimo tyto prostory.

²³ § 65, Zákon č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)



5. Poskytovatel, který využívá sledovací systémy, zejména kamerový systém nebo GPS, zpracuje pravidla sledování fyzických osob a případné ukládání osobních údajů. Příslušný dokument je součástí vnitřní dokumentace.
6. Přenos osobních údajů, zejména zvláštní kategorie, jiným příjemcům musí být vždy náležitě zabezpečen. Za bezpečné cesty lze považovat:
 - a) přenos osobních údajů fyzickou osobou, jíž se týkají,
 - b) doporučenou zásilku,
 - c) využití služeb bezpečného přepravce,
 - d) datovou schránku,
 - e) zabezpečené úložiště.
7. Poskytovatel určí odpovědnou osobu, případně pověřence, která zajišťují trvalý dohled, a pravidelné hodnocení řízení bezpečnosti a ochrany osobních údajů.
8. Poskytovatel zajistí pravidelné školení odpovědné osoby v cyklech odpovídajících minimálně pravidelnému monitorování dodržování Kodexu. Všichni zaměstnanci musí být rovněž pravidelně seznamováni s pravidly Kodexu, zásadami GDPR a konkrétními pravidly uplatňovanými v zařízení poskytovatele.
9. Organizační opatření pro zajištění osobních údajů jsou uvedena i v dalších ustanoveních Kodexu.

13. Vnitřní dokumentace GDPR

13. 1 Základní pravidla vedení vnitřní dokumentace

1. Každý poskytovatel vede vnitřní dokumentaci, jejímž prostřednictvím dokládá soulad zpracování osobních údajů fyzických osob s GDPR.
2. Vnitřní dokumentace obsahuje:
 - a) záznamy o činnostech zpracování,
 - b) a další dokumenty nezbytné pro doložení souladu s GDPR.
3. Poskytovatel je povinen vnitřní dokumentaci dodržovat. Poskytovatel vnitřní dokumentaci pravidelně reviduje a aktualizuje, zpravidla v cyklech odpovídajících povinnému monitorování dodržování Kodexu. V případě závažných změn při zpracování osobních údajů, z důvodů změny činnosti nebo legislativy jsou úpravy prováděny neprodleně.
4. Poskytovatel je na požádání povinen předložit vnitřní dokumentaci oprávněné organizaci nebo Úřadu pro ochranu osobních údajů.
5. Vnitřní dokumentace se ukládá po dobu stanovenou Úřadem ochranu osobních údajů.



13.2 Záznamy o činnostech zpracování

1. Každý poskytovatel vede záznamy o činnostech zpracování, za něž odpovídá, a které nesou tyto informace:
 - a) jméno a kontaktní údaje správce, odpovědnou osobu, případně pověřence pro ochranu osobních údajů,
 - b) účel a právní důvod zpracování,
 - c) kategorie fyzických osob a kategorie zpracovávaných osobních údajů,
 - d) kategorie příjemců, kterým jsou, nebo případně mohou či budou, osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo v mezinárodních organizacích,
 - e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci,
 - f) plánované lhůty pro výmaz jednotlivých kategorií údajů,
 - g) obecný popis technických a organizačních bezpečnostních opatření,

2. Záznamy o činnostech zpracování jsou součástí vnitřní dokumentace a vyhotovují se písemně nebo elektronicky.

13.3 Další dokumenty

1. Jedná se především o:
 - a) analýzu a vyhodnocení rizik,
 - b) zdůvodnění nejmenování pověřence,
 - c) písemné informace o právech fyzické osoby a formy zveřejnění,
 - d) souhlasy fyzických osob,
 - e) identifikační a kontaktní údaje pověřence pro ochranu osobních údajů, pokud byl jmenován nebo identifikační a kontaktní údaje pověřené osoby,
 - f) evidenci osob, které zpracovávají osobní údaje, zejména zvláštní kategorie a rozsah zpracování,
 - g) evidenci školení pověřené osoby a zaměstnanců v oblasti GDPR,
 - h) zpracovatelské smlouvy,
 - i) dokumentaci bezpečnostních incidentů,
 - j) smlouvu s profesní organizací,
 - k) smlouvu s oprávněnou organizací,
 - l) monitorovací zprávy - Atesty,
 - m) další dokumenty pro dokladování souladu s GDPR zpracované poskytovatelem.



