

Dokumentace

GDPR

nařízení o ochraně osobních údajů

Poskytovatel zdravotních služeb:

.....

Adresa (sídlo):

.....

IČO:

dále jen „správce“ nebo „správce osobních údajů“

Tato dokumentace obsahuje

- Směrnici upravující technicko-organizační opatření při zpracování osobních údajů
- Informaci pro pacienty o zpracování osobních údajů
- Rizika pro práva a svobody subjektů údajů
- Záznamy o činnostech zpracování osobních údajů
- Vyhodnocení rizik pro práva a svobody subjektů údajů
- Právní rozbor (zdůvodnění) nejmenování pověřence pro ochranu osobních údajů
- Právní rozbor (zdůvodnění) neprovedení vlivu na ochranu osobních údajů
- Informaci pro zaměstnance o zpracování osobních údajů
- Záznamy o seznámení zaměstnanců s technicko-organizačními opatřeními při zpracování osobních údajů a nakládání s osobními údaji
- Dokumentace všech případů porušení zabezpečení osobních údajů

Směrnice upravující eliminaci rizik při správě osobních údajů – technicko-organizační opatření

1. Účel

Tento pracovní postup stanovuje pravidla pro řízení rizik při zpracování osobních údajů u poskytovatele zdravotních služeb jako Správce. Správce zpracovává osobní údaje při:

- vedení zdravotnické dokumentace ve zdravotnickém zařízení
- vedení objednávacích systémů
- zpracování výkazů pro zdravotní pojišťovny
- účetních a daňových operací
- vedení evidence stížností
- vedení seznamů vyřazené dokumentace
- vedení osobních spisů zaměstnanců, mzdová agenda, záznamy o provedených školeních
- vedení evidence a hlášení nežádoucích příhod a nežádoucích účinků
- vedení evidence daňových dokladů vystavených dodavateli.

2. Oblast platnosti

Tento pracovní postup je závazný pro všechny zaměstnance poskytovatele.

3. Pojmy a zkratky

3.1. Pojmy

Riziko

- je obecně pravděpodobnost výskytu nežádoucí události s negativními dopady
- je spojeno s pravděpodobností nebo možností vzniku škody
- je kvantitativní a kvalitativní vyjádření ohrožení
- vyjadřuje pravděpodobnost, že nastane negativní jev
- vyjadřuje, kolikrát se negativní jev vyskytne a co způsobí
- definuje se jako kombinace pravděpodobnosti nežádoucí události a rozsahu, závažnosti možného zranění, škody nebo poškození zdraví.

Míra rizika – kombinace pravděpodobnost vzniku události a následků, které tato událost může způsobit.

Analýza rizik – základní a nezbytný krok pro zvládnutí řízení rizik v organizaci, zvláště pak těch rizik, která ohrožují správný chod organizace.

4. Řízení rizik

4.1. Prevence a řízení rizik

Prevencí rizik se rozumí všechna opatření, která mají za cíl předcházet rizikům, snižovat je na přijatelnou úroveň a realizovat účinná preventivní opatření k jejich odstranění.

Podmínkou účinné a účelné prevence rizik je jejich identifikace a porozumění jejich příčinám. Proto je organizace povinná rizika vyhledávat, zjišťovat jejich příčiny a zdroje a přijímat příslušná opatření.

Pro hodnocení rizik a zjištění jejich příčin a zdrojů se používají různé metody, které se od sebe liší mírou objektivity, pracností a účelem, ke kterému má hodnocení rizik sloužit. Zvolení metody je na zvážení organizace.

4.2. Analýza rizik

Největší překážkou při hodnocení rizik je obvykle nedostatek dat a informací. Protože hodnocení rizik slouží jako základní zdroj informací pro rozhodování, je důležité znát a být si vědom omezení použitých metod. Základní podmínkou je dostatečná transparentnost jednotlivých kroků, jak pro uživatele výsledků hodnocení, tak pro ty, jichž se následky rizika mohou dotknout.

4.3. Pracovní postup

1. Poskytovatel je odpovědný za zpracování „Katalogu rizik“.
2. Aktualizace Katalogu rizik probíhá podle potřeb.

4.4. Základní zásady eliminace rizik

1. Ochrana osobních údajů je zajišťována prostřednictvím ochrany médií/zařízení, která se používají k jejich zaznamenání. Tato ochrana je nezbytná pro snížení rizika neautorizovaného přístupu k datům a k zajištění ochrany proti ztrátě nebo poškození. Pozornost musí být věnována umístění a likvidaci médií/zařízení, která osobní údaje obsahují.
2. Média/Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozba a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.
3. V případě použití elektronických zařízení pro zpracování a uchování osobních dat musí být zařízení chráněno před selháním napájení (např. použití záložních zdrojů UPS) a před dalšími výpadky způsobenými selháním podpůrných služeb.
4. Ochrana proti škodlivým programům je založena na detekci škodlivých programů, opravných programů a na bezpečnostním povědomí uživatelů. Instalace a pravidelná aktualizace antivirových detekčních a opravných programů pro kontrolu počítačů a médií je prováděna pravidelně a ve výjimečných případech ad-hoc způsobem.
5. Záložní kopie důležitých informací a programového vybavení organizace jsou pořizovány a testovány v pravidelných intervalech. Záložní kopie zdravotnické dokumentace je pořizována v intervalech stanovených právními předpisy.
6. Zálohy jsou ukládány na bezpečném místě, v dostatečné vzdálenosti od ordinace, aby v případě havárie nebyly poškozeny nebo zničeny.
7. Při správě vyměnitelných médií obsahujících osobní údaje je nutno dbát potřebné opatrnosti. Pokud média obsahují osobní údaje a jsou dále provozně neupotřebitelná, měla by být bezpečně zlikvidována, například spálením, skartováním nebo smazáním dat před jejich opětovným použitím jiným způsobem v rámci Správce.
8. Pro zabránění neautorizovanému přístupu nebo zneužití osobních údajů jsou stanovena zvláštní pravidla pro manipulaci s nimi a pro jejich ukládání (viz Přílohy č. 2–5).
9. Přístupová pravidla a oprávnění k osobním údajům jsou jasně stanovena pro každého uživatele (viz Přílohy č. 3, 4) a jsou pravidelně monitorována a kontrolována.
10. Všichni zaměstnanci užívají jako způsob autentizace při použití výpočetní techniky k ověření své identity heslo.
11. Při použití mobilní výpočetní techniky jsou přijata zvláštní opatření na ochranu proti rizikům použití mobilních výpočetních a komunikačních prostředků (viz Příloha č. 5)
12. Média/zařízení, na nichž jsou osobní údaje uloženy, jsou skladována a archivována pouze po nezbytně nutnou dobu (zásada minimalizace).

