NEMOCNICE TŘINEC, příspěvková organizace,
Kaštanová 268, Dolní Líštná,
739 61 Třinec

IMPLEMENTACE OCHRANY OSOBNÍCH ÚDAJŮ DLE OBECNÉHO NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 V NEMOCNICI TŘINEC

Členové týmu:
Bc. Lenka Samiecová
Mgr. Halina Musiołová

Tel.: 558 309 111
Fax: 558 309 100
ID DS: n3ek6pv

IČ: 00534242
DIČ: CZ00534242

www.nemtr.cz
e-mail: info@nemtr.cz

Osnova

1. Souhrn

Obecné nařízení Evropského parlamentu a Rady o ochraně osobních údajů č. 2016/679, neboli General Data Protection Regulation (GDPR) bylo přijato v dubnu 2016 po čtyřletém vyjednávání. Je platné od 24. května 2016, ale účinné od 25. května 2018. Nařízení platí pro 28 členských států EU + pro území EFTA (Norsko, Island, Lichtenštejnsko). V oblasti ochrany osobních údajů přináší mnoho změn a společnostem zpracovávajícím osobní údaje nemálo nových povinností. Mezi takové subjekty patří bezesporu zaměstnavatelé.

Ochrana osobních údajů je ošetřena evropskou směrnicí a v návaznosti na ni naším zákonem na ochranu osobních údajů. Nyní přichází GDPR, kterým je třeba se řídit. Jednoduše řečeno, nařízení EU má přednost před naším zákonem. GDPR vzniklo jako reakce na technologický pokrok v oblasti informačních a komunikačních technologií. Při zpracování osobních údajů se totiž používají nové metody, jako je např. profilování nebo automatizované zpracování.

Obecné nařízení vnáší do oblasti ochrany dat nový rozměr a hlavně posiluje její společenský význam. Ten byl dosud bagatelizován zejména těmi, kteří z rozsáhlého shromažďování osobních dat nejvíce profitovali. Také sami občané a aktivisté dlouho význam osobních dat podceňovali. Poskytování dat se stalo téměř zvykem, ať už při nakupování online, registraci do aplikací a služeb, či sdělováním údajů o platebních kartách a osobních dokladech.

Osobní data tvoří důležitou a nedílnou součást naší osobní identity. Proto představují pro velkou škálu subjektů cennou a strategicky významnou komoditu. Z těchto v podstatě protichůdných zájmů vyplývá nutnost nastolit mezi nimi jistou rovnováhu, a o to se právě GDPR pokouší.

Hlavní znaky GDPR:

- Je jednotně aplikovatelné v celé EU.
- Rozšiřuje pojem osobních údajů – nově také biometrické prvky (sken oční sítnice).
- Zpřesňuje souhlas se zpracováním osobních údajů – nově zákaz předvyplněných políček.
- Vyžaduje vyšší technickou a organizační bezpečnost správců a zpracovatelů.
- Při rozsáhlém a systematickém zpracování osobních údajů požaduje jmenování pověřence na ochranu osobních údajů.
- Při rizikových zpracování osobních údajů požaduje příchozí provedení posouzení vlivu na ochranu osobních údajů.
- Posiluje stávající práva fyzických osob a zakládá práva nová – právo být zapomenut či právo na přenositelnost údajů.

- Porušení ochrany dat musí být oznámeno do 72 hodin jak fyzické osobě, tak Úřadu pro ochranu osobních údajů.
- Zavádí nepoměrně vyšší sankce za porušení ochrany osobních údajů – oproti současnosti (maximálně 10 000 000 korun) bude možné uložit až 20 000 000 eur nebo 4 % celosvětového obratu podniku.

