Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Implementace GDPR ve zdravotnictví

Eva Nouzová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Eva Nouzová

Podnikání a administrativa

Název práce

Implementace GDPR ve zdravotnictví

Název anglicky

Implementation of GDPR in Healthcare

Cíle práce

- analýza právních úprav v oblasti ochrany osobních údajů a práv pacientů
- analýza procesu implementace GDPR ve vybraném zdravotnickém zařízení
- potvrzení či vyvrácení hypotézy o povědomí pacientů o svých právech se zaměřením na GDPR s případnými návrhy na zlepšení
- navržení podnětů jak přistoupit k internímu auditu ve vybraném zdravotnickém zařízení k posouzení dodržování nových právních povinností dle GDPR

Metodika

Práce bude rozdělena na teoretickou a praktickou část.

V teoretické části bude použita zejména metoda literární rešerše, výklad práva a analýza právních úprav v oblasti ochrany osobních údajů a práv pacientů. Dále bude použita srovnávací metoda k porovnání vývoje práv pacientů.

V praktické části bude využita zejména analytická metoda a bude vypracována případová studie o průběhu implementace GDPR ve vybraném zdravotnickém zařízení. Dále bude provedeno dotazníkové šetření s cílem zjistit povědomí pacientů o svých právech. Výsledky budou statisticky zpracovány. Pro účely zhodnocení implementace GDPR ve vybraném zdravotnickém zařízení budou navrženy podněty k přístupu k internímu auditu.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

GDPR, DPO, osobní údaje, subjekt, správce, zpracovatel, práva pacientů, interní audit

---

Doporučené zdroje informací

Etický kodex, Statut a Manuál interního auditu v resortu Ministerstva zdravotnictví České republiky, 2018.

JANEČKOVÁ, E. GDPR – Praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.

Metodika Ministerstva zdravotnictví České republiky a Ústavu zdravotnických informací a statistiky České republiky – Jak implementovat nařízení evropského parlamentu a rady 2016/679, 2017.

Nařízení evropského parlamentu a rady (EU) 2016/679, 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).

Návrh nového zákona o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů.

NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. GDPR / Obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0.

PETROV, J., VÝTISK, M., BERAN, V. Občanský zákoník. Komentář. Praha: C. H. Beck, 2017. ISBN 978-80-7400-653-1.

Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

ŽŮREK, J. Praktický průvodce GDPR. Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

JUDr. Jitka Mráčková, CSc.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 7. 11. 2018

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 12. 11. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 27. 03. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Implementace GDPR ve zdravotnictví" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 29. 3. 2019 _____

Poděkování

Ráda bych touto cestou poděkovala vedoucí mé diplomové práce, JUDr. Jitce Mráčkové, CSc., za odborné vedení a za množství času, které mi věnovala. Dále bych ráda poděkovala své rodině za podporu při studiu.

Implementace GDPR ve zdravotnictví

Abstrakt

Tato diplomová práce je věnována problematice GDPR, konkrétně GDPR ve zdravotnictví. Cílem práce je analyzovat celý proces implementace GDPR ve vybraném zdravotnickém zařízení.

Teoretická část této práce analyzuje právní úpravu v oblasti ochrany osobních údajů a práv pacientů, vymezuje základní pojmy, kterými jsou např. osobní údaj, DPO, subjekt, správce či zpracovatel. Dále se věnuje základním zásadám a principům GDPR a specifikům v oblasti zdravotnictví. Pozornost je věnována také právům pacientů.

Praktická část je rozdělena na dvě části. První je založena na případové studii, která analyzuje proces implementace GDPR ve vybraném zdravotnickém zařízení. K posouzení dodržování nových právních povinností dle GDPR jsou navrženy podněty k přístupu k internímu auditu, které bude moci zdravotnické zařízení nyní využít. Druhá část je věnována dotazníkovému šetření s cílem zjištění informovanosti pacientů o svých právech v souvislosti s poskytováním zdravotní péče a povědomí o nových právech v souvislosti s účinností GDPR. V závěru praktické části této práce jsou získané výsledky statisticky vyhodnoceny.

Klíčová slova: GDPR, osobní údaj, DPO, DPIA, subjekt, správce, zpracovatel, zdravotnictví, práva pacientů, interní audit

Implementation of GDPR in Healthcare

Abstract

Thesis deals with GDPR with focus on GDPR in health care. The goal of the thesis is to analyse the process of GDPR implementation in selected healthcare facility.

The theoretical part of this thesis analyses the legislation in the area of personal data protection and patients' rights, defines basic terms, such as personal data, DPO, data subject, data controller or data processor. It also deals with the basic principles of GDPR and its specifics in the field of health care. Attention is also paid to patients' rights.

The practical part is divided into two parts. The first is based on a case study that analyses the process of implementation of GDPR in a selected healthcare facility. To assess compliance with the new legal obligations under the GDPR, suggestions for approach to internal audit are proposed, which the healthcare facility will now be able to use. The second part focuses on the survey among patients with the aim to determine patients' awareness of their rights in association with the provision of health care and of their awareness of the GDPR rights. Gathered data are statistically evaluated at the end of the practical part of this work.

Keywords: GDPR, personal data, DPO, DPIA, data subject, data controller, data processor, healthcare, patients' rights, internal audit

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam použitých zkratek

atd.	a tak dále
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	Evropská unie
GDPR	General Data Protection Regulation
např.	například
MPSV ČR	Ministerstvo práce a sociálních věcí České republiky
MV ČR	Ministerstvo vnitra České republiky
MZ ČR	Ministerstvo zdravotnictví České republiky
NOZ	Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
obr.	obrázek
př.	případně
Sb.	Sbírka zákonů
tab.	tabulka
tzv.	takzvaně
ÚOOÚ	Úřad pro ochranu osobních údajů
ÚZIS	Ústav zdravotnických informací a statistiky ČR

1 Úvod

GDPR neboli General Data Protection Regulation je novým právním rámcem ochrany osobních údajů, který má dopad na každého, kdo jakýmkoli způsobem osobní údaje zpracovává. Jeho hlavním cílem je hájit a zvýšit ochranu osobních údajů.

GDPR a vůbec ochrana osobních údajů není ničím novým. Základní principy sahají až do 18. století, konkrétně do roku 1789, kdy došlo k přijetí Deklarace práv člověka a občana. Dnes ji lze považovat za základ a vzor všech dnešních právních předpisů týkajících se úpravy lidských práv a svobod.

Velmi důležitým mezníkem byla Směrnice evropského parlamentu a rady[1]. Jelikož však vstoupila v platnost před více než dvaceti lety, jednalo se o legislativu značně zastaralou, a to především díky technologickému pokroku. Neupravovala totiž problematiku sociálních sítí, cloudových úložišť, nakupování po internetu apod. Započala tedy mnohá jednání, jejichž výsledkem je právě GDPR.

V celé diplomové práci je užíván pojem „GDPR“, kterým je myšleno 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).

Teoretická část je věnována vybraným pojmům GDPR. Jedním z nejvýraznějších nově zavedených pojmů je DPO neboli pověřenec pro ochranu osobních údajů. GDPR s sebou přineslo také šest základních zásad a principů, kterými je třeba se řídit, aby došlo k souladu s GDPR. Jsou jimi zásada zákonnosti, korektnosti a transparentnosti, omezení účelem, minimalizace údajů, dále také přesnost či omezení uložení a poslední zásadou je integrita a důvěrnost.

Značná část diplomové práce se týká specifikům pro resort zdravotnictví, jelikož zde existuje mnoho výjimek. Ve zdravotnictví dochází často ke zpracování zvláštní kategorie osobních údajů neboli citlivých osobních údajů, pro jejichž zpracování platí přísnější podmínky. Ke zpracování může docházet na základě souhlasu subjektu údajů nebo na základě zákonné povinnosti. Jedná se např. o nakládání se zdravotnickou dokumentací nebo zpracování pro vědeckovýzkumné účely.

[1] 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, ze dne 24. října 1995.

Poslední část teoretické části této diplomové práce je věnována právům pacientů, především pak se zaměřením na nová práva vyplývající z GDPR. Jedná se o právo na výmaz, právo na přenositelnost údajů a právo vznést námitku.

V praktické části je na případové studii analyzován celý proces implementace GDPR ve vybraném zdravotnickém zařízení. Pro jeho zhodnocení jsou dále navrženy podněty k přístupu k internímu auditu, které bude moci vybrané zdravotnické zařízení v budoucnu využít.

Součástí této části práce je také dotazníkové šetření s cílem zjištění povědomí pacientů o svých právech v souvislosti s poskytováním zdravotní péče a zároveň zjištění povědomí o nových právech v souvislosti s účinností GDPR.

V praktické části je užíván pojem „Nemocnice“, jelikož vybrané zdravotnické zařízení si přálo být uváděno anonymně.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem teoretické části této diplomové práce je analýza právních úprav v oblasti ochrany osobních údajů a práv pacientů.

Cílem praktické části je analýza procesu implementace GDPR ve vybraném zdravotnickém zařízení. K posouzení dodržování nových právních povinností dle GDPR ve vybraném zdravotnickém zařízení je cílem navržení podnětů, jak přistoupit k internímu auditu.

V další části praktické části této práce je cílem potvrzení či vyvrácení hypotézy o povědomí pacientů o svých právech se zaměřením na GDPR s případnými návrhy na zlepšení.

2.2 Metodika

Tato diplomová práce je věnována problematice GDPR, konkrétně GDPR ve zdravotnictví. Práce je rozdělena na teoretickou a praktickou část.

V teoretické části je použita zejména metoda literární rešerše, pro kterou bylo nutné provést vyhledání příslušné odborné literatury. Dále je použit výklad práva a analýza právních úprav v oblasti ochrany osobních údajů a práv pacientů, se zaměřením na 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) a v oblasti zdravotnictví na zákon č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů.

Jsou zde vymezeny vybrané pojmy, zásady a principy GDPR, které jsou důležitým podkladem pro vypracování praktické části této diplomové práce.

K porovnání vývoje práv pacientů je použita srovnávací metoda.

V praktické části je využita zejména analytická metoda a je vypracována případová studie o průběhu implementace GDPR ve vybraném zdravotnickém zařízení. Jsou zde využity především pracovní zkušenosti získané v daném zdravotnickém zařízení.

Pro účely zhodnocení implementace jsou navrženy podněty k přístupu k internímu auditu.

Dále bylo provedeno dotazníkové šetření, které probíhalo v několika fázích.

V úvodu dotazníkového šetření byl stanoven cíl, kterým bylo zjištění informovanosti pacientů o svých právech v souvislosti s poskytováním zdravotní péče, a zdali svá práva aktivně využívají. Druhým cílem bylo zjištění povědomí o nových právech v souvislosti s účinností GDPR. K dosažení těchto cílů byly stanoveny dvě hypotézy.

Po stanovení cílů a formulaci hypotéz následovalo samotné sestavení dotazníku.

Z důvodu snadného vyplňování bylo rozhodnuto, že otázky budou pouze uzavřené, maximálně v některých případech s možností doplnění vlastní odpovědi.

Pro lepší přehlednost bude dotazník rozdělen do několika částí, a to na samotná práva pacientů, manipulaci se zdravotnickou dokumentací, povědomí pacientů o právech v souvislosti s GDPR a jejich případnou aplikací. Na závěr budou zařazeny otázky pro účel statistického zpracování.

Při volbě výzkumné metody se nabízí dotazníkové šetření na místě. Vzhledem však k účelu, ke kterému pacienti navštěvují zdravotnická zařízení a samotné náladě při návštěvě, hrozí vysoká neochota pacientů dotazník vyplnit. Zároveň v případě dotazování ambulantních pacientů v čekárně hrozí riziko, že pacienti budou chtít obratem svá práva využít, což by nebylo pro vybrané pracoviště, na kterém by dotazování probíhalo, žádoucí.

Z těchto důvodů bude zvolena elektronická distribuce dotazníků. Dotazník bude veřejně vyvěšen po dobu zhruba jednoho měsíce a jeho vyplňování bude podporováno i dalšími aktivitami, např. rozesíláním emailů či distribuováním na sociálních sítích, aby bylo získáno co největší množství respondentů.

Výzkumný vzorek budou tvořit pouze lidé starší 18 let, jelikož za mladší odpovídají zákonní zástupci.

Před samotnou distribucí bude provedeno pilotní šetření na několika vybraných respondentech, aby byla zjištěna časová náročnost průzkumu a také srozumitelnost a logická návaznost otázek.

Výsledky budou statisticky zpracovány do tabulek a grafů. V závěru bude provedeno celkové zhodnocení dotazníkového šetření a budou potvrzeny či vyvráceny stanovené hypotézy.

3 Teoretická východiska

3.1 Obecně k právní úpravě

3.1.1 Právní úprava v občanském zákoníku

V souvislosti s ochranou osobních údajů je určitě důležité zmínit úpravu ochrany osobnosti v zákoně č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen NOZ). Ochrana osobnosti je v NOZ deklarována již úvodním ustanovením, konkrétně § 3 odst. 2 písm. a), kde je uvedeno, že „*každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí.*“ [2]

Každý člověk má právo na jméno a jeho ochranu. Toto právo je v NOZ zakotveno v oddílu pátém Jméno a bydliště člověka, kde je v § 77 odst. 1 uvedeno, že „*každý člověk má právo užívat své jméno v právním styku, stejně jako právo na ochranu svého jména a na úctu k němu.*“ [3]

Další úprava je obsažena v oddílu šestém Osobnost člověka. Např. lze v pododdílu druhém Podoba a soukromí nalézt úpravu týkající se zachycování a rozšiřování podoby člověka, úpravu zásahu do soukromí jiného, použití písemností osobní povahy, podobizny, obrazového či zvukového záznamu. Dále je zde uvedeno, v jakých případech je vyžadován souhlas dané osoby. Vždy však platí, že „*zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka.*“ [4] V pododdílu třetím je dále uvedena úprava Zásahu do integrity člověka.[5]

3.1.2 Právní úprava v zákoně č. 101/2000 Sb., o ochraně osobních údajů

V České republice ochranu osobních údajů upravoval zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, který je v souladu s právem EU, včetně mezinárodních smluv, jimiž je vázána Česká republika.[6] Kromě práv a povinností při

[2] Viz § 3 odst. 2 písm. a) zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[3] Tamtéž § 77 odst. 1
[4] Tamtéž § 90
[5] Tamtéž pododdíl 3
[6] Viz § 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

zpracování osobních údajů tento zákon také upravuje a stanovuje, kdy a za jakých podmínek je možné předávat osobní údaje do zahraničí.

Od 25. května 2018 je tento zákon v převážné části hmotné úpravy nahrazen 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 (obecné nařízení o ochraně osobních údajů).[7]

3.1.3 Právní úprava v zákoně č. 372/2011 Sb., o zdravotních službách

V oblasti zdravotnictví je nejdůležitějším předpisem Zákon č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů. V oblasti ochrany osobních údajů předpis upravuje v §§ 53–69 především vedení a nakládání se zdravotnickou dokumentací, dále se k němu váže navazující prováděcí vyhláška Ministerstva zdravotnictví České republiky č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů. Další, velmi důležitou částí, je úprava v §§ 70–78, týkající se správy Národního zdravotnického informačního systému a povinností Ústavu zdravotnických informací a statistiky ČR, spolu s navazující prováděcí vyhláškou Ministerstva zdravotnictví České republiky č. 373/2016 Sb., o předávání údajů do Národního zdravotnického informačního systému, ve znění pozdějších předpisů.[8]
Neméně důležitou jsou části upravující poskytování informací o zdravotním stavu pacienta nebo také mlčenlivost lékaře.[9]

3.1.4 Další právní předpisy

Jedním z nejdůležitějších předpisů, co se týká oblasti ochrany osobních údajů, je bezesporu Listina základních práv EU, konkrétně pak čl. 8, ve kterém je ochrana osobních údajů zakotvena jako základní právo.[10] Na vnitrostátní úrovni je pak nutné zmínit Listinu základních práv a svobod České republiky, kde je v článku 10 odst. 3 stanoveno, že „k*ažd*ý

[7] ÚOOÚ. *Desatero omylů* [online]. [cit. 2018-12-28]. Dostupné z: https https://www.uoou.cz/desatero-omylu/ds-4818/archiv=0&p1=3109.
[8] Viz §§ 53–69 a §§ 70–78 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.
[9] Tamtéž část čtvrtá a pátá
[10] Viz čl. 8 odst. 3 Listiny základních práv Evropské unie 2012/C 326/02

má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“ [11]

Co se týká oblasti zdravotnictví, dalším významným předpisem je zákon č. 373/2011 Sb., o specifických zdravotních službách, ve znění pozdějších předpisů. Jak již název napovídá, tento zákon upravuje speciální zdravotní služby, kterými jsou např. asistovaná reprodukce, sterilizace, změna pohlaví, psychochirurgické výkony, genetická vyšetření apod.[12]

Ochrana osobních údajů je ve zdravotnictví upravena i mnoha dalšími předpisy, kterými jsou např.:

- zákon č. 100/2017 Sb. o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon), ve znění pozdějších předpisů,
- zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), ve znění pozdějších předpisů,
- zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů,
- zákon č. 268/2014 Sb., o zdravotnických prostředcích a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů,
- zákon č. 374/2011 Sb., o zdravotnické záchranné službě ve znění pozdějších předpisů.

3.1.5 Nová právní úprava

3.1.5.1 Vývoj GDPR

Z hlediska GDPR sahá ochrana osobních údajů do roku 1981. Dne 28. ledna 1981 byla podepsána smlouva o ochraně osob s ohledem na automatické zpracování osobních údajů, jako Úmluva Rady Evropy č. 108. Dne 1. října 1985 vstoupila v platnost.[13] Úmluva upravovala pouze automatizované zpracování osobních údajů, tedy zpracování prostřednictvím automatizovaných prostředků. Vztahovala se jak na soukromý, tak veřejný

[11] Viz čl. 10 Listiny základních práv a svobod 2/1993 Sb.
[12] Zákon č. 373/2011 Sb., o specifických zdravotních službách, ve znění pozdějších předpisů
[13] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 14.

sektor.[14] V České republice byl kromě Úmluvy v roce 2001 ratifikován i Dodatkový protokol Rady Evropy z 8. listopadu 2001 č. 181, o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice. Dále se Česká republika zavázala, že zásady stanovené v Úmluvě č. 108, bude dodržovat i pro ostatní osobní údaje, které nejsou zpracovávány automatizovaně.[15]

Velmi důležitým mezníkem byla Směrnice evropského parlamentu a rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, ze dne 24. října 1995. V platnost tato směrnice vstoupila dne 13. prosince 1995 a do 24. října 1998 musely členské státy EU provést ve vnitrostátním právu příslušné úpravy.[16] Tato směrnice byla dále doplněna Rámcovým rozhodnutím Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech.[17]

Směrnice hrála v ochraně osobních údajů velmi důležitou roli. Tvořilo ji 72 recitálů a dalších 34 článků. Mimo základních pojmů a povinností, se kterými se setkáváme dodnes, také zřídila pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, známou jako WP29.[18]

Jelikož Směrnice 95/46/ES vstoupila v platnost před více než dvaceti lety, jednalo se o legislativu značně zastaralou, a to především díky technologickému pokroku. Neupravovala totiž problematiku sociálních sítí, cloudových úložišť, nakupování po internetu apod.[19]

Započalo tedy jednání o nové směrnici. Jelikož se jednalo o významnou revizi, probíhaly přes dva roky ve dvou fázích veřejné konzultace. První byla konzultace týkající se právního rámce pro základní právo na ochranu osobních údajů (9. července – 31. prosince 2009). Druhou byla konzultace týkající se komplexního přístupu Komise k ochraně osobních

[14] Viz čl. 2 písm. c) Úmluvy Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob s ohledem na automatizované zpracování osobních údajů.
[15] NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související (č. 101/2000 Sb.) – komentář.* Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-665-5. Str. 9.
[16] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 14.
[17] KOMÍNKOVÁ, M. *Jak vznikalo nařízení o ochraně osobních údajů (GDPR)?* Euroskop [online]. 2018. [cit. 2018-12-26]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/.
[18] Viz čl. 29 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[19] KOMÍNKOVÁ, M. *Jak vznikalo nařízení o ochraně osobních údajů (GDPR)?* Euroskop [online]. 2018. [cit. 2018-12-26]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/.

údajů v EU (4. listopadu 2010 – 15. ledna 2011). Mimo jiné také proběhla během listopadu a prosince roku 2010 konzultace s občany EU.

Většina zúčastněných stran souhlasila, ovšem s upozorněním na velmi rychlý technologický vývoj. Kritizována byla především nejednotnost a dále složitost pravidel, které se týkaly předávání osobních údajů do zahraničí.[20]

Návrh GDPR byl Komisí předložen 25. ledna roku 2012. V následujících čtyřech letech byl ještě několikrát projednáván v institucích EU.

Až 27. dubna roku 2016 bylo v Úředním věstníku EU uveřejněno 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). V tento den vzešlo v platnost s účinností od 25. května roku 2018, známé jako GDPR. Jedná se o významnou právní regulaci, která je velmi rozsáhlá a komplexní, a která se dotkla většiny občanů EU.[21]

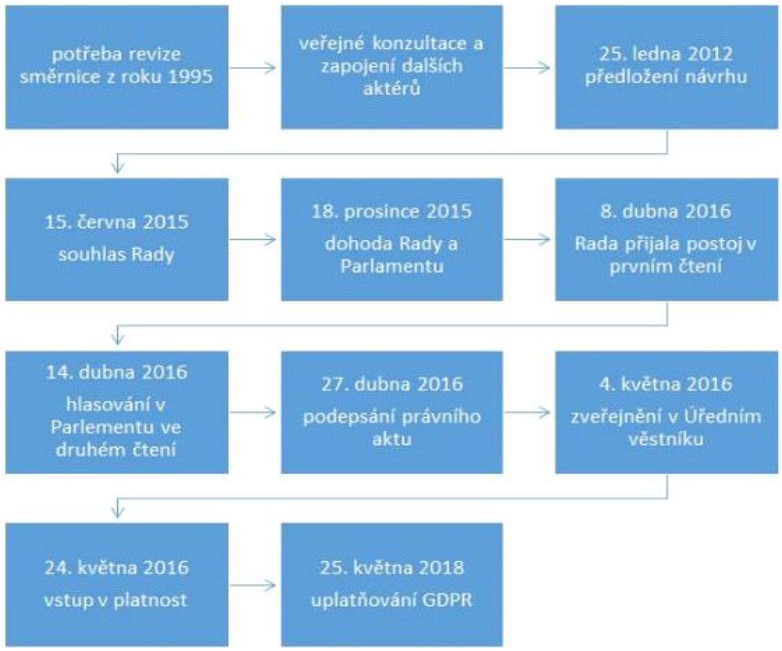
V závěru je nutno podotknout, že GDPR se sice snaží reagovat především na technologický pokrok, avšak vzhledem k tomu, jak dlouho trvala jednání, v dnešní době neuvěřitelně rychlého technického pokroku vyvstává otázka, zdali již dnes není tato úprava opět mírně zastaralá.

Schéma průběhu přijímání GDPR je zobrazeno na následujícím obrázku (Obr. č. 1).

[20] KOMÍNKOVÁ, M. *Jak vznikalo nařízení o ochraně osobních údajů (GDPR)?* Euroskop [online]. 2018. [cit. 2018-12-26]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/.

[21] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 19.

Obrázek č. 1 - Průběh přijímání GDPR



Zdroj: KOMÍNKOVÁ, M. *Jak vznikalo nařízení o ochraně osobních údajů (GDPR)?* Euroskop [online]. 2018. [cit. 2018-12-26]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/.

3.1.5.2 Návrh nového zákona v České republice

GDPR umožňuje, či v cca 50 ustanoveních dokonce ukládá, úpravu národními právními předpisy. Oproti GDPR tyto národní předpisy umožňují odchylnou či zpřesňující úpravu.[22]

V době zpracování této diplomové práce byl v České republice tento předpis připravován, konkrétně pak jde o zákon o zpracování osobních údajů. Nový zákon schválila vláda na návrh Ministerstva vnitra dne 21. března 2018.

Návrh zákona kromě jiného stanovuje výjimky z GDPR. Výjimky se týkají např. povinnosti zřízení funkce pověřence pro ochranu osobních údajů. Dle návrhu nebude muset být jmenován tam, kde by šlo pouze o formalitu, tedy např. v knihovnách.

[22] METODIKA MZ ČR A ÚZIS. *Jak implementovat nařízení evropského parlamentu a rady 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES do resortu zdravotnictví* [online]. (PDF). [cit. 2018-07-20]. Dostupné z: http://www.uzis.cz/system/files/u44/GDPR_20180102_metodika_implementace_ve_zdravotnictvi.pdf.

Dalším velkým tématem je zpracování dat mladistvých na internetu, a dále stanovení věkové hranice, pro kterou je nutný souhlas u dítěte se zpracováním jeho údajů. Dle GDPR je možné minimální hranici stanovit mezi 13 až 16 lety. V návrhu zákona je hranice stanovena na 15 let. Do té doby pak bude dítě, např. k využívání sociální sítě, vždy potřebovat souhlas svého zákonného zástupce.[23]

Otázkou také zůstávají sankce pro obce a kraje. Jejich výše nesmí být likvidační, proto byla hranice snížena na 15 000 Kč. Dne 12. 3. 2019 však Poslanecká sněmovna Parlamentu České republiky schválila návrh, ve kterém došlo k úplnému zrušení těchto sankcí.[24]

Po přijetí tohoto zákona dojde ke zrušení zákona č. 101/2000 Sb., o ochraně osobních údajů. Nový zákon také provede i trestněprávní směrnice, která bude upravovat zpracování osobních údajů justičními a policejními orgány.[25]

Závěrem lze říci, že pokud správce či zpracovatel ještě před účinností dodržoval zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v případě resortu zdravotnictví dále také zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), neměl by mít s implementací GDPR příliš velký problém.[26]

3.2 Vybrané pojmy GDPR

3.2.1 Osobní údaj

Osobním údajem se podle čl. 4 odst. 1 GDPR rozumí jakákoli „*informace o identifikované nebo identifikovatelné fyzické osobě.*“ [27] Takovou osobou je fyzická osoba, kterou je možné přímo či nepřímo identifikovat. Takovým identifikátorem může být

[23] Návrh nového zákona o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů.
[24] ČESKÁ TELEVIZE. *Obcím a krajům nebudou za porušení GDPR hrozit pokuty, rozhodli poslanci* [online]. [cit. 2019-03-18]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/2757596-zive-poslanci-maji-znovu-rozhodnout-o-zdaneni-nahrad-cirkvim-a-resit-mohou-i-faltynka.
[25] VITNEROVÁ, M. *Vláda schválila návrh zákona o zpracování osobních údajů* [online]. [cit. 2018-12-30]. Dostupné z: https://www.mvcr.cz/clanek/vlada-schvalila-navrh-zakona-o-zpracovani-osobnich-udaju.aspx.
[26] METODIKA MZ ČR A ÚZIS. *Jak implementovat nařízení evropského parlamentu a rady 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES do resortu zdravotnictví* [online]. (PDF). [cit. 2018-07-20]. Dostupné z: http://www.uzis.cz/system/files/u44/GDPR_20180102_metodika_implementace_ve_zdravotnictvi.pdf.
[27] Viz čl. 4 odst. 1 GDPR.

identifikační číslo, nebo jednoduše jméno a příjmení. Při porovnání se Směrnicí 95/46/ES[28] došlo k rozšíření definice tohoto pojmu o technické údaje, jako je IP adresa[29], cookies[30] nebo lokační údaje.

Zvláštní skupinou osobních údajů je tzv. zvláštní kategorie osobních údajů. Jedná se o citlivé osobní údaje, kde může být identifikátorem jeden zvláštní prvek, nebo i více zvláštních prvků fyzické, ekonomické, genetické či kulturní identity dané fyzické osoby.[31] Konkrétně tak do této kategorie můžeme zařadit údaje o rasovém či etnickém původu, sexuální orientaci, náboženství, údaje týkající se členství v odborech či biometrické údaje. Všechny tyto údaje řadíme do této kategorie na základě toho, že samy o sobě mohou subjekt údajů poškodit ve společnosti, v zaměstnání, případně mohou zapříčinit jeho diskriminaci. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů.[32]

3.2.2 Zpracování osobních údajů

Zpracováním je dle GDPR „*jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.*“ [33]

Oproti předešlé legislativě zde nedochází k žádným změnám. I přes takto konkrétní výčet je však někdy velmi složité určit, kdy se jedná o zpracování a kdy nikoli. Z toho důvodu dále existují vodítka skupiny WP 29, která by tyto sporné situace měla vyřešit.[34]

---

[28] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
[29] Pozn.: identifikátor síťového rozhraní v síti využívající IP protokol.
[30] Pozn.: soubor umožňující zaznamenání informací o návštěvě webové stránky.
[31] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 31 – 32.
[32] GDPR. *Citlivé osobní údaje.* [online]. [cit. 2018-11-13]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/.
[33] Viz čl. 4 odst. 2 GDPR.
[34] EUROPEAN COMMISSION. *Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti* [online]. [cit. 2018-11-15]. Dostupné z: http://ec.europa.eu/justice/data-protection/index_cs.htm.

3.2.3 Pověřenec pro ochranu osobních údajů

Při prokazování souladu s GDPR je velmi důležitou osobou tzv. DPO (anglicky Data Protection Officer), neboli pověřenec pro ochranu osobních údajů.

Jedním z jeho hlavních úkolů je monitorovat soulad zpracování osobních údajů s GDPR. Za nedodržování GDPR však pověřenec nenese osobní odpovědnost.[35]

Z GDPR pověřenci vzniká povinnost vykonávat alespoň následující úkoly:

1. poskytovat informace a poradenství správcům, zpracovatelům, ale také zaměstnancům, kteří zpracovávají osobní údaje,
2. monitorovat soulad s dalšími předpisy EU, případně s předpisy členských států, a dále také s koncepcemi správce či zpracovatele,
3. rozdělovat odpovědnosti, zvyšovat povědomí a odbornou přípravu pracovníků, kteří jsou zapojeni do operací se zpracováním osobních údajů,
4. na požádání poskytovat poradenství týkající se posouzení vlivu na ochranu osobních údajů a monitorovat jeho uplatňování,
5. spolupracovat s dozorovým úřadem a působit pro něj jako kontaktní místo.[36]

Jmenování pověřence je povinné pouze v některých případech. Tuto povinnost mají:

1. orgány veřejné moci a veřejné subjekty, pouze s výjimkou soudů. Jedná se např. o vysoké školy, kraje, obce či ministerstva.
2. Správci či zpracovatelé, jejichž hlavní činnost spočívá v pravidelném a systematickém monitorování subjektu údajů. Jedná se o takovou činnost, která je nezbytná pro dosažení cíle organizace. Příkladem může být nemocnice, kde je to poskytování zdravotní péče. Jelikož by bez zpracování osobních údajů pacientů nemohla tuto činnost řádně a účinně vykonávat, vzniká tak nemocnici povinnost pověřence jmenovat.
3. Správci či zpracovatelé, kteří rozsáhle zpracovávají zvláštní kategorie osobních údajů, nebo kteří rozsáhle zpracovávají osobní údaje, které se týkají trestních věcí a činů. Jaké zpracování je rozsáhlé, však v GDPR není konkrétně definováno. V rámci běžné činnosti nemocnice však může jít např. o zpracování osobních údajů o pacientech[37]

[35] GDPR. *DPO čili Pověřenec pro ochranu osobních údajů* [online]. [cit. 2018-08-30]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/.
[36] Viz čl. 39 odst. 1 GDPR.
[37] WP29. *Guidelines on Data Protection Officers ('DPOs')* [online]. (PDF) [cit. 2018-07-20]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=44100.