5. Přílohy

Příloha č. 1: Katalog rizik

Příloha č. 2: Plán eliminace rizik při vedení dokumentace v elektronické podobě

Příloha č. 3: Plán eliminace rizik při vedení zdravotnické dokumentace v listinné podobě

Příloha č. 4: Plán eliminace rizik při správě osobních údajů mimo režim zdravotnické dokumentace

Příloha č. 5: Plán eliminace rizik při použití mobilní výpočetní techniky

Příloha č. 1: Katalog rizik

Druh hrozby	Možné příčiny vzniku
Narušení důvěrnosti údajů (s údaji se seznámil někdo, kdo k tomu neměl oprávnění)	<ul style="list-style-type: none"> - nedostatečné zabezpečení sítě - prolomení přístupových práv uživatelů - neexistence IT bezpečnostní strategie - nezabezpečení dat při výpadku informačních systémů - nedostatečné zabezpečení přenosu dat - nedostatečná antivirová ochrana - nedostatečné nastavení bezpečnosti IT infrastruktury - možnost nahrávat data pacientů na nosiče (CD, DVD, flash disk, externí hard disk) - nedodržování pravidel při předávání důvěrných informací o zdrav. stavu - chybějící záznam souhlasu s poskytováním informací o zdrav. stavu - chybná volba vhodného místa pro předávání informací - porušení povinnosti zachování mlčenlivosti - nedostatečné ověření totožnosti osob určených pacientem k poskytování informací - únik dat ze systému - nezabezpečený přístup do papírové i elektronické dokumentace (volně přístupné kartotéky, klíče ve dveřích z vnější strany, neodhlášení se z PC atd.)
Narušení integrity údajů (údaje byly pozměněny či upraveny)	<ul style="list-style-type: none"> - provozování kritických prvků výpočetní techniky nad mez životnosti - používání kritických prvků bez zabezpečení podpory - nedostatečné zabezpečení sítě - prolomení přístupových práv uživatelů - neexistence IT bezpečnostní strategie
Narušení dostupnosti údajů (údaje sice existují, nelze je ale použít)	<ul style="list-style-type: none"> - fyzická ztráta zdravotnické dokumentace - nedostatečné znalosti a kvalifikace personálu, selhání lidského činitele, nedostatečné proškolení uživatelů IS nebo správců, administrátorů IS - porušení interních předpisů - nekonzistence dat v důsledku chyb IS - provozování kritických prvků výpočetní techniky nad mez životnosti
Ztráta údajů (údaje byly nenávratně ztraceny)	<ul style="list-style-type: none"> - nezabezpečení při výpadku informačních systémů (serverů) - nedostatečná antivirová ochrana - nedostatečná kontrola - nedostatečné nastavení bezpečnosti IT infrastruktury - chybné nastavení IS - nedostatečné znalosti a kvalifikace personálu, uživatelů IS - počítače, výpočetní a archivační technika používaná nad mez životnosti - nedostatečná kontrola - nebezpečí krádeže, nedostatečný režim uložení přístupových klíčů - nedostatečná kontrola vhodnosti prostředí pro IT (provozní teplota, vlhkost atd.) - nebezpečí vzniku požáru - zastarání techniky, datových médií

Příloha č. 2: Plán eliminace rizik při vedení dokumentace v elektronické podobě

Povinnosti jednotlivých zaměstnanců, které souvisejí s bezpečností a nakládání s daty a elektronickými dokumenty:

- 1) při zpracovávání informací pomocí výpočetní techniky musí být především zabezpečena ochrana všech dat uložených na pevném disku počítače, přičemž se zde uplatňuje vždy ochrana heslem a stanovením rozsahu jednotlivých přístupových oprávnění v souladu s pracovní náplní toho konkrétního zaměstnance. Dále platí pravidlo, že pokud má uživatel oprávnění vkládat či měnit data uložená v systému, musí být zajištěna jeho jednoznačná identifikace při jeho přístupu k datům,
- 2) rozsah přístupu k datům a informacím a oprávnění k jejich využívání, včetně změn, vkládání nebo případného vymazání dat, musí odpovídat obsahu pracovních povinností, které má zaměstnanec podle jeho pracovního zařazení a právním předpisům
- 3) za určení rozsahu přístupových práv každému zaměstnanci jako uživateli IT techniky a informačního systému odpovídá poskytovatel zdravotních služeb
- 4) za samotné nastavení rozsahu přidělených přístupových práv každému zaměstnanci odpovídá poskytovatel zdravotních služeb (případně jím určený správce IT)
- 5) pro zálohování dat a archivaci vedených pomocí výpočetní techniky platí zvláštní předpis, přičemž ta data, která se nearchivují, musí být neustále a bezpečně zálohována do té doby, než dojde podle příslušného právního předpisu nebo dohody smluvních stran k jejich skartaci/zničení.

Příloha č. 3: Plán eliminace rizik při vedení zdravotnické dokumentace v listinné podobě

Povinnosti jednotlivých zaměstnanců, které souvisejí s bezpečností a nakládání s daty a listinnými dokumenty:

- 1) rozsah přístupu k datům a informacím a oprávnění k jejich využívání, včetně změn, vkládání nebo případného vymazání dat, musí odpovídat obsahu pracovních povinností, které má zaměstnanec podle jeho pracovního zařazení a právních předpisů;
- 2) dokumentace je uchovávána odděleně a je k ní zajištěn pouze zabezpečený přístup (kartotéka je uzamykatelná nebo je pod stálým dohledem zaměstnance poskytovatele);
- 3) po vyjmutí karty pacienta z kartotéky je karta přístupná pouze lékaři a sestře, příp. další osobám podle příslušných ustanovení zákona č. 372/2011 Sb.; karta je následně ihned uložena zpět do kartotéky;
- 4) veškeré nakládání se zdravotnickou dokumentací probíhá podle příslušných ustanovení zákona č. 372/2011 Sb. a dalších právních předpisů.

Příloha č. 4: Plán eliminace rizik při správě osobních údajů mimo režim zdravotnické dokumentace

Povinnosti jednotlivých zaměstnanců, které souvisejí s bezpečností a nakládání s daty v elektronické podobě a listinnými dokumenty mimo režim zdravotnické dokumentace:

- 1) rozsah přístupu k datům a informacím a oprávnění k jejich využívání, včetně změn, vkládání nebo případného vymazání dat, musí odpovídat obsahu pracovních povinností, které má zaměstnanec podle jeho pracovního zařazení a právních předpisů;
- 2) média/data jsou uchovávána na místech, kde je zabráněno vstupu neoprávněným osobám;
- 3) osobní údaje jsou zpracovávány pouze v souladu se stanoveným účelem zpracování;
- 4) přístupová pravidla a oprávnění k osobním údajům jsou pravidelně monitorována a kontrolována;
- 5) média/zařízení, na nichž jsou osobní údaje uloženy, jsou skladována a archivována pouze po nezbytně nutnou dobu (zásada minimalizace). Po uplynutí této doby jsou skartována.

Příloha č. 5: Plán eliminace rizik při použití mobilní výpočetní techniky

1. Při použití mobilních výpočetních prostředků, například notebooků, tabletů a mobilních telefonů musí být věnována zvláštní pozornost tomu, aby nebyly prozrazeny zpracovávané osobní údaje.
2. Mobilní výpočetní prostředky musí být chráněny proti zcizení a možnosti získání osobních údajů v nich obsažených (např. vzdálené vypnutí, možnost vzdáleného vymazání dat). Zařízení, obsahující zpracovávané osobní údaje nesmí zůstat bez dohledu, mělo by být fyzicky zabezpečeno nebo by jeho funkce měly být zajištěny speciálním uzamčením.
3. Při použití mobilních výpočetních zařízení připojených k sítím musí být zajištěna vhodná ochrana (antivirový program, heslování) a vzdálený přístup k osobním údajům prostřednictvím veřejných sítí musí být umožněn pouze po úspěšné identifikaci a autentizaci, a to s nasazením vhodných mechanismů řízení přístupu.
4. Zvláštní pozornost musí být věnována použití mobilních výpočetních zařízení na veřejných místech a jiných nechráněných místech mimo prostor ordinace.

