



SMĚRNICE č. Sm-G005

O nakládání a zpracování osobních údajů

2. vydání ze dne: 15. 12. 2022

Verze: 1

Účinnost od: 15. 12. 2022

Skartační znak: A

Stupeň důvěrnosti: N1

	Jméno	Funkce	Datum	Podpis
Odborný garant	prof. MUDr. Roman Havlík, Ph.D.	ředitel Fakultní nemocnice Olomouc		
	Mgr. Sabina Procházková	vedoucí Právního odboru		
	Mgr. Pavla Fiurášková	pověřenec pro ochranu osobních údajů		
Schválil	prof. MUDr. Roman Havlík, Ph.D.	ředitel Fakultní nemocnice Olomouc		



1 ÚVODNÍ USTANOVENÍ

1.1 Účel

- 1.1.1 Tato směrnice o nakládání a zpracování osobních údajů (dále jen tato směrnice a/nebo směrnice) se vydává na základě ust. § 46 zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění a současně na základě Nařízení EU 679/2016.
- 1.1.2 Směrnice stanovuje taková opatření a pravidla, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů spravovaných a zpracovávaných FNOL.
- 1.1.3 Ochranou osobních údajů je míněno zajištění důvěrnosti spravovaných a zpracovávaných osobních údajů, jejich integrity, dostupnosti a dalších bezpečnostních aspektů všech osobních údajů v míře potřebné pro činnost FNOL a to v souladu se zákonem a jinými právními předpisy.
- 1.1.4 Tato směrnice se zabývá ochranou všech osobních údajů ve vlastnictví nebo ve správě FNOL, bez ohledu na jejich podobu (tištěnou, psanou, uloženou elektronicky, odesílanou poštou, předávanou elektronicky, ústním podáním, telefonem, faxem apod.).
- 1.1.5 Za účelem ochrany osobních údajů je ve FNOL definován tzv. systém řízení ochrany osobních údajů, fungující v souladu s těmito dokumenty:
 - Řd-001 Organizační řád FNOL,
 - Řd-002 Pracovní řád,
 - Sm-G003 Spisový řád,
 - Sm-G004 Provozování kamerových systémů ve FNOL,
 - Sm-L009 Lékařská a ošetrovatelská dokumentace,
 - Sm-I004 Zdravotnická statistika,
 - MP-I001-03 Pravidla a postupy pro uživatele při používání prostředků ICT,
 - MP-I001-04 Řízení přístupu uživatelů k informačnímu systému,
 - a s touto směrnicí.
- 1.1.6 Systém ochrany osobních údajů definovaný touto směrnicí je navržen a zpracován v souladu s Nařízením 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), někdy také General Data Protection Regulation (dále jen Nařízení GDPR).
- 1.1.7 Přehled spravovaných agend osobních údajů je zaměstnancům FNOL k dispozici u Pověřence. Katalog osobních údajů, Katalog operací osobních údajů a Záznamy o činnostech zpracování jsou aktualizovány.

1.2 Závaznost

- 1.2.1 Směrnice je závazná pro všechny zaměstnance Fakultní nemocnice Olomouc.

1.3 Správa normy

- 1.3.1 Správa normy se řídí směrnicí Sm-G001 Vznik a řízení organizačních norem.

2 VYMEZENÍ POJMŮ

2.1 Zkratky



FNOL	Fakultní nemocnice Olomouc
DPO	Pověřenec
GDPR	(General Data Protection Regulation) - „obecné nařízení o ochraně osobních údajů“. Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů
IS	Informační systém
OG	Odborný garant
ON	Organizační norma
ZZ	Zdravotnické zařízení

2.2 Definice

Pro účely této směrnice se rozumí:

- 2.2.1 **„osobními údaji“** veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „**subjekt údajů**“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;
- 2.2.2 **„zvláštními kategoriemi osobních údajů“** osobní údaje, které vypovídají 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 orientaci fyzické osoby;
- 2.2.3 **„biometrickými údaji“** osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;
- 2.2.4 **„zpracováním“** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
- 2.2.5 **„omezením zpracování“** označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;
- 2.2.6 **„pseudonymizací“** zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;
- 2.2.7 **„anonymizací“** zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů a subjekt údajů není nebo již přestal být identifikovatelným;
- 2.2.8 **„evidencí“** jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;
- 2.2.9 **„správcem“** FNOL jako orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
- 2.2.10 **„zpracovatelem“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;