Splnit podmínky nařízení GDPR stoji nemalé úsilí a s tím spojené finanční náklady. Minimálně je potřeba upravit interní dokumenty, zmapovat, jak se ve firmě zachází s osobními údaji, zajistit školení zaměstnanců, kteří s osobními údaji nakládají, zajistit dokumentaci k záznamům o činnostech zpracování, zajistit bezpečnost zpracování osobních údajů vyhodnotit možná rizika a zavést potřebná technická opatření.

2. Stručná charakteristika zdravotnického zařízení

Zřizovatelem Nemocnice Třinec, p.o. je Moravskoslezský kraj a nemocnice funguje jako příspěvková organizace. Nemocnice prošla řadou rekonstrukcí, je moderně vybavená, oddělení disponují dvou a třílůžkovými pokoji s vlastním sociálním zařízením. U každého lůžka je dorozumívací zařízení a centrální přívod kyslíku. Samozřejmostí je i možnost Wi-Fi připojení pro pacienty. Některá oddělení nabízejí za poplatek nadstandardně vybavené pokoje. O zdraví klientů se stará 17 odborných ambulancí a 14 oddělení s celkovou kapacitou 361 lůžek. V Nemocnici Třinec pracovalo k 31. 12. 2017 celkem 765 zaměstnanců s úvazkem 757, 95, tabulka č. 1.
Zaměstnanci nemocnice se dělí do čtyř základních kategorii:

- lékaři,
- nelékaři,
- dělníci a provozní pracovníci,
- technicko-hospodářští pracovníci (dále jen THP).

Novorozenecké oddělení Nemocnice Třinec, p.o. je od roku 2002 držitelem ocenění Baby Friendly Hospital (Nemocnice přátelská k dětem) pod záštitou UNICEF a snaží se o podporu kojení u všech maminek. Požadavkem pro získání ocenění je zavedení do praxe všech „Deset kroků k úspěšnému kojení“. Až 90 % dětí odchází domů plně kojeno, děti jsou kojeny podle vlastního rytmu a potřeb. Maminky dostávají telefonní číslo na Klub pro ženy a dívky, působící v třinecké nemocnici, kam se můžou při potížích kdykoliv poradit.
V říjnu roku 2008 získala nemocnice po dvouleté přípravě akreditaci, jako oficiální potvrzení kvality poskytované péče, kterou po úspěšném šetření udělila Spojená akreditační komise České republiky

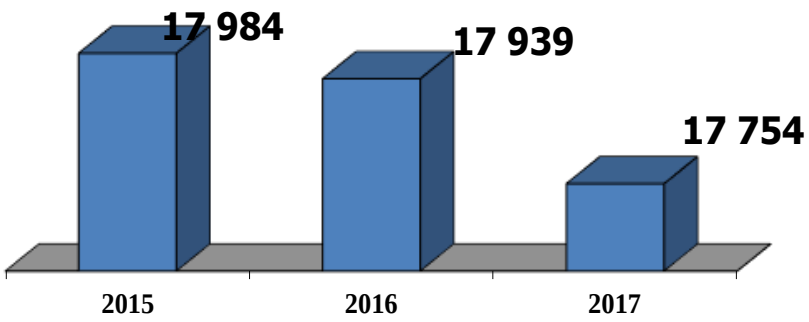
na dobu tří let. V roce 2011 nemocnice získala druhou reakreditaci a v roce 2014 třetí reakreditaci a v roce 2017 již čtvrtou reakreditaci.

Rok 2008 byl pro nemocnici velice úspěšný a v prosinci se Nemocnice Třinec, p.o. stala držitelem titulu Nemocnice roku 2008. Anketu pořádá Health-Care Institut a probíhá dotazníkovým šetřením. Nemocnice získala ocenění na základě porovnání pohledů pacientů, zdravotníků a úspěšného hospodaření zdravotnických zařízení s penězi. V dubnu roku 2017 byl v nemocnici nainstalován nový nemocniční informační systém Fons Enterprise, díky kterému můžeme uvažovat o elektronické medikaci.