Ve všech těchto případech by měla být správci nebo zpracovateli nápomocna osoba, která má odborné znalosti v oblasti právních předpisů a také se orientuje v postupech týkajících se ochrany osobních údajů.[38]

Pověřencem může být jak fyzická osoba (např. zaměstnanec organizace nebo externě spolupracující osoba, která funkci vykonává na základě jiné než pracovní smlouvy), tak právnická osoba (např. advokátní kancelář). Pokud je však za pověřence zvolena právnická osoba, musí být jmenovitě určena také konkrétní fyzická osoba, která bude funkci pověřence fakticky vykonávat.[39]

Pokud je správce či zpracovatel veřejným subjektem nebo orgánem veřejné moci, případně jedná li se o skupinu podniků, je možné jmenování pouze jednoho pověřence pro několik takových orgánů či subjektů.[40]

Ať už je pověřencem zaměstnanec správce, či se jedná o externě poskytovanou službu, pověřenec musí plnit své povinnosti a úkoly nezávislým způsobem. Může mít v organizaci i jiné funkce, nikdy však nesmí dojít ke střetu zájmů.[41] Mezi ním a vedením organizace nesmí být žádná další osoba, především kvůli předávání informací, tzn., že pověřenec musí mít k vedení organizace přímý přístup.[42]

Některé organizace mohou dobrovolné jmenování považovat za dobrý krok, což je podporováno i dozorovými orgány. V případě, kdy organizace tuto možnost využije, je pak nutné se řídit platnou legislativou pro pověřence.[43]

3.2.4 Subjekt

Subjektem údajů je dle čl. 4 odst. 1 GDPR *„fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor.“* [44] Nikdy se nemůže jednat

[38] ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3. Str. 103.
[39] MVČR. *Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí* [online]. (PDF). [cit. 2018-07-19]. Dostupné z: https://www.mvcr.cz/odk2/soubor/metodicke-doporuceni-k-cinnosti-obci-k-organizacne-technickemu-zabezpeceni-funkce-poverence-pro-ochranu-osobnich-udaju-podle-obecneho-narizeni-o-ochrane-osobnich-udaju-v-podminkach-obci.aspx.
[40] METODIKA MZ ČR A ÚZIS. *Jak implementovat nařízení evropského parlamentu a rady 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES do resortu zdravotnictví* [online]. (PDF). [cit. 2018-07-20]. Dostupné z: http://www.uzis.cz/system/files/u44/GDPR_20180102_metodika_implementace_ve_zdravotnictvi.pdf.
[41] ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3. Str. 103.
[42] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 41.
[43] ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3. Str. 104.
[44] Viz čl. 4 odst. 1 GDPR.

o osobu právnickou a zároveň nejsou osobními údaji takové údaje, které se k právnické osobě vztahují. GDPR se také nevztahuje na osoby zemřelé.[45]

3.2.5 Správce

Správcem údajů může být jak fyzická, tak i právnická osoba, dále orgán veřejné moci, agentura, případně jiný subjekt určující *„účely a prostředky zpracování osobních údajů.“* [46] Zpracování správce provádí za účelem, který vyplývá z jeho činnosti nebo pro vlastně určené účely. Těmi může být např. oprávněný zájem, který ale nikdy nesmí převýšit zájem na ochraně lidských práv a svobod fyzických osob.[47]

Správce provádí shromažďování, zpracování a uchování osobních údajů. Odpovídá za jejich dostatečné zabezpečení, dále za dodržování povinností upravených GDPR a za dodržování zásad zpracování.[48]

3.2.6 Zpracovatel

Zpracovatelem je ten, kdo zpracovává osobní údaje pro správce. Může jím být opět *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt.“*[49] Zároveň platí, že zpracovatel může provádět pouze takové činnosti, ke kterým ho pověří správce, případně ty, které z dané činnosti vyplývají. Za tímto účelem musí správce se zpracovatelem uzavřít písemnou smlouvu o zpracování osobních údajů (Příloha č. 1), případně musí veškeré náležitosti zakomponovat do jiné (již platné) smlouvy. Zpracovatel také může na základě získaného souhlasu správce do zpracování osobních údajů zapojit dalšího zpracovatele. Poté jde o tzv. řetězení zpracovatelů.[50]

---

[45] GDPR. *Subjekt údajů* [online]. [cit. 2018-09-06]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/subjekt-udaju/.
[46] Viz čl. 4 odst. 7 GDPR.
[47] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 32.
[48] GDPR. *Správce osobních údajů* [online]. [cit. 2018-09-06]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/spravce-osobnich-udaju/.
[49] Viz čl. 4 odst. 8 GDPR.
[50] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 39 – 40.

3.2.7 Zabezpečení osobních údajů

3.2.7.1 Úvodem

Osobní údaje musí být adekvátním způsobem zabezpečeny. Je možné použít pseudonymizaci údajů, anonymizaci či šifrování. Je nutno podotknout, že mnohdy k takovému zabezpečení správce nemá technické prostředky. I tak je však nutná alespoň minimální úroveň zabezpečení.[51]

3.2.7.2 Pseudonymizace

Jedná se o proces, kdy jsou osobní údaje nahrazeny, případně rozděleny do více souborů a je k nim doplněn umělý identifikátor či pseudonym. K identifikování dané osoby je tak potřeba oddělený klíč, většinou se jedná o převodní tabulku. Osobní údaje v takovéto podobě jsou ideální pro analýzy a další zpracování.[52]

Tabulka č. 1 – Pseudonymizace – původní data

Jméno	Příjmení	Rodné číslo	Diagnóza
Jan	Novák	920423/2546	Hepatitida A
Marie	Novotná	845621/1245	Diabetes
Petr	Vomáčka	860425/2794	Cirhóza jater

Zdroj: vlastní zpracování

Tabulka č. 2 a č. 3 – Pseudonymizovaná data

ID	Jméno	Rodné číslo
1	Jan	920423/2546
2	Marie	845621/1245
3	Petr	860425/2794

Zdroj: vlastní zpracování

ID	Příjmení	Diagnóza
1	Novák	Hepatitida A
2	Novotná	Diabetes
3	Vomáčka	Cirhóza jater

Zdroj: vlastní zpracování

Na uvedeném příkladu je zřejmé, že původní data (Tab. č. 1) byla rozdělena do dvou oddělených souborů (Tab. č. 2 a č. 3) a byl k nim doplněn umělý identifikátor, sloupec ID.

[51] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 54.
[52] GDPR. *Anonymizace a pseudonymizace jsou dvě rozdílná slova* [online]. [cit. 2018-11-30]. Dostupné z: https://www.gdpr.cz/blog/anonymizace-a-pseudonymizace-jsou-dve-rozdilna-slova/.

Díky tomuto identifikátoru může uživatel vlastnící oba soubory jasně spojit konkrétní osobu s její diagnózou.

3.2.7.3 Anonymizace

Na rozdíl od pseudonymizace se jedná o nevratný proces, kdy již není možné osobu zpětně identifikovat, protože při tomto postupu dochází k trvalému odstranění identifikátorů dané osoby. Takováto data již nejsou osobními údaji, proto dále nepodléhají GDPR. To je pro správce osobních údajů velmi výhodné, jelikož může údaje zpracovávat bez jakéhokoli zabezpečení a ochrany.[53]

Tabulka č. 4 – Anonymizace – původní data

Jméno	Příjmení	Rodné číslo	Diagnóza
Jan	Novák	920423/2546	Hepatitida A
Marie	Novotná	845621/1245	Diabetes
Petr	Vomáčka	860425/2794	Cirhóza jater

Zdroj: vlastní zpracování

Tabulka č. 5 – Anonymizovaná data

Jméno	Příjmení	Rodné číslo	Diagnóza
XXX	YYY	920XXX/XXX	Hepatitida A
XXX	YYY	845XXX/XXX	Diabetes
XXX	YYY	860XXX/XXX	Cirhóza jater

Zdroj: vlastní zpracování

Tab. č. 4 obsahuje původní neanonymizovaná data. Z Tab. č. 5 je po anonymizaci zřejmé, že osobu nelze identifikovat, stále však zůstává část rodného čísla a diagnóza. Taková data jsou cenná např. pro výzkum, jelikož je možné určit počet osob trpící danou chorobou, jejich věk a pohlaví.

[53] PLATH, S. *Anonymisation and poedonymisation* [online]. (PDF). 2016. [cit. 2018-11-30]. Dostupné z: https://www.pwc.lu/en/general-data-protection/docs/pwc-anonymisation-and-pseudonymisation.pdf.

3.2.7.4 Šifrování

Jedná se o proces, kdy se za pomoci kryptografických postupů převádí nezabezpečená elektronická data na data šifrovaná. Data jsou následně čitelná pouze pomocí dešifrovacího klíče. Šifrování může být symetrické či asymetrické.

Symetrické šifrování funguje na principu hesla. Jedna osoba soubor pomocí hesla zašifruje a druhá osoba jím po doručení naopak daný soubor dešifruje. Jedná se o velice rychlou metodu, problémem je však bezpečné předávání hesla. Často jsou využívány komprimační programy typu WinRar, WINZIP apod.[54]

Asymetrické šifrování probíhá pomocí dvou klíčů – soukromého a veřejného, kdy soukromý zná pouze vlastník klíče a veřejný je dostupný komukoli. Zprávu zašifrovanou pomocí veřejného klíče je pak možné dešifrovat pouze pomocí soukromého klíče. Jedná se o pomalejší metodu, než je metoda systematického šifrování, odpadá zde však problém s předáváním hesla.[55]

3.2.8 Dozorová činnost

3.2.8.1 Úvodem

Na dodržování předpisů dohlíží příslušné dozorové orgány, a to jak vnitrostátní, tak na úrovni EU. To není žádnou novinkou, již ve Směrnici 95/46/ES[56] byla stanovena povinnost zřízení tzv. orgánu dozoru. V České republice se jedná konkrétně o Úřad pro ochranu osobních údajů, zkráceně ÚOOÚ. Co se týká evropské úpravy, již dříve byla zřízena pracovní skupina „*The Article 29 Data Protection Working Party“, [57]* známá pod zkratkou WP29. Jednalo se o poradní orgán Evropské komise, mezi jejíž členy patří také ÚOOÚ. Od účinnosti GDPR byla tato skupina nahrazena Evropským sborem pro ochranu osobních údajů.[58]

---

[54] BUKOVSKÝ, J. *Změny v legislativě – Zákon GDPR, změny v zákonu o kybernetické bezpečnosti a v nařízení eIDAS.* Školení Českého institutu interních auditorů. 2018-02-19.
[55] SOOM. *Symetrické a asymetrické šifrování* [online]. [cit. 2018-11-29]. Dostupné z: https://www.soom.cz/clanky/1126--Symetricke-a-asymetricke-sifrovani.
[56] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[57] Stanoviska WP29. *Article 29 working party archives 1997 - 2016*[online]. [cit. 2019-01-29]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/index_en.htm.
[58] EDPB. O Evropském sboru pro ochranu osobních údajů [online]. [cit. 2018-12-28]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb_cs.

3.2.8.2 Vnitrostátní dozorový úřad v ČR

V ČR je vnitrostátním dozorovým úřadem ÚOOÚ. Jedná se o nezávislý orgán se sídlem v Praze, který:

a) dohlíží na to, zda dochází k dodržování povinností vyplývajících ze zákona v souvislosti se zpracováním osobních údajů,
b) pokud dojde k porušení těchto povinností, tak ÚOOÚ přijímá stížnosti a podměty, případně uděluje pokuty,
c) má povinnost vést registr zpracování osobních údajů,
d) o své činnosti zpracovává výroční zprávu, kterou zpřístupňuje veřejnosti,
e) v případě potřeby poskytuje konzultace,
f) dohlíží na to, aby byly plněny veškeré požadavky, které České republice vyplývají z mezinárodních smluv,
g) spolupracuje i s dalšími úřady pro ochranu osobních údajů působících v jiných státech, dále také s orgány EU, vůči kterým má oznamovací povinnost.[59]

ÚOOÚ nyní hraje velice důležitou roli při porušení ochrany osobních údajů. Správce či zpracovatel má povinnost mu hlásit všechna porušení, při kterých může dojít k rizikům pro práva a svobodu fyzických osob. Ohlášení musí být provedeno bez zbytečného odkladu, ideálně pak do 72 hodin.[60] Zde bude vždy velice náročné rozhodnout, která porušení hlásit a která nikoli.

Co se týká kontrolní činnosti v České republice, je velice zajímavý vývoj počtu provedených kontrol. V případě roku 2018 v prvním pololetí proběhlo 53 kontrol, zatímco ve druhém pololetí pouze 33 kontrol. Je však nutno podotknout, že nynější kontroly jsou mnohem komplexnější. Oproti tomu velmi vzrostl počet stížností, což je pro ÚOOÚ výrazná administrativní zátěž.

Další zajímavostí je, že ve zmíněném druhém pololetí ÚOOÚ neudělil žádné pokuty. Je otázkou, jaký vliv má na tuto skutečnost absence adaptačního zákona, jelikož existují obavy, zdali má ÚOOÚ vůbec takové kompetence.[61]

---

[59] Viz § 29 Zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
[60] ÚOOÚ. *Porušení zabezpečení* [online]. [cit. 2019-3-14]. Dostupné z: https://www.uoou.cz/poruseni-zabezpeceni/ds-5020.
[61] PATTYNOVÁ, J. *Šest měsíců s GDPR: novinky a průběh kontrol dozorového orgánu.* Právní prostor [online]. [cit. 2019-3-12]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/sest-mesicu-s-gdpr-novinky-a-prubeh-kontrol-dozoroveho-organu.

Je otázkou, jak se nyní budou správci a zpracovatelé dále k ochraně osobních údajů stavět, když v praxi vidí, že nedochází k udělování pokut. Avšak lze se domnívat, že tento stav je pouze prozatímní.

3.2.8.3 Evropský sbor pro ochranu osobních údajů

Evropský sbor pro ochranu osobních údajů neboli EDPB (European Data Protection Board), je orgán EU, který má za úkol od 25. května 2018 uplatňování GDPR. Sbor tvoří vždy vedoucí každého úřadu pro ochranu osobních údajů dané země a evropský inspektor ochrany údajů. Může se jednat i o jejich zástupce. Schůzek Sboru se účastní také vnitrostátní orgány dohledu států Evropského sdružení volného obchodu/Evropského hospodářského prostoru, ovšem nemají hlasovací právo.[62]

Sbor má velice důležitý úkol, kterým je zajištění toho, aby se GDPR uplatňovalo v EU konzistentně, a aby mezi sebou jednotlivé úřady pro ochranu osobních údajů efektivně spolupracovaly. Dále vydává instrukce týkající se interpretace základních pojmů. Pokud dojde ke sporům v oblasti mezinárodního zpracování osobních údajů, tak bude jeho úkolem přijímat závazná rozhodnutí. Je totiž velmi důležité zajistit, aby bylo uplatňování pravidel v rámci EU jednotné a aby nedocházelo k případům, kdy by byl stejný případ řešen odlišně v různých jurisdikcích.[63]

3.2.9 Pokuty a sankce

Pokud dojde k porušení GDPR, hrozí nově subjektům osobních údajů velmi vysoké pokuty. Uložení pokuty však není pravidlem. Správce může být na porušení nejprve pouze upozorněn, může mu být uděleno napomenutí. Také mu může být nařízeno, aby zpracování osobních údajů uvedl do souladu s GDPR.[64]

Pokuty jsou rozděleny do dvou kategorií, a to dle závažnosti porušení. V první kategorii, kam spadá např. posouzení vlivu na ochranu osobních údajů či porušení

---

[62] EDPB. *O Evropském sboru pro ochranu osobních údajů* [online]. [cit. 2018-12-28]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb_cs.
[63] EVROPSKÁ KOMISE. *Co je to Evropský sbor pro ochranu osobních údajů (European Data Protection Board, EDPB)?* [online]. [cit. 2018-12-28]. Dostupné z:: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_cs.
[64] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 43.

ustanovení týkajících se záznamů o činnostech zpracování, maximální výše pokuty dosahuje 10 000 000 EUR nebo, jde-li o podnik, až do 2 % celkového ročního celosvětového obratu. V druhé kategorii, kam jsou zahrnuta např. porušení povinností upravujících podmínky zpracování zvláštních kategorií osobních údajů, dále také třeba porušení práv subjektu údajů, maximální výše pokuty dosahuje až 20 000 000 EUR nebo opět, jde-li o podnik, až do 4 % celkového ročního celosvětového obratu. Vždy záleží na tom, která z částek je vyšší.[65]

Výše pokuty se odvíjí od mnoha faktorů, kterými jsou např. závažnost a povaha porušení, doba, po kterou porušení trvalo, počet poškozených subjektů údajů a také celkový rozsah škody. V potaz však jsou brány také kroky, které správce či zpracovatel osobních údajů podnikl ke zmírnění následků vzniklých porušením GDPR. Na co ale zřetel brán není, je velikost společnosti, která se přestupku dopustí. Maximální výší pokuty tak může být postihnuta jak menší společnost s deseti zaměstnanci, tak ale i velká nadnárodní korporace.

Kromě finančních postihů mohou následovat také žaloby podané subjekty osobních údajů a s nimi spojené požadavky na náhradu škody, a to v případě jak hmotné, tak nehmotné újmy. Dalším nezanedbatelným následkem porušení GDPR je bezesporu ztráta důvěry a dobré pověsti společnosti.[66]

3.3 Zásady a principy GDPR

3.3.1 Úvodem

GDPR s sebou nese šest základních zásad, které říkají, jak ke zpracování osobních údajů přistupovat. Lze je chápat jako souhrn těch nejdůležitějších povinností, kterými je třeba se řídit.[67]

3.3.2 Zákonnost, korektnost a transparentnost

Jedná se o jednu z nejdůležitějších zásad celé ochrany osobních údajů, která říká, že osobní údaje musí správce zpracovávat na základě alespoň jednoho právního aktu. Dále vůči subjektu musí údaje zpracovávat korektně a transparentně.[68]

---

[65] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 44.
[66] GDPR. *Jaké sankce hrozí firmám, které budou GDPR ignorovat* [online]. [Cit. 2018-10-17]. Dostupné z: https://www.gdpr.cz/gdpr/sankce/.
[67] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 49.
[68] GDPRSAFE. *Zásady zpracování* [online]. [Cit. 2019-01-12]. Dostupné z: https://gdprsafe.cz/ukazka/priprava-na-gdpr/zasady-zpracovani/.

Právním aktem, na základě kterého může dojít ke zpracování, může být kromě zákonného důvodu i poskytnutý souhlas se zpracováním osobních údajů.

Korektností se rozumí, že správce osobní údaje zpracovává pouze k přiměřeným účelům. Pokud by chtěl správce získané osobní údaje využít i k jiným účelům, musí opět získat souhlas subjektu. Také se nesmí stát, že by správce v původním souhlasu uvedl např. pouze v poznámkách pod čarou, že subjekt souhlasí i s jiným zpracováním svých údajů. Subjekt by tak mohl s jiným využitím souhlasit nevědomky pouze díky nepozornosti.
Transparentností je myšleno, že správce subjektu poskytne veškeré údaje, které o něm zpracovává, a to v takové formě, aby podaným informacím subjekt rozuměl. Informování subjektu musí vždy proběhnout ještě před začátkem samotného zpracování osobních údajů. Nikdy nesmí dojít k situaci, kdy by správce zatajoval účel zpracování. Díky transparentnosti tak může mít subjekt veškeré zpracování pod kontrolou.[69]

Ve zkratce, aby tedy správce zásadu neporušil, musí dodržet následující:

a) co se týká jeho identity, musí být zcela otevřený a upřímný,
b) musí subjekt osobních údajů informovat o tom, jak je s jeho údaji nakládáno,
c) osobní údaje může zpracovávat pouze tak, jak může subjekt rozumně předpokládat,
d) zpracování osobních údajů musí probíhat tak, aby nemělo na subjekt neoprávněně žádný negativní vliv.[70]

3.3.3 Omezení účelem

Tato zásada jasně určuje, jak může správce osobní údaje využívat. Ke zpracování musí mít správce legitimní účel a nikdy nesmí osobní údaje zpracovávat takovým způsobem, který by byl s tímto legitimním účelem neslučitelný.[71] Jasné určení účelu je velice důležité i pro další zásady a principy GDPR. Kromě toho, že musí být legitimní, musí být také výslovný a určitý. Pokud by nebylo zcela jasné, k jakému zpracování osobních údajů bude docházet, nebylo by pak možné posoudit soulad s GDPR.[72]

---

[69] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 52 – 57.
[70] NULÍČEK, M. a kolektiv. *GDPR/Obecné nařízení o ochraně osobních údajů – praktický komentář.* Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0. Str. 109.
[71] GODDARD, M. *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact.* International Journal of Market Research [online]. [cit. 2018-03-15]. Dostupné z: https://journals.sagepub.com/doi/abs/10.2501/IJMR-2017-050. Str. 703.
[72] NULÍČEK, M. a kolektiv. *GDPR/Obecné nařízení o ochraně osobních údajů – praktický komentář.* Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0. Str. 110.

3.3.4 Minimalizace údajů

Dle třetí zásady nesmí správce zpracovávat žádné další osobní údaje než ty, které potřebuje pro legitimní účel, ke kterému údaje sbírá. V GDPR jsou v této souvislosti uvedeny pojmy, jako je přiměřenost, relevantnost či omezení na nezbytný rozsah. Dále už zde ale není vymezena specifikace těchto termínů. Obzvláště důležité je této zásadě věnovat pozornost, pokud se jedná o zpracování zvláštní kategorie osobních údajů (tzv. citlivých).

Existuje zde výjimka, která říká, že subjekt osobní údaje může zpracovávat i v případě, kdy je přímo nepotřebuje. Jedná se o zpracování pro předvídatelnou událost, ke které však ani nemusí dojít.[73]

3.3.5 Přesnost

Tato zásada říká, že údaje, které jsou správcem zpracovávány, musí vždy odpovídat skutečnosti. Nutno upozornit, že tímto není zaručena pravdivost údajů, jelikož subjekt může poskytnout nepřesné údaje. I když za tyto nepřesné informace správce neodpovídá, musí vždy přijmout takový systém opatření, aby zajistil, že ke zpracování nepřesných či chybných údajů nebude docházet. Tato kontrola však nemusí probíhat nepřetržitě.

Pokud nepřesnost odhalí subjekt údajů, je oprávněn podat žádost o opravu. Pokud je žádost důvodná, je správce povinen ji vyhovět.[74]

3.3.6 Omezení uložení

Zásada omezení uložení určuje, že je správce povinen osobní údaje uchovávat pouze po určenou dobu. Po uplynutí doby, kdy pomine účel, pro který byly údaje uchovávány, musí dojít ke smazání údajů, případně k jejich anonymizaci. Tato doba nikdy nesmí být zcela neurčitá.[75]

---

[73] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 62.
[74] ÚOOÚ. *K problematice aktualizace zpracovávaných osobních údajů* [online]. [cit. 2018-01-14]. Dostupné z: https://www.uoou.cz/k-problematice-aktualizace-zpracovavanych-osobnich-udaju/d-1595.
[75] NULÍČEK, M. a kolektiv. *GDPR/Obecné nařízení o ochraně osobních údajů – praktický komentář.* Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0. Str. 116 – 117.

3.3.7 Integrita a důvěrnost

Poslední zásadou je zásada integrity a důvěrnosti, týkající se ochrany a bezpečnosti dat. Správce tak musí osobní údaje zabezpečit před jejich ztrátou, neoprávněným zpracováním či poškozením.[76]

K zajištění souladu s touto zásadou musí správce jasně určit odpovědnou osobu za ochranu dat, musí mít odpovídající technické i fyzické zabezpečení a také musí být připraven případné porušení ochrany dat ihned řešit a mít pro tento případ nastaveny odpovídající procesy.[77]

3.4 Posouzení vlivu na ochranu osobních údajů

DPIA neboli Data Protection Impact Assessment, vychází z odpovědností správce, tedy z jednoho ze základních principů GDPR. Jedná se o tzv. posouzení vlivu na ochranu osobních údajů. Cílem DPIA je především identifikace a zhodnocení rizik plynoucích ze zpracování osobních údajů.[78] Výsledkem je dokumentace, která umožní správci přijetí potřebných opatření, díky kterým se zmírní rizika zpracování a prokáže se soulad s GDPR.[79]

DPIA je požadováno v případech, kdy bude mít zpracování osobních údajů vysoký dopad (riziko) na práva a svobodu daného subjektu údajů. Provést tuto analýzu je tedy nutné alespoň v případech, kdy se jedná o:

- *„systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob včetně profilování“,* [80]
- rozsáhlé zpracování citlivých osobních údajů,
- rozsáhlé systematické monitorování veřejných prostor.[81]

Mohou existovat operace, které v tomto výčtu nejsou uvedeny, jelikož se jedná pouze o demonstrativní seznam. Přesto u těchto operací může existovat vysoké riziko, z toho důvodu by se na ně také měla vztahovat povinnost posouzení provést. Proto by měl správce osobních údajů zvážit, zdali operace zpracování neobsahuje následujících devět faktorů.

---

[76] JANEČKOVÁ, E. GDPR – Praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. Str. 9.
[77] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 74.
[78] NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4. Str. 98.
[79] NULÍČEK, M. a kolektiv. *GDPR/Obecné nařízení o ochraně osobních údajů – praktický komentář.* Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0. Str. 341.
[80] Viz recitál 91 GDPR.
[81] Tamtéž.

1. Profilování a jiné hodnocení či bodování subjektu údajů včetně předpovídání – jedná se o předpovídání aspektů souvisejících např. se zdravotním stavem subjektu za účelem posouzení rizika nemoci či zdravotních rizik.
2. Automatizované rozhodování, které má právní či jiný obdobně významný účinek – jedná se např. o takové zpracování, které může vést k vyloučení či diskriminaci jednotlivce. Na zpracování, které nemá žádný dopad na subjekt, případně pouze minimální, se tento faktor nevztahuje.
3. Systematické monitorování subjektu údajů – kromě zpracování sloužícího k monitorování, pozorování či kontrole subjektu sem řadíme i systematické monitorování veřejných prostor. Jednotlivec často nemůže zabránit tomu, aby nebyl na veřejných místech subjektem tohoto zpracování.[82]
4. Zpracování citlivých údajů – samozřejmostí je zařazení zpracování osobních údajů dle čl. 9 a 10 GDPR,[83] dále sem patří ale také osobní údaje, které zvyšují dopad (riziko) na práva a svobodu fyzické osoby. Jedná se např. o elektronickou komunikaci, osobní deníky, údaje o poloze či platební kartě. Velmi aktuální problematikou je zpracování údajů z aplikací, které zaznamenávají údaje o denní a sportovní aktivitě subjektu.
5. Zpracování osobních údajů ve velkém rozsahu – v GDPR není konkrétně definováno, co se rozumí pod pojmem „rozsáhlé“. Nicméně existují doporučení, kterými by se správce měl řídit. Faktory pro určení, jestli je zpracování rozsáhlé, jsou počet dotčených subjektů, objem údajů a rozsah jejich zpracování, délka či trvání zpracování a zeměpisný rozsah zpracování.
6. Kombinování a slučování osobních údajů z datových souborů – v případě, kdy by docházelo ke zpracování údajů ze dvou nebo více operací takovým způsobem, že by zpracování přesahovalo přiměřené očekávání subjektu.
7. Zpracování osobních údajů týkajících se zvlášť zranitelných osob – jedná se o případy, kdy existuje nerovnováha mezi správcem a subjektem. Mezi zranitelné subjekty tak je možné zařadit např. děti, osoby se sníženou schopností rozpoznávání důsledků svého jednání, především pak z důvodu stáří či duševní choroby, dále zaměstnance nebo pacienty.

[82] WP 29. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* [online]. (PDF) [cit. 2018-07-20]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=44137.
[83] Pozn.: zvláštní kategorie osobních údajů a osobní údaje týkající se rozsudků v trestních věcech a trestných činů.

8. Inovativní užití či aplikace technologických nebo organizačních řešení – posouzení je důležité z toho důvodu, že důsledky zavedení nových technologií mohou být velmi nepředvídatelné. Jedná se především o zpracování biometrických údajů, kterými jsou otisk prstu či rozpoznávání na základě obličeje.
9. Bránění subjektům údajů v uplatňování jejich práv v používání některé služby či v uzavření smlouvy – pokud dojde k situaci, kdy na základě zpracování subjekt nemůže využívat některou ze služeb správce. Může se jednat o případ, kdy pojišťovna při uzavírání rizikového životního pojištění prověřuje klienta na základě aspektů týkajících se zdravotního stavu. Na základě toho s klientem pojištění uzavře či nikoli.

V momentě, kdy správce dojde k závěru, že operace splňuje dva a více z výše uvedených faktorů, měl by posouzení provést. Příkladem může být nemocnice, ve které dochází ke zpracování údajů o zdravotním stavu pacientů. Protože se jedná o citlivé údaje pacientů a pacienti jsou zároveň zranitelnými osobami, je nutné, aby správce osobních údajů (nemocnice) posouzení provedl.[84]

Mohou nastat případy, kdy povinnost provést DPIA není zcela zřejmá. I přesto je však doporučeno posouzení provést, jelikož se jedná o užitečný nástroj, který správcům může pomoci k zajištění souladu s právními předpisy týkajících se ochrany osobních údajů.

V případech, kdy si jsou operace podobné, a zpracování představuje podobné riziko, stačí pro více takových operací vypracování pouze jednoho DPIA. [85]

3.5 Specifika GDPR pro resort zdravotnictví

3.5.1 Zpracování osobních údajů

3.5.1.1 Úvodem

Kromě osobních údajů jsou ve zdravotnictví často zpracovávány i zvláštní kategorie osobních údajů, pro které GDPR stanoví přísnější podmínky. Dochází ke zpracovávání především údajů o zdravotním stavu, kam se řadí veškeré údaje týkající se jak tělesného, tak

[84] NULÍČEK, M. a kolektiv. *GDPR/Obecné nařízení o ochraně osobních údajů – praktický komentář.* Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0. Str. 342 – 343.
[85] WP 29. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* [online]. (PDF) [cit. 2018-07-20]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

duševního zdraví fyzické osoby. Dále genetické údaje, týkající se genetických znaků a údaje biometrické.[86]

Údaje mohou být získány přímo od subjektu osobních údajů, nebo mohou být získány od jiného zpracovatele. Jedná se o veškeré ostatní údaje, které byly získány jinak než od samotného subjektu. Mohou to být např. výsledky extramurální péče[87] nebo laboratorní výsledky.[88]

Existují dva hlavní důvody pro zpracování osobních údajů, zpracování na základě zákonné povinnosti a na základě udělení souhlasu subjektu údajů.