- 2.2.11 „**příjemcem**“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty;
- 2.2.12 „**souhlasem**“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
- 2.2.13 „**porušením zabezpečení osobních údajů**“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášovaných, uložených nebo jinak zpracovávaných osobních údajů;
- 2.2.14 „**údaji o zdravotním stavu**“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;
- 2.2.15 „**záznamem o činnostech zpracování**“ záznamy vedené FNOL o zpracování osobních údajů. Záznamy obsahují jméno a kontaktní údaje správce, účely zpracování, rozsah zpracovávaných osobních údajů, informace o příjemcích daných osobních údajů, o předávání údajů do třetích zemí, lhůtách pro výmaz jednotlivých kategorií údajů a popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů;
- 2.2.16 „**dozorovým úřadem**“ Úřad pro ochranu osobních údajů;
- 2.2.17 „**Uníí**“ Evropská unie;

2.3 Odborné funkce

- 2.3.1 **Pověřenec pro ochranu osobních údajů** - je jmenován ředitelem FNOL a představuje konkrétní osobu zodpovědnou za plnění těchto úkolů:
- poskytování informací a poradenství vedoucím pracovníkům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;
 - monitorování souladu s touto směrnicí, Nařízením GDPR a dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s vnitřními předpisy FNOL v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
 - vedení centrální evidence zpracování osobních údajů a její aktualizaci,
 - zajištění pravidelného posuzování a hodnocení účinnosti zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle směrnice O nakládání a zpracování osobních údajů;
 - zajištění monitoringu legislativních změn v oblasti ochrany osobních údajů a návrh na jejich implementaci v rámci FNOL;
 - poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 Nařízení GDPR;
 - spolupráce s dozorovým úřadem;
 - působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 Nařízení GDPR, a případně vedení konzultací v jakékoli jiné věci;
 - působení jako kontaktní místo pro subjekty údajů. Subjekty údajů se mohou obracet na Pověřence ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle Nařízení.

Pověřenec bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.

Pověřenec je přímo podřízen řediteli FNOL.



Pověřenec je v souvislosti s výkonem svých úkolů vázán mlčenlivostí, a to v souladu s právem Unie nebo zákony a právními předpisy České republiky. Pověřenec může plnit i jiné úkoly a povinnosti, které však nesmějí vést ke střetu zájmů jeho činností.

- 2.3.2 **Zodpovědné osoby** - ke každé agendě osobních údajů je určena Zodpovědná osoba (Zodpovědné osoby jsou uvedeny v Katalogu osobních údajů a operací a v Záznamech o činnosti zpracování osobních údajů, které jsou zaměstnancům k dispozici u Pověřence).

Každá Zodpovědná osoba má právo podat Pověřenci návrh na změnu této směrnice, Záznamu o činnostech zpracování, Posouzení vlivu nebo zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle Směrnice.

Zodpovědné osoby mají právo a zároveň povinnost:

- pro případy vzniku nových druhů osobních údajů tuto skutečnost co nejdříve nahlásit Pověřenci, který provede aktualizaci Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
- informovat bezodkladně Pověřence o všech skutečnostech, které mají vliv na aktuálnost Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
- zajistit, aby každý zaměstnanec FNOL před prvním přístupem ke spravovaným osobním údajům byl prokazatelně seznámen a proškolen se zásadami ochrany osobních údajů a touto směrnicí, písemně potvrdil seznámení,
- zajistit prokazatelné opakování tohoto proškolení v frekvenci co 2 roky;
- při uzavírání smluv s třetími stranami dbát na to, aby obsahovaly zásady zajištění ochrany osobních údajů, pokud je to vzhledem k povaze obsahu smlouvy relevantní.

- 2.3.3 **Uživatelé osobních údajů** - uživatelem osobních údajů je zaměstnanec FNOL používající spravované osobní údaje k plnění svých pracovních povinností. Všichni Uživatelé osobních údajů mají za povinnost:

- dodržovat zásady vyplývající z této Směrnice;
- hlásit veškeré bezpečnostní incidenty svému nadřízenému, případně přímo Pověřenci;
- informovat Pověřence o zjištěných bezpečnostních slabínách;
- informovat Pověřence o změnách ve způsobu zpracování a nakládání s osobními údaji;
- vykonávat další činnosti vyplývající z platných vnitřních předpisů, především zajistit průběh skartačního řízení v souladu se Spisovým řádem Sm-G003.