Informace pro pacienty o zpracování osobních údajů

podle 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)

I. Správce osobních údajů

Správce je poskytovatelem zdravotních služeb v souladu se zákonem č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, ve znění pozdějších předpisů.

II. Účel/y zpracování osobních údajů

Vaše osobní údaje zpracováváme za účelem

- poskytování zdravotních služeb
- vykazování hrazených zdravotních služeb
- vyúčtování nehrazených zdravotních služeb
- sdělování údajů o zdravotním stavu Vám a dalším oprávněným osobám
- organizace poskytování zdravotních služeb (objednávání pacientů)
- vedení evidence o našich příjmech a výdajích, přijatých platbách a o hospodaření, jak vyplývají z předpisů upravujících daně a účetnictví

III. Právní základ zpracování osobních údajů

Právním základem pro zpracování Vašich osobních údajů uvedených v bodu II. je

- splnění naší zákonné povinnosti (zejména zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, zákon č. 563/1991 Sb., o účetnictví, zákon č. 586/1992 Sb., o daních z příjmů, zákon č. 634/1992, o ochraně spotřebitele)
- splnění závazků ze smlouvy o péči o zdraví, na jejímž základě Vám poskytujeme zdravotní služby (tato smlouva nemusí být uzavřena písemně)

IV. Příjemci osobních údajů

Příjemci Vašich osobních údajů mohou v souladu s ustanoveními právních předpisů v konkrétních případech kromě Vás být: poskytovatel zdravotních služeb, orgány veřejné moci a osoby oprávněné nahlížet do zdravotnické dokumentace podle § 31, § 32, § 33 a § 65 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. Osobní údaje mohou být pro zajištění výše popsaných účelů zpracovávány vedle správce také zpracovateli, a to na základě smluv o zpracování osobních údajů uzavřených v souladu s obecným nařízením o ochraně osobních údajů.

Vaše osobní údaje nepředáváme do zahraničí.

V. Doba zpracování osobních údajů

Osobní údaje obsažené ve zdravotnické dokumentaci jsou zpracovávány po dobu stanovenou vyhláškou č. 98/2012 Sb., o zdravotnické dokumentaci. Osobní údaje zpracovávají pro další účely uvedené v bodu III jsou zpracovávány po dobu stanovenou zákonem nebo po dobu, po kterou budete naším pacientem, a následně po dobu jednoho roku poté, co naším pacientem přestanete být.

VI. Práva subjektu údajů

Při zpracování osobních údajů máte následující práva týkající se ochrany svých osobních údajů:

- právo požadovat od nás přístup k Vaším osobním údajům;
- právo na opravu Vašich osobních údajů, které zpracováváme;
- právo na omezení zpracování. Omezení zpracování znamená, že musíme Vaše osobní údaje, u nichž bylo zpracování omezeno, označit a po dobu trvání omezení je nesmíme dál zpracovávat s výjimkou jejich uložení. Právo na omezení zpracování máte tehdy, jestliže

- popíráte přesnost osobních údajů, a to na dobu potřebnou k tomu, abychom mohli přesnost osobních údajů ověřit;
- zpracování je protiprávní a Vy odmítáte výmaz osobních údajů a žádáte místo toho o omezení jejich použití;
- jestliže již Vaše osobní údaje nepotřebujeme pro účely zpracování, ale Vy je požadujete pro určení, výkon nebo obhajobu právních nároků;
- jestliže jste vznesl/a námitku proti zpracování uvedenou níže v bodu VII., dokud nebude ověřeno, zda naše oprávněné důvody pro zpracování převažují nad Vašimi zájmy nebo právy a svobodami;

- právo na výmaz osobních údajů. Právo na výmaz osobních údajů se vztahuje jen na osobní údaje, které zpracováváme k jiným účelům, než je poskytování zdravotních služeb. Údaje, které o Vás vedeme za účelem poskytování zdravotních služeb (např. ve zdravotnické dokumentaci), vymazat nesmíme;
- právo na přenositelnost údajů. Můžete žádat, abychom Vám Vaše osobní údaje poskytli za účelem jejich předání jinému správci osobních údajů, nebo abychom je sami předali jinému správci osobních údajů. Toto právo však máte pouze ohledně těch údajů, které zpracováváme automatizovaně na základě Vašeho souhlasu nebo smlouvy s Vámi. Údaje, které o Vás vedeme za účelem poskytování zdravotních služeb (např. ve zdravotnické dokumentaci), však smíme poskytnout jen Vám a za zákonných podmínek též jinému poskytovateli zdravotních služeb nebo orgánu veřejné moci.
- právo podat stížnost u dozorového úřadu, a to v případě, že se domníváte, že zpracováním osobních údajů dochází k porušení právních předpisů o ochraně osobních údajů. Stížnost můžete podat u dozorového úřadu v místě svého obvyklého bydliště, místě výkonu zaměstnání nebo v místě, kde došlo k údajnému porušení. V České republice je dozorovým úřadem Úřad na ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7, www.uoou.cz.

VII. Právo vznést námitku proti zpracování

V případě, že Vaše osobní údaje zpracováváme pro účely oprávněných zájmů našich nebo někoho dalšího (právní základy zpracování jsou uvedeny v bodu III), máte kdykoliv právo vznést proti takovému zpracování námitku. Námitku můžete vznést na naší adrese uvedené v bodu I. Pokud takovou námitku vznesete, budeme oprávněni v takovém zpracování pokračovat jen tehdy, pokud prokážeme závažné oprávněné důvody pro zpracování, které převažují nad Vašimi zájmy nebo právy a svobodami, a dále tehdy, pokud půjde o zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků.

VIII. Povinné zpracování a povinnost poskytnout osobní údaje

Zpracování Vašich osobních údajů pro účely poskytování zdravotních služeb je zákonným požadavkem. Neposkytnutím Vašich osobních údajů může znamenat, že Vám nebudeme moci poskytnout zdravotní služby, čímž může dojít k poškození Vašeho zdraví či přímému ohrožení života (§ 41 odst. 1 písm. d) zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování). Povinnost poskytnout osobní údaje pacienta se týká i jeho zákonného zástupce nebo opatrovníka (§ 41 odst. 2 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování).