3.5.1.2 Zákonná povinnost

Zákonná povinnost je splněna, pokud je zpracování nezbytné pro účely pracovního či preventivního lékařství nebo k němu dochází a je nezbytné z důvodu zájmu veřejnosti nebo z důvodu v oblasti veřejného zdraví.[89] V takovém případě se povinnost zpracování osobních údajů uplatňuje nezávisle na udělení souhlasu subjektu údajů. Nutno podotknout, že ve zdravotnictví se jedná o většinu procesů, typickým příkladem je vedení zdravotnické dokumentace či osobních spisů[90]

3.5.1.3 Souhlas subjektu údajů

Osobní údaje mohou být zpracovávány na základě výslovného souhlasu subjektu údajů. Takové případy jsou vždy jasně specifikovány v daném souhlasu. Jeho poskytnutí je vždy dobrovolné a je kdykoli odvolatelné stejně snadným způsobem, jako jeho poskytnutí.[91] V některých případech může být udělení souhlasu podmínkou pro vykonání některé z činností, jako je např. zařazení subjektu údajů do výzkumu či klinické studie. Pokud byl

[86] GDPR SOLUTIONS. *GDPR ve zdravotnictví* [online]. [cit. 2018-12-10]. Dostupné z: https://www.gdprsolutions.cz/gdpr-ve-zdravotnictvi/.
[87] Pozn.: péče, která je poskytnuta jiným zdravotnickým zařízením.
[88] METODIKA MZ ČR A ÚZIS. *Jak implementovat nařízení evropského parlamentu a rady 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES do resortu zdravotnictví* [online]. (PDF). [cit. 2018-07-20]. Dostupné z: http://www.uzis.cz/system/files/u44/GDPR_20180102_metodika_implementace_ve_zdravotnictvi.pdf.
[89] GDPR SOLUTIONS. *GDPR ve zdravotnictví* [online]. [cit. 2018-12-10]. Dostupné z: https://www.gdprsolutions.cz/gdpr-ve-zdravotnictvi/.
[90] POLICAR, R. *GDPR a ochrana soukromí ve zdravotnictví*, prezentace ze dne 26. 4. 2018.
[91] JANEČKOVÁ, E. GDPR – Praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1. Str. 14.

souhlas poskytnut ještě před účinností GDPR, musí být s GDPR v naprostém souladu, jinak není platný.[92]

3.5.2 Nakládání se zdravotnickou dokumentací

Zdravotnická dokumentace je základním zdrojem osobních údajů, a především pak zvláštní kategorie osobních údajů, pacientů. Jedná se o zpracování na základě zákonné povinnosti, z toho důvodu není vyžadován souhlas subjektu. Ze stejného důvodu pacient nemůže poskytnutí či zpracování údajů odmítnout.

Dokumentace může být uchovávána jak v písemné, tak elektronické podobě, samozřejmostí je důkladné zabezpečení proti nepovolaným osobám.[93]

3.5.3 Zpracování údajů pro vědeckovýzkumné účely

V tomto případě není zpracování prováděno na základě zákonné povinnosti, z toho důvodu je vyžadován souhlas subjektu. Souhlas není vyžadován pouze v případech, kdy jsou již informace součástí zdravotnické dokumentace pacienta. Pro účely vědeckovýzkumné činnosti jsou data často anonymizována, v tomto případě souhlas také není vyžadován, jelikož se již nejedná o zpracování osobních údajů dle GDPR.

Stejně se postupuje, pokud jde o zpracování v rámci klinických studií. Také platí, že souhlas se zpracováním osobních údajů nikdy nesmí být součástí souhlasu k provedení klinické studie.

3.5.4 Archivace osobních údajů

Osobní údaje musí být uchovávány v souladu s legislativou a se zásadou minimalizace dat. V některým případech, především pokud jde o ochranu práv, oprávněných či ekonomických zájmů zdravotnického zařízení, může být lhůta pro uchovávání prodloužena.

---

[92] GDPR SOLUTIONS. *GDPR ve zdravotnictví* [online]. [cit. 2018-12-10]. Dostupné z: https://www.gdprsolutions.cz/gdpr-ve-zdravotnictvi/.

[93] OTEVŘEL, R. *Klinické hodnocení a ochrana osobních údajů* [online]. [cit. 2019-01-08]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/klinicke-hodnoceni-a-ochrana-osobnich-udaju-nove-upozorneni-sukl.

Osobní údaje, které jsou zpracovávány na základě poskytnutého souhlasu subjektu údajů, mohou být zpracovávány pouze po dobu, na kterou je souhlas poskytnut, případně do doby, kdy je souhlas subjektem údajů odvolán.[94]

Co se týká zdravotních služeb, jsou standartní doby uchování osobních údajů následující. Doba je vždy počítána od doby poslední návštěvy pacienta či vyřazení z péče. V případě úmrtí pacienta je doba v uvedených případech 10 let.

Tabulka č. 6 – Doba uchovávání osobních údajů

Zdravotní služby	Délka uchování
Registrující poskytovatel	10 let[95]
Ostatní ambulantní péče	5 let
Specializovaná ambulantní péče	50 let
Dispenzární péče	10 let
Lůžková péče	40 let
Následná a dlouhodobá lůžková péče	20 let

Zdroj: vlastní zpracování dle Přílohy č. 3 „Doby uchování zdravotnické dokumentace nebo jejích částí“ vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů.

3.6 Práva pacientů

3.6.1 Historický vývoj

Nejstarším kodexem, který upravuje vztah mezi pacientem a lékařem, je známá Hippokratova přísaha z pátého století před naším letopočtem. Dlouhá staletí se tento vztah vyvíjel, než se v nějaké podobě ustálil. Vše poté fungovalo na tzv. paternalistickém modelu.[96] Pacient se na svého lékaře obracel s plnou důvěrou a pouze lékař určoval léčbu. Dále také určoval, zda o zdravotním stavu bude pacienta informovat či nikoli.

[94] EVROPSKÁ KOMISE. *Jak dlouho mohou být osobní údaje uchovávány a je třeba je aktualizovat?* [online]. [cit. 2018-12-10]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_cs.
[95] Pozn.: 5 let v případně zubního lékaře či lékaře v oboru gynekologie a porodnictví.
[96] Pozn.: tzv. otcovský/rodičovský model, kdy se nemocný obrací na lékaře jako dítě na svého otce/rodiče.

Samozřejmostí bylo, že o stavu případně informoval i pacientovy nejbližší.[97] Je zajímavé sledovat, že i když od toho modelu, kdy se lékař zajímá především o samotnou nemoc, a ne o osobu pacienta, bylo dávno upuštěno, dodnes se s ním můžeme u některých lékařů setkat. Jedná se pak především o lékaře starší generace.[98]

K postupným změnám začalo docházet v poválečném období. Pro tyto změny existovalo mnoho důvodů, kdy mezi nejdůležitější patřila lidská práva a individuální svobody, které byly zakotveny ve Všeobecné deklaraci lidských práv a svobod OSN. Zde došlo k velikému posunu, jelikož pacient začal být stavěn na stejnou úroveň jako lékař. Dalším z důvodů bylo vzdělání obyvatelstva, rozvoj vědecké medicíny, ale také nová dilemata. Jelikož došlo k rozvoji medicíny, začala také nabízet nové léčebné postupy a jejich kombinace. Protože každý z postupů má své výhody i nevýhody, pacient by s nimi měl být seznámen. Pacientův názor by poté měl lékař brát v zřetel.[99]

Postavení pacienta a lékaře bylo zakotveno v několika deklaracích, za zmínku stojí Ženevská deklarace Světové lékařské asociace z roku 1948, která obsahovala slib, který říkal, že lékař vždy bude stát *„na straně humanitárních cílů medicíny.“* [100] Další např. Lisabonská deklarace o právech pacientů z roku 1981, která se dotýkala práv nemocných. Práva pacientů zde byla zakotvena velice obecně, mezi nejdůležitější lze zařadit právo očekávat mlčenlivost ošetřujícího lékaře nebo právo odmítnutí léčby.[101]

V České republice došlo k výraznému kroku v roce 1992, kdy byla jako součást ústavního pořádku vyhlášena Listina základních práv a svobod, dále také Úmluva o ochraně lidských práv a svobod[102], která byla sjednána v Římě již roku 1950.

Důležitým milníkem se stal rok 1966 díky zákonu č. 20/1966 Sb., o péči o zdraví lidu. Zákon obsahoval např. povinnost lékaře informovat pacienta (př. rodinného příslušníka) o povaze jeho onemocnění, a to vhodným způsobem. Dále obsahoval právo pacienta nahlížet do své zdravotnické dokumentace a pořizovat si z ní výpisy. Tento zákon

---

[97] TĚŠINOVÁ, J., ŽĎÁREK, R., POLICAR, R. *Medicínské právo*. Praha: C. H. Beck, 2011. ISBN 978-80-7400-050-8. Str. 5.
[98] PTÁČEK, R., BARTŮNĚK, P. a kolektiv. *Etika a komunikace v medicíně.* Praha: Grada Publishing, a.s. Publishing, a.s., 2011. ISBN 978-80-247-3976-2. Str. 193.
[99] HAŠKOVCOVÁ, H. *Práva pacientů – komentované vydání.* Havířov: Nakladatelství Aleny Krtilové, 1996. ISBN 80-902163-0-7. Str. 12-15.
[100] MASARIKOVA UNIVERZITA. *Významné mezinárodní dokumenty k etice výzkumu* [online]. [cit. 2018-12-29]. Dostupné z: https://vyzkum.rect.muni.cz/cs/zazemi/etika-vyzkumu/etika-vyzkumu/mezinarodni-dokumenty-k-etice-vyzkumu.
[101] Lisabonská deklarace o právech pacientů, 1981
[102] Sdělení č. 209/1992 Sb. Sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

byl mnohokrát novelizován, výsledkem bylo jeho úplné zrušení a nahrazení zákonem č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), který je platný do dnešního dne.[103]

Další významný posun přinesla Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny: Úmluva o lidských právech a biomedicíně. Jedná se o mezinárodní smlouvou, která byla přijata členskými státy Rady Evropy ve španělském Oviedu dne 4. dubna 1997. V České republice došlo k ratifikaci v červnu roku 2001. Jejím hlavním posláním byla ochrana lidských práv a důstojnosti lidské bytosti. Tato smlouva zaručovala práva všem lidem bez rozdílu státního občanství, finančních možností apod. [104]

Co se týká vývoje práv pacientů, je určitě důležité zmínit etické kodexy, které však neřadíme mezi všeobecně závazné právní předpisy.[105] Jedním z nejdůležitějších je Etický kodex Práva pacientů[106] centrální etické komise Ministerstva Zdravotnictví České republiky z roku 1992, který je dodnes platný (Příloha č. 2). Jako další je možné jmenovat Etický kodex České lékařské komory z roku 1996[107].

Ve 21. století stojí za zmínku program Světové zdravotnické organizace "Zdraví pro všechny ", který také vnímání práv pacientu významně ovlivnil.

3.6.2 Jednotlivá práva pacientů

Jednotlivá práva jsou uvedena především v zákoně č. 372/2011 Sb., o zdravotních službách. Konkrétně se jedná o část čtvrtou „*Postavení pacienta a jiných osob v souvislosti s poskytováním zdravotních služeb“*, Hlavu I „*Práva a povinnosti pacienta a jiných osob“*.[108] Dále jsou zakotvena v GDPR v Kapitole III „*Práva subjektu údajů“[109]*. Jedná se o níže uvedená práva:

---

[103] Zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů
[104] TĚŠINOVÁ, J., ŽĎÁREK, R., POLICAR, R. Medicínské právo. Praha: C. H. Beck, 2011. ISBN 978-80-7400-050-8. 1. Str. 115.
[105] KRAJSKÝ ÚŘAD – JIHOČESKÝ KRAJ. *Práva pacientů* [online]. (PDF). [cit. 2018-12-30]. Dostupné z: https://www.kraj-jihocesky.cz/file.php?par[id_r]=140391&par[view]=0.
[106] MPSV ČR. *Etický kodex Práva pacientů*. [online]. [cit. 2018-12-30]. Dostupné z:https://www.mpsv.cz/cs/840.
[107] ČESKÁ LÉKAŘSKÁ KOMORA. *Etický kodex České lékařské komory* [online]. (PDF). [cit. 2018-12-30]. Dostupné z: https://www.lkcr.cz/doc/cms_library/10_sp_c_10_eticky_kodex-100217.pdf
[108] Viz část čtvrtá zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.
[109] Viz kapitola tři GDPR.

Právo na zdravotní péči

Každý člověk má právo na zdravotní péči, které je zaručeno dokonce ústavou.[110] Má právo na takovou péči, která je poskytována na náležité odborné úrovni. Odbornou úrovní se rozumí dle § 4 odst. 5 *„poskytování zdravotních služeb podle pravidel vědy a uznávaných medicínských postupů, při respektování individuality pacienta, s ohledem na konkrétní podmínky a objektivní možnosti.“* [111]

Právo na informovaný souhlas

Souhlasem se dle čl. 4 odst. 11 GDPR rozumí *„jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.“* [112] Osoba tedy nikdy nemůže být k souhlasu nucena. To, že je souhlas výslovný, znamená, že není možné na formuláři předem zaškrtnout políčko udělující souhlas, případně za souhlas považovat mlčení.

Existují samozřejmě i výjimky, které jsou výslovně uvedené v zákoně. Lékařská péče pak může být poskytnuta i bez souhlasu. Jedná se např. o případy, kdy se jedná o osobu, která je nositelem závažné přenosné nemoci, je jí nařízeno povinné léčení, případně pokud se jedná o osobu, od které není možné získat souhlas vzhledem jejímu zdravotnímu stavu, a přitom se jedná o neodkladný výkon kvůli záchraně zdraví nebo života.[113]

Každý pacient má v této souvislosti právo na informace týkající se daného léčebného postupu či výkonu, jelikož bez těchto informací by se nemohl rozhodnout, zda daný souhlas chce či nechce poskytnout. Důležité je také dané osobě sdělit i případná rizika související s výkonem, případně jiné alternativy léčby.[114]

Právo na odmítnutí zdravotního výkonu

Po tom, co je osoba opakovaně náležitě informována, a nejedná se o poskytnutí zdravotní péče bez souhlasu, má právo potřebný zdravotní výkon odmítnout. V takovém

[110] MZ ČR. *Práva pacienta* [online]. [cit. 2018-12-20]. Dostupné z: http://www.mzcr.cz/kvalitaabezpeci/obsah/prava-pacienta_2401_18.html.
[111] Viz § 4 odst. 5 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.
[112] Viz čl. 4 odst. 11 GDPR.
[113] Viz § 38 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.
[114] MZ ČR. Práva pacienta [online]. [cit. 2018-12-20]. Dostupné z: http://www.mzcr.cz/kvalitaabezpeci/obsah/prava-pacienta_2401_18.html.

případě je však nutné písemné prohlášení dané osoby, tzv. písemný reverz, spolu s jejím podpisem.[115]

Právo na informace

Každý má právo na to znát, jaké informace jsou o jeho osobě shromažďovány. Informace může poskytnout zdravotnický pracovník, případně má každý pacient právo na nahlížení do své zdravotnické dokumentace, pořizování si jejich výpisů, opisů či kopií. V takovém případě je však vždy nutné podat žádost u daného zdravotnického zařízení.[116]

Zde se zákon částečně dostává do kolize s GDPR, jelikož dle GDPR musí být pořízení kopie subjektu údajů poskytnuta bezúplatně. Dle zákona č. 372/2011 Sb., o zdravotních službách má však zdravotnické zařízení právo na náhradu nákladů, které byly vynaloženy na pořízení kopie.[117]

Právo nebýt informován

Stejně jako má každý právo na to být informován, má i právo na to nebýt informován. Každý se poučení o zákroku může zcela vzdát nebo k jeho přijetí může určit jinou osobu. Touto osobou může být buď osoba blízká, nebo kterákoliv jiná osoba, kterou si pacient určí. Může se však stát, že je osoba informována i proti své vůli. Nastane tak v případě, kdy je to v jejím zájmu, či v zájmu ochrany některých jiných osob, např. pak pokud se jedná o osobu mající infekční onemocnění. [118]

Právo na ochranu soukromí

Vždy je pouze na konkrétní osobě, zdali si přeje, aby o jejím zdravotním stavu byl informován i někdo jiný. Takovou osobu či osoby, které mohou být informovány, musí pacient uvést v informovaném souhlasu. Lze i uvést a případně omezit, v jakém rozsahu má být která osoba informována. Také lze uvést osoby, kterým se informace podávat nesmějí. Samozřejmostí je možnost tento souhlas kdykoli změnit či úplně odvolat.[119]

Může nastat i situace, kdy se pacient nachází ve zdravotním stavu, kdy osobu, popř. osoby, nemůže určit. V takovém případě pak mohou být o jeho zdravotním stavu

[115] Viz § 34 Odst. 3 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.
[116] Tamtéž viz §§ 65 – 69.
[117] BUREŠOVÁ, R. a kolektiv. *Jak se připravit na GDPR v 5 krocích – ve zdravotnictví.* Verlag Dashöfer, nakladatelství, s.r.o., 2018. Str. 72.
[118] MZ ČR. *Práva pacienta* [online]. [cit. 2018-12-20]. Dostupné z: http://www.mzcr.cz/kvalitaabezpeci/obsah/prava-pacienta_2401_18.html.
[119] Viz § 34 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.

informovány pouze osoby blízké. Pokud však pacient osoby blízké vyloučil v informovaném souhlasu, pak je možné je informovat pouze když je to v zájmu ochrany jejich zdraví příp. v zájmu ochrany zdraví dalších osob.[120]

Stejně se postupuje, pokud jde o informování pacientových pozůstalých. Informace o smrti, příčině úmrtí, případně o výsledcích pitvy mají vždy osoby blízké, pokud pacient za svého života neurčil jinak. V případě vyloučení osob blízkých v informovaném souhlasu platí stejná pravidla jako v předchozím případě.

Veškeré osoby, které mají právo na informace o pacientově zdravotním stavu, mají také právo nahlížet do jeho zdravotní dokumentace a pořizovat z ní výpisy, pokud pacient neurčil jinak.[121]

Právo na volbu lékaře a zdravotní pojišťovny

Toto právo není vždy zaručeno a existují zde zákonné výjimky. Poskytovatel zdravotních služeb může pacienta odmítnout v případě, kdy by „*přijetím pacienta bylo překročeno únosné pracovní zatížení nebo jeho přijetí brání provozní důvody, personální zabezpečení nebo technické a věcné vybavení zdravotnického zařízení.*“ [122]

Dalším důvodem pro odmítnutí pacienta může být velká vzdálenost místa trvalého bydliště od zdravotnického zařízení pro výkon návštěvní služby. V neposlední řadě se také jedná o případ, kdy je pacient pojištěn u pojišťovny, která nemá s daným poskytovatelem zdravotnických služeb uzavřenu smlouvu dle zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů.[123]

Pokaždé však, kdy se odmítnutý pacient cítí poškozen, musí lékař či zdravotnické zařízení pacientovi vydat písemnou zprávu, ve které uvede důvody pro odmítnutí. Dalším krokem je, že se pacient s písemnou zprávou obrátí na svou zdravotní pojišťovnu, případně na zřizovatele zdravotnického zařízení. [124]

Nesmí se tak nikdy stát v akutních případech, ve kterých by hrozila újma na pacientově zdraví nebo životě.

---

[120] Tamtéž viz § 33 Odst. 3.
[121] MZ ČR. *Práva pacienta* [online]. [cit. 2018-12-20]. Dostupné z: http://www.mzcr.cz/kvalitaabezpeci/obsah/prava-pacienta_2401_18.html.
[122] Viz § 48 Odst. 1 a 5 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.
[123] Tamtéž
[124] Tamtéž

Kromě svobodné volby lékaře má také každá osoba právo na výběr zdravotní pojišťovny. Lze ji měnit jednou za 12 měsíců, vždy pouze k 1. dni kalendářního pololetí. Toto neplatí při narození dítěte. Novorozenec je dnem narození vždy pojištěncem zdravotní pojišťovny, kde je pojištěna jeho matka.[125]

3.6.3 Nová práva v souvislosti s GDPR

3.6.3.1 Právo na výmaz

Někdy se můžeme setkat také s označením „právo být zapomenut“. Každý má právo požádat správce, aby jeho osobní údaje smazal a nadále je neuchovával.

Smazání údajů je provedeno na základě žádosti subjektu a při splnění některé z podmínek, kdy:

a) správce osobních údajů již shromážděné údaje nepotřebuje pro účely, pro které byly původně shromážděny případně jinak zpracovány,
b) správce osobní údaje zpracovává na základě souhlasu, který subjekt osobních údajů odvolal, a také pokud dnes již pro zpracování nemá žádný právní důvod,
c) subjekt údajů proti zpracování vznese námitku a správce nemá oprávněné důvody pro zpracování, jež by byly převažující,
d) správce osobní údaje zpracovává protiprávně,
e) se na správce vztahuje právní povinnost (stanovena v právu EU nebo členského státu), kdy musí osobní údaje vymazat,
f) se jedná o osobní údaje, které správce shromáždil v rámci nabídky služeb některé z informačních společností.[126]

Je však nutné zmínit, že většinou by měl správce vymazat údaje sám od sebe, tedy bez nutnosti žádosti samotného subjektu osobních údajů.

Existují však i výjimky, kdy osobní údaje není možné vymazat, nejedná se tedy o právo absolutní. U každé žádosti bude na správci, aby posoudil, zdali se na uchovávání osobních údajů nevztahuje některá z výjimek.[127] Jedná se o výjimky, kdy je zpracování nezbytné:

---

[125] Viz § 11a zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů.
[126] Viz čl. 17 odst. 1 GDPR.
[127] NULÍČEK, M. a kolektiv. *GDPR/Obecné nařízení o ochraně osobních údajů – praktický komentář.* Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0. Str. 230.

a) *„pro výkon práva na svobodu projevu a informace“* [128] – s touto výjimkou se tak lze setkat např. v žurnalistice, jelikož se jedná o svobodu projevu, případně u veřejných rejstříků, kde se jedná o právo na informace,
b) pokud se na správce vztahuje právní povinnost podle práva EU či členského státu, nebo pokud správce uchovává osobní údaje kvůli splnění úkolu, který je proveden v zájmu veřejnosti, ke kterému je správce pověřen, anebo při vykonávání veřejné moci,[129]
c) „z důvodů veřejného zájmu v oblasti veřejného zdraví,
d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely,
e) pro určení, výkon nebo obhajobu právních nároků.“ [130]

Zde je důležité zdůraznit, že je vždy nutné daný případ posoudit, aby byl v souladu se zásadou minimalizace údajů.

3.6.3.2 Právo na přenositelnost údajů

Subjekt údajů má právo na získání osobních údajů od správce ve strukturované, strojově čitelné a běžně používané podobě a má právo na předání takovýchto údajů jinému správci.[131] Hlavním cílem je, aby měli jednotlivé subjekty nad svými osobními údaji kontrolu. Při žádosti na přenos údajů se musí brát zřetel na to, zdali je přímý přenos od jednoho správce ke druhému technicky proveditelný. Obecně však původní správce údajů přednosu nikdy nesmí bránit. Je nutné upozornit, že se toto právo vztahuje pouze na údaje, které jsou zpracovávány automatizovaně.

Pokud subjekt požádá o uplatnění tohoto práva, nemá jeho žádost vliv na žádná další práva. Subjekt může v takovém případě využívat veškeré služby, které mu do doby podání žádosti poskytoval správce jeho údajů. V žádném případě nedojde žádostí o přenositelnost automaticky k výmazu dat, tedy k uplatnění práva na výmaz a nemá vliv ani na lhůty týkající se doby uchovávání údajů. [132]

Existují dvě podmínky, které musí být splněny, aby mohlo být právo na přenositelnost uplatněno. První podmínkou je, že se osobní údaje musí týkat subjektu údajů.

---

[128] Viz čl. 17 odst. 3GDPR.
[129] NULÍČEK, M. a kolektiv. *GDPR/Obecné nařízení o ochraně osobních údajů – praktický komentář.* Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0. Str. 232.
[130] Viz čl. 17 odst. 3 GDPR.
[131] Viz čl. 20, odst. 1 GDPR.
[132] WP 29. Guidelines on the right to data portability [online]. (PDF) [cit. 2018-07-24]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

Druhou, že se musí jednat o údaje, které poskytl sám subjekt údajů. Ten je může poskytnout buď vědomě (emailová adresa) nebo se jedná o data poskytnuta na základě využívání nějaké služby (historie vyhledávání, údaje o pohybu a lokaci).

Toto právo však nelze uplatnit ve všech případech. Pokud ke zpracování nedochází na základě souhlasu či na základě smlouvy, správce žádosti na přenositelnost nemusí vyhovět. Také žádosti nevyhoví, pokud se sice jedná o data poskytnutá subjektem, ale jedná se o data dovozená. Jedná se např. o přidělení skóre samotným správcem na základě zdravotního dotazníku.[133] Zároveň platí, že vyhovění žádosti nesmí mít negativní dopad na práva nebo také svobody jakýchkoli jiných osob.[134]

3.6.3.3 Právo vznést námitku

Jedná se o vznesení námitky proti zpracování osobních údajů. Může ji vznést subjekt, pokud je zpracování nezbytné *„pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce“* nebo *“pro účely oprávněných zájmů příslušného správce či třetí strany.“* [135]

K dalšímu zpracování by správce musel doložit oprávněný důvod k zpracování, který by převážil zájmy, práva a svobody subjektu.

Tuto námitku je možné vznést proti zpracování údajů, které jsou zpracovávány za účelem přímého marketingu nebo také profilování.[136] Subjekt údajů na toto právo musí být jasně upozorněn, a to nejpozději při první komunikaci. Upozornění musí být zřetelné a oddělené od všech ostatních informací.[137]

3.6.4 Další práva v souvislosti s GDPR

GDPR upravuje i další práva subjektu údajů, kterými jsou právo:

1) na transparentní, srozumitelné a snadno dostupné informace o osobních údajích subjektu, ať už byly získány se souhlasem či bez souhlasu. Informace může mít více podob, může být elektronická nebo písemná a na vyžádání subjektu i ústní. V případě,

[133] Tamtéž str. 9.
[134] Viz recitál 68 a článek 20, odst. 3 a 4 GDPR
[135] Viz čl. 6 odst. 1 e) a f) GDPR
[136] ÚOOU. *Základní příručka k GDPR* [online]. [cit. 2018-01-07]. Dostupné z https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744. Kapitola 6.
[137] GUARD7. *Právo vznést námitku* [online]. [cit. 2018-01-07]. Dostupné z: http://www.guard7.cz/gdpr/pravo-vznest-namitku.

kdy jsou informace získány od subjektu, informace musí být podána v okamžiku, kdy správce údaje získá. V opačném případě je toto právo omezené,

2) na přístup k osobním údajům, kdy na žádost subjektu mu musí správce sdělit, jaké údaje o něm zpracovává, př. mu je předat v plném rozsahu,
3) na opravu,
4) na omezení zpracování,
5) nebýt předmětem automatizovaného rozhodování, kam řadíme také profilování,
6) na podání stížnosti, která je podána dozorovému úřadu,
7) na účinnou soudní ochranu,
8) na zastoupení neziskovým subjektem,
9) na náhradu újmy, kdy se může jednat o újmu hmotnou i nehmotnou.[138]

3.7 Shrnutí

Právní úprava (3.1 Obecně k právní úpravě) ochrany osobních údajů není ničím novým, avšak nově ji doplňuje právě GDPR. Obzvláště před rokem bylo velkým tématem. Zavedlo nové pojmy, povinnosti i práva. Zřejmě většinu správců zaujala především hrozba až milionových pokut.

Co se týká nových pojmů (3.2 Vybrané pojmy), nejvýraznějším je určitě DPO neboli pověřenec pro ochranu osobních údajů. Zajímavé je, že ne všechny pojmy jsou definovány zcela přesně. Např. doba nezbytně nutná. Nikde není uvedeno, jak dlouhá tato doba je. Dalo by se říci, že její stanovení zůstává na vlastním uvážení, což je ale v pořádku, jelikož pro každý druh zpracování osobních údajů je nutné ji stanovit individuálně.

Pokud by někdo v GDPR hledal přesný návod, jak k ochraně osobních údajů přistupovat, hledal by marně. Avšak je v něm uvedeno šest základních zásad a principů (3.3 Zásady a principy GDPR), kterými je třeba se řídit, aby došlo k souladu. Jak bude správce či zpracovatel postupovat, to už je zcela na něm.

Z odpovědnosti správce, tedy z jednoho ze základních principů GDPR, vychází povinnost provést DPIA neboli posouzení vlivu na ochranu osobních údajů (3.4 Posouzení vlivu na ochranu osobních údajů). Výsledkem je dokumentace, která umožní správci přijetí potřebných opatření, díky kterým se zmírní rizika zpracování osobních údajů a prokáže se

[138] Viz čl. 12–22 a 77–82 GDPR.

soulad s GDPR. Vzhledem k tomu, že se jedná o velmi užitečný nástroj, dalo by se provedení DPIA doporučit i v těch případech, kdy provedení není povinné.

Ve zdravotnictví (3.5 Specifika GDPR pro resort zdravotnictví) dochází také často ke zpracování zvláštní kategorie osobních údajů neboli citlivých osobních údajů, pro jejichž zpracování platí přísnější podmínky. Ani zde však GDPR nestanovuje přesný návod, určuje jen konečný výsledek, jak mají být údaje chráněny.

Kromě rozšíření stávajících práv (3. 6 Práva pacientů) s sebou GDPR přineslo i tři nová práva, kterými jsou právo na výmaz, právo na přenositelnost údajů a právo vznést námitku. Každý ze správců či zpracovatelů se musel připravit na to, že je budou chtít lidé prostřednictvím žádostí uplatňovat.

Celkově lze říci, že hlavní změnou oproti předešlému stavu je, že se o ochraně osobních údajů začalo konečně mluvit. Správci a zpracovatelé, kteří na ochranu osobních údajů dbali již dříve, s implementací neměli takové potíže. Naopak ti, kteří se této problematice nevěnovali, se pod hrozbou vysokých pokut začali zpracováním a nakládáním s osobními údaji zabývat.

4 Vlastní práce

4.1 Vybrané zdravotnické zařízení

4.1.1 Charakteristika zdravotnického zařízení

Analýza implementace GDPR je založena na případové studii ve vybraném zdravotnickém zařízení. Pro toto nejmenované zařízení bude v následující části diplomové práce používán výraz „Nemocnice“.

Jedná se o státní příspěvkovou organizaci, zřízenou na základě zřizovací listiny, která je v přímé řídící působnosti Ministerstva zdravotnictví České republiky.

Jedná se o poskytovatele základní, specializované a zvlášť specializované léčebné, ošetřovatelské, ambulantní a diagnostické péče, a to jak pro děti, tak dospělé. Dále Nemocnice zajišťuje komplexní lékárenskou péči, včetně distribuce léčiv, přípravy cytostatik a sterilních léčivých přípravků, diagnostik, zdravotnických prostředků a rehabilitačních pomůcek.