Tab. 1 počet úvazků lékařů, nelékařů, dělníků a THP

Zaměstnanec	Počet úvazků
Lékaři	112,51
Nelékaři	534,26
Dělníci, provozní pracovníci	58,35
Technicko-hospodářští pracovníci	52,83
Celkem	757,95

Nemocnice Třinec zajišťuje hospitalizační služby pro obyvatele celého regionu Třinecka, Jablunkovska a částečně i pro obyvatele Českého Těšína a blízkého okolí. V roce 2016 měla spádová oblast nemocnice 103390 obyvatel. Jak uvádí graf 1 v posledních třech letech (2015, 2016, 2017) bylo v nemocnici hospitalizováno v průměru 17892 pacientů.



Graf 1 počet hospitalizovaných Nemocnice Třinec 2015 - 2017

3. Zdůvodnění projektu (definice projektu)

Obecné nařízení GDPR představuje nový, jednotný právní rámec ochrany osobních údajů v evropském prostoru, který od 25. května 2018 určuje pravidla pro zpracování osobních údajů, včetně práv subjektu údajů (fyzické osoby). V českém právním prostředí tak Obecné nařízení od 25. května 2018 nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů, který bude novelizován a nadále bude upravovat pouze některé dílčí oblasti. GDPR se vztahuje na všechny subjekty, bez ohledu na právní formu, které vlastní a zpracovávají osobní a citlivé údaje občanů EU. Nemocnice Třinec, p.o. ve spolupráci se zřizovatelem, kterým je Moravskoslezský kraj provedla analýzu a zavedla změny.

4. Cíle projektu

Hlavním cílem projektu je zavést fungující systém ochrany osobních údajů v nemocnici v souladu s GDPR, kterého bychom chtěli dosáhnout do konce roku 2018.

V rámci strategických cílů tohoto projektu je snaha:

- zmapovat, jak se ve firmě zachází s osobními údaji,
- upravit interní dokumenty,
- zajistit školení zaměstnanců,
- zajistit bezpečnost zpracování osobních údajů vyhodnotit možná rizika a zavést potřebná technická opatření.

Strategických cílů bychom rádi dosáhli do začátku platnosti nařízení.

5. Analýza situace

5.1 SWOT analýza

Metodou Swot analýzy jsme identifikovali silné (ang: Strengths) a slabé (ang: Weaknesses) stránky, příležitosti (ang: Opportunities) a hrozby (ang: Threats), spojené s naším projektem, v tabulce 3 je vše pro přehlednost zobrazeno.

Mezi **silné stránky** našeho zdravotnického zařízení patří především podpora vedení nemocnice, zaměstnanci a velmi dobrý spolupráce odpovědných osob v rámci pracovní skupiny.
Jako **slabé stránky** jsme identifikovali nedostatečně nastavený a zmapovaný systém zpracování a ochrany osobních údajů, chybějící interní předpis, nedostatečnou informovanost na www stránkách Nemocnice, neurčení odpovědné osoby za zpracování osobních údajů, neexistující následnou kontrolu,

nestanovené kompetence odpovědných pracovníků, chybějící školení pracovníků a také nedstatečné technicko-organizační opatření.

Příležitost zavedení nových postupů a procesů a zlepšení ochrany osobních údajů.

Hrozbou pro naši nemocnici jsou lidé jako možný únik informací, hrozba stížností a soudních sporů, kybernetický útok, příp. sankce ze strany dozorového úřadu v případě porušení ochrany osobních údajů.

