**Směrnice upravující eliminaci rizik při správě osobních údajů – technicko – organizační opatření v rozsahu ochrany osobních údajů a ve znění ust. § 55d zák. č. 372/2011 Sb., o zdravotních službách**

Obsah

1. **Účel**
2. **Oblast platnosti**
3. **Pojmy**
4. **Řízení rizik**

**Přílohy**

# Účel

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

* vedení zdravotnické dokumentace pacientů v elektronické/ listinné formě dle aktuálně platného znění zákona č. 372/2011 Sb., o zdravotních službách a vyhl. č. 444/2025 Sb., o zdravotnické dokumentaci.
* vedení evidence stížností v rámci zákona č. 372/2011 Sb., o zdravotních službách
* vedení evidencí plynoucích z dalších činností poskytovatele…..
* vedení adresářů dodavatelů a spolupracujících subjektů
* zpracování výkazů pro zdravotní pojišťovny
* zpracování mzdové agendy
* účetních a daňových operacích
* osobních spisů zaměstnanců
* vedení evidence daňových dokladů vystavených dodavatelům a dalším subjektům

# Oblast platnosti

Tento pracovní postup je závazný pro všechny zaměstnance správce.

# Pojmy a zkratky

## 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.

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

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

##  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 správce povinen 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.

## 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.

## Pracovní postup

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

## 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 hrozeb 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 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.
6. Zálohy jsou ukládány na bezpečném místě, 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).

# Přílohy

Příloha č. 1: Katalog rizik

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

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

Příloha č. 4: Plán eliminace rizik při správě osobních údajů

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)* | * 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
* chybějící záznam souhlasu s poskytováním informací
* chybná volba vhodného místa pro předávání informací
* porušení povinnosti zachovávání mlčenlivosti
* 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)* | * 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)* | * fyzická ztráta
* 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)* | * 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
* nebezpečí vzniku požáru
* zastarání techniky, datových médií
 |

## Příloha č. 2:

**Plán eliminace rizik při vedení dokumentů 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
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
4. za samotné nastavení rozsahu přidělených přístupových práv každému zaměstnanci odpovídá 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 dokumentů 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. dokumenty jsou uchovávány odděleně a je k nim zajištěn pouze zabezpečený přístup (prostor/skříň je uzamykatelný/á nebo je pod stálým dohledem zaměstnance správce).

**Příloha č. 4:**

**Plán eliminace rizik při správě osobních údajů**

Povinnosti jednotlivých zaměstnanců, které souvisejí s bezpečností a nakládání s daty v elektronické podobě 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. média/data jsou uchována 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 zůstávat 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 mechanizmů řízení přístupu.
4. Zvláštní pozornost musí být věnována použití mobilních výpočetních zařízení na veřejných místech a jiných nechráněných místech mimo prostor zaměstnavatele.

Revize ze dne ……………

V rozsahu ust. § 55d zák. č. 372/2011 Sb., o zdravotních službách, byla provedena revize stávající GDPR dokumentace vztahující se k vedení zdravotnické dokumentace, byla zhodnocena technická a organizační opatření v souvislosti s nakládáním a ochranou osobních a zvláštních osobních údajů. Tato revize byla provedena ke dni účinnosti ust. § 55d zákona o zdravotních službách a v souvislosti s pravidelnou obsahovou kontrolou nakládání s osobními údaji, když poskytovatel konstatuje, že přijal dostupná organizační a technická opatření v rámci svých objektivních možností reflektujících právní úpravu platnou ke dni provedení revize, jmenovitě obecné nařízení o ochraně osobních údajů, zákon o zpracování osobních údajů, zákon o zdravotních službách a vyhlášku o zdravotnické dokumentaci