RIZIKA pro práva a svobody fyzických osob

ÚDAJE A HROZBY			PRÁVA A SVOBODY (čísla v modré části tabulky představují význam konkrétního práva na stupnici 1 až 5)							
zdroj údajů (podle záznamů o činnostech zpracování)	hrozba (identifikace možných hrozeb)	zhodnocení míry pravděpodobnosti naplnění hrozby (na stupnici 1 až 5)	4	3	2	5	4	2	3	2
			právo na soukromí	právo na ochranu cti a důstojnosti	právo na informační sebeurčení	právo na život	právo na duševní a tělesnou integritu	právo na informace	právo na ochranu osobních údajů	zákaz diskriminace
Číslo v bílé části tabulky představují zhodnocení závažnosti dopadu konkrétní realizované hrozby do konkrétního práva subjektu údajů na stupnici 1-5										
zdravotnická dokumentace	narušení důvěrnosti údajů	2	5	4	1	1	2	0	5	0
	narušení integrity údajů	1	1	2	0	3	3	3	3	0
	narušení dostupnosti údajů	1	1	1	0	3	3	4	2	0
	ztráta údajů	1	1	1	1	3	2	3	5	0
objednávací systémy (knihy, záznamníky, diáře)	narušení důvěrnosti údajů	3	2	1	0	0	0	0	2	0
	narušení integrity údajů	3	0	0	0	0	0	0	1	0
	narušení dostupnosti údajů	3	0	0	0	0	0	0	0	0
	ztráta údajů	3	0	0	0	0	0	0	2	0
výkazy poskytnutých hrazených služeb	narušení důvěrnosti údajů	1	5	4	1	1	2	0	5	0
	narušení integrity údajů	1	1	2	0	3	3	3	3	0
	narušení dostupnosti údajů	1	1	1	0	0	0	0	0	0
	ztráta údajů	0	0	0	0	0	0	0	0	0
příjmové doklady, faktury, vyúčtování poskytnutých zdravotních služeb	narušení důvěrnosti údajů	1	2	2	0	0	0	0	3	0
	narušení integrity údajů	1	1	1	0	1	1	0	3	0
	narušení dostupnosti údajů	1	0	0	0	0	0	0	0	0
	ztráta údajů	3	0	0	0	0	0	0	0	0
evidence stížností; stížnostní spis	narušení důvěrnosti údajů	2	5	4	1	1	2	0	5	0
	narušení integrity údajů	1	1	2	0	0	1	3	3	0
	narušení dostupnosti údajů	1	1	1	0	1	2	3	2	0
	ztráta údajů	1	1	1	1	1	2	3	5	0
evidence a hlášení nežádoucích příhod a nežádoucích účinků	narušení důvěrnosti údajů	1	3	2	0	0	0	0	2	0
	narušení integrity údajů	1	0	0	0	0	1	0	1	0
	narušení dostupnosti údajů	1	0	0	0	0	1	0	0	0
	ztráta údajů	1	0	0	0	0	1	0	2	0
seznam vyřazené zdravotnické dokumentace (skartační deník)	narušení důvěrnosti údajů	1	1	0	0	0	0	0	2	0
	narušení integrity údajů	1	0	0	0	0	0	0	1	0
	narušení dostupnosti údajů	1	0	0	0	0	0	0	0	0
	ztráta údajů	2	0	0	0	0	0	0	2	0
evidence a hlášení případů porušení zabezpečení osobních údajů	narušení důvěrnosti údajů	1	3	2	0	0	0	0	2	0
	narušení integrity údajů	1	0	0	0	0	1	0	1	0
	narušení dostupnosti údajů	1	0	0	0	0	1	0	0	0
	ztráta údajů	1	1	1	0	0	1	0	2	0
osobní spis zaměstnance	narušení důvěrnosti údajů	2	5	4	1	1	2	0	5	0
	narušení integrity údajů	1	1	2	0	1	2	3	3	0
	narušení dostupnosti údajů	1	1	1	0	1	2	4	2	0
	ztráta údajů	1	1	1	1	1	2	3	5	0
daňové doklady vystavené dodavateli	narušení důvěrnosti údajů	1	1	0	0	0	0	0	2	0
	narušení integrity údajů	1	0	0	0	0	0	0	1	0
	narušení dostupnosti údajů	3	0	0	0	0	0	0	0	0
	ztráta údajů	2	0	0	0	0	0	0	2	0
mzdová agenda	narušení důvěrnosti údajů	2	5	4	1	1	2	0	5	0
	narušení integrity údajů	1	1	2	0	1	2	3	3	0
	narušení dostupnosti údajů	1	1	1	0	1	2	4	2	0
	ztráta údajů	1	1	1	1	1	2	3	5	0
záznamy o provedených školeních, instruktážích	narušení důvěrnosti údajů	2	1	0	0	0	0	0	2	0
	narušení integrity údajů	1	0	0	0	0	0	0	1	0
	narušení dostupnosti údajů	1	0	0	0	0	0	0	0	0
	ztráta údajů	1	0	0	0	0	0	0	2	0

ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

pověřenec pro ochranu osobních údajů:		nebyl jmenován, protože (i) správce není orgánem veřejné moci ani veřejným ani (iii) v rozsáhlém zpracování zvláštních kategorií osobních údajů (bližší odůvodnění)				
posouzení vlivu zpracování na ochranu osobních údajů:		nebylo provedeno, protože správce neprovádí zpracování, které by pravděpodobně				
Zdroj údajů	Kategorie subjektů údajů	Právní titul	Účel zpracování	Druhy zpracování	Forma zpracování	Kateg. příjemců Vlastní potřeba
zdravotnická dokumentace	pacienti; příbuzní pacientů; osoby nahlízející do zdravotnické dokumentace; doprovázející osoby; zdravotničtí pracovníci	splnění právní povinnosti správce (§ 53 odst. 1 zák. č. 372/2011 Sb.)	poskytování zdravotních služeb; vykazování hrazených zdravotních služeb; sdělování údajů o zdravotním stavu	shromáždění; zaznamenání; uložení; vyhledání; nahlédnutí; použití; zpřístupnění; omezení; výmaz; zničení	listinná; elektronická	správce a jeho zaměstnanci při výkonu svého povolání (§ 65 odst. 2 písm. a) zák. č. 372/2011 Sb.)
objednávací systémy (knihy, záznamníky, diáře)	pacienti; zdravotničtí pracovníci	splnění smlouvy	organizace poskytování zdravotních služeb	shromáždění; zaznamenání; uložení; vyhledání; použití; zpřístupnění; omezení; výmaz; zničení	listinná; elektronická	správce a jeho zaměstnanci při výkonu svého povolání
výkazy poskytnutých hrazených služeb	pacienti	splnění smlouvy (čl. 4 odst. 4 přílohy č. 3 vyhl. č. 618/2006 Sb.)	vykazování hrazených zdravotních služeb	zaznamenání; uložení; vyhledání; nahlédnutí; použití; zpřístupnění; výmaz; zničení	listinná; elektronická	správce
příjmové doklady, faktury, vyúčtování poskytnutých zdravotních služeb	pacienti; zákonní zástupci pacientů; zaměstnavatelé pacientů	splnění právní povinnosti správce (§ 45 odst. 2 písm. a) zák. č. 372/2011 Sb.; § 16 odst. 1 zák. č. 634/1992 Sb.)	vyúčtování zdravotních služeb; daňová evidence/vedení účetnictví	zaznamenání; uložení; vyhledání; nahlédnutí; použití; zpřístupnění; výmaz; zničení	listinná; elektronická	správce a jeho zaměstnanci při výkonu svého povolání
evidence stížností; stížnostní spis	pacienti; zákonní zástupci; stěžovatelé; zdravotničtí pracovníci	splnění právní povinnosti správce (§ 93 odst. 3 písm. c), d) zák. č. 372/2011 Sb.)	vyřizování stížností podle zák. č. 372/2011 Sb.	shromáždění; zaznamenání; uložení; vyhledání; použití; zpřístupnění; omezení; výmaz; zničení	listinná; elektronická	správce a jeho zaměstnanci při výkonu svého povolání
evidence a hlášení nežádoucích příhod a nežádoucích účinků	pacienti; zdravotničtí pracovníci	splnění právní povinnosti správce (§ 70 odst. 2 zák. č. 268/2014 Sb., § 93b odst. 1 zák. č. 378/2007 Sb.)	ochrana zdraví při používání zdravotnických prostředků a léčivých přípravků	shromáždění; zaznamenání; uložení; vyhledání; nahlédnutí; použití; výmaz; zničení	listinná; elektronická	správce a jeho zaměstnanci při výkonu svého povolání
seznam vyřazené zdravotnické dokumentace (skartační deník)	pacienti; zdravotničtí pracovníci	splnění právní povinnosti správce (příloha č. 2 vyhl. č. 98/2012 Sb.)	ochrana osobních údajů	shromáždění; zaznamenání; uložení; vyhledání; použití; výmaz; zničení	listinná; elektronická	správce a jeho zaměstnanci při výkonu svého povolání
evidence a hlášení případů porušení zabezpečení osobních údajů	pacienti; příbuzní pacientů; osoby nahlízející do zdravotnické dokumentace; doprovázející osoby; zdravotničtí pracovníci	splnění právní povinnosti správce (čl. 33, 34 nařízení Evropského parlamentu a Rady (EU) č. 2016/679)	ochrana osobních údajů	shromáždění; zaznamenání; uložení; vyhledání; použití; výmaz; zničení	listinná; elektronická	správce
osobní spis zaměstnance	zaměstnanci správce	splnění právní povinnosti správce (§ 312 odst. 1 zák. č. 262/2006 Sb.)	výkon práv a povinností vyplývajících ze základního pracovně právního vztahu	shromáždění; zaznamenání; uložení; vyhledání; použití; zpřístupnění; výmaz; zničení	listinná; elektronická	správce
daňové doklady vystavené dodavateli	dodavatelé správce	splnění právní povinnosti správce (§ 7b zák. č. 586/1992 Sb., § 9 a násl. zák. č. 563/1991 Sb.)	daňová evidence/vedení účetnictví	shromáždění; zaznamenání; uložení; vyhledání; použití; výmaz; zničení	listinná; elektronická	správce
mzdová agenda	zaměstnanci správce a jejich rodinní příslušníci	splnění právní povinnosti správce (§ 38j zák. č. 586/1992 Sb., § 10 odst. 2 zák. č. 48/1997 Sb., § 95 zák. č. 187/2006 Sb., § 22c zák. č. 589/1992 Sb.)	zpracování mzdové agendy, placení daně z příjmu, odvod pojistného na zdravotní pojištění a sociální zabezpečení	shromáždění; zaznamenání; uložení; vyhledání; použití; výmaz; zničení	listinná; elektronická	správce
záznamy o provedených školeních, instruktážích	zaměstnanci správce; osoby provádějící školení či instruktáž	splnění právní povinnosti správce (§ 103 odst. 3 zák. č. 262/2006 Sb., § 61 odst. 3 zák. č. 268/2014 Sb.)	vedení předepsané evidence o provedených školeních a instruktážích	shromáždění; zaznamenání; uložení; vyhledání; použití; výmaz; zničení	listinná; elektronická	správce