Tab. 3 SWOT analýza

Silné stránky	Slabé stránky
Podpora vedení	lidé
lidé	Nedostatečně nastavený systém zpracování a ochrany osobních údajů
Spolupráce odpovědných osob v rámci pracovní skupiny	Chybějící interní předpis
	Nedostatečná informovanost veřejnosti na www stránkách
	Neexistující analýza jednotlivých činností zpracování osobních údajů a jejich zabezpečení
	Neurčena odpovědná osoba za zpracování osobních údajů v rámci nemocnice
	Neexistující následná kontrola
	Nestanovené kompetence odpovědných pracovníků
	Nevedena evidence a rozsah zpracování osobních údajů pacientů ani zaměstnanců
	Chybějící školení pracovníků
	Nedostatečná technicko-organizační opatření

Příležitosti	Hrozby
Zavedení nových postupů a procesů	Lidé – únik informací
	Stížnosti a soudní spory
	Kybernetický útok
	Při porušení ochrany osobních údajů – Sankce ze strany dozorového orgánu

5.2 Analýza provozních dějů

V nemocnici před zavedení systému ochrany osobních údajů v souladu s GDPR, bylo provedená analýza na základě check-listu s následujícím zjištěním.

Úroveň shody s požadavky zákona č. 101/2000 Sb.

Legenda k hodnocení:

1 – **shoda** (plně zajištěno)

2 – **připomínka** (částečně zajištěno)

3 – **neshoda** (nezajištěno)

Požadavek	**Hodnocení**		
	1	**2**	**3**
Stanovení účelu zpracování	☐	☐	☒
Identifikace subjektů údajů	☐	☒	☐
Formální stanovení subjektů údajů	☐	☐	☒
Identifikace kategorií osobních údajů	☐	☒	☐
Formální stanovení kategorií osobních údajů	☐	☐	☒
Identifikace zdrojů osobních údajů	☐	☒	☐
Formální stanovení zdrojů osobních údajů	☐	☐	☒
Identifikace příjemců osobních údajů	☐	☒	☐
Formální stanovení příjemců osobních údajů	☐	☐	☒
Identifikace a stanovení doby zpracování osobních údajů	☐	☒	☐
Formální stanovení doby zpracování osobních údajů	☐	☒	☐
Identifikace a stanovení předávání osobních údajů do zahraničí	☐	☒	☐
Formální stanovení předávání osobních údajů do zahraničí	☐	☐	☒
Identifikace jednotlivých zpracování	☐	☐	☒
Formální stanovení jednotlivých zpracování	☐	☐	☒
Identifikace registrační povinnosti	☐	☐	☒
Splnění registrační povinnosti	☐	☐	☒
Identifikace a stanovení způsobu zveřejnění informací o realizovaném zpracování	☐	☐	☒
Splnění zveřejnění informací o realizovaném zpracování	☐	☐	☒
Identifikace povinnosti získání souhlasu od subjektů údajů	☐	☒	☐
Splnění povinnosti získání souhlasu od subjektů údajů	☐	☒	☐
Identifikace rozsahu povinnosti podání informací subjektům údajů	☐	☐	☒

Požadavek		Hodnocení		
		1	2	3
Splnění povinnosti podání informací subjektům údajů		☐	☐	☒
Manuální i automatizované zpracování				
	Identifikace a formální stanovení prostředků zpracování - míst, objektů a prostor	☐	☐	☒
	Identifikace a formální stanovení prostředků zpracování - osob	☐	☒	☐
	Identifikace a formální stanovení prostředků zpracování - technických prostředků a zařízení	☐	☒	☐
	Identifikace a formální stanovení prostředků zpracování - činností a procesů	☐	☒	☐
	Identifikace a formální stanovení prostředků zpracování - prostředků ICT	☐	☒	☐
	Formální stanovení způsobu zpracování	☐	☐	☒
Identifikace stávajících bezpečnostních opatření				
	Personálních	☐	☒	☐
	Fyzických	☐	☒	☐
	Administrativních	☐	☒	☐
	Organizačních a režimových	☐	☒	☐
	V oblasti ICT	☐	☒	☐
Formální stanovení bezpečnostních opatření				
	Personálních	☐	☐	☒
	Fyzických	☐	☐	☒
	Administrativních	☐	☒	☐
	Organizačních a režimových	☐	☐	☒
	V oblasti ICT	☐	☒	☐