Další z hlavních činností je vědeckovýzkumná činnost, provádí základní a klinický výzkum. Působí i jako vzdělávací zařízení, umožňuje tedy odborné praktické vyučování žáků středních i vyšších škol a provádí kvalifikační kurzy k získání způsobilosti k výkonu povolání nižších a pomocných zdravotnických pracovníků.

Jedná se o jedno z největších zdravotnických zařízení v České republice. Nemocnici tvoří přes 40 zdravotnických pracovišť, mezi kterými jsou kliniky, ústavy a samostatná oddělení.[139]

4.1.2 Organizační struktura

Organizační strukturu nemocnice definuje Organizační řád. Vymezuje jak strukturu, tak působnosti, odpovědnosti, pravomoci a základní pravidla řízení nemocnice.

Činnost nemocnice řídí ředitel, který je jmenován ministrem zdravotnictví. Jedná se o statutární orgán. Nejvyšším orgánem řízení Nemocnice je Vedení.

Celá Nemocnice je tvořena jedním organizačně jednotným celkem, který je dále členěn. Základ tvoří jednotlivé úseky, v jejichž čele stojí náměstek ředitele. Úseky mohou být dále členěny na odbory případně jednotlivá oddělení. V případě zdravotnické části je

[139] Pozn.: Údaje získané z výroční zprávy Nemocnice.

základem zdravotnické pracoviště, kterým je nejčastěji klinika, dále ústav či oddělení. V případě kliniky či ústavu je vedoucím přednosta, v případě samostatného oddělení primář.

Všichni vedoucí zaměstnanci organizačních jednotek mohou svou funkci vykonávat na základě jmenování.

4.2 Proces implementace GDPR

4.2.1 Úvodem

Cílem implementace bylo, aby veškeré zpracování osobních údajů v Nemocnici probíhalo v souladu s GDPR. Bylo rozděleno do čtyř etap.

V první řadě byly provedeny různé analýzy, bylo provedeno mapování osobních údajů, na základě kterého byly určeny dopady zpracování.

Po seznámení se s požadavky a povinnostmi vyplývajícími z GDPR, které jsou analyzovány v teoretické části práce, byly navrženy jednotlivé kroky, které povedou k naplnění pravidel GDPR, spolu se stanovením priorit.

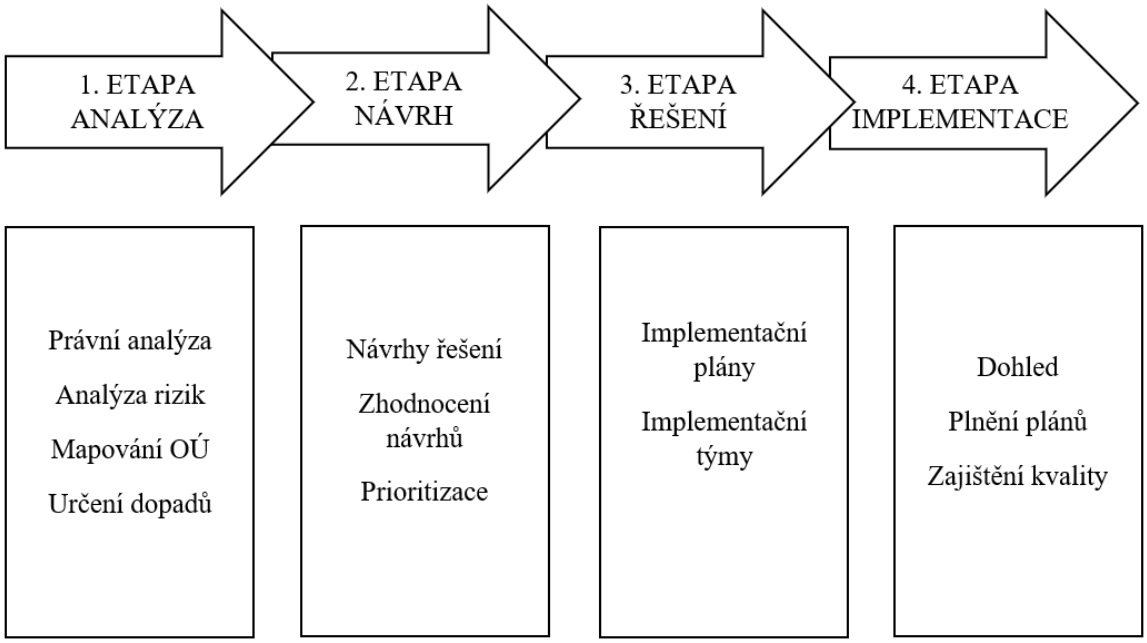
Před účinností GDPR byl vydán příkaz ředitele, ve kterém byly jednotlivé kroky stanoveny, rozpracovány a byly přiřazeny termínované úkoly členům vedení a příslušným vedoucím pracovníkům. Jednotlivé kroky v tomto implementačním plánu také byly rozděleny podle toho, zdali je bylo nutné realizovat před nebo až po 25. 5. 2018. Byla identifikována jednotlivá rizika a s nimi spojena opatření vedoucí k minimalizaci dopadu těchto rizik.

Důležitým krokem bylo vytvoření implementačního týmu věnujícího se problematice GDPR. Tvoří ho pověřenec pro ochranu osobních údajů, manažer bezpečnosti informací, projektový manažer, legislativně právní odbor a IT specialisté. Vše probíhá ve spolupráci se členy Vedení Nemocnice. Důležitou roli hraje také externí pracovník, který Nemocnici pomáhal s veškerými kroky implementace a dodnes poskytuje případné poradenství.

Neméně důležitým krokem v celé implementaci bylo dohlížení na plnění plánu, tedy dohlížení na plnění příkazu ředitele.

Harmonogram celého projektu implementace GDPR v Nemocnici je naznačen na Obr. č. 2.

Obrázek č. 2 – Harmonogram projektu



Zdroj: vlastní zpracování

4.2.2 Určení pověřence pro ochranu osobních údajů

Pověřence pro ochranu osobních údajů (dále jen DPO) jmenoval ředitel Nemocnice a zároveň byla tato skutečnost nahlášena na ÚOOÚ, čímž byla splněna ohlašovací povinnost. V této souvislosti došlo ke změnám v řídicí dokumentaci, kde byla tato funkce zařazena do organizační struktury a byly vymezeny kompetence, dále byla nastavena agenda DPO.

Do této funkce byl jmenován vedoucí interního auditu. V rámci psaní této diplomové práce však bylo na internetových stránkách Ministerstva financí dohledáno stanovisko Centrální harmonizační jednotky Ministerstva financí (Příloha č. 3). Ta vydala 13. 4. 2018 a dále 21. 9. 2018 aktualizovala stanovisko[140], které se otázkou jmenování interního auditora do funkce DPO zabývá. V něm je uvedeno, že interní auditor nemůže funkci DPO vykonávat, a to z důvodu zajištění nezávislého postavení a zabránění střetu zájmů obou funkcí. Stanovisko však je pouhou reakcí na položený dotaz a k jeho vydání došlo velmi pozdě, jelikož většina organizací již měla DPO jmenovaného. Nebyl to problém, který by se

[140] CENTRÁLNÍ HARMONIZAČNÍ JEDNOTKA MINISTARSTVA FINANCÍ. *Stanovisko č. 1b/2018* [online]. (PDF). [cit. 2019-02-5]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Metodika_2018_CHJ-2018-1-Stanovisko-k-povereni-interniho-auditora-funkci-DPO-GDPR_v02.pdf

týkal pouze Nemocnice. V této souvislosti bylo jinou organizací poskytnuto stanovisko ÚOOÚ. Ten se k problematice staví tak, že nesmí dojít ke střetu zájmů, takže by byl individuálně posuzován případ od případu.[141] I ten se však odkazuje na výše uvedené stanovisko, i přes to, že je velmi obecné. Dodnes tedy není zcela zřejmé, zda může interní auditor funkci DPO vykonávat, avšak zatím nebyl nikdo sankcionován.

4.2.3 Mapování procesů

Před samotnými kroky implementace bylo velice důležité zmapovat, k jakému zpracování osobních údajů v Nemocnici vůbec dochází. Bylo nutné analyzovat, v rámci jakého procesu jsou osobní údaje zpracovávány, v jakých úložištích jsou ukládány, zdali se jedná o elektronické úložiště či úložiště v listinné podobě (např. kartotéky), k jakému účelu jsou osobní údaje zpracovávány, po jak dlouhou dobu jsou uchovávány, nebo zdali se předávají jiným subjektům a případně kterým. Také bylo nutné věnovat pozornost tomu, v jaké pozici se Nemocnice nachází. Zdali je v pozici správce, zpracovatele či příjemce.

V rámci mapování procesů byla oslovena veškerá pracoviště Nemocnice. Za každé pracoviště byli určeni jeho zástupci, kteří odpovídali za implementaci GDPR. V úvodu proběhly schůzky, jejichž cílem bylo přestavení GDPR, jeho dopadů a stanovení postupu mapování jednotlivých procesů zpracování osobních údajů.

Výsledkem této fáze implementace bylo zmapování téměř 700 procesů a 400 IT aplikací, přičemž veškeré získané údaje byly zaneseny do registru osobních údajů.

4.2.4 Vytvoření registru zpracování osobních údajů

Vzhledem k povinnosti vést záznamy o činnostech zpracování, Nemocnice musela vytvořit registr zpracování osobních údajů. Byly vytvořeny registry pro administrativní a pro klinickou část Nemocnice, dále byl vytvořen IT registr osobních údajů, který obsahuje elektronická úložiště a využívané systémy.

Při vytváření registru se problémem stala nejednotnost úvodních schůzek s jednotlivými zástupci pracovišť Nemocnice. Schůzky byly vedeny dvěma školiteli, přičemž každý měl na problematiku mírně odlišný pohled. Řešením by mohla být společná úvodní schůzka pro všechny zástupce zároveň, přičemž odlišné požadavky pracovišť by

[141] Pozn.: Z hlediska §§ 28-29 Zákona č. 320/2001 Sb., o finanční kontrole, ve znění pozdějších předpisů.

následně byly řešeny individuálně. Všichni zástupci by tak měli stejné vstupní informace a výsledný registr osobních údajů by tak byl více konzistentní.

V současné době probíhá pravidelná aktualizace veškerých registrů, zároveň jsou registry upravovány při změnách, kterými jsou např. změny či ukončení zpracování osobních údajů. V případě nového zpracování osobních údajů je vždy důležité skutečnost oznámit s dostatečným předstihem, aby mohlo dojít k jeho posouzení. Zaměstnanci by měli využívat stanovený formulář, v praxi se tak však neděje.

4.2.5 Kontrola poskytnutých souhlasů se zpracováním osobních údajů

Bylo nutné ověřit, zda jsou současné souhlasy se zpracováním osobních údajů v souladu s GDPR, zda nejsou sbírány při některých procesech nadbytečné souhlasy, případně zdali není nutné u nějakých druhů zpracování souhlasy sbírat. V této souvislosti tedy byla provedena velká revize veškerých souhlasů. Byly nalezeny jednotlivé případy, kdy souhlas nebyl v souladu s požadavky GDPR a ve spolupráci s legislativně právním odborem tedy došlo k jejich úpravě a jejich opětovnému znovuzískání. Je nutné zamezit využívání souhlasů, které nebyly schváleny legislativně právním odborem, z toho důvodu by bylo vhodné technické opatření, které by např. zabránilo provádění změn textace v již schválených předpřipravených souhlasech.

Jednalo se o časově velice náročný proces, jelikož jsou souhlasy uchovávány v listinné podobě. V budoucnu bude nutná elektronizace dokumentů, avšak v takové podobě, aby s dokumenty mohlo být efektivně pracováno.

4.2.6 Kontrola uzavřených smluv

Nejprve byl úsekem informatiky vytvořen seznam zpracovatelů, který tvoří veškeří identifikovaní zpracovatelé osobních údajů. U smluv, ve kterých nebylo nakládání s osobními údaji jasně ustanoveno, bylo nutné uzavření smlouvy o zpracování osobních údajů, případně uzavření dodatku k již stávající smlouvě. Jednalo se o revizi stovek smluv.

U servisních smluv bylo doplněno ustanovení týkající se mlčenlivosti, jelikož může dojít k situaci, kdy je k servisu předána zdravotnická technika, která obsahuje osobní údaje.

Stejným způsobem bylo postupováno v případě příjemců osobních údajů, tedy těch, kterým nemocnice osobní údaje zasílá. Jsou jimi např. různé zdravotní registry. Zároveň bylo nutné řešit bezpečný přenos osobních údajů k těmto příjemcům.

V seznamu zpracovatelů budou dále uvedeni i tzv. společní správci osobních údajů, tedy takoví správci, kteří zpracovávají osobní údaje pacientů Nemocnice i pro své vlastní účely. Příkladem mohou být farmaceutické firmy, které zpracovávají osobní údaje v rámci klinických studií. Tento krok ještě nebyl realizován, ale je v současné době v procesu.

Může dojít i situaci, kdy dochází k předávání osobních údajů vzhledem k dalšímu úvazku zaměstnance Nemocnice. Jedná se o případ, kdy zaměstnanec předává osobní údaje např. nadaci. V takovém případě jsou důležitá vhodná opatření, mezi které patří např. získání souhlasu subjektu údajů se zpracováním, zasmluvnění či případná anonymizace osobních údajů. Přehled smluv, které mají zaměstnanci uzavřeny, je v kompetenci legislativně právního odboru. Pro tato zpracování prozatím nebyl nastaven kontrolní mechanismus.

4.2.7 Implementace technických opatření

Na základě vytvořeného IT registru a analýzy rizik u jednotlivých systému zpracovávajících osobní údaje bylo nutné implementovat vhodná technická opatření k zajištění ochrany osobních údajů. Bylo nutné především zabezpečit šifrování dat, nastavit proces pseudonymizace či anonymizace osobních údajů.

Důležitou částí bylo nastavení zabezpečené komunikace mimo Nemocnici. Prostřednictvím emailu je nyní možné komunikovat pouze po podepsání vlastním kvalifikovaným elektronickým podpisem, zasláním šifrovaného emailu nebo po získání souhlasu pacienta se zasíláním informací nezabezpečeným emailem (Příloha č. 4).

Velkým problémem je fakt, že při komunikaci s pacienty mimo Nemocnici je možné komplikace s šifrováním dokumentů a emailů vyřešit zasláním emailu z jiného než pracovního emailu, tedy nezabezpečenou cestou. Využívání svého osobního emailu je samozřejmě v rozporu s řídicí dokumentací, avšak není mu nijak technicky zabráněno.

Dalším problémem je ukládání osobních údajů na externí média (USB flash disky, CD, DVD atd.). Prvním krokem byla analýza používaných médií s posouzením, zdali je nutné médium používat a zdali není možné využívat bezpečnější formou, tedy ukládání na cloudové úložiště. Druhým je technické vynucení používání pouze zašifrovaných médií. Druhý krok však souvisí s pořízením nového software, proto doposud nedošlo k jeho aplikaci. V současné době je tedy možné data ukládat i na soukromá nezabezpečená média, i přesto že je to opět v rozporu s řídicí dokumentací. Neexistuje nástroj, který by takovéto chování dokázal detekovat. K čemu však došlo, je využívání cloudových úložišť. Pro

Nemocnici se jedná o velký krok. Samozřejmostí je, že v souladu s GDPR je využíváno pouze úložiště v rámci Evropského hospodářského prostoru.

V neposlední řadě bylo nutné nastavení procesů přístupových oprávnění a provedení revize současných oprávnění ve veškerých nemocničních systémech. Přístupová práva je třeba pravidelně kontrolovat a revidovat.

Co se týká zabezpečení osobních údajů v listinné podobě, i zde bylo nutné provést analýzu zabezpečení. Byly vytipovány, stavebně a technicky upraveny prostory, kde dochází k ukládání dokumentů. V některých případech byly kartotéky se zdravotnickou dokumentací umístěny ve veřejně přístupných prostorách. I když byly vždy důkladně uzamčeny, došlo k jejich přemístění. Eliminovalo se tak riziko, kdy by některý ze zaměstnanců zapomněl kartotéku uzamknout. Aby mohlo být ukládání dostatečně zhodnoceno, probíhají pravidelné audity fyzického zabezpečení.

4.2.8 Uchovávání osobních údajů

Je nezbytně nutné dodržovat princip minimalizace. U osobních údajů, u kterých již neexistuje žádný titul pro jejich zpracování, bylo nutné nastavit proces periodického výmazu případně anonymizace. Nyní se každoročně bude hodnotit, u kterých osobních údajů již uplynuly archivační lhůty a je tedy nutné je skartovat.

Pro každý proces zpracování osobních údajů bylo nutné nastavit archivační lhůty. Většinou se jedná o lhůty stanovené zákonem a jsou dodržovány, avšak existují výjimky. Např. z důvodu právní ochrany Nemocnice, kdy dochází k soudním sporům s pacienty, ale také při nakládání se zdravotnickou dokumentaci. Standardně je možné ji uchovávat pouze po dobu 5 let[142]. Avšak v některých případech takto krátké lhůty nejsou příliš vhodné. Pokud se jedná o onkologicky nemocného pacienta, je nutné tuto lhůtu z důvodu možného návratu onemocnění prodloužit. Tato informace je uvedena i v informačním memorandu pro pacienty.

4.2.9 Osobní údaje zaměstnanců

U zaměstnanců bylo problémem uchovávání osobních údajů nejen na personálním úseku, ale také na jednotlivých pracovištích. Jednalo se především o životopisy uchazečů, mzdové výměry, zdravotní prohlídky atd. Veškerá pracoviště tedy byla vyzvána ke skartaci osobních údajů, které nemusí nutně uchovávat. V některých případech je uchovávání

[142] Viz § 5 Odst. 2 Vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů.

opodstatněné, např. z důvodu státní kontroly či auditu. Zde je však otázka, zdali není možné takovou kontrolu odkázat na personální úsek. Došlo však k případům, že některá pracoviště se požadavku zalekla a následně byly skartovány veškeré dokumenty s osobními údaji zaměstnanců, včetně těch, které jsou pracoviště povinna evidovat a uchovávat u sebe. Jednalo se např. o doklad úspěšného absolvování školení týkajícího se bezpečnosti a ochrany zdraví při práci. Příště tedy bude nutné lépe specifikovat požadavek, aby k těmto nežádoucím událostem již nedošlo.

V případě uchazečů o zaměstnání a souvisejícího náborového procesu bylo nutné jasně přiřadit odpovědnosti a stanovit pravidla pro zpracování osobních údajů. V reakci na tuto problematiku bylo rozhodnuto, že bude zřízeno jedno speciální oddělení spadající pod personální úsek. Veškerá komunikace s uchazeči o zaměstnání bude probíhat přes jednu emailovou adresu, kterou bude spravovat toto nové oddělení.

V rámci náborového procesu může dojít k několika specifickým situacím. Uchazeč může přijít osobně na personální úsek, kde se ptá na možné volné pozice. Je mu dán k podpisu souhlas se zpracováním osobních údajů, poté jsou osobní údaje uchovávány dva roky od podpisu. Pokud je pro něj nalezeno vhodné pracovní místo je uchazeč odeslán na příslušné pracoviště.

Stejně tak uchazeči mohou zaslat svůj životopis bez jakékoli návaznosti na volnou pracovní pozici elektronicky. Opět je jim zaslán výše uvedený souhlas. Pokud uchazeč souhlas nezašle podepsaný zpět, jeho osobní údaje jsou skartovány.

V případě, kdy se nejedná o vhodné kandidáty a je rozhodnuto, že se jejich osobní údaje nebudou evidovat pro případ uvolnění vhodné pracovní pozice v budoucnu, jsou jejich osobní údaje a veškeré poskytnuté dokumenty také skartovány. Souhlas se zpracováním osobních údajů pak není vyžadován.

Co se týká neúspěšných uchazečů o zaměstnání, bylo nezbytné nastavení procesu skartace. Osobní údaje jsou skartovány po třech měsících po skončení výběrového řízení. Delší dobu je možné tyto údaje uchovávat opět pouze po podpisu souhlasu se zpracováním osobních údajů.

Celý náborový proces včetně následného uchovávání osobních údajů zaměstnanců bude vydán formou interního předpisu. Nyní probíhá zavádění nového personálního systému, který vyřeší mimo jiné duplicitní ukládání listinných dokumentů, jelikož vše bude probíhat elektronicky.

4.2.10 Interní předpisy

V souvislosti s GDPR bylo nutné upravit a vydat mnoho nových řídicích dokumentů. Jedním z nejdůležitějších dokumentů je aktualizovaná směrnice o ochraně osobních údajů. V ní jsou obsaženy veškeré pravomoci, povinnosti a postupy při práci s osobními údaji. Obsahuje informace o evidenci, zpracování, uchovávání a zabezpečení osobních údajů, nebo také postup při podezření na únik osobních údajů. Dále došlo k úpravě např. organizačního řádu či směrnic týkajících se informačních systémů a bezpečnosti informací.

V rámci implementace GDPR byla v Nemocnici legislativně právním odborem vypracována dvě memoranda, čímž došlo ke splnění povinností vyplývajících z článků 13 a 14 GDPR. Jedná se o memorandum pro zaměstnance a memorandum pro pacienty a další návštěvníky nemocnice (např. rodinné příslušníky).

Informační memorandum pro pacienty je veřejně dostupné všem pacientům a dalším návštěvníkům Nemocnice na nemocničních internetových stránkách. Jedná se o poměrně rozsáhlý dokument, obsahující např.:

- jaké osobní údaje jsou Nemocnicí shromažďovány a jak jsou následně zpracovávány,
- z jakých zdrojů jsou osobní údaje získávány,
- jak dlouho jsou Nemocnicí osobní údaje uchovávány,
- jak je zajištěna ochrana osobních údajů,
- zdali Nemocnice osobní údaje předává i třetím stranám a případně kterým,
- jaká mají pacienti práva v souvislosti s osobními údaji a jejich ochranou,
- odkaz, kam se pacienti případně mohou obrátit k získání dalších informací.

Infomační memorandum pro zaměstnance je určeno stávajícím zaměstnancům a je dostupné na interních internetových stránkách. V mnohých věcech kopíruje informační memorandum pro pacienty.

4.2.11 Školení zaměstnanců

Aby byla splněna povinnost informování veškerých zaměstnanců Nemocnice, byl vytvořen e-learningový test. Ten museli ve stanoveném termínu absolvovat všichni zaměstnanci. Termín se nepodařilo dodržet v plném rozsahu, avšak dodnes test absolvovalo přes 90 % zaměstnanců.

Dále byla problematika GDPR zařazena do testů ISMS (systém řízení bezpečnosti informací). V současné době test ISMS musí absolvovat všichni nově nastupující

zaměstnanci a současní zaměstnanci ho absolvují v pravidelných intervalech. Díky tomu by i zaměstnanci, kteří neabsolvovali speciální školení na GDPR, měli být s touto problematikou srozuměni.

O nastavených procesech jsou zaměstnanci Nemocnice informováni také prostřednictvím aktualizované řídicí dokumentace.

V rámci školení zaměstnanců byly spuštěny speciální intranetové stránky, kde jsou kromě jiných obecných informací shromažďovány také nejčastější dotazy spolu s odpověďmi. Jednalo se o velice praktický tah, jelikož předtím se pracoviště obracela na DPO, který musel odpovídat na desítky dotazů, které se mnohdy opakovaly.

Často kladené otázky zde byly přehledně rozděleny do několika kategorií, mezi hlavní patří souhlas pacienta, nakládání s osobními údaji, bezpečná komunikace a bezpečnostní incidenty. Níže je uveden příklad nejčastěji kladených otázek spolu s odpověďmi.

- Je při vedení zdravotnické dokumentace nutné vyžadovat souhlas pacienta se zpracováním jeho osobních údajů?
  (Vzhledem k tomu, že se jedná o plnění právní povinnosti, souhlas není vyžadován.)
- Je souhlas nutné vyžadovat v případě vědeckého výzkumu a klinické studie?
  (Pacient musí souhlas udělit v případě, kdy jsou sbírány další osobní údaje, které nejsou součástí zdravotnické dokumentace.)
- Je možné uchovávat kontaktní údaje oprávněných osob, především opatrovníků a zákonných zástupců?
  (Ano, jelikož zpracování těchto údajů vychází ze zákona, jedná se také o právo pacienta.)
- Je potřeba pacientův souhlas získávat opakovaně při každém pokusu o nezabezpečenou elektronickou komunikaci?
  (Pokud budou zasílány pouze údaje ve stejném rozsahu, ke kterým byl udělen souhlas, není třeba ho získávat opakovaně.)
- Lze komunikovat e-mailem s jiným lékařem či laborantem mimo Nemocnici běžnou e-mailovou zprávou?
  (Ne, komunikace musí být vždy zabezpečená.)
- Je možné předat výsledky vyšetření či recept rodinnému příslušníkovi pacienta?
  (Ano, ale pouze v případě podepsaného souhlasu pacienta a následné identifikace osoby.)

- Jak jsou osobní údaje chráněny před samotnými zaměstnanci Nemocnice?
  (Ke všem osobním údajům je řízený přístup, který spravuje úsek informatiky.)

4.2.12 Proces identifikace a řešení úniku osobních údajů

V souladu s GDPR byl v Nemocnici zaveden systém pro identifikaci a interní oznamování incidentů a možného úniku osobních údajů. Je rozlišováno, zdali se jedná o IT únik nebo o procesní pochybení.

IT únikem může být např. ztráta mobilního telefonu, USB flash disku či odeslání emailu obsahujícího osobní údaje nezabezpečenou cestou. V Nemocnici již před účinností GDPR fungoval ServiceDesk, který byl pro tento účel nyní využit. Byla v něm založena další kategorie, do které mají všichni zaměstnanci povinnost podezření na únik osobních údajů nahlásit. Ve výjimečné situaci je také možné kontaktovat přímo DPO. V řídicí dokumentaci byl stanoven jasný postup, co má takové nahlášení obsahovat.

Po zadání zaměstnancem do ServiceDesku je následně nutné vyhodnotit, zdali opravdu došlo k porušení ochrany osobních údajů, případně v jakém rozsahu. Šetření provádí především manažer pro bezpečnost informací ve spolupráci s příslušným pracovištěm, na kterém k podezření z porušení ochrany osobních údajů došlo.

ServiceDesk dále také plní funkci evidence. Jsou zde uloženy veškeré podklady týkající se úniku, včetně protokolu (Příloha č. 5), který je vyhotovován vždy na závěr celého šetření. Obsahuje veškeré důležité informace a průběh samotného šetření. Fyzické úložiště těchto protokolů má na starost DPO.

Tzv. procesní úniky, tedy úniky v listinné podobě (např. ztráta zdravotnické dokumentace) je zaměstnanci zaznamenávána do odděleného systému. Je to z toho důvodu, že tento systém byl pro takovéto události využíván již dříve a zaměstnanci jsou na něj zvyklí. Následně je incident manažerem pro bezpečnost informací zaznamenán i do ServiceDesku. I když se tento postup v začátcích jevil jako velmi chaotický a nepraktický, nebylo od něj upuštěno. Je využíván i v současné době a je plně funkční.

V relevantních případech, kdy by došlo ke zjištění porušení zabezpečení osobních údajů, ať již IT nebo procesních, je nutno tuto skutečnost bez zbytečného odkladu nahlásit ÚOOÚ, případně dotčenému subjektu. Tuto povinnost má v Nemocnici DPO. Pro určení, zdali k nahlášení dojde, je klíčové posouzení rizik spojených s porušením zabezpečení osobních údajů. Provádí ho především manažer pro bezpečnost informací.

Po úniku osobních údajů je samozřejmostí přijetí nápravných opatření, aby nedošlo k opakování stejného incidentu.

Po účinnosti GDPR se Nemocnice doposud setkala s celkem devíti podezřeními na únik osobních údajů, což se dá považovat za velmi dobrý výsledek. Obzvláště proto, že se nejednalo o příliš závažná podezření. Ve čtyřech případech se jednalo o odcizení služebního telefonu zaměstnance. Telefony neobsahovaly žádné osobní údaje pacientů, pouze některé osobní údaje zaměstnanců, konkrétně jméno, příjmení a pracovní telefonní číslo. Bylo vyhodnoceno, že riziko pro subjekty osobních údajů je minimální.

Další případy se týkaly manipulace se zdravotnickou dokumentací, ale i zde bylo riziko pro subjekty osobních údajů zanedbatelné a vše bylo obratem napraveno.

4.3 Posouzení vlivu na ochranu osobních údajů

Bylo rozhodnuto, že za provedení DPIA bude zodpovídat DPO. Ve spolupráci s externím pracovníkem tedy byly vytipovány procesy, na které bude nutno DPIA provést. Až počátkem roku 2019 byly vydány pokyny ÚOOÚ, na základě kterých bylo nutné původně vytipované procesy přehodnotit a současně přehodnotit jejich priority. Ve většině případů DPIA nebylo prováděno pouze na jednotlivé procesy, ale bylo vždy spojeno několik souvisejících procesů dohromady. Jako nejdůležitější byly vyhodnoceny klinické studie a výzkum, včetně archivace dat a předávání dat zdravotním pojišťovnám, registrům a státním orgánům. Úzce navazovalo předávání dat jiným zdravotnickým zařízením, kam byly zařazeny i externí laboratoře. Mezi další vytipované procesy patřilo např. monitorování kamerami, systematické monitorování aktivit zaměstnanců atd. Naopak mezi procesy, pro které DPIA nebylo nutné provést, bylo zařazeno veškeré zpracování osobních údajů v rámci ambulantní péče, zpracování na základě právní povinnosti, případně pokud jde o zpracování na základě veřejného zájmu. Nutno podotknout, že taková je většina zpracování.

DPIA bylo rozděleno do sedmi kroků:

První krok – bylo vyhodnoceno, zda proces byl vytipován správně a zda je provedení DPIA opravdu potřebné. V tomto kroku bylo jasně definováno, jaký je účel daného procesu a z jakého důvodu byl tento proces pro DPIA vybrán.

Druhý krok – byl zmapován celý proces zpracování. Tento krok byl rozdělen do několika dalších bodů. Nejprve byla popsána podstata celého zpracování. Je zde tedy uvedeno, jakým způsobem dochází ke shromažďování osobních údajů, jak je s nimi nakládáno, jaké jsou archivační lhůty. Dále je zde definováno, kdo má k těmto osobním

údajům přístup a zdali budou předávány třetím stranám. Dále byl stanoven rozsah zpracování, tedy jaké množství osobních údajů bude shromažďováno a zdali mezi nimi budou i citlivé osobní údaje. V dalším bodu byl popsán kontext zpracování, tedy jaký má např. Nemocnice vztah k subjektu údajů, jaká je míra kontroly subjektu údajů nad zpracovávanými osobními údaji, případně zdali nejsou mezi subjekty i zranitelné skupiny osob, např. děti. Posledním bodem bylo popsání účelu zpracování včetně toho, jaký užitek z tohoto zpracování Nemocnice má. Může jít např. o použití v důkazním řízení (při řešení stížností atd.).

