ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Bakalářská práce

Problematika GDPR ve vybraném subjektu

The issue of GDPR in the selected entity

Aneta Vašáková

Plzeň 2019

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta ekonomická
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Aneta VAŠÁKOVÁ**
Osobní číslo:	**K16B0368P**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Podniková ekonomika a management**
Název tématu:	**Problematika GDPR ve vybraném subjektu**
Zadávající katedra:	**Katedra financí a účetnictví**

Zásady pro vypracování:

1. Zpracujte teoretická východiska k problematice ochrany osobních údajů.
2. Na příkladu konkrétního subjektu proveďte analýzu problematiky GDPR.
3. Zhodnoťte dopady implementace GDPR na daný subjekt.
4. Stanovte doporučení a závěry.

Rozsah grafických prací: **neuveden**

Rozsah kvalifikační práce: **40 - 60**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

- **JANEČKOVÁ, Eva.** *GDPR: praktická příručka implementace.* **Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.**
- **Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).**
- **NEZMAR, Luděk.** *GDPR: praktický průvodce implementací.* **Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4.**
- **ŽŮREK, Jiří.** *Praktický průvodce GDPR.* **Olomouc: ANAG, 2017. ISBN 978-80-7554-097- 3.**

Vedoucí bakalářské práce: **Ing. Pavlína Hejduková, Ph.D.**
Katedra financí a účetnictví

Datum zadání bakalářské práce: **23. října 2018**

Termín odevzdání bakalářské práce: **23. dubna 2019**

Doc. Ing. Michaela Krechovská, Ph.D.
děkanka

L.S.

Ing. Pavlína Hejduková, Ph.D.
vedoucí katedry

V Plzni dne 23. října 2018

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma

„*Problematika GDPR ve vybraném subjektu*“

vypracovala samostatně pod odborným dohledem vedoucí bakalářské práce za použití pramenů uvedených v přiložené bibliografii.

Plzeň dne ……. ……..……..…

podpis autora

List s poděkováním

Děkuji vedoucí bakalářské práce paní Ing. Pavlíně Hejdukové, Ph.D., za ochotu, za cenné rady a její čas. Poděkování patří i společnosti TrenDent s. r. o., která mi poskytla své podklady pro praktickou část mé bakalářské práce. Dále bych chtěla poděkovat své rodině, která mi poskytovala zázemí při studiu a byla k dispozici pokaždé, když jsem jejich pomoc potřebovala.

Obsah

Úvod

Mezi aktuální témata patří ochrana při poskytování osobních údajů. Diskuse vedené na toto téma nejen v odborné literatuře, ale prakticky ve všech médiích, svědčí o tom, že je obecně vnímána jako ochrana každého z nás.

Nejrůznější osobní údaje o sobě poskytuje každá fyzická osoba v souvislosti s různými činnostmi. Osobní údaje se používají v zaměstnání, vzdělání, v rámci sociálních sítí či nejrůznějších obchodních operací. Ne vždy se jedná o poskytnutí osobních údajů na základě vlastního rozhodnutí. Existují totiž rozličné skutečnosti, které vedou ke zpracování a předávání osobních údajů. Ochrana osobních údajů je velmi významná, a proto je i právně vymezena.

Téma práce bylo zvoleno z důvodu jeho aktuálnosti, jelikož zpracování osobních údajů bylo v rámci Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů regulováno. Nařízení vešlo v platnost 25. května 2018 a přineslo zpřísnění podmínek pro zpracovatele osobních údajů a více práv osob, jejichž osobní údaje jsou zpracovávány.

Práce je členěna do 10 kapitol. První kapitoly zpracovávají východiska k problematice ochrany osobních údajů. Postupně je charakterizována právní úprava, vývoj ochrany osobních údajů v České republice, rysy a cíle GDPR, nové přístupy a povinnosti dle GDPR. Dále jsou definovány základní pojmy problematiky jako osobní údaj, subjekt údajů, správce, zpracovatel, pověřenec a profilování. Následně jsou definovány zásady GDPR. Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů nově přineslo i práva osob, které jsou charakterizovány v rámci další kapitoly. Práce obsahuje i kapitolu aplikace GDPR, která je zaměřená na kroky implementace a kontrolu dodržení GDPR. Dále je charakterizováno zdravotnictví jako resort a vymezena jeho specifika, jelikož vybraným subjektem je zubní klinika.