Následně byla rovněž provedená analýza na způsob řízení ochrany osobních údajů v nemocnici na základě check-listu

Způsob řízení ochrany osobních údajů v nemocnici

Legenda k hodnocení:

1 – **shoda** (plně zajištěno)

2 – **připomínka** (částečně zajištěno)

3 – **neshoda** (nezajištěno)

Požadavek	Hodnocení		
	1	2	3
Vymezení místa a způsobu řízení ochrany osobních údajů v celkovém systému řízení nemocnice	☐	☐	☒
• Ochrana osobních údajů v nemocnici je vymezena interním předpisem, které: o řeší zpracování osobních údajů pouze v rámci zdravotnické dokumentace (pro všechna ostatní zpracování osobních údajů příslušné zdokumentování chybí); o opatření k ochraně osobních údajů v něm vymezená zdaleka nepokrývají všechny požadavky zákona č. 101/2000 Sb.			
Formální stanovení kompetencí v oblasti ochrany osobních údajů	☐	☐	☒
• Pro ochranu osobních údajů u organizace: o není stanovena potřebná řídící infrastruktura; o odpovědným zaměstnancům nejsou stanoveny příslušné kompetence.			
Provedení inventarizace zpracovávaných osobních údajů	☐	☐	☒
• V rámci realizované analýzy nebyly získány důkazy o provedení „inventarizace" všech zpracovávaných osobních údajů ani o následné identifikaci všech realizovaných zpracování v rámci organizace.			
Identifikace jednotlivých zpracování	☐	☐	☒
• Na základě realizované analýzy lze pouze odůvodněně předpokládat, že se jedna zejména o následující zpracování: o personálně-mzdová agenda; o agenda výběrových řízení; o agenda vzdělávání; o agenda fotografií; o docházka; o lékařská knihovna; o agenda BOZP; o agenda pochval a stížností; o agenda dárců krve; o zdravotnická dokumentace; o agenda klientských karet (lékárna); o agenda dopravní služby.			
Identifikace rolí správce a zpracovatele u jednotlivých zpracování	☐	☐	☒

Požadavek	Hodnocení		
	1	2	3
• Na základě realizované analýzy lze odůvodněně předpokládat, že zde existuje minimálně jeden vztah správce x zpracovatel (organizace poskytující služby v rámci správy IS): o nebyla předložena příslušná smlouva k přezkoumání, ale lze předpokládat, že v ní nejsou stanoveny nezbytné bezpečnostní aspekty pro ochranu osobních údajů u zpracovatele.			
Zařazení problematiky vzdělávání v oblasti ochrany osobních údajů do systémů vzdělávání zaměstnanců:	☐	☐	☒
• Nebylo zjištěno, že by u organizace byla do systému vzdělávání zařazena problematika oblasti ochrany osobních údajů.			
Jiné:	☐	☐	☒

Požadavek	Hodnocení		
	1	2	3
• Zpracování fotografií zaměstnanců bez souhlasu zaměstnanců a registrace u Úřadu pro ochranu osobních údajů. • Zveřejňování životopisů včetně fotografií zaměstnanců oddělení IT (i bývalých) na webových stránkách organizace. Přes tvrzení vedoucího oddělení IT, že disponuje souhlasy těchto osob, nám tyto nebyly předloženy. Lze tedy předpokládat, že souhlas nemusí být v souladu se zákonem č. 101/2000 Sb. • Uchovávání životopisů uchazečů o zaměstnání po dobu delší než je nezbytně nutná (po ukončení výběrového řízení) a bez registrace u Úřadu pro ochranu osobních údajů. Rozsah informace uchazečům o zpracování (uchovávání) jejich osobních údajů nepokrývá požadavky zákona č. 101/2000 Sb. • Uchovávání osobních údajů uživatelů lékařské knihovny po dobu delší, než je nezbytně nutná (po uplynutí registrační lhůty). Rozsah informace uživatelům o zpracování osobních údajů dostatečně nepokrývá požadavky zákona č. 101/2000 Sb. • Zpracování osobních a citlivých údajů klientů lékárny (Žádost o vydání klientské karty) bez registrace u Úřadu pro ochranu osobních údajů. Rozsah informace klientům lékárny o zpracování osobních a citlivých údajů dostatečně nepokrývá požadavky zákona č. 101/2000 Sb. • Zpracování citlivých údajů (údaj o členství v odborových organizacích) v rámci personálně-mzdové agendy v IS VEMA. • Zpracování kopií občanských průkazů uživatelů sociálních služeb za účelem přebírání důchodu. Nebyl předložen souhlas uživatelů k tomuto zpracování. • Předávání osobních i citlivých údajů klientů transfuzní stanice jiným subjektům. Nebyla předložena smlouva k nahlédnutí.			