subjektem, jeho hlavní činnosti (ii) nespočívají v operacích zpracování, které by vyžadovaly rozsáhlé pravidelné a systematické monitorování subjektů údajů, provedeno v právním rozboru v části Právní rozbor)

mohlo mít za následek vysoké riziko pro práva a svobody fyzických osob (bližší odůvodnění provedeno v právním rozboru v části Právní rozbor)

Kategorie údajů		Předání do zahraničí	Výmaz/zničení
Externí subjekt	Standardní		
osoby oprávněné nahlížet do zdravotnické dokumentace (§ 65 zák. č. 372/2011 Sb.); osoby oprávněné získávat informace o zdravotním stavu pacienta; poskytovatelé zdravotních služeb; zdravotní pojišťovny	jméno; příjmení; datum narození; pohlaví; rodné číslo; adresa pobytu; doručovací adresa; kontaktní údaje (telefon, e-mail); informace o vykonávané epidemiologicky závazné činnosti; povolání či pracovní pozice; zaměstnavatel	informace o zdravotním stavu pacienta (včetně celkového), o průběhu a výsledku poskytovaných zdravotních služeb a o dalších významných okolnostech, souvisejících se zdravotním stavem pacienta a s postupem při poskytování zdravotních služeb, včetně anamnestických údajů potřebných pro poskytování zdravotních služeb, včetně obrazové dokumentace; informace o svéprávnosti pacienta; záznam o uznání nebo ukončení dočasné pracovní neschopnosti pacienta, posuzování zdravotního stavu v době jejího trvání, údaje o stanoveném režimu dočasné práce neschopného pojištěnce a jeho změnách, záznam o započítání potřeby ošetřování a jeho délce	NE podle skartačního řádu (příloha č. 3 vyhl. č. 98/2012 Sb.)
poskytovatel pokračující v poskytování zdravotních služeb	jméno; příjmení; datum narození; čas sjednaného ošetření; telefon; e-mail	NE	NE do konce kalendářního roku následujícího po zaznamenaném datu ošetření
zdravotní pojišťovna; zpracovatel výkazů	jméno; příjmení, číslo pojištěnce;	poskytnuté hrazené zdravotní služby	NE 5 let od předání zdravotní pojišťovně
pacient; jiný plátcе poskytnutých zdravotních služeb; zpracovatel účetnictví správce; orgán veřejné moci	jméno; příjmení; datum narození; adresa pobytu	poskytnuté zdravotní služby	NE podle předpisů upravujících vedení daňové evidence/účetnictví
stěžovatel; orgán veřejné moci	jméno; příjmení; datum narození; adresa pobytu	informace o zdravotním stavu pacienta, o průběhu a výsledku poskytovaných zdravotních služeb a o dalších významných okolnostech, souvisejících se zdravotním stavem pacienta a s postupem při poskytování zdravotních služeb, včetně anamnestických údajů potřebných pro poskytování zdravotních služeb; informace o svéprávnosti pacienta; záznam o uznání nebo ukončení dočasné pracovní neschopnosti pacienta, posuzování zdravotního stavu v době jejího trvání, údaje o stanoveném režimu dočasné práce neschopného pojištěnce a jeho změnách, záznam o započítání potřeby ošetřování a jeho délce	NE stížnostní spis do 1 roku od vyřízení stížnosti; evidence stížností do zániku oprávnění správce k poskytování zdravotních služeb
orgán veřejné moci	jméno; příjmení; datum narození	popis nežádoucí příhody a její následky pro zdraví a život postižené osoby	NE při výmazu/zničení zdravotnické dokumentace pacienta
orgán veřejné moci	jméno; příjmení; datum narození	NE	NE do zániku oprávnění správce k poskytování zdravotních služeb
orgán veřejné moci; dotčené subjekty údajů	jméno; příjmení; datum narození; adresa pobytu	NE	NE do 1 roku od oznámení případů porušení
zpracovatel mezd	jméno; příjmení; datum narození; rodné číslo; adresa pobytu; kontaktní údaje; členství v profesní organizaci; členství v odborných společnostech; odborná a specializovaná způsobilost; celoživotní vzdělávání	zdravotní způsobilost; bezúhonnost; dočasná pracovní neschopnost; členství v odborové organizaci	NE v souladu s právními předpisy upravujícími sociální zabezpečení a vedení daňové evidence/účetnictví
zpracovatel daňové evidence/účetnictví	jméno; příjmení; IČO; adresa sídla; kontaktní údaje (telefon, e-mail); poskytnuté služby	NE	NE podle předpisů upravujících vedení daňové evidence/účetnictví
zpracovatel mzdové agendy	jméno; příjmení; datum narození; rodné číslo; adresa pobytu; kontaktní údaje	doplňte, které zvláštní kategorie osobních údajů budou zpracovávány (možnosti: informace o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuální životě nebo sexuální orientaci fyzické osoby)	NE podle předpisů upravujících pojištění a sociální zabezpečení a daň z příjmu fyzických osob
orgán veřejné moci; osoba pokračující v poskytování zdravotních služeb	jméno; příjmení; datum narození; adresa pobytu; kontaktní údaje	NE	NE podle předpisů ukládajících vedení záznamů