- 2.3.4 **Správce informačního systému** je zaměstnanec FNOL, většinou pracovník Odboru informatiky, v jehož působnosti je správa systému. Správou systému je myšlen soubor činností, které zajišťují funkčnost informačního systému (odstranění nebo zamezení vzniku chybových stavů IS), archivaci a zabezpečení (elektronických) dat uživatelů (mimo lokální disky a externí datová úložiště (FDD, externí HDD) a je odpovědný za řízení a implementaci bezpečnosti informačních systémů. Správce IS zabezpečuje spolupráci s jednotlivými uživateli osobních údajů při ochraně osobních údajů uložených v osobních počítačích, včetně těch přenosných.

3 VLASTNÍ TEXT

3.1 Zásady zpracování osobních údajů

- 3.1.1 Osobní údaje musí být:

- ve vztahu k subjektu údajů **zpracovávány korektně a zákonným** a transparentním způsobem („*zákonnost, korektnost a transparentnost*“);
- shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro



- statistické účely se podle čl. 89 odst. 1 Nařízení GDPR nepovažuje za neslučitelné s původními účely („účelové omezení“);
- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);
 - přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“);
 - uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 Nařízení GDPR, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných Nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);
 - zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“).
- 3.1.2 Standardně jsou zpracovávány pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Spis vedený Uživatelem osobních údajů obsahuje pouze informace relevantní pro průběh řízení a agendu s ohledem na minimalizaci údajů k dosažení účelu zpracování.
- 3.1.3 Písemnosti obsahující osobní údaje podléhají procesu fyzické a elektronické skartace v souladu se Spisovým řádem.
- 3.1.4 Pro statistické účely je nutné osobní údaje anonymizovat.
- 3.1.5 Je třeba zamezit neoprávněnému přístupu ke shromážděným údajům.
- ## 3.2 Zákonnost zpracování osobních údajů
- 3.2.1 FNOL jako správce osobních údajů zpracovává pouze takové osobní údaje, jejichž zpracování je zákonné. Zpracování osobních údajů je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:
- a) zpracování je nezbytné pro splnění právní povinnosti, která se vztahuje na FNOL jako správce osobních údajů;
 - b) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
 - c) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
 - d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
 - e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřena FNOL jako správce osobních údajů;
 - f) zpracování je nezbytné pro účely oprávněných zájmů FNOL jako správce osobních údajů či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě. Toto se netýká zpracování prováděného FNOL jako správcem osobních údajů při plnění jeho úkolů jako orgánu veřejné moci.



- 3.2.2 Účel zpracování osobních údajů musí vycházet z výše uvedených právních základů. Osobní údaje nesmí být použity k jinému účelu, než ke kterému byly pořízeny nebo musí být takové zpracování nutné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřena FNOL jako správce osobních údajů.
- 3.2.3 Pokud je zpracování založeno na souhlasu, musí být Uživatel osobních údajů schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů.
- a) Souhlas musí být udělen samostatně a musí být jasně odlišitelný od ostatních sdělení (jako samostatný dokument).
 - b) Subjekt údajů vždy musí obdržet jednu kopii uděleného souhlasu včetně informace o způsobu odvolání uděleného souhlasu.
 - c) Pro zpracování zvláštních kategorií osobních údajů (biometrické údaje, fotografie, audio, video, zdravotní stav, sociální postavení a další) je nutné vždy udělit samostatný souhlas, oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji). V případě fotodokumentace, ze které není možná identifikace osoby/pacienta, je umožněno pořízení bez uděleného samostatného souhlasu.
 - d) Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně dostupné jako jej poskytnout.
 - e) Uživatel osobních údajů je povinen ve spolupráci se Správcem IS zajistit výmaz osobních údajů v případě odvolání souhlasu se zpracováním osobních údajů, včetně výmazu v zálohách a kopiích dat.
- 3.2.4 Zpracování údajů na základě uděleného souhlasu subjektu údajů je využíváno pouze v krajních případech, kdy je zpracování nezbytné a neexistuje jiné oprávnění pro nakládání s osobními údaji.