5.3 Analýza lidských zdrojů

Zavedení systému ochrany osobních údajů v nemocnici v souladu s GDPR se v našem zdravotnickém zařízení týkalo všech zaměstnanců.

Tab. 3 analýza lidských zdrojů

Zaměstnanec	Počet
Lékaři	112
Nelékaři	534
Dělníci a provozní pracovníci	58
THP	61
CELKEM	**765**

5.4Finanční analýza

Rozpočet projektu obsahuje pořizovací náklady

Tab. 6 finanční analýza

Aktivita	Odhad nákladů, případně výnosů
Analýza	40.000,--
Pověřenec na ochranu osobních údajů	200.000,--
Školení zaměstnanců	20.000,--
Nákup skartovacích strojů	100.000,--
Zabezpečení dokumentace (nákup, příp. montáž uzamykatelných skříní, zámků, kartoték…)	140.000,--
Celkem	500.000,--

6. Návrh a zdůvodnění řešení problému

Na základě vstupních analýz jsme stanovili následné aktivity potřebné k naplnění požadavků ochrany osobních údajů v souladu s GDPR.

Potřebné aktivity:

- Provedení a vyhodnocení vnitřního auditu GDPR – cílem je zjistit, zda jsou v organizaci zavedeny procesy související s ochranou osobních údajů
- Jmenování pracovního týmu pro implementaci GDPR v Nemocnici Třinec

- Výběr Pověřence pro ochranu osobních údajů včetně začlenění do organizační struktury Nemocnice Třinec
- Zpracování informace pro pacienty a zaměstnance v souvislosti se zpracováním OÚ
- Vypracování směrnice Ochrana osobních údajů včetně nastavení procesů a zodpovědnosti zaměstnanců Nemocnice Třinec
- Vytvoření procesů pro uplatňování práv subjektů údajů
- Vytvoření katalogu zpracování osobních údajů za všechna pracoviště Nemocnice Třinec
- Provedení kontroly související se zpracování osobních údajů prováděných na základě oprávněného zájmu – v Nemocnici Třinec kamerový systém
- Zavedení procesu řešení bezpečnostních incidentů z pohledu ochrany osobních údajů
- Vložení informací do nemocničního informačního systému - podání informací pacientovi o zpracování osobních údajů
- Vytvoření nových štítků pacientů
- Zajištění dostupnosti informací o zpracování osobních údajů pro pacienty a zaměstnance – tisk dokumentů a distribuce na všechna pracoviště nemocnice
- Vytvoření a zprovoznění webové sekce „ Ochrana osobních údajů“ a zveřejnění povinných informací vyplývajících z Nařízení Evropského parlamentu a rady (EU) 2016/679
- Analýza webu (cookies, formuláře, souhlasy)
- Vytvoření seznamu smluvních partnerů
- Zaslání oslovovacího dokumentu smluvním partnerům
- Vytvoření vzorové zpracovatelské smlouvy
- Uzavírání zpracovatelských smluv – dle článku 28 Nařízení
- Revize stávajících smluvních vztahů – posouzení jednotlivých smluv s ohledem na to, zda je třeba uzavřít dodatek k mlčenlivosti příp. Zpracovatelskou smlouvu dle článku 28 Nařízení
- Aktualizace pracovní smlouvy – doplnění informací pro zaměstnance o rozsahu zpracování osobních údajů
- Aktualizace osobního dotazníku dle zásady minimalizace
- Zajištění proškolení stávajících zaměstnanců zpracovávajících osobní údaje
- Zařazení školícího modulu do adaptačního procesu u nových zaměstnanců
- Revize ostatních organizačních směrnic – vytvoření seznamu směrnic, ve kterých je v souvislosti s Nařízením nutné provést změny
- Implementace změn v souvislosti s Nařízením do interních dokumentů
- Nastavení procesu konzultace ochrany osobních údajů v nových interních předpisech
- Nastavení fyzické ochrany - technicko-organizační opatření – doplnění zámků do všech úložných prostor na dokumenty, průběžná kontrola dodržování nastavených opatření (uzamčené kanceláře, sesterny, ambulance po odchodu pracovníka, pořádek na pracovních