Třetí krok – zvážení konzultace s dotčenými subjekty, případně s jinými odborníky, např. bezpečnostními. Ve většině případů bylo vyhodnoceno, že se jedná o zcela běžnou činnost Nemocnice, a proto konzultace nebyla provedena.

Čtvrtý krok – posouzení nezbytnosti a proporcionality, tedy posouzení, na jakém právním základě ke zpracování dochází. Bylo vyhodnocováno, zdali by nebylo možné využít nějakou jinou metodu k dosažení stejného účelu zpracování, jakým způsobem bude zaručena zásada minimalizace apod.

Pátý krok – došlo k identifikaci a posouzení rizik. Byly vymezeny zdroje rizika a ke každému riziku byla stanovena pravděpodobnost újmy, její vážnost a celková výše rizika.

Šestý krok – úzce navázal na předešlý krok, protože v tomto kroku byla identifikována opatření vedoucí ke zmírnění rizik.

Sedmý krok – posledním krokem byly záznamy o schválení spolu s komentářem a doporučeními DPO. Ředitel Nemocnice byl oprávněn zde vyjádřit případný nesouhlas s navrhovanými doporučeními, spolu s uvedením důvodů, proč je zamítl.

Této části implementace GDPR nejprve nebyla věnována přílišná pozornost, avšak později se ukázalo, že se jedná o velice náročný a časově zdlouhavý proces.

4.4 Práva pacientů

4.4.1 Registr žádostí

V souladu s GDPR má každý pacient možnost uplatnit svá práva prostřednictvím podání žádosti. Z toho důvodu byl vytvořen systém, ve kterém jsou žádosti evidovány a jsou u nich monitorovány lhůty pro vyřízení. Zpracování žádostí a jejich vyřizování zajišťuje v Nemocnici DPO. Součástí tohoto kroku bylo také vytvoření šablon pro odpovědi. Vzhledem k počtu žádostí se tento krok může jevit jako mírně nadbytečný, jelikož jednotlivé

odpovědi je možné vytvářet operativně, a především individuálně na základě požadavků žadatele.

Samotnou žádost je možné zaslat několika způsoby, vždy je však nutné dbát na ověření totožnosti žadatele. Žádost je možné zasílat emailem s kvalifikovaným elektronickým podpisem, datovou schránkou, osobním doručením nebo poštou.

V případě ověřování totožnosti dochází k paradoxní situaci. Může dojít k případu, kdy např. pacient žádá o uplatnění práva na výmaz. Aby k němu ale mohlo dojít, je nutné danou osobu ověřit (na základě občanského průkazu), čímž dochází k dalšímu sběru osobních údajů.

4.4.2 Uplatňování práv

V případě práva na přenositelnost bylo nutné rozhodnutí, jaký rozsah dat bude exportován, případně jakým způsobem budou osobní údaje předávány. Jak již bylo uvedeno v teoretické části této diplomové práce, toto právo je možné uplatnit pouze v případě, kdy jsou osobní údaje zpracovávány buď na základě uděleného souhlasu se zpracováním osobních údajů nebo na základě smluvní dohody. Zároveň platí, že osobní údaje musí být zpracovávány automaticky.

V případech, kdy by právo bylo možné uplatnit, bylo rozhodnuto, že proces není možné stanovit obecně, a proto bude každá žádost posuzována individuálně.

Dále bylo nutné zajistit technickou realizaci a stanovit způsob, jakým bude export osobních údajů realizován. V průběhu tohoto procesu však bylo identifikováno několik systémů, ze kterých není provedení exportu technicky reálné. Veškeré tyto systémy jsou označeny v IT registru.

Identicky bylo postupováno i v případě práva na výmaz. Kromě toho se musela určit oblast dat, která bude moci být smazána, a to s ohledem na archivační lhůty. Výmaz bude vždy prováděn po konzultaci s legislativně právním odborem. Případný výmaz musí být vždy zaznamenán v seznamu provedených výmazů.

Problém technické proveditelnosti nenastal pouze u elektronických dat, ale i u osobních údajů uložených v listinné podobě. Příkladem může být žadatel, který bude chtít vymazat veškeré údaje, které o něm Nemocnice uchovává. Takový žadatel však může být mimo jiné uveden jinou osobou na informovaném souhlasu, na kterém je uvedeno jeho jméno, příjmení a kontakt. Vzhledem k tomu, že jsou tyto souhlasy uchovávány v listinné podobě, není možné žadatele dohledat a údaje vymazat.

Co se týká práva na informace a na opravu údajů, opět byl nastaven celý proces a byly přiřazeny odpovědnosti. Pokud je žádost konkrétní, není problém informace podat. Avšak pokud je velmi neurčitá a žadatel chce poskytnout informaci o veškerých svých údajích, dochází ke stejným komplikacím uvedeným výše.

Celkově byl učiněn závěr, že ke každé žádosti se musí přistupovat individuálně.

V některých relevantních případech, kdy dojde k výkonu práv subjektu, má Nemocnice oznamovací povinnost vůči zpracovateli či příjemci dotčených osobních údajů. Na základě registru osobních údajů tedy byly vytipovány scénáře, kdy by k této situaci mohlo dojít. Takovou třetí stanou může být např. o organizátor klinické studie. Tento proces zatím bohužel nefunguje automatizovaně.

4.4.3 Přijaté žádosti

Do dnešního dne Nemocnice přijala celkem 5 žádostí.

Jedna žádost byla podána anonymem, z toho důvodu byl žadatel vyzván k prokázání totožnosti. Jelikož se jednalo o neúplnou žádost, nebyla zahájena ani 30denní lhůta pro vyřízení. Byla vyžádána potřebná stanoviska, avšak žadatel se neprokázal, proto žádost nebyla dále řešena.

Další žádost byla opět neúplná, proto byl žadatel požádán o prokázání totožnosti a o sdělení korespondenční adresy. Protože žadatel již dále nereagoval, Nemocnice se žádostí již dále nezabývala.

Dvě žádosti byly podány přímo zaměstnanci nemocnice a týkaly se žádosti o výmaz. Vzhledem k tomu, že se jednalo o zaměstnance a žádost byla zaslána ze zaměstnaneckého emailu, nebylo nutné žadatele dále ověřovat. Jejich žádostem bylo vyhověno.

Poslední žádost se týkala žádosti o výmaz, avšak Nemocnice osobní údaje zpracovává ze zákonných důvodů, proto žádosti nebylo vyhověno. Jednalo se o jedinou žádost v listinné podobě.

Celkově bylo podáno velmi malé množství žádostí, kompletní žádosti byly pouze tři, z toho byly dvě podány zaměstnanci Nemocnice. Před účinností GDPR byl očekáván mnohem vyšší zájem o uplatňování práv pacientů.

4.5 Podněty k přístupu k internímu auditu

Pro účely zhodnocení implementace GDPR v Nemocnici jsou v této kapitole stručně navrženy podněty, jak přistupovat k internímu auditu.

Vzhledem k tomu, že úkolem každého interního auditu je nějaké ujištění, cílem auditu zaměřeného na GDPR je ujištění, že Nemocnice splňuje veškeré jeho požadavky a vyplývající povinnosti. Předmětem je tedy především ověření souladu s řídicí dokumentací a související legislativou.

Vzhledem k tomu, že v Nemocnici byl na pozici DPO jmenován vedoucí útvaru interního auditu, bylo by velice důležité dbát na nezávislost. Tato situace se dá snadno vyřešit tím, že vedoucí pověří k provedení tohoto auditu podřízeného interního auditora, který dále povede celý auditní tým.

Na druhou stranu je velikou výhodou, že interní auditoři Nemocnice nemusí nijak zkoumat charakter, organizační strukturu ani základní procesy zpracování osobních údajů, jelikož je oproti externím pracovníkům již znají. Další výhodou je, že interní auditoři znají většinu problémů, se kterými se Nemocnice při implementaci GDPR potýkala a mohou se na ně tak zaměřit.

Vzhledem problémům s vytvářením registru osobních údajů hned na začátku implementace (4.2.3 Vytvoření registru zpracování osobních údajů), a dále tomu, že neexistuje žádný kontrolní mechanismus, by mělo být vytipováno několik procesů, které by se detailně ověřily, zda je celý proces v registru popsán správně. Při zavádění nových procesů by měli zaměstnanci využívat stanovený formulář, v praxi ho však nevyužívají. Audit by měl zhodnotit, z jakého důvodu formulář není využíván. Na základě toho navrhnout buď jeho úplné zrušení či úpravu, jelikož nynější stav je v rozporu s řídicí dokumentací.

Důležitou částí toho interního auditu by mělo být zabezpečení osobních údajů. To, že je celý proces správně nastaven v řídicí dokumentaci ještě neznamená, že je opravdu dodržován v praxi. Zde je důležité navázat spolupráci s úsekem informatiky. Opět je zde výhodou provádění auditu interními zaměstnanci, jelikož spolupráce s nimi se dá očekávat na vyšší úrovni nežli spolupráce s externími pracovníky.

Kromě elektronického zabezpečení by bylo nutné zkontrolovat také fyzické zabezpečení osobních údajů. Jedná se především o kartotéky se zdravotnickou dokumentací v případě osobních údajů pacientů či personální spisy zaměstnanců. Současně by mělo být hodnoceno také dodržování archivačních lhůt, především pak s ohledem na zásadu minimalizace osobních údajů.

Co se týká souhlasu se zpracováním osobních údajů, v průběhů implementace jich bylo revidováno opravdu velké množství, lze zde shledat riziko chyby lidského faktoru, proto by mělo být vytipováno na vybraných pracovištích několik souhlasů, kde by došlo

k ověření jejich obsahové správnosti a souladu s požadavky GDPR. Zde by bylo vhodné navázat spolupráci s legislativně právním odborem. Stejně tak by mělo být postupováno v případě ověřování uzavřených smluv př. dodatků k již uzavřeným smlouvám.

V rámci implementace měli být proškoleni všichni zaměstnanci Nemocnice. I přesto, že většina z nich vyplnila test týkající se GDPR, není zde zaručeno, že jsou všichni dostatečně informováni. Nikde není ošetřeno, aby za zaměstnance test nevyplnil někdo jiný. Proto by měly být provedeny rozhovory se zaměstnanci nemocnice, aby byly jejich znalostí týkajících se problematiky GDPR ověřeny.

Důležitou součástí interního auditu by mělo být zhodnocení postupu pro vyřizování žádostí subjektu údajů, včetně ověření postupu při hlášení porušení zabezpečení osobních údajů jak na ÚOOÚ, tak subjektu osobních údajů. Vzhledem k tomu, že na tomto procesů spolupracují kromě DPO také podřízení interní auditoři, musel by se dávat velký pozor na dodržení nezávislosti. Naproti tomu je zde výhoda, že interní auditoři vědí, jak vyřizování probíhá v praxi, proto by bylo snadné tento postup porovnat s řídicí dokumentací.

Vzhledem ke zjištěním týkajících se jmenování DPO (4.2.1 Určení pověřence pro ochranu osobních údajů), je nutné se touto problematikou dále zabývat. Interní audit je ideální k tomu, aby tuto problematiku dále analyzoval a případně podal ujištění, že postup při jmenování DPO byl v souladu s platnou legislativou.

V závěru tohoto interního auditu by byla navržena doporučení k odstranění případných zjištěných nedostatků.

4.6 Dotazníkové šetření

4.6.1 Stanovení cíle a hypotéz

Na začátku výzkumného šetření byl stanoven cíl, tedy zjistit informovanost pacientů o svých právech v souvislosti s poskytováním zdravotní péče, a zdali svá práva aktivně využívají. Dalším cílem bylo zjistit povědomí o nových právech v souvislosti s účinností GDPR. K dosažení cíle byly formulovány následující dvě hypotézy:

H1: Pacienti neznají svá práva v souvislosti s poskytováním zdravotní péče.

H2: Pacienti nemají povědomí o nových právech v souvislosti s GDPR.

4.6.2 Dotazník

Jedná se o kvantitativní výzkum, kterého se účastnilo celkem 408 respondentů. Výzkumný vzorek tvořili lidé starší 18 let.

Při volbě výzkumné metody se nabízelo dotazníkové šetření na místě. Pacientům by byl dán dotazník při propouštění z nemocnice. Hrozila však neochota pacientů dotazník vyplnit (spěchají domů), v případě odnesení domů hrozila nízká návratnost dotazníku. V případě dotazování ambulantních pacientů v čekárně hrozilo riziko, že pacienti budou chtít obratem svá práva využít, což by nebylo pro vybrané pracoviště, na kterém by dotazování probíhalo, žádoucí.

Z těchto důvodů výzkumné šetření probíhalo elektronicky. Dotazník byl vyvěšen po dobu jednoho měsíce a byl volně přístupný veřejnosti. Vyplňování bylo podporováno rozesíláním emailů, oslovováním konkrétních pacientů a distribuováním na sociálních sítích. Se staršími pacienty byl dotazník vyplňován s asistencí.

Otázky byly z důvodu snadného vyplňování uzavřené, v některých případech s možností doplnění vlastní odpovědi. Samotný dotazník obsahoval celkem 32 otázek. Prvních 15 otázek se týkalo samotných práv pacientů, 4 otázky byly zaměřeny na manipulaci se zdravotnickou dokumentací. Následovalo 8 otázek zjišťující povědomí pacientů o právech v souvislosti s GDPR a jejich případnou aplikací. Na závěr bylo zařazeno 5 otázek pro účel statistického zpracování.

Před samotnou distribucí bylo provedeno pilotní šetření na 5 vybraných respondentech (kolegové v práci a rodina), aby byla zjištěna časová náročnost průzkumu a také srozumitelnost a logická návaznost otázek. I přes větší počet otázek byla časová náročnost cca 4,5 minuty.

4.6.3 Výsledky dotazníkového šetření

Respondentům byly pokládány následující otázky. První část se týkala samotných práv pacientů.

1. Jak je to dlouho, co jste byl (a) naposledy u lékaře/ve zdravotnickém zařízení?

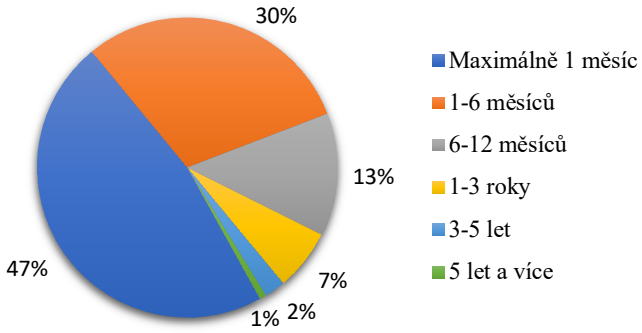
První otázka měla zjistit, jak často lidé navštěvují lékaře, jelikož pokud někdo k lékaři příliš nechodí, zřejmě se ani tolik neorientuje v právech pacientů.

Tabulka č. 7 – Návštěva lékaře

Odpověď	Počet
Maximálně 1 měsíc	192
měsíců	123
6-12 měsíců	54
1-3 roky	27
3-5 let	9
5 let a více	3
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 1 – Návštěva lékaře



Zdroj: vlastní zpracování

Bylo zjištěno, že téměř polovina respondentů navštívila lékaře během posledního měsíce. Ze 408 dotázaných jich 39 navštívilo lékaře před více než jedním rokem a pouze 3 respondenti lékaře navštívili před více než 5 lety. Tito 3 respondenti dokázali odpovědět správně průměrně na 4 otázky týkajících samotných práv pacientů z 10.

2. Myslíte si, že je důležité, aby lidé znali svá práva (práva pacientů)?

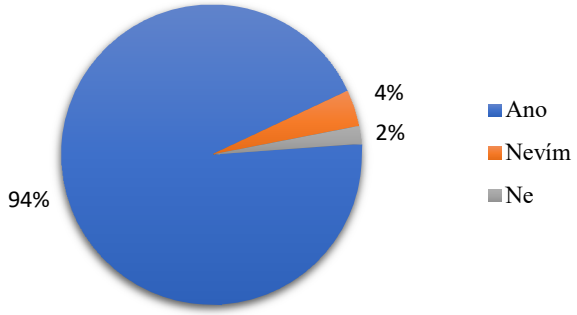
Druhá otázka zkoumala, jestli si pacienti vůbec myslí, že je důležité znát svá práva, nebo o tuto tématiku vůbec nejeví zájem.

Tabulka č. 8 – Důležitost znalostí

Odpověď	Počet
Ano	384
Nevím	16
Ne	8
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 2 – Důležitost znalostí



Zdroj: vlastní zpracování

Tato otázka byla zařazena především z důvodu, že pokud by si lidé mysleli, že není důležité práva znát, nebylo by žádným překvapením, kdyby svá práva neznali. Pokračování

v takovém výzkumném šetření by následně postrádalo smysl. Většina respondentu však uvedla, že svá práva je důležité znát.

3. Myslíte si, že Vy osobně znáte svá práva?

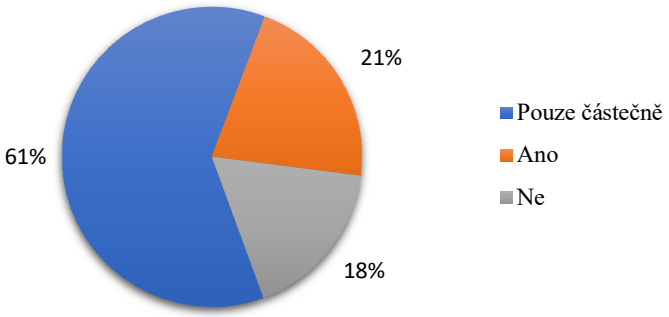
Ve třetí otázce měli pacienti odhadnout své znalosti práv pacientů.

Tabulka č. 9 – Znalost práv

Odpověď	Počet
Pouze částečně	250
Ano	87
Ne	71
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 3 – Znalost práv



Zdroj: vlastní zpracování

Tato otázka byla mimo výše uvedené zařazena také v návaznosti na předchozí otázku. Vzhledem k tomu, že většina respondentů považuje za důležité znalost svých práv, dalo by se očekávat, že je také znají. Kladně však označilo odpověď pouze 21 % respondentů. Dalších 61 % se však domnívá, že svá práva znají alespoň částečně.

4. Z jakého zdroje se o svých právech dozvídáte?

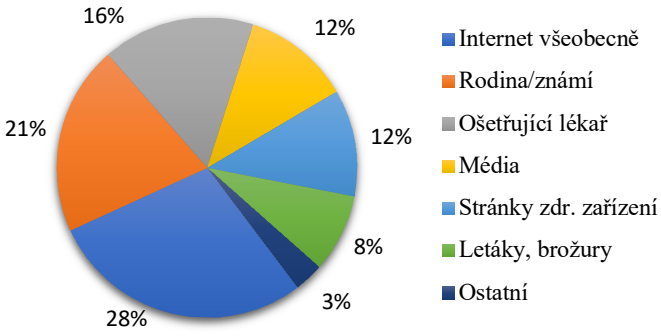
Pokud respondent v předešlé otázce odpověděl „ano“ nebo „pouze částečně“, byl dále dotázán, z jakého zdroje se o svých právech dozvídá. Respondent mohl zvolit více možností, měl i možnost připojit vlastní odpověď.

Tabulka č. 10 – Zdroj informací

Odpověď	Počet
Internet všeobecně	239
Rodina/známí	172
Ošetřující lékař	138
Média	97
Internetové stránky zdravotnického zařízení	97
Letáky, brožury	71
Ostatní	27

Zdroj: vlastní zpracování

Graf č. 4 – Zdroj informací



Zdroj: vlastní zpracování

Nejčastěji se lidé o svých právech dozvídají z internetu nebo od rodiny a známých. Ošetřující lékař je až na třetím místě. Mezi vlastními odpověďmi, převládala škola, kterou zvolilo 7 respondentů z 27, dále právní předpisy, které zvolilo 6 respondentů. Další odpovědi byly spíše ojedinělé, např. nemocniční ombudsman, pojišťovna př. zaměstnání v oblasti zdravotnictví.

5. Máte právo na volbu př. změnu lékaře/zdravotnického zařízení?

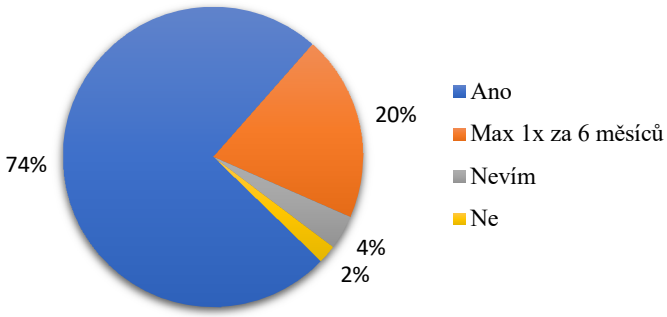
Pátá otázka již testovala znalost konkrétního práva, a to práva na volbu či změnu lékaře nebo zdravotnického zařízení.

Tabulka č. 11 – Volba/změna lékaře

Odpověď	Počet
Ano	303
Ano, ale změna je možná maximálně 1x za 6 měsíců	82
Nevím	15
Ne	8
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 5 – Volba/změna lékaře



Zdroj: vlastní zpracování

Ze 408 dotázaných zvolilo správnou odpověď 74 % respondentů. Dalších 20 % si myslí, že lékaře mohou změnit maximálně jednou za 6 měsíců. Je možné se domnívat, že tito respondenti si změnu lékaře pletou se změnou zdravotní pojišťovny, jelikož zde je opravdu toto omezení (kromě dalších podmínek, uvedených v teoretické části této diplomové práce, konkrétně v kapitole 3.6.2 Jednotlivá práva pacientů).

6. Máte právo na volbu zdravotnického zařízení v případě převozu rychlou záchrannou službou?

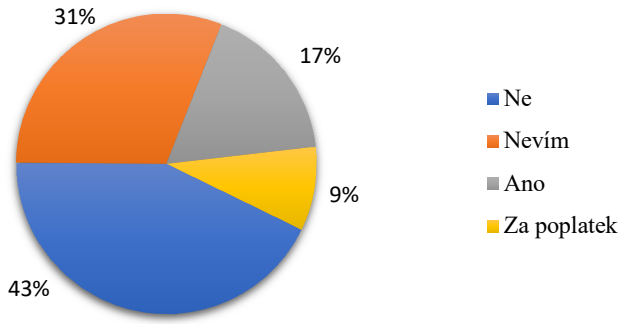
Další otázka se týkala možnosti volby zdravotnického zařízení, pokud jde o převoz rychlou záchrannou službou.

Tabulka č. 12 – Rychlá záchranná služba

Odpověď	Počet
Ne	175
Nevím	126
Ano	70
Ano, ale pouze za poplatek	37
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 6 – Rychlá záchranná služba



Zdroj: vlastní zpracování

Pouze 43 % respondentů uvedlo správnou odpověď, tedy že na volbu zdravotnického zařízení v případě převozu rychlou záchrannou službou nemají. 26 % respondentů si myslí, že právo na volbu mají, a to buď zdarma, nebo za poplatek. V případě, kdy pacient takový převoz potřebuje, může vést tato neznalost k problémům. Pro lékaře, kteří potřebují vykonávat svou práci je velmi vyčerpávající se s dotyčnými pacienty dohadovat.

7. Máte právo na odmítnutí poskytnutí Vašich základních identifikačních údajů?

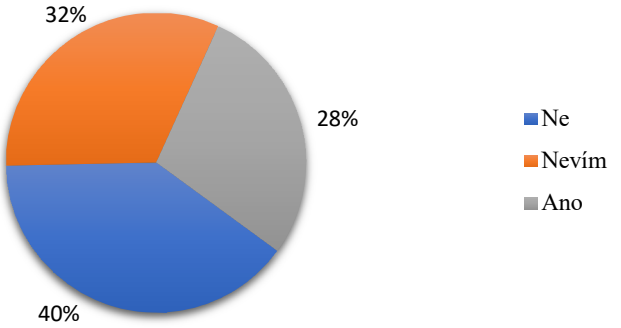
Mnoho lidí se v současné době domnívá, že má právo téměř na vše, proto byla zařazena otázka, zdali si dotazovaní myslí, že mohou v případě návštěvy lékaře odmítnout poskytnutí základních identifikačních údajů.

Tabulka č. 13 – Identifikační údaje

Odpověď	Počet
Ne	162
Nevím	131
Ano	115
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 7 – Identifikační údaje



Zdroj: vlastní zpracování

U této otázky pouze 40 % respondentů uvedlo správnou odpověď, že toto právo nemají. Povinnost poskytnutí základních identifikačních údajů k prokázání totiž patří mezi povinnosti pacienta, plynoucí ze zákona č. č. 372/2011 Sb. o zdravotních službách

a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů. 32 % respondentů uvedlo, že neví a 28 % si myslí, že toto právo má. Avšak pokud pacient poskytnutí odmítne, lékař ho v případě běžné situace není povinen ošetřit.

8. Máte právo na poskytnutí informací o léčbě Vaším ošetřujícím lékařem?

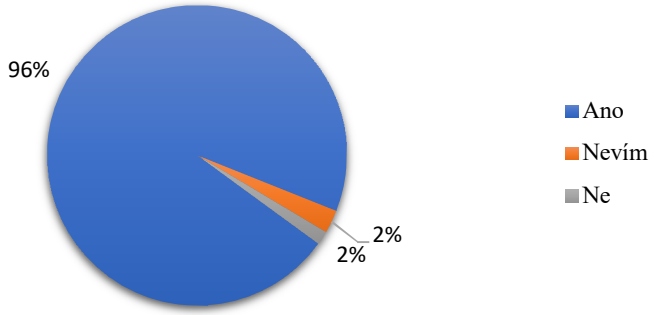
Toto právo by mělo být naprosto samozřejmé, proto u této otázky bylo předpokládáno, že téměř všichni respondenti odpovědí správně.

Tabulka č. 14 – Právo na informace

Odpověď	Počet
Ano	392
Nevím	10
Ne	6
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 8 – Právo na informace



Zdroj: vlastní zpracování

Správně odpovědělo 96 % dotázaných. Je zarážející, že 10 respondentů odpověď nevědělo a 6 si dokonce myslelo, že toto právo nemají. Polovina těchto dotazovaných byla ve věkové kategorii 18 – 25 let.

9. Máte právo nebýt informován o léčbě?

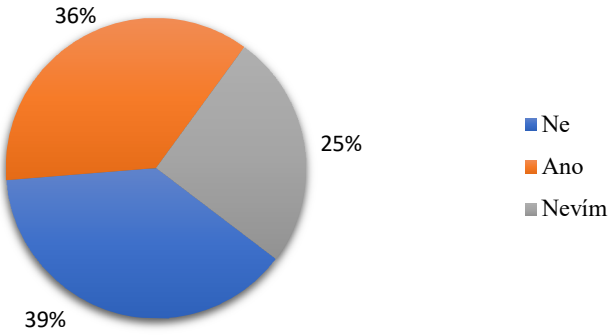
Devátá otázka byla zvolena v souvislosti s předchozí otázkou, jelikož zkoumá přesný opak. Tedy právo, zdali pacient může odmítnout sdělení informací o svém zdravotním stavu.

Tabulka č. 15 – Neinformování o léčbě

Odpověď	Počet
Ne	157
Ano	148
Nevím	103
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 9 – Neinformování o léčbě



Zdroj: vlastní zpracování

Tato otázka je první, u které převládá špatná odpověď. Odpověď „ne“ označilo 39 % respondentů a dalších 25 % označilo „nevím. Dokonce i respondenti, kteří pracují ve zdravotnictví, a předpokládá se u nich tedy vysoká znalost práv pacientů, měli správnou odpověď uvedenou pouze v 61 %.

10. Máte právo na odmítnutí zdravotního výkonu?

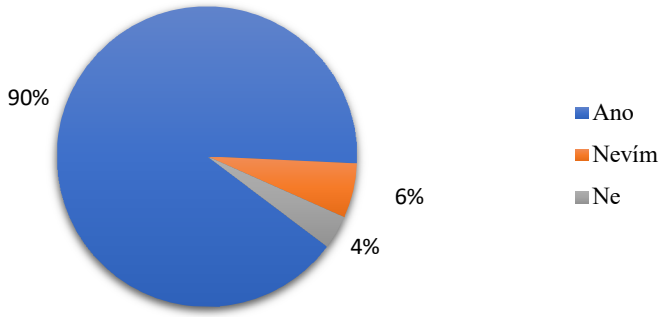
Tato otázka zkoumá znalost práva na odmítnutí zdravotního výkonu. Opět se jedná o otázku, u které se předpokládají téměř stoprocentně správné odpovědi.

Tabulka č. 16 – Odmítnutí výkonu

Odpověď	Počet
Ano	369
Nevím	24
Ne	15
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 10 – Odmítnutí výkonu



Zdroj: vlastní zpracování

U této otázky byl ještě menší počet správných odpovědí, konkrétně 90 %, než u otázky č. 8, u které byly také očekávány většinou správné odpovědi. Vzhledem k neznalosti může dojít k situaci, kdy pacient podstoupí nějaký výkon i přesto, že s ním nesouhlasí.

Zajímavý byl však věk respondentů. Polovina respondentů, kteří označili chybně „ne“, byli starší než 51, z toho 4 respondenti byli v kategorii 71 let a více. Je možné, že se zde projevuje princip paternalismu, který je analyzován v teoretické části této diplomové práce v kapitole 3.6.1. Historický vývoj. Tyto osoby pak plně spoléhají na osobu lékaře.

11. Máte právo na zamezení sdělování informací o svém zdravotním stavu osobám blízkým či dalším osobám?

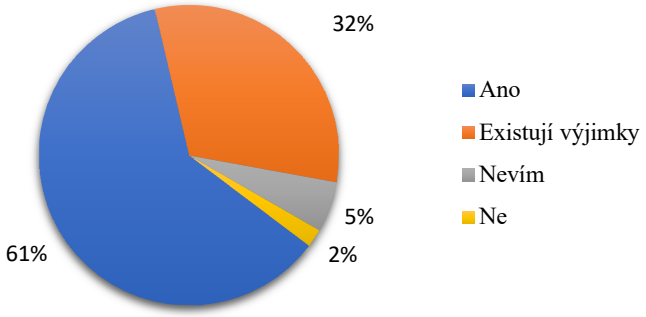
Jedenáctá otázka zkoumala znalost práva týkající se informovaného souhlasu, konkrétně možnosti uvedení osoby, o které si pacient nepřeje, aby byla informována o jeho zdravotním stavu.

Tabulka č. 17 – Sdělování informací

Odpověď	Počet
Ano	249
Existují výjimky	129
Nevím	22
Ne	8
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 11 – Sdělování informací



Zdroj: vlastní zpracování

Z 378 respondentů, kteří věděli, že právo na zamezení sdělování informací o svém zdravotním stavu mají, pouze 129 respondentů, tedy 32 % z celkového počtu, vědělo, že toto právo není neomezené. Existují totiž výjimky uvedené v kapitole 6.3.2 Jednotlivá práva pacientů.