3.3 Opatření pro ochranu osobních údajů

- 3.3.1 Uživatel osobních údajů je povinen dodržovat pravidlo čistého stolu (neponechávat volně položené písemnosti obsahující osobní údaje bez dozoru na svém pracovním stole, po ukončení pracovního dne je každý zaměstnanec povinen takové listinné písemnosti uložit do uzamykatelných úložných prostor a klíče zajistit tak, aby k nim neměly přístup osoby bez oprávnění). Výjimkou z této povinnosti je případ, kdy má zaměstnanec k dispozici samostatnou kancelář, v této kanceláři probíhá úklid výhradně za jeho přítomnosti a klíče od této kanceláře má k dispozici pouze daný zaměstnanec.
- 3.3.2 Uživatel osobních údajů je povinen v případě odchodu z kanceláře, kde se již nenachází žádný další zaměstnanec, zavřít okna a tuto místnost zamknout.
- 3.3.3 Uživatel osobních údajů je povinen v případě přítomnosti cizí osoby v kanceláři a nutnosti odchodu zaměstnance z kanceláře, kde se již nenachází žádný další zaměstnanec, vyprovodit cizí osobu na chodbu, kancelář zamknout a opětovný vstup cizí osoby do kanceláře umožnit až při vlastním návratu zaměstnance ZZ do kanceláře (neponechávat cizí osoby bez dozoru v kanceláři).
- 3.3.4 Uživatel osobních údajů je povinen využívat pro elektronické zpracování osobních údajů k tomu určené aplikační software (SW) FNOL. V případě, že není možné tuto dokumentaci ukládat prostřednictvím SW FNOL, je možné ukládání dat s osobními údaji na síťové disky, ke kterým je nastaveno příslušné oprávnění (nastavuje správce IS).
- 3.3.5 Uživatel osobních údajů je povinen udržovat písemnosti obsahující osobní údaje uložené na pevných discích a ve svých emailových schránkách v souladu s lhůtami stanovenými pro zpracování dle Spisového řádu a v minimálním rozsahu umožňujícím dosažení účelu zpracování.



- 3.3.6 Uživatel osobních údajů je povinen využívat pro ukládání fyzické dokumentace obsahující osobní údaje (včetně fyzických nosičů elektronické dokumentace) k tomu určené zabezpečené úložné prostory a tyto úložné prostory při opuštění kanceláře uzamknout. Uživatel osobních údajů je povinen písemnostem obsahujícím osobní údaje přiřazovat spisové znaky dle platného Spisového řádu.
- 3.3.7 Uživatel osobních údajů je povinen udržovat v tajnosti své přístupové údaje (přihlašovací jméno a heslo) k informačním systémům FNOL, tyto přístupové údaje si nezapisovat (na papír, do souboru, apod.) ani je neprozrazovat žádné další osobě.
- 3.3.8 Uživatel osobních údajů je povinen při tisku písemností obsahujících osobní údaje tyto nikdy neponechávat bez dozoru na tiskárně.
- 3.3.9 Uživatel osobních údajů není oprávněn přeposílat písemnosti obsahující osobní údaje na své nebo cizí soukromé emailové schránky (např. www.seznam.cz, www.gmail.com apod.).
- 3.3.10 Uživatel je oprávněn pro předání osobních údajů využít Českou poštu, případně Informační systém datových schránek.
- 3.3.11 Uživatel osobních údajů není oprávněn ukládat na veřejné servery Internetu (např. www.uloz.to, www.uschovna.cz, apod.) jakékoli písemnosti obsahující osobní údaje.
- 3.3.12 Uživatel osobních údajů není oprávněn provádět na svěřených prostředcích jakékoliv hardwarové zásahy (např. měnit komponenty počítače, připojovat vlastní externí zařízení apod.) a spouštět či instalovat jakýkoliv nepovolený software.
- 3.3.13 Uživatel osobních údajů je oprávněn využívat mobilní zařízení FNOL (mobilní telefon, notebook, apod.) pouze při dodržení pravidel pro jejich zabezpečení definovaných Správcem IS viz. MP-I001-03 Pravidla a postupy pro uživatele při používání prostředků ICT a MP-I001-04 Řízení přístupu uživatelů k informačnímu systému.
- 3.3.14 Uživatel osobních údajů není oprávněn jakkoliv měnit nastavení, případně vypínat ochranu proti škodlivému kódu (antivirový program, antispyware apod.) na svěřených prostředcích.
- 3.3.15 Uživatel osobních údajů je povinen hlásit jakoukoli závadu nebo podezření na nestandardní fungování PC svému nadřízenému nebo správci IS.
- 3.3.16 Uživatel osobních údajů není oprávněn ukládat na vyměnitelná média jakékoliv písemnosti obsahující osobní údaje bez jejich zabezpečení anonymizací nebo šifrováním.
- 3.3.17 Každý zaměstnanec, který přichází do styku s písemnostmi obsahujícími osobní údaje uloženými na médiích (CD, DVD, papírové dokumenty, flash paměťové moduly) je povinen zajistit jejich bezpečnou likvidaci (skartování, vymazání, fyzické zničení).
- 3.3.18 Klíče od určených kanceláří jsou zaměstnancům FNOL vydávány prokazatelným způsobem a je vedena evidence vydaných klíčů. Je zajištěno ukládání a zabezpečení náhradních klíčů od kanceláří a úložných prostor.
- 3.3.19 Zaměstnanci FNOL nejsou oprávněni hovořit (osobně i telefonicky) o osobních údajích v přítomnosti třetích osob, které nemají právo danou informaci vědět. Tato povinnost se vztahuje též na předávání informací zaměstnancům, kteří nemají na tuto informaci právo.