stolech, umístění dokumentů určených k průběžné skartaci na předem určených místech, používání, umístění dokumentace pacientů na určených místech…. atd.)

- Nákup skartovacích strojů včetně nastavení procesů průběžné skartace dokumentů obsahujících osobní údaje pacientů i zaměstnanců
- Revize Organizační směrnice Spisový a skartační řád, včetně upřesnění procesů fyzické likvidace (skartace) dokumentů po uplynutí skartační lhůty
- Aktualizace souhlasů se zpracováním osobních údajů u zpracování založeného na základě souhlasu subjektu údajů – individuální konzultace Pověřence na ochranu osobních údajů dle jednotlivých případů
- Analýza procesu nahrávání operačních výkonů – vytipování oborů
- Analýza - Facebook Nemocnice Třinec

Připravujeme pro rok 2019

- Nastavení pseudonymizace záznamů operačních výkonů
- Průběžné změny interních dokumentů dle jejich termínů revize
- Následný audit jednotlivých opatření zavedených v souvislosti s GDPR
- Nový registr docházky včetně stravovacího systému
- Nový systém změn hesel v rámci přístupových oprávnění do informačního systému Nemocnice Třinec
- Pořízení nového kartového dveřního systému – řízený vstup oprávněných osob na vybraná pracoviště
- Pravidelné proškolení stávajících zaměstnanců dle požadavků EN

7. Časový plán zajištění projektu

Tab. 7 časový plán pro rok 2018

Aktivita	Zodpovědná osoba	2-3	4-5	6-8	8-10	10-12
Provedení a vyhodnocení vnitřního auditu	ředitel	⇨				
Jmenování pracovního týmu	ředitel	⇨				
Výběr Pověřence pro ochranu OU (DPO)	ředitel	⇨				
Zpracování povinných informací pro subjekty údajů	DPO, NOP		⇨			

Vypracování interní organizační směrnice	DPO		→			
Vytvoření procesů pro uplatňování práv subjektů	DPO		→			
Vytvoření katalogu zpracování osobních údajů	DPO, NOP, TN, EPN		→			
Provedení analýzy – zpracování OU na základě oprávněného zájmu	DPO		→			
Zavedení procesu řešení bezpečnostních incidentů	DPO		→			
Analýza obsahu a vložení informací do nemocničního informačního systému – informace pro pacienty o zpracování OU	IT, NOP		→			
Vytvoření nových štítků pacientů	IT, NOP		→			
Tisk a distribuce informací o zpracování osobních údajů pro pacienty a zaměstnance	DPO, Ř		→			
Vytvoření a zprovoznění webové sekce „Ochrana osobních údajů“	IT		→			
Vytvoření seznamu smluvních partnerů, jejich průběžné oslovování a uzavírání zpracovatelských smluv dle článku 28 Nařízení	EN, TN, DPO, NOP		→			
Revize stávajících smluvních vztahů	DPO, P, EN, TN		→			
Aktualizace pracovní smlouvy pro zaměstnance	DPO		→			
Aktualizace osobního dotazníku dle zásady minimalizace OU	DPO		→			
Proškolení stávajících zaměstnanců zpracovávajících OU	DPO			→		