12. Stalo se vám někdy, že vás lékař dostatečně neinformoval o Vašem zdravotním stavu?

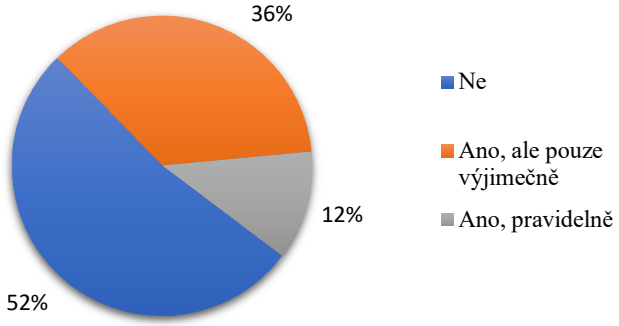
Každý pacient má právo na informace. Tato otázka byla zaměřena na to, zdali je toto právo porušováno a pacientům se tak stává, že nejsou vždy dostatečně informováni.

Tabulka č. 18 – Informování lékařem

Odpověď	Počet
Ne	214
Ano, ale pouze výjimečně	146
Ano, pravidelně	48
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 12 – Informování lékařem



Zdroj: vlastní zpracování

Ze 408 respondentů zkušenost, že by nebyli dostatečně informováni lékařem, nemá 52 % dotazovaných. Na druhou stranu, 12 % dotazovaných se s nedostatečným informováním setkává pravidelně.

13. Ocenil (a) byste, kdyby Vás lékař více informoval?

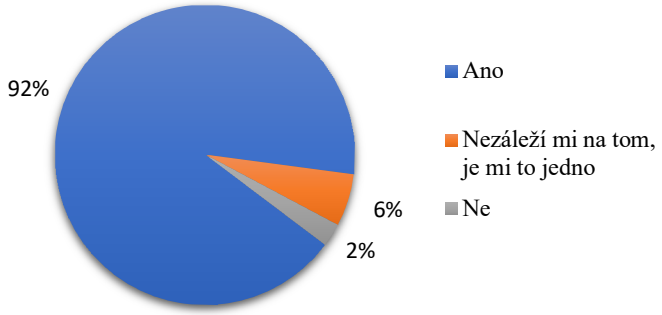
Tato otázka přímo navazovala na předešlou otázku. Byla pokládána pouze respondentům, kteří u předešlé otázky odpověděli, že se setkávají s nedostatečným informováním o svém zdravotním stavu ze strany lékaře, tedy zvolili možnost „Ano, ale pouze výjimečně“ nebo „Ano, pravidelně“.

Tabulka č. 19 – Více informací

Odpověď	Počet
Ano	180
Nezáleží mi na tom, je mi to jedno	11
Ne	5
Celkem	**196**

Zdroj: vlastní zpracování

Graf č. 13 – Více informací



Zdroj: vlastní zpracování

Většina respondentů, konkrétně 92 %, by v tomto případě ocenila, kdyby je lékař více informoval. Všech 5 respondentů, kteří o více informací nestojí, byly ženy. U 4 se jednalo o ty, kteří se s nedostatečným informováním setkali pouze výjimečně.

14. Může Vám informace o Vašem zdravotním stavu poskytnout i nelékařský zdravotnický personál (např. sestřička)?

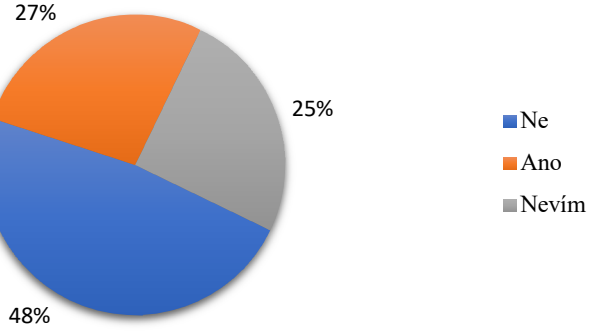
Tato otázka zkoumala, zdali respondenti vědí, kdo jim může podávat informace o jejich zdravotním stavu. V praxi je totiž poměrně běžné, že informace podává např. sestřička, a to obzvlášť při telefonickém sdělování výsledků.

Tabulka č. 20 – Nelékařský personál

Odpověď	Počet
Ne	195
Ano	111
Nevím	102
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 14 – Nelékařský personál



Zdroj: vlastní zpracování

Téměř polovina respondentů, konkrétně 48 %, ví, že nelékařský personál informace o zdravotním stavu sdělovat nemůže. Avšak 27 % respondentů si myslí, že ano. Lze se domnívat, že se s touto situací běžně setkávají, a proto volili tuto odpověď. Dalších 27 % respondentů si u této otázky nebylo jistých a odpovědělo „Nevím“.

15. Využil (a) jste někdy možnost konzultace s jiným lékařem/v jiném zdravotnickém zařízení?

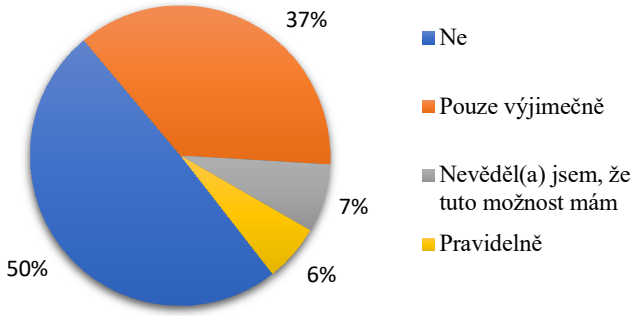
Tato otázka se zajímala o to, zdali respondenti využívají svého práva na konzultaci u jiného lékaře nebo v jiném zdravotnickém zařízení, případně zdali vůbec ví, že toto právo mají.

Tabulka č. 21 – Konzultace

Odpověď	Počet
Ne	202
Pouze výjimečně	151
Nevěděl (a) jsem, že tuto možnost mám	30
Pravidelně	25
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 15 – Konzultace



Zdroj: vlastní zpracování

Přesně polovina dotazovaných možnost konzultace s jiným lékařem případně v jiném zdravotnickém zařízení nikdy nevyužila a dalších 7 % respondentů také ne, protože vůbec nevědělo, že tuto možnost má. Dalších 37 % dotázaných možnosti konzultace využívá pouze výjimečně. Pouze 25 % dotazovaných uvedlo, že možnost konzultace využívá pravidelně.

Nutno konstatovat, že z hlediska zdravotnictví a efektivního čerpání finančních prostředků je tento výsledek uspokojivý.

16. Myslíte si, že má pacient právo nahlížet do své zdravotnické dokumentace?

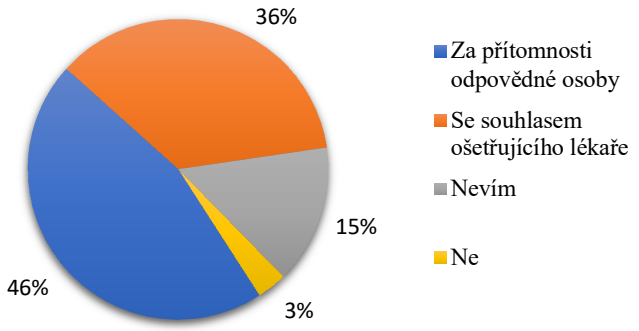
Další čtyři otázky se týkaly zdravotnické dokumentace. První z nich se zaměřovala na to, zdali respondenti vědí, že mají právo do ní nahlížet.

Tabulka č. 22 – Nahlížení

Odpověď	Počet
Za přítomnosti odpovědné osoby	187
Se souhlasem ošetřujícího lékaře	147
Nevím	61
Ne	13
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 16 – Nahlížení



Zdroj: vlastní zpracování

Fakt, že pacient má právo do své zdravotnické dokumentace nahlížet, vědělo 82 % respondentů. Pouze necelá polovina dotazovaných, konkrétně 46 % respondentů vědělo, že k nahlížení má právo pouze za přítomnosti odpovědné osoby. Souhlas ošetřujícího lékaře, na nahlížení není potřeba a nemá v této věci žádný vliv. Tuto možnost chybně označilo 36 % respondentů. Pouze 3 % respondentů si myslí, že právo na nahlížení do své zdravotnické dokumentace nemají.

17. Využil (a) jste někdy možnosti nahlédnutí do zdravotnické dokumentace?

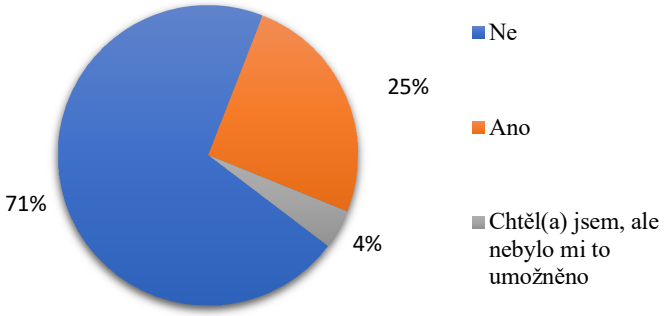
Druhá otázka týkající se zdravotnické dokumentace byla položena pouze 334 respondentům, kteří věděli, že mají právo na nahlížení do své zdravotnické dokumentaci, bez ohledu na to, zdali znali podmínky nahlížení či nikoli.

Tabulka č. 23 – Využití nahlédnutí

Odpověď	Počet
Ne	236
Ano	84
Chtěl (a) jsem, ale nebylo mi to umožněno	14
Celkem	**334**

Zdroj: vlastní zpracování

Graf č. 17 – Využití nahlédnutí



Zdroj: vlastní zpracování

Většina respondentů, konkrétně 72 %, možnost nahlédnutí do své zdravotnické dokumentace ještě nikdy nevyužila.

Je velice zajímavé a zarážející, že u 25 % respondentů, kteří tuto možnost využili, jich pouze 52 % znalo podmínky nahlížení, tedy že nahlížení je možné pouze za přítomnosti odpovědné osoby. U těchto respondentů byla předpokládána mnohem vyšší znalost tohoto práva, obzvlášť s ohledem na to, že respondenti, kteří možnost nahlížení nevyužili, podmínky znali ve větším rozsahu, konkrétně je znalo 57 % dotázaných.

Další 4 % respondentů možnost chtěli využít, ale nahlédnutí jim nebylo umožněno. Ani u těchto respondentů nebyla prokázána vyšší znalost podmínek k nahlédnutí, podmínky znala přesně polovina respondentů.

18. Může být pořízení kopie z vlastní zdravotnické dokumentace zpoplatněno?

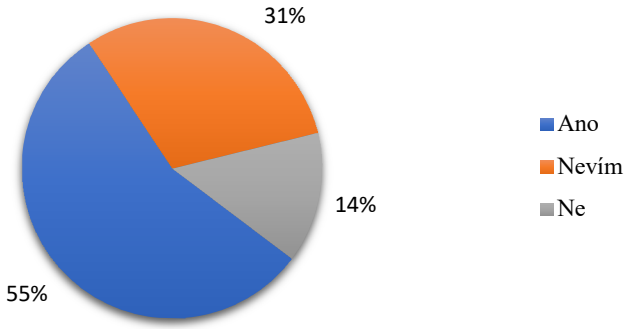
Třetí otázka týkající se zdravotnické dokumentace zkoumala znalost, zdali může být nahlédnutí zpoplatněno. Opět byla pokládána pouze respondentům, kteří věděli, že mají právo na nahlížení do své zdravotnické dokumentaci, bez ohledu na to, zdali znali podmínky nahlížení či nikoli.

Tabulka č. 24 – Pořízení kopie

Odpověď	Počet
Ano	185
Nevím	102
Ne	47
Celkem	**334**

Zdroj: vlastní zpracování

Graf č. 18 – Pořízení kopie



Zdroj: vlastní zpracování

Větší polovina dotázaných, konkrétně 55 %, uvedla správnou odpověď, tedy že pořízení kopie ze zdravotnické dokumentace může být zpoplatněno. 31 % respondentů odpověď nevědělo a 14 % respondentů si myslelo, že pořízení kopie zpoplatněno být nemůže.

U této otázky došlo na rozdíl od předchozí otázky k potvrzení předpokladu, že respondenti, kteří již někdy do své zdravotnické dokumentace nahlíželi, budou oproti těm, co do ní nikdy nenahlíželi spíše vědět, zdali může být pořízení kopie zpoplatněno. Správnou

odpověď označilo 63 % respondentů, oproti 57 % respondentům, kteří do své zdravotnické dokumentace nenahlíželi. I přes to, že byl předpoklad potvrzen, byl očekáván větší rozdíl.

19. Jakým způsobem dochází k předání zdravotnické dokumentace při změně lékaře?

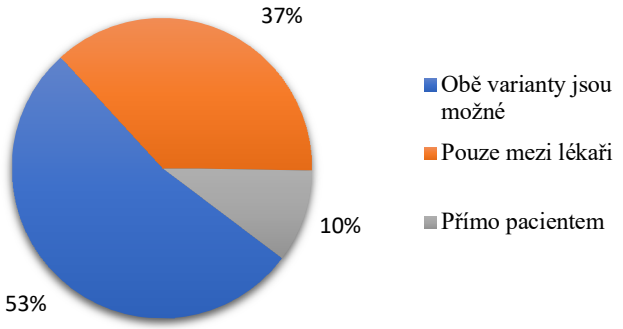
Poslední otázka týkající se zdravotnické dokumentace byla zaměřena na její předávání. Již byla pokládána opět všem 408 respondentům.

Tabulka č. 25 – Předávání

Odpověď	Počet
Obě varianty jsou možné	216
Pouze mezi lékaři	151
Přímo pacientem	41
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 19 – Předávání



Zdroj: vlastní zpracování

Jde o druhou otázku, kde je na prvním místě špatná odpověď. 63 % respondentů si myslí, že zdravotnická dokumentace může být předávána samotným pacientem, s tím, že 10 % respondentů si myslí, že jde o jedinou možnost.

Správně, tedy že k předávání zdravotnické dokumentace může docházet pouze mezi lékaři, v tomto případě odpovědělo pouze 37 % respondentů. Dá se předpokládat, že výsledky jsou dány zkušeností respondentů.

20. Víte, že GDPR přináší pacientům rozšířená i zcela nová práva?

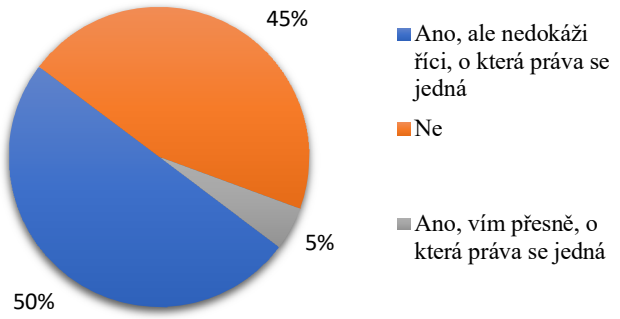
Dalších 8 otázek se týkalo GDPR. První otázka byla obecná a zkoumala, zdali respondenti vůbec vědí, že jim GDPR přineslo rozšířená i zcela nová práva.

Tabulka č. 26 – Novinky GDPR

Odpověď	Počet
Ano, ale nedokáži říci, o která práva se jedná	204
Ne	185
Ano, vím přesně, o která práva se jedná	19

Zdroj: vlastní zpracování

Graf č. 20 – Novinky GDPR



Zdroj: vlastní zpracování

I přes to, že GDPR bylo velkým tématem, 45 % dotázaných vůbec nevědělo, že došlo k rozšíření i zavedení zcela nových práv pacientů. Pouze 5 % respondentů uvedlo, že o této novince ví, a zároveň že i přesně ví, o která práva se jedná.

21. Víte, jaká máte nová práva po účinnosti GDPR?

Tato otázka navazuje na předešlou otázku. Byla pokládána pouze respondentům, kteří věděli, že GDPR přineslo pacientům rozšířená i zcela nová práva. Pokládání této otázky respondentům, kteří o této novince nic nevědí, by postrádalo smysl a zbytečně by tak byly ovlivněny výsledky tohoto dotazníkového šetření.

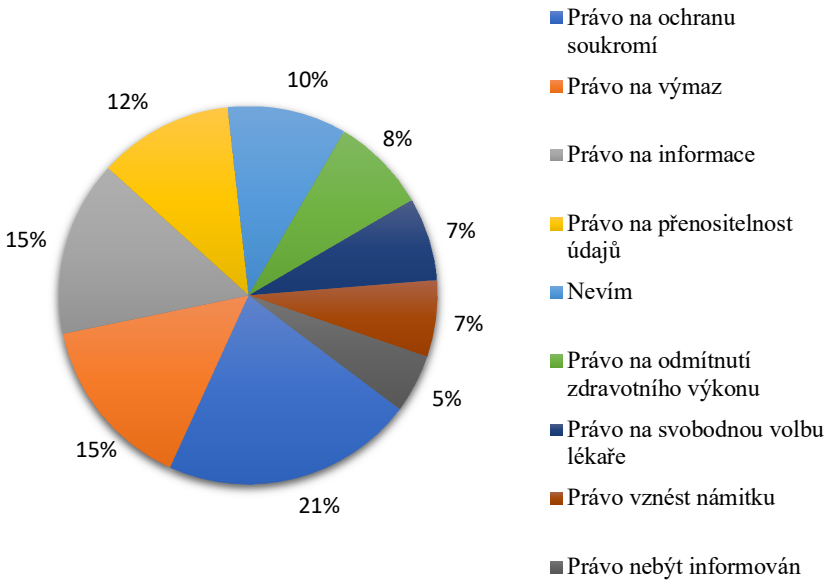
Vzhledem k tomu, že GDPR přineslo 3 zcela nová práva (právo na výmaz, přenositelnost a vznést námitku), mohli u této otázky respondenti zvolit více možných odpovědí.

Tabulka č. 27 – Nová práva po účinnosti GDPR

Odpověď	Počet
Právo na ochranu soukromí	121
Právo na výmaz	84
Právo na informace	84
Právo na přenositelnost údajů	65
Nevím	57
Právo na odmítnutí zdravotního výkonu	46
Právo na svobodnou volbu lékaře	40
Právo vznést námitku	37
Právo nebýt informován	28

Zdroj: vlastní zpracování

Graf č. 21 – Nová práva po účinnosti GDPR



Zdroj: vlastní zpracování

Nejčetnější odpovědí bylo právo na ochranu soukromí, což ale není správná odpověď. Jedna ze tří správných odpovědí „Právo vznést námitku“, skončila až na předposledním místě.

Co se týká těch, kteří v předchozí otázce uvedli, že o novince vědí, ale nedokáží přesně říct, o která práva se jedná, byli z 204 respondentů 2 respondenti, kteří přesto dokázali odpovědět zcela správně, tedy označit všechna 3 nová práva, aniž by označili chybně i nějaká další práva. Jednalo se o ženy s vyšším odborným nebo vysokoškolským vzděláním, které obě pracují ve zdravotnictví. Dalších 15 respondentů dokázalo označit správná práva, ale zároveň chybně označili i nějaké další právo, které není novinkou. Z toho však 3 respondenti označili všechna nabízená práva.

Co se týká těch, kteří v předchozí otázce označili, že vědí konkrétně, o jaká práva se jedná, zcela správně odpověděl z 19 respondentů pouze jeden respondent. Jednalo se o ženu s vyšším odborným nebo vysokoškolským vzděláním, která nepracuje ve zdravotnictví. Dalších 6 respondentů dokázalo označit správná práva, ale zároveň chybně označili i nějaké další právo, které není novinkou. Z toho ale 5 respondentů označilo všechna nabízená práva.

22. Víte, co znamená právo na přenositelnost údajů?

Tato otázka zkoumá, jestli si respondenti něco představí pod jedním z nových práv, konkrétně právem na přenositelnost údajů. Je pouze obecná a zajímá se o to, zdali tento pojem již respondenti někdy slyšeli, a pokud ano, v jakém rozsahu mají informace.

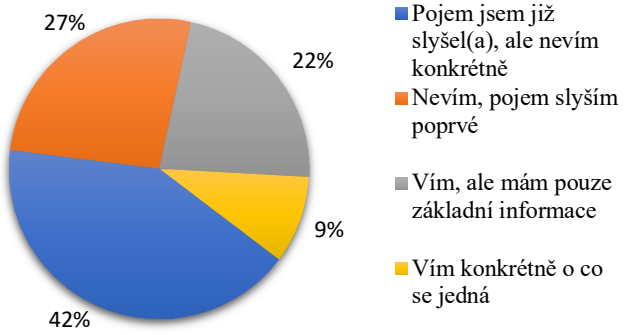
Tato otázka byla opět pokládána pouze respondentům, kteří věděli, že GDPR přineslo pacientům rozšířená i zcela nová práva.

Tabulka č. 28 – Přenositelnost

Odpověď	Počet
Pojem jsem již slyšel (a), ale nevím konkrétně	93
Nevím, pojem slyším poprvé	59
Vím, ale mám pouze základní informace	50
Vím konkrétně, o co se jedná	21
Celkem	**223**

Zdroj: vlastní zpracování

Graf č. 22 – Přenositelnost



Zdroj: vlastní zpracování

Z 223 respondentů, kterým tato otázka byla položena, pojem někdy slyšelo 73 % respondentů, avšak pouze 9 % respondentů ví konkrétně, o co se jedná. Zbývajících 27 % respondentů pojem nikdy neslyšelo.

23. Vztahuje se GDPR i na osobní údaje zemřelých?

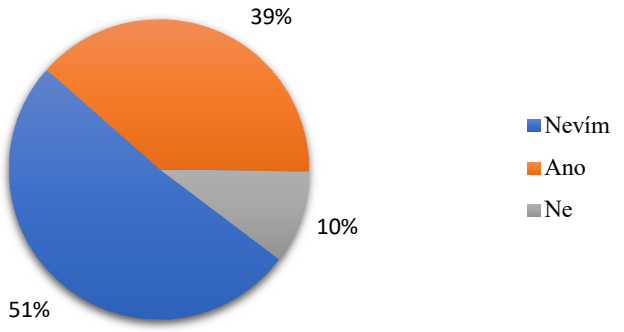
GDPR bylo velkým tématem, avšak informace tom, zdali se práva dle GRPD vztahují i na údaje zemřelých příliš nezaznívala. Proto byla zařazena tato otázka, která testuje povědomí respondentů o této problematice.

Tabulka č. 29 – Zemřelí

Odpověď	Počet
Nevím	209
Ano	158
Ne	41
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 23 – Zemřelí



Zdroj: vlastní zpracování

Dle předpokladu více než polovina respondentů, konkrétně 51 % označilo odpověď „Nevím. Dalších 39 % dotázaných se chybně domnívá, že práva dle GDPR se vztahují i na údaje zemřelých. Správnou odpověď „Ne“ označilo pouze 10 % respondentů. V 71 % se jednalo o respondenty s vyšším odborným nebo vysokoškolským vzděláním. Zastoupení mužů a žen bylo rovnoměrné (vzhledem k jejich zastoupení v celkovém vzorku).

24. Může Vám lékař sdělit výsledek vyšetření po telefonu či emailem?

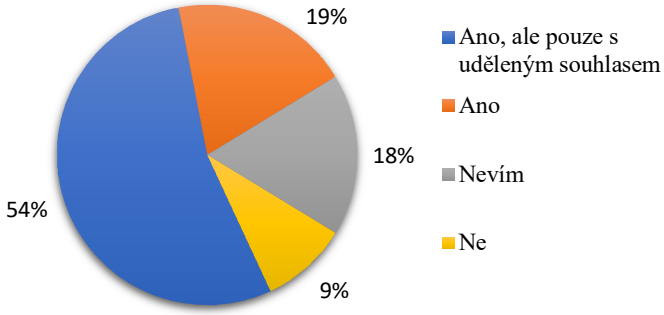
Ke sdělení výsledků po telefonu či po emailu je nyní vyžadován souhlas. Tato otázka zkoumající znalost této problematiky byla položena všem 408 respondentům.

Tabulka č. 30 – Sdělení výsledku

Odpověď	Počet
Ano, ale pouze s uděleným souhlasem	220
Ano	79
Nevím	71
Ne	38
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 24 – Sdělení výsledku



Zdroj: vlastní zpracování

Něco málo přes polovinu dotázaných, konkrétně 54 %, označilo správnou odpověď, tedy že „Ano, ale pouze s uděleným souhlasem“. Odpověď na otázku nevědělo 18 % respondentů a 9 % respondentů si myslí, že lékař výsledky po telefonu nebo emailem nemůže sdělovat. Mezi těmito respondenty nebyl nalezen žádný společný ukazatel.

25. Podal (a) jste v souvislosti s účinností GDPR nějakou žádost?

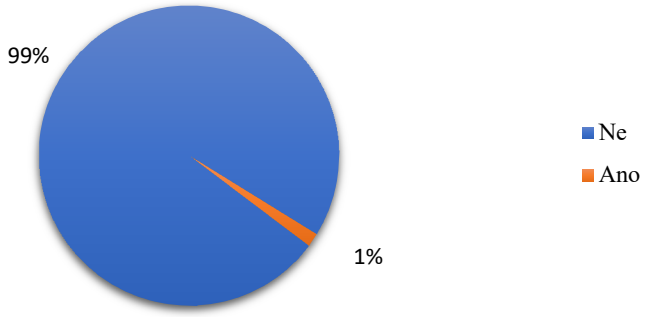
Subjekty osobních údajů se mohou dožadovat svých práv v souvislosti s GDPR prostřednictvím podání žádosti. Pro většinu správců a zpracovatelů se jednalo o velké téma a byly prováděny velké přípravy, aby mohlo být žadatelům případně vyhověno. Tato otázka zkoumá, zdali se opravdu jedná o tak velké téma a lidé žádosti ve velkém využívají, jak bylo předpokládáno.

Tabulka č. 31 – Žádost

Odpověď	Počet
Ne	402
Ano	4
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 25 – Žádost



Zdroj: vlastní zpracování

Z výsledků této otázky je zřejmé, že možnost podat žádost není příliš využívána. Využili ji pouze 4 respondenti tvořící necelé 1 %. Jednalo se o respondenty s vyšším odborným nebo vysokoškolským vzděláním, 3 ze 4 byli muži, z toho 1 pracující ve zdravotnictví.

Obavy správců a zpracovatelů osobních údajů tak nebyly na místě. Tímto výsledkem se i potvrdilo, že nízký počet žádostí evidovaný Nemocnicí není ničím zvláštním a ojedinělým.

26. Jakého práva se žádost týkala?

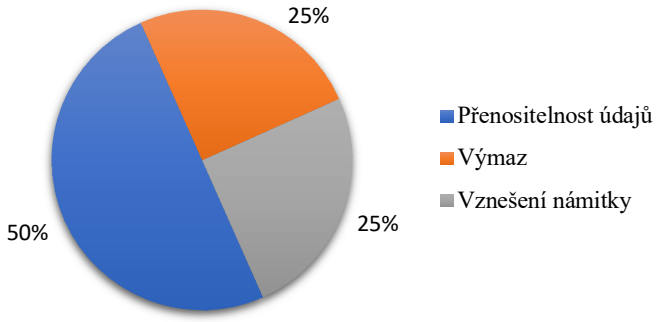
Další otázka navazovala na předchozí otázku. Byla pokládána pouze respondentům, kteří využili možnost podání žádosti. Vzhledem k tomu, že žádost se nemusí týkat pouze jednoho práva, mohl respondent označit více možných odpovědí.

Tabulka č. 32 – Žádost (právo)

Odpověď	Počet
Právo na přenositelnost údajů	2
Právo na výmaz	1
Právo vznést námitku	1

Zdroj: vlastní zpracování

Graf č. 26 – Žádost (právo)



Zdroj: vlastní zpracování

Všichni 4 respondenti uvedli, že se prostřednictvím žádosti dožadovali pouze jednoho práva. Právo vznést námitku využila žena, ostatní žádosti byly podány muži.

27. S jakým výsledkem byla Vaše žádost vyřízena?

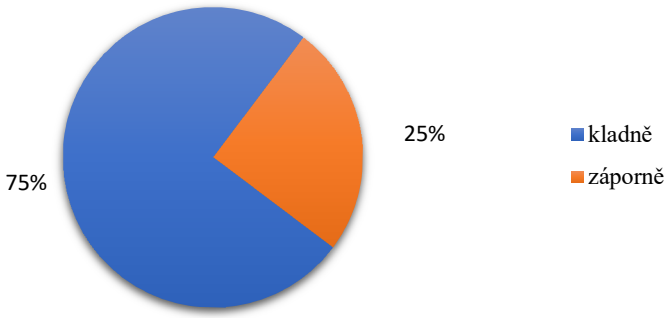
Jedná se o druhou otázku navazující na otázku č. 25, zkoumá, s jakým výsledkem byly podané žádosti vyřízeny.

Tabulka č. 33 – Výsledek žádosti

Odpověď	Počet
kladně	3
záporně	1
Celkem	**4**

Zdroj: vlastní zpracování

Graf č. 27 – Výsledek žádosti



Zdroj: vlastní zpracování

Většina žádostí byla vyřízena kladně, pouze jedna záporně. Záporně vyřízená žádost se týkala práva na výmaz, podala ji muž s vyšším odborným nebo vysokoškolským vzděláním, ve věku 26 – 50 let, žijící na vesnici do 2 000 obyvatel, nepracující ve zdravotnictví. Ostatní respondenti, kterým byla žádost vyřízena kladně, jsou také s vyšším odborným či vysokoškolským vzděláním a žijí ve velkoměstě nad 500 001 obyvatel.

28. Jaký je Váš věk?

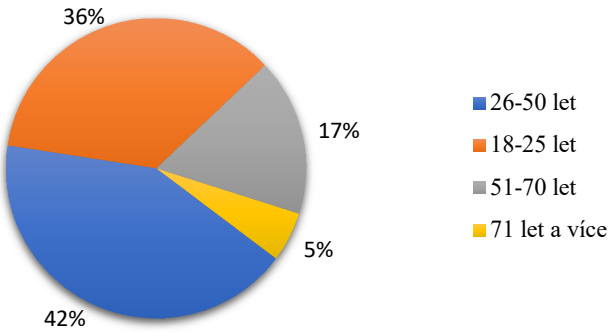
Poslední skupinou otázek byly otázky sloužící ke statistickému zpracování získaných dat. První z otázek zkoumala věk respondentů.

Tabulka č. 34 – Věk

Odpověď	Počet
26 – 50 let	172
18 – 25 let	145
51 – 70 let	69
71 let a více	22
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 28 – Věk



Zdroj: vlastní zpracování

Respondenti byli rozděleni do čtyř věkových kategorií. Nejvíce respondentů se podařilo nasbírat v nejširší kategorii 26 – 50 let, tito respondenti tvořili 42 %. Naopak nejméně respondentu je v kategorii 71 let a více, pouze 5 % respondentů.

29. Jaké je Vaše pohlaví?

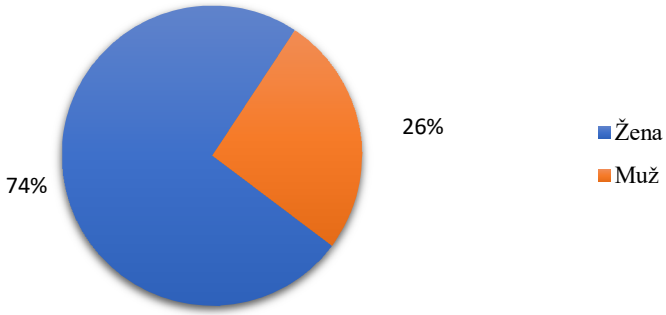
Další otázka zkoumala pohlaví respondentů.