Článek 14

Ohlašování bezpečnostních incidentů Úřadu pro ochranu osobních údajů

1. Jakékoliv porušení zabezpečení osobních údajů ohlásí poskytovatel, správce, písemně nebo elektronicky:
 - a) Úřadu pro ochranu osobních údajů do 72 hodin od okamžiku, kdy se o něm dozvěděl, v případě opoždění sdělí dozorovému úřadu důvody zpoždění,
 - b) Grémiu do 72 hodin.
2. Zpracovatel je povinen porušení zabezpečení osobních údajů hlásit bezodkladně poskytovateli, správci.
3. Hlášení přinejmenším obsahuje:
 - a) popis daného případu, kategorie a počet fyzických osob, kterých se bezpečnostní incident týká, a přibližné množství záznamů,
 - b) jméno a kontaktní údaje osoby, která může poskytnout bližší informace, odpovědné osoby nebo pověřence,
 - c) popis pravděpodobných důsledků bezpečnostního incidentu,
 - d) popis přijatých opatření pro vyřešení daného bezpečnostního incidentu včetně opatření ke zmírnění možných nepříznivých dopadů.
4. Není-li možné informace poskytnout současně, jsou poskytnuty postupně bez zbytečného odkladu.
5. Veškeré bezpečnostní incidenty jsou dokumentovány včetně popisu, dopadů a přijatých nápravných opatření.
6. Dokumentace je uložena a na vyžádání předložena Úřadu pro ochranu osobních údajů a oprávněné organizaci dle článku 19.

Článek 15

Oznamování bezpečnostních incidentů fyzické osobě

1. Poskytovatel oznámí fyzické osobě porušení zabezpečení osobních údajů v případě, že v jeho důsledku může dojít k vysokému riziku ohrožení práv a svobody této fyzické osoby.
2. Oznámení musí být jasné a srozumitelné a musí obsahovat minimálně tyto informace:
 - a) jméno a kontaktní údaje odpovědné osoby nebo pověřence, kteří mohou poskytnout bližší informace,
 - b) popis pravděpodobných důsledků porušení ochrany osobních údajů,
 - c) popis nápravných opatření.



3. Oznámení fyzické osobě se nevyžaduje:
- a) pokud dotčené osobní údaje byly šifrované, například při předávání dat zdravotním pojišťovám,
 - b) poskytovatel přijal následná opatření, která zajistí omezení vysokých rizik pro práva a svobody dotčené fyzické osoby,
 - c) v případech, kdyby takové oznámení, například velkému počtu fyzických osob, vyžadovalo úsilí nepřiměřené organizačním a technickým možnostem poskytovatele. Fyzické osoby mohou být za této situace informovány pomocí veřejného oznámení, třeba na webových stránkách poskytovatele nebo Grémia.

Článek 16

Odovědnost poskytovatele a náhrada újmy

1. Poskytovatel je odpovědný za újmu, kterou způsobí zpracováním osobních údajů takovým způsobem, který je v rozporu s Kodexem a GDPR. Zpracovatel je za újmu zodpovědný pouze v případě, že neplnil povinnosti stanovené GDPR nebo jednal v rozporu s pokyny poskytovatele, správce.
2. Fyzická osoba, která utrpěla v důsledku porušení Kodexu a GDPR hmotnou či nehmotnou újmu, má právo obdržet od poskytovatele náhradu.
3. Poskytovatel může na základě zmocnění využít pomoc Grémia při jednání o mimosoudním vyrovnání a při dalších postupech pro řešení sporů s fyzickými osobami v souvislosti se zpracováním osobních údajů dle článku 40 odstavce 2. k) GDPR.

Článek 17

Posouzení vlivu na ochranu osobních údajů

1. Poskytovatel, který zpracovává osobní údaje na základě povinnosti stanovené právními předpisy, zejména zákonem o sociálních službách a zákonem o zdravotních službách, má podle příslušného ustanovení zákona o ochraně osobních údajů²⁴ výjimku z povinnosti provádět posouzení vlivu zpracování na ochranu osobních údajů.
2. Poskytovatel, který vykonává i jiné činnosti, než je poskytování sociálních případně zdravotních služeb, a zpracovává osobní údaje fyzických osob za jiným účelem a v rozsahu neupraveném Kodexem, je povinen posoudit míru rizika pro práva a svobody fyzických osob a nutnost zpracování posouzení vlivu na ochranu osobních údajů dle § 37 zákona o ochraně osobních údajů.