Zařazení školícího modulu do adaptačního procesu u nástupu nových zaměstnanců	DPO		→			
Revize ostatních organizačních směrnic	Odpovědné osoby			→		
Zabezpečení fyzické ochrany – technicko-organizační opatření	DPO, TN		→			
Nákup skartovacích strojů včetně nastavení procesů průběžné skartace dokumentů s OU	TN, DPO, NOP			→		
Revize organizační směrnice Spisový a skartační řád, včetně upřesnění procesů fyzické likvidace (skartace) dokumentů po uplynutí skartační lhůty.	TN, DPO		→			
Aktualizace souhlasů se zpracováním osobních údajů u zpracování založeného na základě souhlasu subjektu údajů	DPO			→		
Analýza nahrávání operačních výkonů – vytipování oborů	DPO, NLP			→		
Analýza – facebook Nemocnice	IT, DPO			→		
Kontrolní činnost – kontrola nastavených procesů a opatření na pracovištích + konzultace	DPO				→	

8. Udržitelnost a opakovatelnost projektu

Projekt bude relizován komplexně – analýza aktuálního stavu zpracování osobních údajů pacientů i zaměstnanců nemocnice a zacházení s těmito údaji. Dále pak vypracování hlavního interního předpisu ochrana osobních údajů a revize stávajících předpisů, proškolení všech zaměstnanců, aby věděli, jaké změny vstupují v platnost s novým Nařízení EU, jaká mají nově práva pacienti i zaměstnanci a také zaměstnavatel a kde budou všechny informace dostupné. V neposlední řadě bude potřeba zrevidovat

a zajistit bezpečnost zpracování osobních údajů, na základě vyhodnocených rizik pak pravidelně kontrolovat dodržování nastavených postupů a procesů včetně technicko-organizačních opatření.

9. Monitorování a vyhodnocování

Monitoring celého procesu analýzy aktivit, úpravy vnitřních předpisů, školení pracovníků a zavádění technicko-organizačních opatření bude řídit pověřenec ochrany osobních údajů, který bude velmi úzce v jednotlivých oblastech zpracování osobních údajů spolupracovat se všemi vedoucími pracovníky. Pověřenec bude následně provádět ve spolupráci s vedoucími jednotlivých pracovišť také dodržování nastavených procesů.

10. Závěr

Od tohoto projektu očekáváme:

1. Splnění zákonných povinností Nemocnice Třinec, p.o. jako zpracovatele osobních údajů pacientů i zaměstnanců
2. Zvýšení bezpečnosti při zpracování osobních údajů
3. Informování zaměstnanců o nově nastavených procesech a právech, které Nařízení EU nově dává subjektům údajů
4. Zkvalitnění všech procesů, které vedou na ochranu osobních údajů včetně technicko-organizačních opatření.
5. Realizaci pravidelných kontrol, vyhodnocování dodržování nastavených procesů a také přijetí opatření v případě nedodržování ve spolupráci s aktivním vedením Nemocnice Třinec, p.o.
6. Nastavení systému konzultací pro zaměstnance v případě, že mají pochybnosti o případném porušení zpracování osobních údajů, případně mají podezření na únik osobních údajů.

První kontroly nastavených procesů proběhly na podzim 2018 na pracovištích poskytujících zdravotní péči s velmi dobrým výsledkem, což považujeme za první úspěch.