Tabulka č. 35 – Pohlaví

Odpověď	Počet
Žena	302
Muž	106
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 29 – Pohlaví



Zdroj: vlastní zpracování

Ve vzorku byly početněji zastoupeny ženy, tvořily 74 %, což bohužel neodpovídá demografickému rozložení České republiky. Tuto nerovnoměrnost může způsobovat větší ochota žen vyplňovat dotazníková šetření.

30. Jaké je Vaše nejvyšší ukončené vzdělání?

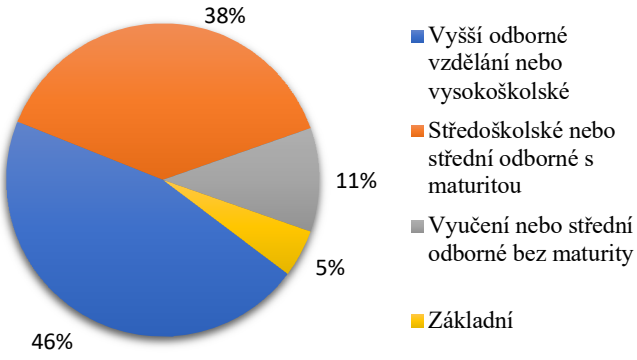
Třicátá otázka byla zaměřena na nejvyšší ukončené vzdělání daných respondentů.

Tabulka č. 36 – Vzdělání

Odpověď	Počet
Vyšší odborné vzdělání nebo vysokoškolské	187
Středoškolské nebo střední odborné s maturitou	157
Vyučení nebo střední odborné bez maturity	44
Základní	20
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 30 – Vzdělání



Zdroj: vlastní zpracování

Nejvíce respondentů disponuje vyšším odborným nebo vysokoškolským vzděláním. Tito respondenti tvoří celkem 46 %, což také bohužel neodpovídá zastoupení v České republice. Naopak nejméně respondentů disponuje základním vzděláním, pouze 5 %.

31. Pracujete ve zdravotnictví?

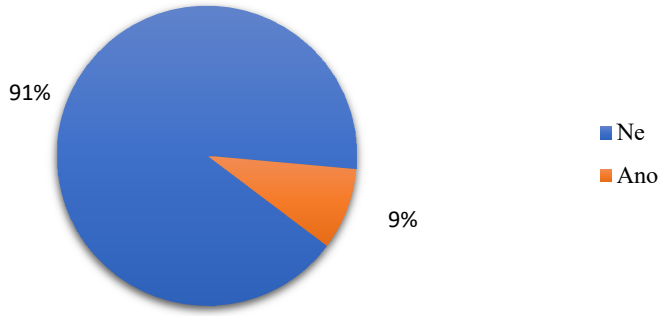
Tato otázka byla položena z toho důvodu, protože bylo předpokládáno, že lidé pracující ve zdravotnictví budou mít větší přehled a budou se v právech pacientů lépe orientovat.

Tabulka č. 37 – Zaměstnání

Odpověď	Počet
Ne	372
Ano	36
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 31 – Zaměstnání



Zdroj: vlastní zpracování

Podíl respondentů pracujících ve zdravotnictví tvořil 9 %. To je poměrně vysoké číslo, nebylo však rozlišováno, na jaké pozici respondent pracuje. Může se tedy jednat i o respondenty pracující sice ve zdravotnictví ale ne se zdravotnickým vzděláním a na zdravotnické pozici. Při další analýze výstupních dat se ukázalo, že lidé pracující ve zdravotnictví dosahovali lepších výsledků, a to jak v první, tak ve druhé části dotazníku.

32. Kolik má vaše bydliště obyvatel?

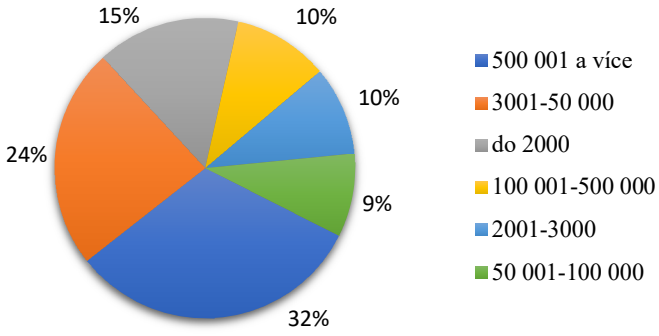
Poslední otázka zkoumala velikost bydliště respondentů.

Tabulka č. 38 – Velikost bydliště

Odpověď	Počet
500 001 a více	130
3 001 – 50 000	97
do 2000	63
100 001 – 500 000	42
2 001 – 3 000	39
50 001 – 100 000	37
Celkem	**408**

Zdroj: vlastní zpracování

Graf č. 32 – Velikost bydliště



Zdroj: vlastní zpracování

Většina respondentů, konkrétně 32 % žije ve velkoměstě nad 500 001 obyvatel. Další početnou kategorií tvořící 24 % jsou respondenti, jejichž bydliště má 3 001 – 50 000 obyvatel. Nejmenší skupinou jsou respondenti, jejich bydliště má 50 001 – 100 000 obyvatel, ti tvořili 9 %.

4.6.4 Shrnutí závěrů a vyhodnocení hypotéz

Účelem celého dotazníkového šetření bylo zjištění informovanosti pacientů o svých právech v souvislosti s poskytováním zdravotní péče, a zdali svá práva aktivně využívají a zároveň zjištění povědomí o nových právech v souvislosti s účinností GDPR. Výsledky jsou posouzeny na základě dvou předem stanovených hypotéz, kterými byly:

H1: Pacienti neznají svá práva v souvislosti s poskytováním zdravotní péče.

H2: Pacienti nemají povědomí o nových právech v souvislosti s GDPR.

V první části dotazníku byly pokládány otázky na obecná práva, které měly potvrdit či vyvrátit H1. Z celkového počtu 408 respondentů tuto část dokázali vyplnit správně pouze 2 respondenti. Jednalo se o muže a ženu, oba s vyšším odborným či vysokoškolským vzděláním, žijící ve velkoměstě nad 500 001 obyvatel.

Respondenti nejčastěji vědí, že mají právo na poskytnutí informací o léčbě jejich ošetřujícím lékařem, tohoto práva si bylo vědomo 96 % respondentů. S velmi dobrým výsledkem skončilo také právo na odmítnutí zdravotního výkonu, zde správně odpovědělo 90 % respondentů. Naopak nejhůře si respondenti v této části dotazníku vedli u otázky

týkající se práva na zamezení sdělování informací o svém zdravotním stavu osobám blízkým či dalším osobám. Povědomí o tomto právu a jeho omezeních mělo pouze 32 % respondentů. Dalším právem s velmi špatným výsledkem bylo právo nebýt informován o léčbě. Tohoto práva si je vědomo jen 36 % respondentů.

Z výsledku dotazníkového šetření vyplynulo, že lidé svá práva v souvislosti s poskytováním zdravotní péče příliš neznají, průměrně bylo správně 54 % odpovědí. Po odečtení výše uvedených významných výkyvů se výsledek snížil na 49 %. U otázek týkajících se aktivního využívání práv odpovědělo kladně průměrně 34 % respondentů.

Z výše uvedených výsledků tedy vyplývá, že došlo k potvrzení H1.

V druhé části dotazníku byly pokládány otázky zaměřené na GDPR, které měly potvrdit či vyvrátit H2.

Z celkového počtu 408 respondentů tuto část dokázali vyplnit správně opět pouze 2 respondenti. Tentokrát se jednalo o ženy, obě s vyšším odborným či vysokoškolským vzděláním, pracující ve zdravotnictví.

Nejlépe v této části dotazníku dopadla otázka týkající se sdělení výsledku vyšetření po telefonu či emailem. To, že je nyní potřeba podepsání souhlasu vědělo 54 % respondentů. Naopak nejhůře dopadla otázka, zdali se GDPR vztahuje i na údaje zemřelých. Že ne, vědělo pouze 10 % respondentů.

I přes to, že GDPR bylo velkým tématem, 45 % dotázaných vůbec nevědělo, že došlo k rozšíření i zavedení zcela nových práv pacientů. Pouze 5 % respondentů uvedlo, že o této novince ví, a zároveň že i přesně ví, o která práva se jedná. Po položení testujících otázek se však ukázalo, že přesně ví, o která práva se jedná pouze 1 % respondentů.

Vzhledem k výsledkům této části dotazníkového šetření došlo k jasnému potvrzení H2.

Co se týká celkového zhodnocení dotazníkového šetření, 21 % respondentů se domnívá, že svá práva zná dobře a 61 % si myslí, že svá práva zná pouze částečně. Ze 408 respondentů však ani jeden respondent nedokázal odpovědět na všechny otázky správně. Tento výsledek je alarmující a je překvapující především u respondentů pracujících ve zdravotnictví, u kterých by se vysoká znalost práv pacientů dala očekávat. Avšak i přesto tito respondenti dosahovali mírně lepších výsledků, a to v obou částech dotazníkového šetření.

V rámci šetření byl dále posuzován vztah mezi dosaženými výsledky a pohlavím. Zde obě pohlaví dosahovala poměrně vyrovnaných výsledků, výkyvy se objevovaly pouze

u jednotlivých otázek. Celkově se dají považovat za informovanější ženy. Co se však týká GDPR, byly naopak mírně lepší muži. Je nutné však upozornit, že vzorek neodpovídal demografickému rozložení České republiky.

Lepších výsledků dosahovali především respondenti s vyšším odborným či vysokoškolským vzděláním. Zajímavé je, že u některých otázek došlo k výrazným výkyvům, kdy nejlépe odpovídali lidé se základním vzděláním. Jednalo se např. o otázku týkající se předávání zdravotnické dokumentace, vědělo ji v této kategorii o 20 % více respondentů oproti jiným kategoriím.

Co se týká věkové kategorie, výsledky byly poměrně vyrovnané až na kategorii 70 let a více. Zde byly výsledky podprůměrné. Dalo by se předpokládat, že se jedná o přetrvávající paternalistický model, na který byla většina respondentů v této věkové kategorii zvyklá. Na druhou stranu však velké množství starších respondentů uvádělo, že by ocenili, kdyby je lékař více informoval.

5 Výsledky a diskuse

5.1 Výsledky teoretické části práce

Právní úprava (3.1 Obecně k právní úpravě) ochrany osobních údajů sahá až do 18. století, dnes je upravena především v zákoně č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a nově právě GDPR. V době psaní této diplomové práce byl v České republice ve schvalovacím procesu zákon o zpracování osobních údajů, kterým bude nahrazen zákon č. 101/2000 Sb., o ochraně osobních údajů. Tento zákon by měl být schválen co nejdříve, protože GDPR nejen že umožňuje, ale v několika desítkách ustanoveních dokonce ukládá, úpravu národními právními předpisy.

GDPR zavedlo nové pojmy (3. 2 Vybrané pojmy GDPR), přičemž nejvýraznějším je DPO neboli pověřenec pro ochranu osobních údajů. Na GDPR se velice zajímavé, že oproti jiným právním předpisům pojmy nedefinuje zcela přesně. Příkladem může být pojem doba nezbytně nutná. GDPR se na ni odkazuje, ale jak je tato doba ve skutečnosti dlouhá, není nikde stanoveno. Dalšími takovými pojmy jsou např. přiměřenost, relevantnost či omezení na nezbytný rozsah.

Další zajímavostí, ke které bylo v rámci analýzy GDPR dojito je, že GDPR obsahuje pouze cíl a konečný výsledek, ke kterému má každý správce či zpracovatel osobních údajů dojít. Není zde stanoven žádný konkrétní postup a návod, jak k ochraně osobních údajů přistupovat. Jsou v něm uvedeny pouze základní zásady a principy (3.3 Zásady a principy GDPR), kterými je třeba se řídit. Z toho tedy vyplývá, že jak bude správce či zpracovatel postupovat, to už je zcela na něm.

V případě, kdy však dojde k úniku osobních údajů (3.2.8 Dozorová činnost), při kterých může dojít k rizikům pro práva a svobodu fyzických osob, má správce povinnost tuto skutečnost oznámit dozorovému úřadu. V České republice pak konkrétně Úřadu pro ochranu osobních údajů. V praxi je ale velmi složité určit, který únik oznámit a který nikoli. Stejně tomu tak je i s oznámením subjektu osobních údajů. S touto problematikou se setkala i Nemocnice. Možností je poté využití konzultace externího odborníka, avšak bylo by vhodné stanovit jasná kritéria, aby k této problematice jednotliví správci přistupovali jednotně.

Pokud dojde k porušení GDPR, může nově Úřad pro ochranu osobních údajů správci udělit až mnohamilionovou sankci (3.2.9 Pokuty a sankce). Platí ale pravidlo, že výše sankcí nesmí být likvidační. Je však velmi problematické určit, co likvidační není a co už je.

Pozornost také byla věnována oblasti zdravotnictví (3.5 Specifika GDPR pro resort zdravotnictví), jelikož zde dochází často ke zpracování zvláštní kategorie osobních údajů neboli citlivých osobních údajů, pro jejichž zpracování platí přísnější podmínky. Ke zpracování může docházet na základě souhlasu subjektu údajů nebo na základě zákonné povinnosti. Souhlasy mohly mnohým zpracovatelům přidělat spoustu potíží, jelikož i veškeré souhlasy poskytnuté ještě před účinností GDPR musí být nyní s GDPR plně v souladu. To mohl být problém obzvláště v případě velkého množství souhlasů v listinné podobě, což by řešila elektronizace a následná databáze veškerých poskytnutých souhlasů.

Opravdu velkou pozornost si zaslouží práva, ale také povinnosti pacientů (3.6 Práva pacientů). Vzhledem k tomu, že každý se v průběhu svého života může stát pacientem, a ve většině případů se jím také stane, měl by každý svá práva znát a měl by si jich být vědom.

Kromě rozšíření stávajících práv s sebou GDPR přineslo i tři nová práva (3.6.3 Nová práva v souvislosti s GDPR), kterými jsou právo na výmaz, právo na přenositelnost údajů a právo vznést námitku. Každý ze správců či zpracovatelů se musel připravit na to, že je budou chtít lidé prostřednictvím žádostí uplatňovat. Jak ale vyplývá ze zkušeností v Nemocnici, lidé možnost podání žádosti zatím příliš nevyužívají. To samé bylo potvrzeno i provedeným dotazníkovým šetřením.

V rámci vyřizování těchto žádostí je velmi důležitým krokem ověření totožnosti žadatele. V případě ověřování totožnosti však dochází k paradoxní situaci. Může dojít k případu, kdy např. pacient žádá o uplatnění práva na výmaz. Aby k němu ale mohlo dojít, je nutné danou osobu ověřit, čímž však dochází k dalšímu sběru a zpracování osobních údajů. Tento problém bude velice obtížné řešit, jelikož ověření žadatele je nezbytné.

5.2 Výsledky praktické části práce

Praktická část této diplomové práce se zabývala implementací GDPR (4.2 Proces implementace GDPR) v anonymně uváděné Nemocnici. Cílem implementace bylo, aby veškeré zpracování osobních údajů v Nemocnici probíhalo v souladu s GDPR, tedy s veškerými požadavky a povinnostmi vyplývajícími z GDPR, které jsou analyzovány v teoretické části této diplomové práce.

Velmi důležitým krokem v celé implementaci bylo stanovení jednotlivých kroků, které povedou k naplnění pravidel GDPR (4.2 Proces implementace GDPR). Jednotlivé kroky byly dále rozpracovány. Díky tomu, že k nim byly přiřazeny i termínované úkoly, měla nad implementací Nemocnice po celou dobu kontrolu. Bylo postupováno podle priorit,

a i když ani dnes nejsou veškeré kroky splněny, vše důležité bylo i přes několik problémů splněno ještě před účinností GDPR. Nyní je hlavně důležité naplánovaný proces dokončit. Vzhledem k tomu, že v Nemocnici probíhá stále velké množství zpracování osobních údajů v listinné podobě, jedná se o běh na dlouhou trať. Postupná elektronizace a vylepšení elektronických systémů bude v budoucnosti nezbytnou nutností. Bude však nutné dbát na to, aby byly elektronizované dokumenty v takové podobě, aby s nimi mohlo být efektivně pracováno.

V současné době je nejdůležitějším krokem rozhodnutí, kdo bude vykonávat funkci DPO (4.2.1 Určení pověřence pro ochranu osobních údajů). Do této funkce byl původně jmenován vedoucí interního auditu, což se v průběhu psaní této diplomové práce ukázalo jako možný problém. Bylo dohledáno stanovisko Centrální harmonizační jednotky Ministerstva financí, ve kterém je uvedeno, že interní auditor nemůže funkci DPO vykonávat, kvůli zajištění nezávislého postavení a zabránění střetu zájmů obou funkcí. K jeho vydání došlo pár dní před účinností GDPR, a protože většina organizací již měla DPO jmenovaného, lze usuzovat, že se tento problém netýká pouze Nemocnice. Vzhledem k získanému stanovisku ÚOOÚ, který se k problematice nestaví tak jednoznačně, je nyní na řediteli nemocnice, aby rozhodl, zdali funkci DPO ponechá beze změny.

K zhodnocení implementace GDPR v Nemocnici byly navrženy podněty, jak přistupovat k internímu auditu (4.5 Podněty k přístupu k internímu auditu). Zřejmě největším problémem, který by mohl nastat, by bylo porušení nezávislosti, jelikož vedoucím útvaru interního auditu je DPO. Tato situace by mohla být řešena tím, že by vedoucí k provedení tohoto auditu pověřil podřízeného interního auditora. Ten by dále vedl celý auditní tým.

Významnou částí této diplomové práce tvoří dotazníkové šetření (4.6 Dotazníkové šetření), které zkoumá povědomí lidí o právech pacientů. Bylo rozděleno na dvě části.

V první části dotazníku byly pokládány otázky na obecná práva v souvislosti s poskytováním zdravotní péče. Z celkového počtu 408 respondentů tuto část dokázali vyplnit správně pouze 2 respondenti, což poukazuje na velkou neznalost práv pacientů.

Druhá část dotazníku byla věnována GDPR. I přes to, že GDPR bylo velkým tématem, ani polovina dotázaných nevěděla, že došlo k rozšíření i zavedení zcela nových práv pacientů. Pouze 5 % respondentů uvedlo, že o této novince ví, a zároveň že i přesně ví, o která práva se jedná. Jejich opravdová znalost však byla ověřována pokládáním testujících

otázek. Tím se ukázalo, že opravdové povědomí o právech v souvislosti s GDPR má pouze 1 % respondentů.

Pokud jde o celkové zhodnocení dotazníkového šetření, ze 408 respondentů ani jeden respondent nedokázal odpovědět na všechny otázky správně. Tento výsledek je alarmující a je nutné tuto situaci řešit. Výsledek je překvapující především u respondentů pracujících ve zdravotnictví, u kterých by se znalost práv pacientů dala očekávat na vysoké úrovni. Otázkou je, kde je příčina této neznalosti, zdali se jedná o nedostatečnou komunikaci mezi pacientem a lékařem nebo spíše o nezájem pacientů.

Většina respondentů odpověděla, že se o svých právech dozvídá především z internetu, což není vzhledem k technologickému pokroku příliš překvapivé. Avšak neoficiální informace na internetu mohou být zkreslené a neúplné. Vzhledem k tomu by mohla být vhodným řešením oficiální internetová kampaň pod záštitou Ministerstva zdravotnictví České republiky, šířená např. pomocí sociálních sítí a různých televizních a rozhlasových médií. Jednalo by se však pouze o podpůrnou činnost, jelikož primárním zdrojem informací by měl být vždy ošetřující lékař. Bohužel v době, kdy jsou lékaři nadměrně vytíženi, nemají na jednotlivé pacienty příliš času a jsou hodnoceni na základě počtu provedených výkonů, je velice těžké je do této povinnosti nutit.

Problém s informovaností pacientů o svých právech by se dále dal řešit přímo v čekárně lékaře. Ve většině případů je zde mnoho informativních letáků a plakátů, které si při čekání na ošetření mají pacienti čas přečíst. Místo spíše stresujících letáků a reklam na léky by zde mohla být práva pacientů vyvěšena. Tato povinnost pacienty informovat o svých právech by však musela vycházet ze zákonné povinnosti, jelikož dobrovolně by si zřejmě takovouto informaci lékař nikdy v ordinaci nevyvěsil.

Závěr

Tato diplomová práce se zabývala stále velmi aktuálním tématem, kterým je GDPR, jelikož se jedná o nový právní rámec ochrany osobních údajů a má dopad na každého, kdo jakýmkoli způsobem osobní údaje zpracovává.

Cílem diplomové práce bylo analyzovat proces implementace GDPR ve vybraném zdravotnickém zařízení. K posouzení dodržování nových právních povinností dle GDPR byly navrženy podněty, jak přistoupit k internímu auditu. Dalším cílem bylo potvrzení či vyvrácení hypotézy o povědomí pacientů o svých právech se zaměřením na GDPR.

V teoretické části se práce zaměřila na analýzu právní úpravy (3.1 Obecně k právní úpravě) a na vymezení základních pojmů v souvislosti s GDPR, kterými jsou osobní údaje, subjekt, správce, zpracovatel či DPO (3.2 Vybrané pojmy GDPR). Důležitou součástí bylo vymezení šesti základních zásad GDPR (3.3 Zásady a principy GDPR), které říkají, jak ke zpracování osobních údajů přistupovat. Lze je chápat jako souhrn těch nejdůležitějších povinností, kterými je třeba se řídit.

Jelikož byl proces implementace analyzován v nemocničním zařízení, část práce se věnovala specifikům GDPR v resortu zdravotnictví (3.5 Specifika GDPR pro resort zdravotnictví).

Nedílnou součást této práce tvořila část zabývající se právy pacientů (3.6 Práva pacientů), kde byl analyzován jejich historický vývoj a byla vymezena jednotlivá práva, především se zaměřením na GDPR. Tato část byla důležitým podkladem pro dotazníkové šetření realizované v praktické části.

V praktické části byly využity poznatky získané z teoretické části této práce. Tyto poznatky byly aplikovány na případovou studii týkající se implementace GDPR ve vybraném zdravotnickém zařízení.

V první fázi implementace (4.2 Proces implementace GDPR) byl vytvořen harmonogram s jednotlivými kroky, aby byla Nemocnice na GDPR včas připravena. V rámci tohoto harmonogramu proběhlo mapování veškerých procesů, na základě kterých byly sestaveny registry zpracování osobních údajů a IT registr. V další fázi proběhla kontrola veškerých dosavadních souhlasů se zpracováním osobních údajů a také uzavřených smluv. Nedílnou součástí byla implementace technických opatření. Byly nastaveny nové procesy nakládání s osobními údaji a také proces identifikace a řešení úniků osobních údajů. Nutností byla úprava řídicí dokumentace s následným proškolením všech zaměstnanců.

I přes to, že se Nemocnice při implementaci GDPR setkala s mnoha problémy a všechny kroky nebyly splněny včas, na základě získaných poznatků lze říci, že Nemocnice zvládla implementaci GDPR na vysoké úrovni. Nyní je však nutné veškeré nastavené procesy ověřit v praxi, proto byly v rámci této diplomové práce navrženy podněty k přístupu k internímu auditu, které nyní bude moci Nemocnice využít (4.5 Přístup interního auditu).

V rámci této diplomové práce bylo dále provedeno dotazníkové šetření (4.6 Dotazníkové šetření), kterého se účastnilo celkem 408 respondentů. Jeho cílem bylo zjištění informovanosti pacientů o svých právech v souvislosti s poskytováním zdravotní péče, a zdali svá práva aktivně využívají a zároveň zjištění povědomí o nových právech v souvislosti s účinností GDPR.

Výsledky dotazníkového šetření poukázaly na velkou neznalost práv pacientů. Toto tvrzení dokládá, že ani jeden z respondentů neznal odpověď na všechny otázky (4.6.3 Výsledky dotazníkového šetření). Lidé se více orientují v obecných právech, avšak ani zde nejsou znalosti dostatečné. Co se týká nových práv dle GDPR, znalosti jsou minimální. Výsledky také ukázaly, že svá práva pacienti příliš nevyužívají. Možnost uplatnit svá práva prostřednictvím podání žádosti dle GDPR využilo minimum respondentů (Tab. 31). Tento výsledek odpovídá i praxi v Nemocnici, kde bylo evidováno také pouze minimální množství žádostí (4.4.3 Přijaté žádosti).

Dle předpokladu lepších výsledků dosahovali respondenti pracující ve zdravotnictví. Co se týká pohlaví, byly výsledky spíše vyrovnané, u obecných práv celkově mírně lepších výsledků dosahovaly ženy, co se týká GDPR, zde byly mírně lepší výsledky u mužů. Další souvislost byla prokázána u vzdělání, čím vyšší vzdělání lidé mají, tím vyšší mají povědomí o svých právech. Výkyvy byly pouze u několika málo otázek, kdy dosahovali poměrně vysokých výsledků lidé se základním vzděláním. Vyrovnaných výsledků dosahovali respondenti ve všech věkových kategoriích, kromě kategorie 70 let a více. V této kategorii byla znalost práv oproti ostatním podprůměrná. Mírná závislost byla prokázána u bydliště, lepší povědomí o svých právech mají lidé z velkoměst nad 500 000 obyvatel a na druhou stranu také z vesnic do 2 000 obyvatel.

6 Seznam použitých zdrojů

ODBORNÁ LITERATURA

BUKOVSKÝ, J. *Změny v legislativě – Zákon GDPR, změny v zákonu o kybernetické bezpečnosti a v nařízení eIDAS.* Školení Českého institutu interních auditorů. 2018-02-19.

BUREŠOVÁ, R. a kolektiv. *Jak se připravit na GDPR v 5 krocích – ve zdravotnictví.* Verlag Dashöfer, nakladatelství, s.r.o., 2018.

HAŠKOVCOVÁ, H. *Práva pacientů – komentované vydání.* Havířov: Nakladatelství Aleny Krtilové, 1996. ISBN 80-902163-0-7.

JANEČKOVÁ, E. *GDPR – Praktická příručka implementace.* Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.

NEZMAR, L. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017. ISBN 978-80-271-0668-4.

NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související (č. 101/2000 Sb.) – komentář.* Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-665-5.

NULÍČEK, M. a kolektiv. *GDPR/Obecné nařízení o ochraně osobních údajů – praktický komentář.* Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-766-0.

PTÁČEK, R., BARTŮNĚK, P. a kolektiv. Etika a komunikace v medicíně. Praha: Grada Publishing, a.s., 2011. ISBN 978-80-247-3976-2.

TĚŠINOVÁ, J., ŽĎÁREK, R., POLICAR, R. *Medicínské právo*. Praha: C. H. Beck, 2011. ISBN 978-80-7400-050-8.

ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3.

PRÁVNÍ PŘEDPISY A JUDIKATURA

Deklarace práv člověka a občana ze dne 26. 8. 1789.

Lisabonská deklarace o právech pacientů, 1981.

Listina základních práv Evropské unie 2012/C 326/02.

Listina základních práv a svobod 2/1993 Sb.

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).

Návrh nového zákona o zpracování osobních údajů, který nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů.

Příloha č. 3 „Doby uchování zdravotnické dokumentace nebo jejích částí“ vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů.

Sdělení č. 209/1992 Sb., sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob s ohledem na automatizované zpracování osobních údajů.

Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů.

Zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů.

Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

ELEKTRONICKÉ ZDROJE

EDPB. *O Evropském sboru pro ochranu osobních údajů* [online]. [cit. 2018-12-28]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb_cs.

ČESKÁ LÉKAŘSKÁ KOMORA. *Etický kodex České lékařské komory* [online]. (PDF). [cit. 2018-12-30]. Dostupné z: https://www.lkcr.cz/doc/cms_library/10_sp_c_10_eticky_kodex-100217.pdf

ČESKÁ TELEVIZE. *Obcím a krajům nebudou za porušení GDPR hrozit pokuty, rozhodli poslanci* [online]. [cit. 2019-03-18]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/2757596-zive-poslanci-maji-znovu-rozhodnout-o-zdaneni-nahrad-cirkvim-a-resit-mohou-i-faltynka.

EUROPEAN COMMISSION. *Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti* [online]. [cit. 2018-11-15]. Dostupné z: http://ec.europa.eu/justice/data-protection/index_cs.htm.

EVROPSKÁ KOMISE. *Co je to Evropský sbor pro ochranu osobních údajů (European Data Protection Board, EDPB)?* [online]. [cit. 2018-12-28]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_cs.

GDPR. *Anonymizace a pseudonymizace jsou dvě rozdílná slova* [online]. [cit. 2018-11-30]. Dostupné z: https://www.gdpr.cz/blog/anonymizace-a-pseudonymizace-jsou-dve-rozdilna-slova/.

GDPR. *Citlivé osobní údaje.* [online]. [cit. 2018-11-13]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/.

GDPR. *DPO čili Pověřenec pro ochranu osobních údajů* [online]. [cit. 2018-08-30]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/.

GDPR. *Jaké sankce hrozí firmám, které budou GDPR ignorovat* [online]. [Cit. 2018-10-17]. Dostupné z: https://www.gdpr.cz/gdpr/sankce/.

GDPR. *Správce osobních údajů* [online]. [cit. 2018-09-06]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/spravce-osobnich-udaju/.

GDPR. *Subjekt údajů* [online]. [cit. 2018-09-06]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/subjekt-udaju/.

GDPRSAFE. *Zásady zpracování* [online]. [Cit. 2019-01-12]. Dostupné z: https://gdprsafe.cz/ukazka/priprava-na-gdpr/zasady-zpracovani/.

GDPR SOLUTIONS. *GDPR ve zdravotnictví* [online]. [cit. 2018-12-10]. Dostupné z: https://www.gdprsolutions.cz/gdpr-ve-zdravotnictvi/.

GODDARD, M. *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact.* International Journal of Market Research [online]. [cit. 2018-03-15]. Dostupné z: https://journals.sagepub.com/doi/abs/10.2501/IJMR-2017-050.

GUARD7. *Právo vznést námitku* [online]. [cit. 2018-01-07]. Dostupné z: http://www.guard7.cz/gdpr/pravo-vznest-namitku.

KOMÍNKOVÁ, M. *Jak vznikalo nařízení o ochraně osobních údajů (GDPR)?* Euroskop [online]. 2018. [cit. 2018-12-26]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/.

KRAJSKÝ ÚŘAD – JIHOČESKÝ KRAJ. *Práva pacientů* [online]. (PDF). [cit. 2018-12-30]. Dostupné z: https://www.kraj-jihocesky.cz/file.php?par[id_r]=140391&par[view]=0.

MASARIKOVA UNIVERZITA. *Významné mezinárodní dokumenty k etice výzkumu* [online]. [cit. 2018-12-29]. Dostupné z: https://vyzkum.rect.muni.cz/cs/zazemi/etika-vyzkumu/etika-vyzkumu/mezinarodni-dokumenty-k-etice-vyzkumu.