VYHODNOCENÍ RIZIK pro práva a svobody fyzických osob

ÚDAJE A HROZBY		PRÁVA A SVOBODY							
zdroj údajů (podle záznamů o činnostech zpracování)	hrozba (identifikace možných hrozeb)	právo na soukromí	právo na ochranu cti a důstojnosti	právo na informační sebeurčení	právo na život	právo na duševní a tělesnou integritu	právo na informace	právo na ochranu osobních údajů	zákaz diskriminace
		Čísla představují číselné zhodnocení míry rizika na stupnici od 0 do 125. Hodnoty jsou vypočteny z údajů v tabulce „Rizika pro práva a svobody“							
zdravotnická dokumentace	narušení důvěrnosti údajů	40	24	4	10	16	0	30	0
	narušení integrity údajů	4	6	0	15	12	6	9	0
	narušení dostupnosti údajů	4	3	0	15	12	8	6	0
	ztráta údajů	4	3	2	15	8	6	15	0
objednávací systémy (knihy, záznamníky, diáře)	narušení důvěrnosti údajů	24	9	0	0	0	0	18	0
	narušení integrity údajů	0	0	0	0	0	0	9	0
	narušení dostupnosti údajů	0	0	0	0	0	0	0	0
	ztráta údajů	0	0	0	0	0	0	18	0
výkazy poskytnutých hrazených služeb	narušení důvěrnosti údajů	20	12	2	5	8	0	15	0
	narušení integrity údajů	4	6	0	15	12	6	9	0
	narušení dostupnosti údajů	4	3	0	0	0	0	0	0
	ztráta údajů	0	0	0	0	0	0	0	0
příjmové doklady, faktury, vyúčtování poskytnutých zdravotních služeb	narušení důvěrnosti údajů	8	6	0	0	0	0	9	0
	narušení integrity údajů	4	3	0	5	4	0	9	0
	narušení dostupnosti údajů	0	0	0	0	0	0	0	0
	ztráta údajů	0	0	0	0	0	0	0	0
evidenze stížností; stížnostní spis	narušení důvěrnosti údajů	40	24	4	10	16	0	30	0
	narušení integrity údajů	4	6	0	0	4	6	9	0
	narušení dostupnosti údajů	4	3	0	5	8	6	6	0
	ztráta údajů	4	3	2	5	8	6	15	0
evidenze a hlášení nežádoucích příhod a nežádoucích účinků	narušení důvěrnosti údajů	12	6	0	0	0	0	6	0
	narušení integrity údajů	0	0	0	0	4	0	3	0
	narušení dostupnosti údajů	0	0	0	0	4	0	0	0
	ztráta údajů	0	0	0	0	4	0	6	0
seznam vyřazené zdravotnické dokumentace (skartační deník)	narušení důvěrnosti údajů	4	0	0	0	0	0	6	0
	narušení integrity údajů	0	0	0	0	0	0	3	0
	narušení dostupnosti údajů	0	0	0	0	0	0	0	0
	ztráta údajů	0	0	0	0	0	0	12	0
evidenze a hlášení případů porušení zabezpečení osobních údajů	narušení důvěrnosti údajů	12	6	0	0	0	0	6	0
	narušení integrity údajů	0	0	0	0	4	0	3	0
	narušení dostupnosti údajů	0	0	0	0	4	0	0	0
	ztráta údajů	4	3	0	0	4	0	6	0
osobní spis zaměstnance	narušení důvěrnosti údajů	40	24	4	10	16	0	30	0
	narušení integrity údajů	4	6	0	5	8	6	9	0
	narušení dostupnosti údajů	4	3	0	5	8	8	6	0
	ztráta údajů	4	3	2	5	8	6	15	0
daňové doklady vystavené dodavateli	narušení důvěrnosti údajů	4	0	0	0	0	0	6	0
	narušení integrity údajů	0	0	0	0	0	0	3	0
	narušení dostupnosti údajů	0	0	0	0	0	0	0	0
	ztráta údajů	0	0	0	0	0	0	12	0
mzdová agenda	narušení důvěrnosti údajů	40	24	4	10	16	0	30	0
	narušení integrity údajů	4	6	0	5	8	6	9	0
	narušení dostupnosti údajů	4	3	0	5	8	8	6	0
	ztráta údajů	4	3	2	5	8	6	15	0
záznamy o provedených školeních, instruktážích	narušení důvěrnosti údajů	8	0	0	0	0	0	12	0
	narušení integrity údajů	0	0	0	0	0	0	3	0
	narušení dostupnosti údajů	0	0	0	0	0	0	0	0
	ztráta údajů	0	0	0	0	0	0	6	0

Stupnice rizika

Zanedbatelné	Velmi nízké	Nízké	Střední	Vysoké	Velmi vysoké
10	20	30	40	124	125

NEJMENOVÁNÍ POVĚŘENCE pro ochranu osobních údajů

právní rozbor

Správce nejmenoval pověřence pro ochranu osobních údajů s přihlédnutím k následujícím skutečnostem a závěrům:

Právní úprava

Podle čl. 37 odst. 1 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) správce jmenuje pověřence pro ochranu osobních údajů v každém případě, kdy

- a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
- b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo
- c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.

Podle čl. 37 odst. 4 obecného nařízení o ochraně osobních údajů musí správce jmenovat pověřence pro ochranu osobních údajů, vyžaduje-li to právo Unie nebo členského státu.

Status správce

Správce je poskytovatelem zdravotních služeb, který podniká podle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. Není orgánem veřejné moci ani veřejným subjektem. Není proto povinen jmenovat pověřence pro ochranu osobních údajů podle čl. 37 odst. 1 písm. a) obecného nařízení o ochraně osobních údajů.

Hlavní činnost správce

Hlavní činností správce je poskytování zdravotních služeb. Právní předpisy ukládají každému poskytovateli zdravotních služeb vést zdravotnickou dokumentaci a další evidence. Vedení zdravotnické dokumentace a dalších evidencí je neoddělitelnou součástí hlavní činnosti správce.

Rozsáhlé a pravidelné monitorování subjektů údajů

Monitorováním subjektů údajů se rozumí zejména jejich sledování a profilování na internetu, zejména za účelem přijetí rozhodnutí, která se jí týkají, nebo za účelem analýzy či odhadu jejich osobních preferencí, postojů a chování (bod 24. odůvodnění obecného nařízení o ochraně osobních údajů), v obecné rovině pak každá aktivita spočívající ve sledování subjektů údajů či jejich chování, a to bez ohledu na to, jestli k němu dochází fyzicky nebo v prostředí internetu. Takové operace správce neuskutečňuje, případně jen v míře nikoliv rozsáhlé. Není proto povinen jmenovat pověřence pro ochranu osobních údajů ani podle čl. 37 odst. 1 písm. b) obecného nařízení o ochraně osobních údajů.

Rozsáhlé zpracování zvláštních kategorií osobních údajů

Do hlavní činnosti správce spadají operace zpracování v rámci vedení zdravotnické dokumentace, tedy i zpracování zvláštních kategorií osobních údajů, zejména pak informací o zdravotním stavu (čl. 9 odst. 1 obecného nařízení o ochraně osobních údajů). Toto zpracování je v souladu s čl. 9 odst. 2 písm. h) obecného nařízení o ochraně osobních údajů. Nejde však o zpracování rozsáhlé. Správce jako poskytovatel ambulantních zdravotních služeb v oboru dermatovenerologie zpracovává zvláštní kategorie osobních údajů v míře, která je i na regionální úrovni nevýznamná, ba zanedbatelná.