3.4 Předávání osobních údajů

- 3.4.1 Dokumentaci obsahující osobní údaje v elektronické podobě je povoleno předávat příjemcům mimo FNOL pouze prostřednictvím datových schránek. V případech, kdy není možné dokumentaci předat prostřednictvím datové schránky nebo ve fyzické podobě, lze dokumentaci zaslat prostřednictvím České pošty. Pokud pacient žádá a souhlasí o zaslání informací ze své zdravotnické dokumentace e-mailem, lze mu vyhovět po podpisu formuláře č. Fm-G005-ZADOST-001 Žádost o předávání informací elektronicky, kde bude upozorněn, že se jedná o nezabezpečený přenos.



3.5 Zveřejňování osobních údajů

- 3.5.1 Při zveřejňování osobních údajů musí dojít k opatřením, kdy veškerá zveřejňovaná dokumentace (text, audio, video) bude anonymizována v rozsahu zajišťujícím minimalizaci rozsahu zveřejňovaných osobních údajů při dosažení účelu zveřejnění uloženého legislativou (dokumentaci anonymizovat vždy, pokud zákon neukládá jinak). Výjimkou jsou osobní údaje, u kterých je udělen Souhlas s takovýmto postupem.
- 3.5.2 Musí dojít k zajištění anonymizace osobních údajů uvedených v uzavřených smlouvách, které jsou zveřejněny v Registru smluv.
- 3.5.3 Při pořizování záznamů z akcí pořádaných FNOL zajistit informování účastníků o pořizování audio/video dokumentace a uvedení účelu tohoto pořízení, případně zajištění jiného než konkludentního souhlasu.
- 3.5.4 Zveřejnění fotografií zaměstnanců ZZ bez výslovného souhlasu je možné pouze u osob, u kterých je to odůvodnitelné (ředitel, zástupce ředitele).

3.6 Získávání informací od subjektu údajů

- 3.6.1 Odpovědný zaměstnanec FNOL (Uživatel osobních údajů) v okamžiku získání osobních údajů poskytne subjektu údajů tyto informace:
- totožnost a kontaktní údaje FNOL;
 - kontaktní údaje Pověřence;
 - účely zpracování, pro které jsou osobní údaje určeny a právní základ pro jejich zpracování;
 - oprávněné zájmy FNOL nebo třetí strany v případě, že je zpracování založeno na opodstatněném zájmu FNOL jako správce osobních údajů;
 - případné příjemce nebo kategorie příjemců osobních údajů;
 - doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
 - existence práva požadovat od FNOL jako správce osobních údajů přístup k osobním údajům týkajících se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;
 - existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním (pokud je zpracování založeno na uděleném souhlasu se zpracováním osobních údajů);
 - existence práva podat stížnost u dozorového úřadu;
 - skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a poučení ohledně možných důsledků neposkytnutí těchto údajů.
- 3.6.2 Naplnění informační povinnosti je zajištěno zveřejněním Informačního memoranda na webových stránkách FNOL a na Altus Portal.
- Jedná se o informace určené pro:
- pacienty (Fm-G005-INFO-001);
 - zaměstnance (Fm-G005-INFO-002);
 - uchazeče o zaměstnání (Fm-G005-INFO-003).
- 3.6.3 Pokud FNOL jako správce osobních údajů hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace v rozsahu dle tohoto článku.



3.7 Práva subjektu údajů

3.7.1 Subjekt údajů může uplatnit tato práva:

- přístup k osobním údajům,
- opravu a výmaz osobních údajů,
- omezení zpracování osobních údajů,
- přenositelnost osobních údajů,
- vznesení námítky.

Práva lze uplatnit pomocí formuláře – Žádost o uplatnění práv subjektu údajů (Fm-G005-ZADOST-003).