METODIKA MZ ČR A ÚZIS. *Jak implementovat nařízení evropského parlamentu a rady 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES do resortu zdravotnictví* [online]. (PDF). [cit. 2018-07-20]. Dostupné z: http://www.uzis.cz/system/files/u44/GDPR_20180102_metodika_implementace_ve_zdravotnictvi.pdf.

MPSV ČR. *Etický kodex Práva pacientů.* [online]. [cit. 2018-12-30]. Dostupné z: https://www.mpsv.cz/cs/840.

MV ČR. *Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí.* [online]. (PDF). [cit. 2018-07-19]. Dostupné z: https://www.mvcr.cz/odk2/soubor/metodicke-doporuceni-k-cinnosti-obci-k-organizacne-

technickemu-zabezpeceni-funkce-poverence-pro-ochranu-osobnich-udaju-podle-obecneho-narizeni-o-ochrane-osobnich-udaju-v-podminkach-obci.aspx.

MZ ČR. *Práva pacienta* [online]. [cit. 2018-12-20]. Dostupné z: http://www.mzcr.cz/kvalitaabezpeci/obsah/prava-pacienta_2401_18.html.

OTEVŘEL, R. *Klinické hodnocení a ochrana osobních údajů* [online]. [cit. 2019-01-08]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/klinicke-hodnoceni-a-ochrana-osobnich-udaju-nove-upozorneni-sukl.

PATTYNOVÁ, J. *Šest měsíců s GDPR: novinky a průběh kontrol dozorového orgánu.* Právní prostor [online]. [cit. 2019-3-12]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/sest-mesicu-s-gdpr-novinky-a-prubeh-kontrol-dozoroveho-organu.

PLATH, S. *Anonymisation and poedonymisation* [online]. (PDF). 2016. [cit. 2018-11-30]. Dostupné z: https://www.pwc.lu/en/general-data-protection/docs/pwc-anonymisation-and-pseudonymisation.pdf.
SOOM. *Symetrické a asymetrické šifrování* [online]. [cit. 2018-11-29]. Dostupné z: https://www.soom.cz/clanky/1126--Symetricke-a-asymetricke-sifrovani.

ÚOOÚ. *Desatero omylů* [online]. [cit. 2018-12-28]. Dostupné z: https://www.uoou.cz/desatero-omylu/ds-4818/archiv=0&p1=3109

ÚOOÚ. *K problematice aktualizace zpracovávaných osobních údajů* [online]. [cit. 2018-01-14]. Dostupné z: https://www.uoou.cz/k-problematice-aktualizace-zpracovavanych-osobnich-udaju/d-1595.

ÚOOÚ. Porušení zabezpečení [online]. [cit. 2019-3-14]. Dostupné z: https://www.uoou.cz/poruseni-zabezpeceni/ds-5020.

ÚOOU. *Základní příručka k GDPR* [online]. [cit. 2018-01-07]. Dostupné z https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744.

VITNEROVÁ, M. *Vláda schválila návrh zákona o zpracování osobních údajů* [online]. [cit. 2018-12-30]. Dostupné z: https://www.mvcr.cz/clanek/vlada-schvalila-navrh-zakona-o-zpracovani-osobnich-udaju.aspx.

WP 29. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* [online]. (PDF) [cit. 2018-07-23]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

WP 29. *Guidelines on the right to data portability* [online]. (PDF) [cit. 2018-07-24]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

WP29. *Guidelines on Data Protection Officers ('DPOs')* [online]. (PDF) [cit. 2018-07-20]. Dostupné z: ec.europa.eu/newsroom/document.cfm?doc_id=44100.

7 Přílohy

Příloha č. 1 – Vzor smlouvy – zpracování osobních údajů

Příloha č. 2 – Etický kodex

Příloha č. 3 – Stanovisko Centrální harmonizační jednotky

Příloha č. 4 – Ukázka výzvy k udělení souhlasu se zasíláním osobních údajů emailem

Příloha č. 5 – Protokol o úniku osobních údajů

Příloha č. 1 – Vzor smlouvy – zpracování osobních údajů[143]

Právní status smlouvy

Smlouva nebo dodatek o zpracování osobních údajů mezi … (dále jen Dodavatel) a … (dále jen Organizace) níže uvedeného dne, měsíce a roku uzavřeli dle čl. 28 nařízení EU č. 2016/679, obecného nařízení o ochraně osobních údajů (dále jen GDPR) tuto smlouvu o zpracování osobních údajů (dále jen smlouva).

1. Předmět smlouvy

1. Organizace je ve smyslu GDPR správcem osobních údajů, neboť v souvislosti se svojí činností v oblasti poskytování zdravotních služeb zpracovává osobní údaje svých pacientů, zaměstnanců, popřípadě dalších osob (dále všichni jen subjekty údajů). Právním základem zpracování osobních údajů je zejm. splnění právní povinnosti, která se na správce vztahuje, zčásti může být právním základem zpracování též oprávněný zájem Správce.

2. Dodavatel poskytuje Organizaci na základě smlouvy č. … ze dne … (dále jen původní smlouva) mj. následující služby: …

3. V rámci poskytování uvedených služeb zpracovává Dodavatel osobní údaje, jejichž správcem je Organizace.

4. Dodavatel je ve smyslu obecného nařízení osobou, která poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření při provádění zpracování osobních údajů.

5. Smluvní strany mají zájem upravit touto smlouvou svá vzájemná práva a povinnosti při zpracování osobních údajů podle čl. 28 obecného nařízení.

2. Definice

1. Osobním údajem se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen subjekt údajů); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat.

2. Zpracováním osobních údajů se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn 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.

3. Další pojmy používané v této smlouvě mají totožný význam, jako pojmy užité v nařízení, ev. mají význam, který je jim přisuzován jinými závaznými právními předpisy.

3. Předmět, povaha a účel zpracování

1. Předmětem zpracování osobních údajů ve smyslu čl. 1 a 2 této smlouvy je zejména: …

2. Osobní údaje jsou zpracovávány jak automatickým způsobem bez lidského zásahu, tak i manuálně v elektronické i papírové podobě. Účelem tohoto zpracování osobních údajů je zajištění chodu uvedených informačních systémů.

3. Dodavatel není oprávněn zpracovávat osobní údaje za jiným účelem, než který mu byl stanoven Organizací prostřednictvím smlouvy a tohoto Dodatku.

[143] Dokument dostupný na interních intranetových stránkách Nemocnice.

4. Typy zpracovávaných osobních údajů a kategorie subjektů

1. Předmětem zpracování jsou následující typy osobních údajů: ...

2. Kategorie subjektů údajů: ...

5. Doba trvání zpracování osobních údajů

Dodavatel zpracovává osobní údaje dle čl. 3 a 4 této smlouvy po dobu nezbytnou, nejdéle však po dobu účinnosti původní smlouvy.

6. Práva a povinnosti Dodavatele

1. V souladu s čl. 28. odst. 3 GDPR Dodavatel zejména:

a. zpracovává osobní údaje výhradně na základě původní smlouvy, této smlouvy a doložených pokynů Organizace, a v souladu s GDPR;

b. plní bezodkladně veškeré pokyny udělené mu Organizací ve vztahu ke zpracování osobních údajů, například přerušení zpracování osobních údajů, jejich úprava, výmaz či vydání kopie;

c. zajišťuje, že se jeho zaměstnanci a případně další osoby mající přístup k osobním údajům Organizace zavázaly k mlčenlivosti;

d. přijme veškerá opatření stanovená článkem 32 GDPR, která jsou blíže stanovena v odst. 3 tohoto článku;

e. poskytne Organizaci, příp. třetí straně pověřené Organizací nebo státnímu orgánu veškerou součinnost nezbytnou ke kontrole činností Dodavatele vykonávaných na základě původní smlouvy a/nebo této smlouvy. V této souvislosti Dodavatel bez zbytečného odkladu poskytne zejména informace, dokumenty přístup do svých prostor a ke svým zařízením a dá k dispozici své relevantní zaměstnance;

f. poskytne Organizaci veškerou součinnost nezbytnou pro včasné vyřízení uplatnění práva subjektu údajů ve smyslu zejm. článků č. 15 až 22 GDPR; g. nezapojí do zpracování žádného dalšího zpracovatele, ledaže by k tomuto předem získal písemné povolení Organizace;

h. je Organizaci nápomocen při zajišťování souladu s jeho povinnostmi podle článků 32 až 36 GDPR;

i. je-li relevantní čl. 35 odst. 1 GDPR, Dodavatel provede posouzení vlivu zpracování osobních údajů a informuje Organizaci o výsledku posouzení bez zbytečného odkladu;

j. je-li relevantní čl. 37 GDPR, Dodavatel jmenuje pověřence pro ochranu osobních údajů a informuje Organizaci o kontaktních údajích tohoto pověřence bez zbytečného odkladu;

k. nepředá osobní údaje do země mimo území Evropské unie bez souhlasu Organizace.

2. Dodavatel bez souhlasu Organizace nesmí svěřit zpracování osobních údajů dle původní smlouvy a této smlouvy třetí osobě. Z tohoto důvodu je Dodavatel povinen si s dostatečným předstihem vyžádat písemný souhlas Organizace ke každému novému třetímu zpracovateli, a stejně tak neprodleně informovat Organizaci o ukončení spolupráce se třetím zpracovatelem způsobem stanoveným v Pokynech pro zpracovatele osobních údajů. Pokud Dodavatel do zpracování osobních údajů dle této smlouvy zapojí dalšího zpracovatele, musí se tento další zpracovatel smluvně zavázat k dodržování stejných zásad pro zpracování osobních údajů, které jsou stanovený touto smlouvou. Poruší-li další

zpracovatel své povinnosti v oblasti zpracování nebo ochrany osobních údajů, za toto porušení odpovídá Organizaci Dodavatel.

3. Dodavatel se zavazuje zavést a udržovat organizační a technická opatření za účelem ochrany zpracovávaných osobních údajů, aby byla zajištěna zejména:

a. důvěrnost, dostupnost a integrita osobních údajů;

b. odolnost systémů a IT služeb sloužících zpracování osobních údajů, aby splňovala požadavky GDPR.

4. Pro případ incidentu, který způsobí narušení některého z principů uvedených v odst. 3, se Dodavatel zavazuje mít připraveny postupy a zdroje umožňující odstranění následků incidentu a obnovu řádného stavu bez zbytečného odkladu. Dodavatel o takovém incidentu neprodleně informuje odpovědné osoby Organizace, a to telefonicky i písemně (e-mailem).

5. V případě ukončení původní smlouvy nebo této smlouvy je Dodavatel povinen:

a. bezodkladně přestat zpracovávat osobní údaje poskytnuté mu Organizací na základě původní smlouvy a/nebo této smlouvy, ledaže mu Organizace vydá jiný pokyn nebo není-li další zpracovávání osobních údajů vyžadováno právem EU nebo právními předpisy ČR;

b. veškeré osobní údaje předat zpět Organizaci v běžně využívané elektronické podobě vhodné pro takovéto předání;

c. po potvrzení převzetí osobních údajů Organizací dle výše uvedeného písm. b) zničit veškeré osobní údaje, které zpracovával na základě Smlouvy a/nebo tohoto Dodatku není-li uložení dalších zpracovávaných osobních údajů vyžadováno právem EU nebo právními předpisy ČR. Povinnost likvidace osobních údajů se týká jejich elektronické i papírové podoby, včetně záloh.

6. Dodavatel se dále zavazuje pravidelně testovat, posuzovat a hodnotit účinnost zavedených technických a organizačních opatření.

7. Dodavatel na požadavek Organizace kdykoli předloží dokumentaci prokazující zavedení a/nebo hodnocení relevantních výše uvedených opatření.

7. Práva a povinnosti Organizace

1. Organizace je ve vztahu k výše uvedenému správcem osobních údajů.

2. Organizace se zavazuje:

a. umožnit Dodavateli přístup k těm osobním údajům, které má Dodavatel na základě Smlouvy pro Organizaci zpracovávat;

b. předávat dodavateli včas informace a pokyny nezbytné k řádnému výkonu činností dle článku 1 tohoto Dodatku;

c. písemně sdělit dodavateli jména, příjmení, pracovní pozice, kontaktní telefonní čísla a e-mailové adresy osob, které jsou oprávněny Dodavateli dávat pokyny v souvislosti se zpracováním osobních údajů;

d. písemně sdělit dodavateli jména, příjmení, pracovní pozice, kontaktní telefonní čísla a e-mailové adresy osob, kterým je Dodavatel povinen hlásit incidenty ve smyslu článku VI. odst. 3 tohoto Dodatku;

e. v případě, že dojde ke změně osob vzhledem k výše uvedeným písm. c) a d); Organizace tuto změnu písemně nahlásí Dodavateli bez zbytečného odkladu.

8. Mlčenlivost

1. Dodavatel se zavazuje zachovávat mlčenlivost ve vztahu ke všem informacím a skutečnostem, které se dozví o Organizaci, jejich zaměstnancích, pacientech atd. v souvislosti s uzavřením a plněním smlouvy, pokud tyto informace mají povahu obchodního tajemství, osobních údajů nebo mají být z jiných důvodů chráněny před zveřejněním. Dodavatel je povinen nakládat s osobními údaji a zejména s údaji o zdravotním stavu, genetickými a biometrickými údaji (dále jen „Osobní údaje") v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 a příslušnými ustanoveními zákona č. 101/2000 Sb., o ochraně osobních údajů.

2. Povinnost mlčenlivosti platí rovněž o skutečnostech, na něž se vztahuje povinnost mlčenlivosti zdravotnických pracovníků, zejména podle ustanovení § 51 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (Zákon o zdravotních službách), a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů.

3. Smluvní strany se zavazují zachovat mlčenlivost též o všech ostatních skutečnostech, ve vztahu, k nimž o to budou druhou stranou písemně požádány. Smluvní strany se též zavazují nevyužít informace podle tohoto odstavce ve svůj prospěch nebo ve prospěch třetích osob v rozporu s účelem jejich předání. Povinnost mlčenlivosti o informacích a skutečnostech obchodního charakteru trvá po dobu 5 let od ukončení této smlouvy, o informacích obsahujících osobní údaje trvá bez časového omezení.

9. Porušení smlouvy a smluvní pokuty

Poruší-li Dodavatel některou ze svých povinností ve vztahu ke zpracování osobních údajů dle této smlouvy, je:

a. Organizace oprávněna požadovat po Dodavateli úhradu smluvní pokuty ve výši … Kč. Úhradou smluvní pokuty není dotčena povinnost Dodavatele odstranit závadný stav, ani povinnost Dodavatele uhradit Organizaci případnou další újmu, například sankci, která byla Organizaci uložena kvůli pochybení Dodavatele.

b. Organizace oprávněna požadovat po Dodavateli nápravu závadného stavu.

10. Prohlášení Dodavatele

Dodavatel prohlašuje, že k datu podpisu této smlouvy zavedl a udržuje veškerá opatření touto smlouvou požadovaná.

11. Kontaktní osoby

1. Osobou oprávněnou jednat za Organizaci ve věcech, které se týkají plnění dle této smlouvy je …

2. Osobou oprávněnou jednat za Dodavatele ve věcech, které se týkají plnění dle této smlouvy je …

3. Každá ze stran může změnit svou kontaktní osobu písemným oznámením zaslaným druhé straně v souladu s tímto ustanovením.

12. Závěrečná ustanovení

1. Tato smlouva se uzavírá na dobu neurčitou.

2. Tato smlouva může být ukončena písemnou dohodou smluvních stran, písemným odstoupením od smlouvy dle odst. 3 tohoto článku nebo písemnou výpovědí dle odst. 4 tohoto článku.

3. Každá smluvní strana je oprávněna od této smlouvy odstoupit, pokud druhá smluvní strana poruší svoji povinnost vyplývající z této smlouvy podstatným způsobem a nezjedná nápravu ani v přiměřené lhůtě určené jí v písemné výzvě dotčenou smluvní stranou.

4. Každá ze smluvních stran je oprávněna kdykoliv vypovědět tuto smlouvu i bez uvedení důvodu s výpovědní dobou … která začíná plynout prvním dnem kalendářního měsíce následujícího po doručení výpovědi druhé smluvní straně.

5. Odstoupením Organizace od této smlouvy nebo výpovědí Organizace nezanikají povinnosti Dodavatele týkající se bezpečnosti a ochrany zpracovávaných osobních údajů až do okamžiku jejich výmazu, povinnost mlčenlivosti ani povinnost k náhradě újmy dle čl. 9.

6. Vztahy mezi smluvními stranami výslovně v této smlouvě neupravené se řídí právním řádem České republiky a EU, zejména GDPR, zákonem a Občanským zákoníkem.

7. Veškeré změny této Smlouvy je možné provést pouze formou očíslovaných písemných dodatků, které se po jejich podpisu oprávněnými zástupci obou Smluvních stran stanou nedílnou součástí této Smlouvy.

8. Smlouva je vyhotovena ve dvou stejnopisech, přičemž každá smluvní strana obdrží po jednom řádně podepsaném vyhotovení.

9. Smlouva nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami.

V … dne …

Oprávněná osoba za Dodavatele

V … dne …

Oprávněná osoba za Organizaci

Příloha č. 2 – Etický kodex pacientů[144]

Práva pacientů ČR

1. Pacient má právo na ohleduplnou odbornou zdravotnickou péči prováděnou s porozuměním kvalifikovanými pracovníky.
2. Pacient má právo znát jméno lékaře a dalších zdravotnických pracovníků, kteří ho ošetřují. Má právo žádat soukromí a služby přiměřené možnostem ústavu, jakož i možnost denně se stýkat se členy své rodiny či s přáteli. Omezení takovéhoto způsobu (tzv. kontinuálních) návštěv může být provedeno pouze ze závažných důvodů.
3. Pacient má právo získat od svého lékaře údaje potřebné k tomu, aby mohl před zahájením každého dalšího nového diagnostického či terapeutického postupu zasvěceně rozhodnout, zda s ním souhlasí. Vyjma případů akutního ohrožení má být náležitě informován o případných rizicích, která jsou s uvedeným postupem spojena. Pokud existuje i více alternativních postupů nebo pokud pacient vyžaduje informace o léčebných alternativách, má na seznámení s nimi právo. Má rovněž právo znát jména osob, které se na nich účastní.
4. Pacient má v rozsahu, který povoluje zákon, právo odmítnout léčbu a má být současně informován o zdravotních důsledcích svého rozhodnutí.
5. V průběhu ambulantního i nemocničního vyšetření, ošetření a léčby má nemocný právo na to, aby byly v souvislosti s programem léčby brány maximální ohledy na jeho soukromí a stud. Rozbory jeho případu, konzultace a léčba jsou věcí důvěrnou a musí být provedena diskrétně. Přítomnost osob, které nejsou na léčbě přímo zúčastněny, musí odsouhlasit nemocný, a to i ve fakultních zařízeních, pokud si tyto osoby nemocný sám nevybral.
6. Pacient má právo očekávat, že veškeré zprávy a záznamy týkající se jeho léčby jsou považovány za důvěrné. Ochrana informací o nemocném musí být zajištěna i v případech počítačového zpracování.
7. Pacient má právo očekávat, že nemocnice musí podle svých možností přiměřeným způsobem vyhovět pacientovým žádostem o poskytování péče v míře odpovídající povaze onemocnění. Je-li to nutné, může být pacient předán jinému léčebnému ústavu, případně tam převezen po té, když mu bylo poskytnuto úplné zdůvodnění a informace o nezbytnosti tohoto předání a ostatních alternativách, které při tom existují. Instituce, která má nemocného převzít do své péče, musí překlad nejprve schválit.
8. Pacient má právo očekávat, že jeho léčba bude vedena s přiměřenou kontinuitou. Má právo vědět předem, jací lékaři, v jakých ordinačních hodinách a na jakém místě jsou mu k dispozici. Po propuštění má právo očekávat, že nemocnice určí postup, jímž bude jeho lékař pokračovat v informacích o tom, jaká bude jeho další péče.
9. Pacient má právo na podrobné a jemu srozumitelné vysvětlení v případě, že se lékař rozhodl k nestandardnímu postupu či experimentu. Písemný vědomý souhlas nemocného je podmínkou k zahájení neterapeutického i terapeutického výzkumu. Pacient může kdykoliv, a to bez uvedení důvodu, z experimentu odstoupit, když byl poučen o případných zdravotních důsledcích takového rozhodnutí.
10. Nemocný v závěru života má právo na citlivou péči všech zdravotníků, kteří musí respektovat jeho přání, pokud tato nejsou v rozporu s platnými zákony.
11. Pacient má právo a povinnost znát a řídit se platným řádem zdravotnické instituce, kde se léčí (tzv. nemocniční řád). Pacient má právo kontrolovat svůj účet a vyžadovat odůvodnění jeho položek bez ohledu na to, kým je účet placen.

Etický kodex "Práva pacientů" navrhla, po připomínkovém řízení definitivně formulovala a schválila Centrální etická komise Ministerstva zdravotnictví České Republiky.
Tato práva pacientů jsou prohlášená za platná za dnem 25. února 1992

[144] MPSV ČR. *Práva pacientů ČR* [online]. [cit. 2019-03-5]. Dostupné z: https://www.mpsv.cz/cs/840.

Příloha č. 3 – Stanovisko Centrální harmonizační jednotky[145]

CHJ 2018/1b

Ministerstvo financí
České republiky

STANOVISKO

ODBORU CENTRÁLNÍ HARMONIZAČNÍ JEDNOTKA
Č. 1b/2018

Dotaz

Může interní auditor vykonávat zároveň funkci pověřence pro ochranu osobních údajů (DPO) v rámci agendy GDPR?

ZAŘAZENÍ DOTAZU

PRÁVNÍ PŘEDPIS	• zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole)
SOUVISEJÍCÍ PRÁVNÍ PŘEDPISY	• 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
KLÍČOVÁ SLOVA	interní audit; GDPR ; pověřenec pro ochranu osobních údaj; DPO
DATUM ZPRACOVÁNÍ	vydáno 13. dubna 2018; aktualizováno 21. září 2018
ZPRACOVATEL	oddělení 4701 – Harmonizace interního auditu

Stanovisko

Interní auditor, který vykonává interní audit podle zákona o finanční kontrole, nemůže být jmenován pověřencem pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů. Pověřenec pro ochranu osobních údajů nemůže být organizačně začleněn do útvaru interního auditu nebo podřízen vedoucímu útvaru interního auditu nebo internímu auditorovi.

Odůvodnění:

Interní audit je definován v ustanovení § 28 odst. 2 zákona o finanční kontrole jako nezávislé a objektivní přezkoumávání a vyhodnocování operací a vnitřního kontrolního systému orgánu veřejné správy. Hlavním úkolem interního auditu je dávat doporučení ke

[145] CENTRÁLNÍ HARMONIZAČNÍ JEDNOTKA MINISTARSTVA FINANCÍ. *Stanovisko č. 1b/2018* [online]. (PDF). [cit. 2019-02-5]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Metodika_2018_CHJ-2018-1-Stanovisko-k-povereni-interniho-auditora-funkci-DPO-GDPR_v02.pdf.

zdokonalování kvality vnitřního kontrolního systému, k předcházení nebo ke zmírnění rizik a k přijetí opatření k nápravě zjištěných nedostatků (srov. § 28 odst. 3 zákona o finanční kontrole). Aby interní audit mohl plnit své úkoly v souladu s požadavky zákona o finanční kontrole, musí být funkčně nezávislý a organizačně oddělen od řídicích výkonných struktur. Tento požadavek je zakotven v ustanovení § 29 odst. 1 zákona o finanční kontrole. Ustanovení § 29 odst. 4 zákona o finanční kontrole tyty požadavky ještě upřesňuje a výslovně stanoví, že útvar interního auditu nelze pověřovat úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů.

Interní auditor by měl mít přístup ke všem informacím, záznamům, dokladům, systémům, operacím, zaměstnancům a k veškerému majetku orgánu veřejné správy. V rámci své činnosti vytváří auditní stopu, ve které zpracovává osobní údaje. Příkladem této auditní stopy jsou zápisy ze schůzek, dotazníky, zprávy o vykonaném interním auditu. Dále je mu umožněno nahlížet do informačních systémů, smluv, faktur a další dokumentace orgánu veřejné správy, které obsahují osobní údaje. Interní auditor tudíž shromažďuje, zaznamenává, ukládá, používá, zpřístupňuje a šíří osobní údaje. Interní auditor je zpracovatelem osobních údajů.

Základní úkoly pověřence pro ochranu osobních údajů jsou stanoveny v čl. 39 obecného nařízení o ochraně osobních údajů. Jde zejména o poskytování poradenství, ověřování souladu s právními předpisy upravujícími ochranu osobních údajů, posuzování vlivu připravovaných opatření na ochranu osobních údajů a spolupráci s dozorovým úřadem. V případě sloučení funkce interního auditora a pověřence pro ochranu osobních údajů se pověřenec dostává do střetu zájmu, protože jako interní auditor plní úkoly, u kterých v široké míře zpracovává osobní údaje a jeho činnost by měla být podřízená nezávislému a objektivní posouzení pověřence pro ochranu osobních údajů. Ve sloučené pozici může mít pověřenec zájem jako interní auditor na určitém způsobu zpracování osobních údajů. Jeho poradenská činnost a doporučení v tomto případě nebude naplňovat požadavek obecného nařízení plnit své povinnosti a úkoly nezávislým způsobem.

I když na první pohled, v důsledku použité terminologie, může vymezení úkolů pověřence pro ochranu osobních údajů evokovat podobnost s úkoly, které jsou svěřeny internímu auditorovi, nelze je zaměňovat. Naplňování povinností vyplývajících orgánu veřejné správy z právních předpisů upravujících ochranu osobních údajů, včetně plnění úkolů pověřence pro ochranu osobních údajů, jsou součástí vnitřního kontrolního systému.

Vnitřním kontrolním systémem v rámci orgánu veřejné správy je souhrn nástrojů, procesů a opatření, které jsou zavedeny v organizaci k ošetření rizik, která ohrožují dosažení stanovených cílů. Jedná se tedy o jakýkoliv řídicí kontrolní mechanismus, včetně výkonu funkce pověřence pro ochranu osobních údajů. Interní auditor podle § 28 odst. 2 zákona o finanční kontrole objektivně a nezávisle přezkoumává vnitřní kontrolní systém a dává doporučení ke zdokonalování jeho kvality. Podle § 29 odst. 4 zákona o finanční

kontrole nelze interního auditora pověřit úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů. V praxi může nastat situace, že činnost pověřence pro ochranu osobních údajů bude prověřována interním auditorem a dle názoru interního auditora nebude pověřenec postupovat v souladu s právními předpisy nebo vnitřními směrnicemi orgánu veřejné správy. V tomto případě interní auditor předloží vedoucímu orgánu veřejné správy doporučení k přijetí opatření k nápravě zjištěných nedostatků. Bude-li funkce pověřence a interního auditora sloučena, ověření interního auditora nebude objektivní a nezávislé, tak jak to stanoví § 28 odst. 2 zákona o finanční kontrole. Zároveň bude porušeno ustanovení § 29 odst. 4 zákona o finanční kontrole, které zakazuje pověřovat interního auditora úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů.

Právní úprava zaručuje internímu auditorovi a pověřenci pro ochranu osobních údajů nezávislé postavení a vylučuje střet zájmů. Tato nezávislost je zaručená pro tyto funkce samostatně. V případě jejich sloučení nebude požadavek na zajištění nezávislosti naplněn ani u jedné z nich.

Výkon funkce pověřence pro ochranu osobních údajů interním auditorem nebo zařazení pověřence do útvaru interního auditu je v rozporu s ustanoveními zákona o finanční kontrole, které upravují funkční nezávislost a postavení interního auditora (zejména ustanovení § 28 odst. 2 a 3, § 29 odst. 1 a 4 zákona o finanční kontrole).

Neslučitelnost funkce pověřence pro ochranu osobních údajů a interního auditora se vztahuje jen na orgány veřejné správy, které zřídily útvar interního auditu nebo výkonem interního auditu zvlášť pověřily zaměstnance podle § 28 odst. 1 zákona o finanční kontrole. Neslučitelnost funkcí se tudíž nevztahuje na obce do 15 000 obyvatel, které dle zákona nahradily interní audit přijetím jiných opatření podle § 29 odst. 6 zákona o finanční kontrole. Z celkového počtu obcí se neslučitelnosti funkcí pověřence pro ochranu osobních údajů a interního auditora vztahuje jen na 89 obcí, které přesahují 15 000 obyvatel.[1]

Dále se neslučitelnost funkcí nevztahuje na organizační složky a příspěvkové organizace, u kterých zřizovatel nahradil funkci útvaru interního auditu výkonem veřejnosprávní kontroly podle § 29 odst. 5 zákona o finanční kontrole.

Zákon o finanční kontrole neupravuje sankce za porušení ustanovení upravujících interních audit. Ministerstvo financí není oprávněno ukládat sankce ani nápravné opatření v případě jeho porušení.

Porušení ustanovení obecného nařízení o ochraně osobních údajů upravující povinnost zajistit, aby pověřenec nevykonával úkoly a povinnosti, které by mohli vést ke střetu

[1] Údaj dle Českého statistického úřadu k 1. 1. 2018.

zájmu, lze podle článku 83 obecného nařízení sankcionovat správní pokutou až do výše 10 mil. EUR.

Příloha č. 4 – Ukázka výzvy k udělení souhlasu se zasíláním osobních údajů emailem[146]

„Jménem Nemocnice jako správce předmětných osobních údajů Vás upozorňuji na rizika jejich zaslání běžným e-mailem, tj. nezabezpečenou e-mailovou zprávou bez využití např. šifrování obsahu.
U nezabezpečeného e-mailu nelze garantovat, mimo jiné to, že jeho obsah nebude po odeslání přečten či upraven neautorizovanou osobou.
Akceptujete-li tato rizika a souhlasíte-li se zasláním předmětných osobních údajů běžným e-mailem, prosím, odpovězte mi na tuto zprávu e-mailem s textem „Souhlasím".
Odpověď Vám následně bude zaslána na e-mailovou adresu, ze které odešlete svůj souhlas.
Podrobnosti o bezpečné komunikaci Nemocnice s pacienty se dočtete zde.„

[146] Dokument dostupný na interních intranetových stránkách Nemocnice.

Příloha č. 5 – Protokol o úniku osobních údajů[147]

Protokol o úniku osobních údajů	
Číslo protokolu	
Správce/Zpracovatel	
Nahlašující osoba	
Datum a čas hlášení	
Řešitelská komise	
Zjištění	
Posouzení rizik	
Zamítnutí incidentu	
Porušení ochrany	
Nahlášení na ÚOOÚ	
Zpracování mimo EU	
Okamžité opatření	
Rozhodnutí	
Údaje k nahlášení	
Návrh systémových opatření	
Návrh upozornění subjektů osobních údajů	
Vyhodnocení úniku	
Zpracovatel za pracoviště	
Schvalovatel	Pověřenec pro ochranu osobních údajů Datum a podpis:

[147] Dokument dostupný na interních intranetových stránkách Nemocnice.