Tento závěr správce vyslovuje s přihlédnutím k absolutnímu počtu svých pacientů, k rozsahu osobních údajů o nich vedených i k době zpracování. Závěr o tom, že správce jako jednotlivý poskytovatel ambulantních zdravotních služeb odpovídá i bodu 91 odůvodnění obecného nařízení o ochraně osobních údajů, podle kterého zpracování osobních údajů nemá být považováno za zpracování velkého rozsahu, pokud se jedná o zpracování osobních údajů pacientů nebo klientů jednotlivými lékaři. Správce vychází z toho, že rozsáhlé zpracování zvláštních kategorií osobních údajů při poskytování zdravotních služeb uskutečňují poskytovatelé zdravotních služeb, kteří zdravotní služby poskytují nejméně 10 ošetřujícími zdravotnickými pracovníky. Ošetřujícím zdravotnickým pracovníkem se přitom v souladu s § 3 odst. 2 zákona o zdravotních službách rozumí zdravotnický pracovník, který navrhuje, koordinuje, poskytuje a vyhodnocuje individuální léčebný postup u konkrétního pacienta a koordinuje poskytování dalších potřebných zdravotních služeb. V podmínkách ambulantního poskytovatele, jímž je i správce, je ošetřujícím zdravotnickým pracovníkem vždy lékař, nikoliv však zdravotní sestra. Je tomu tak proto, že tito nelékařští zdravotničtí pracovníci v ambulanci fakticky nevykonávají své povolání samostatně a návrh, koordinaci, realizaci a vyhodnocení individuálního léčebného postupu vždy zajišťuje lékař.

U poskytovatelů s menším počtem ošetřujících zdravotnických pracovníků, mezi které patří i správce, k rozsáhlému zpracování zvláštních kategorií osobních údajů vzhledem k výše uvedeným kritériím nedochází. Uvedenou hranici správce odůvodňuje tím, že u počtu, který nedosahuje 10, lze hovořit o jednotlivých zdravotnických pracovnících (jde o jednotky osob), o nichž pojednává bod 91 odůvodnění obecného nařízení o ochraně osobních údajů. Počet ošetřujících zdravotnických pracovníků současně limituje kapacitu správce jako poskytovatele zdravotních služeb a tím i rozsah zpracování osobních údajů. Správce proto není povinen jmenovat pověřence pro ochranu osobních údajů ani podle čl. 37 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů.

Požadavek práva Evropské unie nebo práva České republiky

Právo Evropské unie (obecné nařízení o ochraně osobních údajů nebo jiný pro správce závazný předpis) ani právní předpisy České republiky neukládají správci, aby jmenoval pověřence pro ochranu osobních údajů. Správce proto není povinen jmenovat pověřence pro ochranu osobních údajů ani podle čl. 37 odst. 4 obecného nařízení o ochraně osobních údajů.

NEPROVEDENÍ POSOUZENÍ VLIVU na ochranu osobních údajů

právní rozbor

Správce neprovádí posouzení vlivu zpracování na ochranu osobních údajů s přihlédnutím k následujícím skutečnostem a závěrům:

Právní úprava

Podle čl. 37 odst. 1 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) správce provede posouzení vlivu na ochranu osobních údajů, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob. Posouzení vlivu na ochranu osobních údajů je podle čl. 37 odst. 3 obecného nařízení o ochraně osobních údajů nutné zejména v těchto případech:

- a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
- b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo
- c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Pravděpodobnost vysokého rizika pro práva a svobody

Správce je jednotlivým poskytovatelem ambulantních zdravotních služeb v oboru dermatovenerologie. Posouzení vlivu na ochranu osobních údajů nemá být v jeho případě podle bodu 91 poslední věty odůvodnění obecného nařízení o ochraně osobních údajů povinné. Je to dáno tím, že správce vzhledem k rozsahu své činnosti, zákonné regulaci zpracování osobních údajů v rámci vedení zdravotnické dokumentace, své kapacitě a použitým předepsaným metodám zpracování nezpracovává osobní údaje v takovém rozsahu, který by odůvodnil existenci vysokého rizika pro práva a svobody fyzických osob ve smyslu čl. 37 odst. 1 obecného nařízení o ochraně osobních údajů.

Systematické a rozsáhlé vyhodnocování

Správce neprovádí žádné operace vyhodnocování osobních aspektů týkajících se fyzických osob, tím méně pak automatizované, a ani provádění takových operací neplánuje. Správce je poskytovatelem zdravotních služeb, který v rámci své hlavní činnosti povinně zpracovává osobní údaje. Tyto údaje však žádným způsobem nevyhodnocuje, neprovádí profilování ani jiné podobné operace, a to mimo jiné proto, že takové nakládání s osobními údaji, které správce povinně zpracovává, zakazuje zákon.

Rozsáhlé zpracování zvláštních kategorií osobních údajů

Do hlavní činnosti správce spadají operace zpracování v rámci vedení zdravotnické dokumentace, tedy i zpracování zvláštních kategorií osobních údajů, zejména pak informací o zdravotním stavu (čl. 9 odst. 1 obecného nařízení o ochraně osobních údajů). Toto zpracování je v souladu s čl. 9 odst. 2 písm. h) obecného nařízení o ochraně osobních údajů. Nejde však o zpracování rozsáhlé. Správce jako poskytovatel ambulantních zdravotních služeb v oboru dermatovenerologie zpracovává zvláštní kategorie osobních údajů v míře, která je i na regionální úrovni nevýznamná, ba zanedbatelná. Tento závěr správce vyslovuje s přihlédnutím k absolutnímu počtu svých pacientů, k rozsahu osobních údajů

o nich vedených i k době zpracování. Závěr o tom, že správce jako jednotlivý poskytovatel ambulantních zdravotních služeb odpovídá i bodu 91 odůvodnění obecného nařízení o ochraně osobních údajů, podle kterého zpracování osobních údajů nemá být považováno za zpracování velkého rozsahu, pokud se jedná o zpracování osobních údajů pacientů nebo klientů jednotlivými lékaři. Správce vychází z toho, že rozsáhlé zpracování zvláštních kategorií osobních údajů při poskytování zdravotních služeb uskutečňují poskytovatelé zdravotních služeb, kteří zdravotní služby poskytují nejméně 10 ošetřujícími zdravotnickými pracovníky. Ošetřujícím zdravotnickým pracovníkem se přitom v souladu s § 3 odst. 2 zákona o zdravotních službách rozumí zdravotnický pracovník, který navrhuje, koordinuje, poskytuje a vyhodnocuje individuální léčebný postup u konkrétního pacienta a koordinuje poskytování dalších potřebných zdravotních služeb. V podmínkách ambulantního poskytovatele, jímž je i správce, je ošetřujícím zdravotnickým pracovníkem vždy lékař, nikoliv však zdravotní sestra. U poskytovatelů s menším počtem ošetřujících zdravotnických pracovníků, mezi které patří i správce, k rozsáhlému zpracování zvláštních kategorií osobních údajů vzhledem k výše uvedeným kritériím nedochází. Uvedenou hranici správce odůvodňuje tím, že u počtu, který nedosahuje 10, lze hovořit o jednotlivých zdravotnických pracovnících (jde o jednotky osob), o nichž pojednává bod 91 odůvodnění obecného nařízení o ochraně osobních údajů. Počet ošetřujících zdravotnických pracovníků současně limituje kapacitu správce jako poskytovatele zdravotních služeb a tím i rozsah zpracování osobních údajů.