V případě zpracování osobních údajů na základě souhlasu, lze souhlas odvolat (Fm-G005-ODVSOUHL-001).

3.7.2 Naplnění práv subjektů údajů zajišťuje Pověřenec.

3.7.3 Způsob podání žádosti o naplnění práv subjektů údajů je zveřejněn na webových stránkách FNOL případně dalšími vhodnými způsoby.

3.7.4 Subjektu údajů jsou poskytovány informace v souladu se zásadami zpracování osobních údajů, a to především stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, zejména pokud se jedná o informace určené dítěti.

3.7.5 Informace jsou subjektu údajů poskytovány výhradně na základě prokazatelného jednoznačného ověření totožnosti subjektu údajů (občanský průkaz, datová schránka).

3.7.6 Informace jsou subjektu údajů poskytovány písemně nebo jinou formou, připuštěna je ve vhodných případech i elektronická forma. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty pouze ústně.

3.7.7 Informace jsou subjektu údajů poskytovány bez zbytečného odkladu a v každém případě ve lhůtě do jednoho kalendářního měsíce od obdržení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další maximálně dva kalendářní měsíce, kdy subjekt údajů musí být o takovém odůvodněném prodloužení lhůty k poskytnutí údajů informován nejpozději ve lhůtě do jednoho kalendářního měsíce od obdržení žádosti.

3.7.8 Pokud opatření, o něž subjekt údajů požádal, nejsou přijata, musí být subjekt údajů bezodkladně a nejpozději ve lhůtě do jednoho kalendářního měsíce od přijetí žádosti informován o důvodech nepřijetí opatření a o jeho možnosti podat stížnost u dozorového úřadu.

3.7.9 Poskytované informace, veškerá sdělení a veškeré úkony se poskytují a činí bezplatně. Jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, lze přistoupit k:

- a) uložení přiměřeného poplatku zohledňujícího administrativní náklady spojené s poskytnutím požadovaných informací, sdělení, anebo s učiněním požadovaných úkonů;
- b) odmítnutí žádosti vyhovět.

Zjevnou nedůvodnost nebo nepřiměřenost žádosti je nutné odůvodnit a zdokumentovat pro potřebu následného doložení.

3.8 Právo subjektu údajů na přístup k osobním údajům

3.8.1 Subjekt údajů má právo získat od FNOL jako správce osobních údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:

- a) účely zpracování;
- b) kategorie dotčených osobních údajů;



- c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
- d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
- e) existence práva požadovat od FNOL jako správce osobních údajů opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování, anebo vznést námitku proti tomuto zpracování;
- f) právo podat stížnost u dozorového úřadu;
- g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů.

3.8.2 FNOL jako správce osobních údajů poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může FNOL jako správce osobních údajů účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá (datová schránka), pokud subjekt údajů nepožádá o jiný způsob.

3.8.3 Právem získat kopii uvedenou v předchozím odstavci nesmějí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

3.9 Řešení případů porušení zabezpečení osobních údajů

3.9.1 Zjištění případu porušení zabezpečení osobních údajů ohlásí zaměstnanec neprodleně svému nadřízenému a Pověřenci. Poté je nutné vyplnit formulář Fm-G005-OHLASENI-001 – Ohlášení porušení zabezpečení osobních údajů ve FNOL, který je dostupný online na intranetu FNOL v záložce GDPR ([Pracovní web - gdpr](#)) nebo na Altus Portale.

3.9.2 Okamžité hlášení bude obsahovat minimálně tyto informace:

- a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
- b) popis pravděpodobných důsledků porušení zabezpečení osobních údajů pro FNOL jako správce osobních údajů a pro subjekty údajů;
- c) návrh okamžitých opatření k zastavení porušení zabezpečení osobních údajů a případně návrh okamžitých nápravných opatření.

3.9.3 Pověřenec ve spolupráci s Právním odborem, se Zodpovědnou osobou, Uživateli osobních údajů, Správcem IS, relevantními zpracovateli osobních údajů, případně dalšími relevantními zaměstnanci, rozhodne o dalším postupu.

3.9.4 Pověřenec neprodleně informuje ředitele FNOL a předloží mu ke schválení návrh na řešení případu porušení zabezpečení osobních údajů a případně doporučení ohlášení porušení zabezpečení osobních údajů dozorovému úřadu, který předem projedná a schválí s Právním odborem.