²⁴ § 10, zákona č. 110/2019 Sb., Zákon o zpracování osobních údajů



Článek 18

Pověřenec pro ochranu osobních údajů

18.1 Jmenování pověřence pro ochranu osobních údajů

1. Poskytovatel, správce, nemusí jmenovat pověřence pro ochranu osobních údajů (dále jen pověřenec) v případě, že:
 - a) osobní údaje zpracovává jednotlivý sociální pracovník nebo zdravotnický pracovník,
 - b) zpracování zvláštních kategorií údajů, především osobních údajů vedených v sociální či zdravotnické dokumentaci, nelze považovat za rozsáhlé.
2. Poskytovatel musí jmenovat pověřence, pokud její hlavní činnost spočívá v rozsáhlém zpracování zvláštních kategorií údajů.
3. Pověřenec by měl být jmenován na základě znalosti sociální péče, GDPR, sociální a zdravotnické legislativy a ostatních právních předpisů ovlivňujících ochranu osobních údajů a Kodexu.
4. Pověřenec může být zaměstnancem poskytovatele nebo fyzickou či právnickou osobou plnící úkoly na základě smlouvy.
5. Poskytovatel zveřejní kontaktní údaje pověřence v dokumentu o právech klientů, uvede je ve vnitřní dokumentaci a případně na webových stránkách. Sdělí je rovněž Úřadu pro ochranu osobních údajů.

18.2 Postavení a úkoly pověřence

1. Pověřenec v souladu s článkem 39 GDPR plní minimálně následující úkoly:
 - a) poskytuje informace a poradenství poskytovateli a jeho zaměstnancům,
 - b) kontroluje, zda je zpracování osobních údajů fyzických osob poskytovatelem, v souladu s Kodexem,
 - c) spolupracuje s Úřadem pro ochranu osobních údajů a působí jako kontaktní místo,
 - d) bere patřičný ohled na rizika spojená s operacemi zpracování, zejména na zpracování zdravotnické dokumentace a dalších osobních údajů zvláštní kategorie.
2. Poskytovatel pověřence při plnění úkolů podporuje, poskytuje mu k tomu přiměřené zdroje, přístup a zajistí jeho včasné zapojení. Pověřenec je přímo podřízen řídicím pracovníkům.
3. Poskytovatel zajistí pravidelná školení nezbytná k udržování a rozšiřování odborných znalostí pověřence v cyklech odpovídajících pravidelnému monitorování dodržování Kodexu.
4. V souvislosti s plněním úkolů musí být zajištěna nezávislost pověřence, nesmí být sankcionován ani propuštěn.
5. Pověřenec řeší veškeré záležitosti související s ochranou osobních údajů a práv fyzických osob přímo s dotčenými fyzickými osobami.



6. Pověřenec nesmí být při výkonu svých úkolů ve střetu zájmů, je smluvně vázán mlčenlivostí.

Článek 19

Účast na Kodexu a monitorování dodržování Kodexu

1. Poskytovatel, který se dobrovolně rozhodne připojit k účasti na Kodexu (dále jen účastník Kodexu), přijímá potvrzením souhlasu se zněním Kodexu a v něm stanovených požadavků závazek:
- a) dodržovat Kodex,
 - b) uzavřít smlouvu s organizací oprávněnou pro monitorování dodržování Kodexu do 30 dnů od podepsání závazku k jeho dodržování,
 - c) účastnit se pravidelného monitorování dodržování Kodexu v termínech určených oprávněnou organizací,
 - d) účastnit se mimořádného monitorování dodržování Kodexu, v případech kdy došlo nebo by mohlo dojít k závažnému porušení Kodexu,
 - e) oznámit oprávněné organizaci veškeré informace a změny, které by mohly ovlivnit jeho způsobilost dodržovat Kodex,
 - f) oprávněné organizaci předložit na požádání vnitřní dokumentaci, další údaje a podklady potřebné pro monitorování dodržování Kodexu a poskytnout nezbytnou součinnost, včetně přístupu pověřené osoby,
 - g) zaslat oprávněné organizaci hlášení o bezpečnostním incidentu,
 - h) spolupracovat na požádání s Úřadem pro ochranu osobních údajů při plnění jeho úkolů.
2. Grémium vede evidenci účastníků Kodexu a může je z této evidence vyřadit z následujících důvodů:
- a) poskytovatel nesplnil závazek uvedený v odstavci 1/b),
 - b) na základě podnětu oprávněné organizace.

Článek 20

Účinnost Kodexu

Tento Kodex nabývá účinnosti prvním dnem následujícího měsíce po jeho zveřejnění na webových stránkách Grémia.

V Litoměřicích dne 12. 11. 2019

Mgr. LUCIE JURSIKOVÁ BROŽKOVÁ

Předseda

Mgr. JAROMÍRA KÖNIGSMARKOVÁ

Místopředseda