Rozsáhlé systematické monitorování veřejně přístupných prostorů

Správce neprovádí rozsáhlé systematické monitorování veřejně přístupných prostor. Ordinaci ani čekárnu ambulantního poskytovatele zdravotních služeb v oboru dermatovenerologie nelze považovat za veřejně přístupné prostory, veřejnost se (zejména vzhledem k množství a skladbě osob, které k lékaři přicházejí) v těchto prostorách nevyskytuje (k podobnému závěru dospěl i Soudní dvůr EU ve věci C-135/ SCF proti Marco del Corso).

Informace pro zaměstnance o zpracování osobních údajů

podle 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)

I. Správce osobních údajů

Správce je zaměstnavatelem v souladu se zákonem č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

II. Účel/y zpracování osobních údajů

Vaše osobní údaje zpracováváme za účelem

- plnění našich povinností podle zákona č. 262/2006 Sb., zákoník práce a předpisů upravujících pojistné, daně a účetnictví, zejména odvádění pojistného na zdravotní pojištění a sociální zabezpečení, daně z příjmu fyzických osob, vedení mzdové agendy, vedení evidence pracovních úrazů a nemocí z povolání, provádění případných srážek mzdy a evidence našeho hospodaření

III. Právní základ zpracování osobních údajů

Právním základem pro zpracování Vašich osobních údajů uvedených v bodu II. je

- splnění naší zákonné povinnosti (zejména zákon č. 262/2006 Sb., zákoník práce, zákon č. 563/1991 Sb., o účetnictví, zákon č. 586/1992 Sb., o daních z příjmů, zákon č. 592/1992 Sb., o pojistném na zdravotní pojištění a zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení)
- splnění závazků z pracovní smlouvy

IV. Příjemci osobních údajů

Příjemci Vašich osobních údajů mohou v souladu s ustanoveními právních předpisů v konkrétních případech kromě Vás být: zaměstnavatel, vedoucí zaměstnanci a orgány veřejné moci v mezích stanovených právními předpisy. Osobní údaje mohou být pro zajištění výše popsaných účelů zpracovávány vedle správce také zpracovateli, a to na základě smluv o zpracování osobních údajů uzavřených v souladu s obecným nařízením o ochraně osobních údajů.

Vaše osobní údaje nepředáváme do zahraničí.

V. Doba zpracování osobních údajů

Osobní údaje jsou zpracovávány po dobu stanovenou zákonem nebo po dobu trvání smlouvy.

VI. Práva subjektu údajů

Při zpracování osobních údajů máte následující práva týkající se ochrany svých osobních údajů:

- právo požadovat od nás přístup k Vaším osobním údajům;
- právo na opravu Vašich osobních údajů, které zpracováváme;
- právo na omezení zpracování. Omezení zpracování znamená, že musíme Vaše osobní údaje, u nichž bylo zpracování omezeno, označit a po dobu trvání omezení je nesmíme dál zpracovávat s výjimkou jejich uložení. Právo na omezení zpracování máte tehdy, jestliže
 - popíráte přesnost osobních údajů, a to na dobu potřebnou k tomu, abychom mohli přesnost osobních údajů ověřit;
 - zpracování je protiprávní a Vy odmítáte výmaz osobních údajů a žádáte místo toho o omezení jejich použití;
 - jestliže již Vaše osobní údaje nepotřebujeme pro účely zpracování, ale Vy je požadujete pro určení, výkon nebo obhajobu právních nároků;

- jestliže jste vznesl/a námitku proti zpracování uvedenou níže v bodu VII., dokud nebude ověřeno, zda naše oprávněné důvody pro zpracování převažují nad Vašimi zájmy nebo právy a svobodami;

- právo na výmaz osobních údajů. Právo na výmaz osobních údajů se vztahuje jen na osobní údaje, které zpracováváme k jiným účelům, než je odvádění pojistného na zdravotní pojištění a sociální zabezpečení, daně z příjmu fyzických osob, vedení mzdové agendy, vedení evidence pracovních úrazů a nemocí z povolání, provádění případných srážek mzdy a evidence našeho hospodaření;
- právo na přenositelnost údajů. Můžete žádat, abychom Vám Vaše osobní údaje poskytli za účelem jejich předání jinému správci osobních údajů, nebo abychom je sami předali jinému správci osobních údajů. Toto právo však máte pouze ohledně těch údajů, které zpracováváme automatizovaně na základě Vašeho souhlasu nebo smlouvy s Vámi. právo podat stížnost u dozorového úřadu, a to v případě, že se domníváte, že zpracování osobních údajů dochází k porušení právních předpisů o ochraně osobních údajů. Stížnost můžete podat u dozorového úřadu v místě svého obvyklého bydliště, místě výkonu zaměstnání nebo v místě, kde došlo k údajnému porušení. V České republice je dozorovým úřadem Úřad na ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7, www.uoou.cz.

VII. Právo vznést námitku proti zpracování

V případě, že Vaše osobní údaje zpracováváme pro účely oprávněných zájmů našich nebo někoho dalšího (právní základy zpracování jsou uvedeny v bodu III), máte kdykoliv právo vznést proti takovému zpracování námitku. Námitku můžete vznést na naší adrese uvedené v bodu I. Pokud takovou námitku vznesete, budeme oprávněni v takovém zpracování pokračovat jen tehdy, pokud prokážeme závažné oprávněné důvody pro zpracování, které převažují nad Vašimi zájmy nebo právy a svobodami, a dále tehdy, pokud půjde o zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků.

VIII. Povinné zpracování a povinnost poskytnout osobní údaje

Zpracování Vašich osobních údajů pro účely odvodu pojistného na zdravotní pojištění a sociální zabezpečení a daně z příjmu fyzických osob, vedení osobního spisu a mzdové agendy, vedení evidence pracovních úrazů a nemocí z povolání, provádění případných srážek mzdy a evidence našeho hospodaření nám ukládá zákon. Ze zákona plyne i Vaše povinnost nám potřebné údaje poskytnout.

Seznámení zaměstnanců s technicko-organizačními opatřeními při zpracování osobních údajů

Při školení byli zaměstnanci seznámeni se zásadami ochrany osobních údajů při poskytování zdravotních služeb, tak jak vyplývají z Obecného nařízení o ochraně osobních údajů a vnitrostátní legislativy, zejména zákona č. 372/2011 Sb. o zdravotních službách. Dále byli zaměstnanci seznámeni s interní směrnicí upravující eliminaci rizik při správě osobních údajů – technicko-organizační opatření a byli proškoleni, jak příslušná opatření dodržovat a aplikovat v praxi.

Veškerý personál je periodicky proškolen a je hodnocena úroveň zajištění bezpečnosti osobních údajů při jejich zpracování. Toto proškolení je zajištěno minimálně jednou ročně a je v souladu s aktuálními doporučeními.

S technicko-organizačními opatřeními při zpracování osobních údajů byli seznámeni

Jméno:	Datum narození:	Datum:	Podpis:

Dokumentace všech případů porušení zabezpečení osobních údajů

datum	popis případu	účinky porušení zabezpečení	přijatá opatření	Oznámeno ÚOOÚ