3.9.5 Pověřenec neprodleně předloží řediteli FNOL ke schválení návrh nápravných opatření pro zamezení opakování obdobného porušení zabezpečení osobních údajů. Nápravné opatření obsahuje kroky obnovy a postup jak zamezit opakování stejného porušení zabezpečení, termíny realizace opatření, jména zaměstnanců odpovědných za jejich splnění. Realizace nápravných opatření podléhá schválení ředitelem.

3.9.6 Pověřenec provádí kontrolu plnění nápravných opatření a výsledky předkládá řediteli FNOL v termínech k tomu dohodnutých.

3.10 Činnost při zjištění porušení zabezpečení osobních údajů

3.10.1 Jakékoli porušení zabezpečení osobních údajů nebo ztrátu dostupnosti osobních údajů (dále jen incident) nebo podezření na takové porušení je každý povinen hlásit Pověřenci pro ochranu osobních údajů a nadřízenému zaměstnanci.



- 3.10.2 Podezření na incident se posuzuje pro potřeby postupu podle této směrnice stejně jako incident, dokud není zjištěno, že incident nevznikl.
- 3.10.3 Pověřenec pro ochranu osobních údajů je odpovědný za řízení reakce na incident.
- 3.10.4 Pověřenec pro ochranu osobních údajů spolupracuje při řízení reakce na incident s vedoucími zaměstnanci pracoviště, a pokud je potřebné, se smluvními partnery ZZ a orgány veřejné správy.
- 3.10.5 Pověřenec pro ochranu osobních údajů vede dokumentaci činností a komunikace při reakci na incident tak, aby byla úplná a průkazná.
- 3.10.6 Úkony v reakci na incident se provádějí bez zbytečného odkladu, a pokud je to možné, ihned.
- 3.10.7 Hlavními cíli řízení reakce na incident jsou:
- a) Ověřit, zda skutečně došlo k porušení zabezpečení osobních údajů.
 - b) Zjistit, zda došlo k neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů, případně jinému nežádoucímu stavu nebo dopadu.
 - c) Zamezit možnosti neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů.
 - d) Zjistit rozsah incidentu.
 - e) Zjistit, které osoby se mohly neoprávněně s osobními údaji seznámit.
 - f) Zjistit, kde se osobní údaje a informační systémy nacházejí v rozporu s obecně závaznými právními normami.
 - g) Opatřit důkazy pro řízení, vyšetřování nebo dokazování. Pokud je to třeba, použijí se forenzní metody a standardy.
 - h) Zjistit, zda je potřebné oznamovat incident třetím stranám.
 - i) Navrhnout a přijmout taková opatření, aby incident pominul.
 - j) Navrhnout a přijmout taková opatření, aby se incident neopakoval.
 - k) Sdílet nebo předat varování třetím osobám, zejména Úřadu tak aby se předešlo incidentům u dalších správců.
- 3.10.8 Činnost podle tohoto článku se ukončí, jestliže o tom rozhodne Pověřenec na základě předložené zprávy a zabezpečených podkladů a informací, nebo pokud se prokáže, že k incidentu **nedošlo**.

3.11 Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

- 3.11.1 Jakékoli porušení zabezpečení osobních údajů FNOL jako správce osobních údajů bez zbytečného odkladu, a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.
- 3.11.2 Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu FNOL jako správci osobních údajů.
- 3.11.3 Ohlášení případů porušení zabezpečení osobních údajů musí přinejmenším obsahovat:
- a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
 - b) jméno a kontaktní údaje Pověřence nebo jiného kontaktního místa, které může poskytnout bližší informace;
 - c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;



- d) popis opatření, která FNOL jako správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

3.11.4 Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. Pověřenec dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

3.12 Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

3.12.1 Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí FNOL jako správce osobních údajů toto porušení bez zbytečného odkladu subjektu údajů.

3.12.2 V oznámení určeném subjektu údajů se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a opatření uvedené v odst. 3.11 této směrnice.

3.12.3 Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

- a) FNOL jako správce osobních údajů zavedl náležitá technická a organizační ochranná opatření, a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
- b) FNOL jako správce osobních údajů přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektu údajů se již pravděpodobně neprojeví;
- c) oznámení by vyžadovalo nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

3.12.4 Jestliže FNOL jako správce osobních údajů dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil.

3.13 Kontrola dodržování ustanovení směrnice

3.13.1 Vedoucí zaměstnanci zajistí kontrolu plnění povinností vyplývajících z ustanovení této směrnice O nakládání a zpracování osobních údajů ve své působnosti.

3.13.2 Vedoucí zaměstnanci zajistí, aby byli s dokumentem směrnice O nakládání a zpracování osobních údajů seznámeni všichni zaměstnanci.

3.13.3 Pověřenec je zodpovědný za pravidelné posuzování a hodnocení účinnosti zavedených organizačních, fyzických a technických opatření pro zajištění bezpečnosti zpracování dle směrnice O nakládání a zpracování osobních údajů. Při provádění kontrolních činností jsou všichni zaměstnanci FNOL povinni poskytovat Pověřenci součinnost. O provedených zjištěních vede Pověřenec prokazatelnou dokumentaci, kterou předkládá na vědomí řediteli FNOL.

3.13.4 V případě doporučení ke změnám organizačních, fyzických a technických opatření pro zajištění bezpečnosti zpracování osobních údajů předkládá Pověřenec tato doporučení řediteli ke schválení.

3.14 Specifické odpovědnosti a pravomoci

3.14.1 Ředitel - odpovědnost za zajištění ochrany osobních údajů v souladu s Nařízením GDPR nese ředitel FNOL zejména:



- schvaluje směrnici O nakládání a zpracování osobních údajů a její aktualizace,
- vyjadřuje se k osobě, která má vykonávat funkci Pověřence pro ochranu osobních údajů (dále také „Pověřenec“),
- jmenuje Pověřence pro ochranu osobních údajů,
- projednává pravidelnou zprávu o stavu ochrany osobních údajů,
- rozhoduje o přijetí technických, fyzických a organizačních opatření pro zajištění souladu ochrany osobních údajů s Nařízením GDPR.

3.14.2 Vedení FNOL - odpovídají za to, že pravidla ochrany osobních údajů budou dodržovat zaměstnanci, kteří nakládají s osobními údaji a vystupují v roli uživatelů nebo správců osobních údajů.

3.15 Další odborní garanti

3.15.1 Tato ON nemá další odborné guaranty.

4 SOUVISEJÍCÍ DOKUMENTY

4.1 Dokumenty vyšší úrovně

Zákon č. 110/2019 Sb., o zpracování osobních údajů, v platném znění

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů

4.2 Dokumenty FNOL

Řd-001 Organizační řád FNOL

Řd-002 Pracovní řád

Sm-G003 Spisový řád

Sm-G004 Provozování kamerových systémů ve FNOL

Sm-L009 Lékařská a ošetrovatelská dokumentace

Sm-I004 Zdravotnická statistika

MP-I001-03 Pravidla a postupy pro uživatele při používání prostředků ICT

MP-I001-04 Řízení přístupu uživatelů k informačnímu systému

4.3 Vystavené dokumenty

Fm-G005-INFO-001 Informace o zpracování osobních údajů pro pacienty ve FNOL

Fm-G005-INFO-002 Informace o zpracování osobních údajů zaměstnanců ve FNOL

Fm-G005-INFO-003 Informace o zpracování osobních údajů uchazečů o zaměstnání ve FNOL

Fm-G005-ZADOST-001 Žádost o předávání informací elektronicky

Fm-G005-ZADOST-002 Žádost o zaslání dokumentace obsahující zvláštní kategorie osobních údajů

Fm-G005-ZADOST-003 Žádost o uplatnění práv subjektu údajů

Fm-G005-SOUHL-001 Souhlas se zpracováním osobních údajů

Fm-G005-SOUHL-002 Souhlas se zpracováním osobních údajů - hromadný

Fm-G005-ODVSOUHL-001 Odvolání poskytnutého souhlasu se zpracováním osobních údajů

Fm-G005-OHLASENI-001 Ohlášení porušení zabezpečení osobních údajů



5 ZÁVĚREČNÁ USTANOVENÍ

5.1 Účinnost

5.1.1 Tato ON nabývá účinnosti dnem **15. 12. 2022**.

5.1.2 Dnem účinnosti se nahrazuje 1. vydání ze dne 25. 5. 2018.

5.1.3 OG je povinen 1x za 2 roky provést revizi ON. Pokud to stav vyžaduje, musí OG zajistit vypracování nového vydání ON nebo její změny. Záznam o provedené revizi provede správce dokumentace do formuláře Fm-G001-REV-001 „Záznam o revizi ON“.

Povinnost vypracování nové ON nebo změny nastává i v případě, že dojde k zásadním změnám, které se dotýkají obsahu ON.

5.1.4 Přejícná ustanovení nejsou stanovena.

5.2 Přílohy

Nejsou.

Nerízená kopie