Závěrečné dvě kapitoly práce popisují, analyzují a hodnotí problematiku GDPR v zubní klinice TrenDent s. r. o. z resortu zdravotnictví. V závěru práce bude proveden nástin optimálního řešení pro společnost TrenDent s. r. o.

Cíl práce a metodický postup řešení

Hlavním cílem práce je zhodnotit dopady GDPR na příkladu konkrétního subjektu a stanovit případná doporučení tohoto Nařízení pro daný subjekt do budoucna. Bakalářská práce si stanovila též zodpovědět na níže uvedené otázky týkající se sledovaného subjektu:

- Kdo se ve společnosti zabývá problematikou GDPR?
- Kdo zpracoval analýzu rizik a co obsahuje?
- Jak jsou data ve společnosti zabezpečena?
- Kdo a kde se školil?
- Jaké jsou další postupy po školení?
- Kdo bude kontrolovat dodržování směrnic?
- Má společnost pověřence pro ochranu osobních údajů?
- Jak a kdy bude směrnice GDPR aktualizována?
- Kde jsou data společnosti uloženy?

Práce je zpracována zejména na základě tištěných i elektronických publikací, monografií a právních předpisů. Metodami, které byly zvoleny k naplnění stanoveného cíle práce, jsou rešerše, deskripce, analýza a v závěru práce metoda syntézy.

V bakalářské práci bude zhodnocena problematika GDPR ve vybraném subjektu se závěrečným doporučením a vypočítán ušlý zisk, kterého by společnost mohla dosáhnout v případě, kdyby se nemusela zabývat zavedením Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ve své zubní klinice.

1 Charakteristika obecného nařízení GDPR

1.1 Právní úprava

Právním rámcem pro zpracování osobních údajů na celém území EU je obecné nařízení GDPR (anglicky General Data Protection Regulation), plným názvem Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a zrušení směrnice 95/46/ES (Úřad pro ochranu osobních údajů, 2017).

Nařízení o ochraně osobních údajů z roku 1995 bylo nahrazeno novým Nařízením Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, které je výsledkem tvrdého procesu sjednávání s řadou pozměňovacích námětů. Nařízení přináší nejen zvýšení povinností týkající se ochrany osobních údajů, ale i hrozící pokuty. Je tedy potřeba pečlivě přehodnotit vnitřní postupy ochrany osobních údajů, aby bylo dosaženo souladu s GDPR (Voigt, 2017).

Platnost daného nařízení byla stanovena na 25. květen 2018 a substituuje všechny existující zásady ochrany a zpracování údajů, na kterém stojí unijní soustava ochrany osobních údajů (Nezmar, 2017).

Nařízení GDPR je právním předpisem s dopadem na celý svět, jelikož se váže na veškeré subjekty, které zachází s osobními údaji občanů Evropské unie či mají sídlo na území Evropské unie (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Adaptační zákon modifikuje současnou právní úpravu státu pro ochranu osobních údajů. Tento zákon v ČR jako jedné z posledních zemí EU ještě nebyl po téměř roční platnosti GDPR přijat. (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

1.2 Vývoj ochrany osobních údajů v České republice

Zákon č. 87/1862 Sb. z. s., o ochraně svobody osobní zákon č. 88/1862 Sb. z. s., na ochranu svobody domovní, jsou prvotními zákony, které byly v České republice uzákoněny. V rámci samostatného Československa byl přijat Ústavní zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního (podle § 107, 112 a 116 ústavní listiny). Od zmíněného období až do závěru 20. století se zmínky o ochraně

osobních údajů v právním řádě České republiky objevují téměř jen v souvislosti s vydáváním a držením cestovních dokladů, či jiných dokladů, kde se osobní údaje vyskytují. Podrobně se uzákoňovat v České republice začala ochrana osobních údajů zákony teprve v 90. letech 20. století. Ochrana osobních údajů v informačních systémech byla řešena zákonem č. 256/1992 Sb. Následovala Listina základních práv a svobod, vyhlášená Usnesením předsednictva České národní rady č. 2/1993 Sb. Zákon č. 101/2000 Sb., o ochraně osobních údajů, který byl přijat v roce 2000, a který je platný i v současné době. O devět let později, tedy v roce 2009 vstoupila v platnost Lisabonská smlouva, která novelizuje Smlouvu o Evropské unii (Navrátil a kol., 2018).

1.3 Rysy GDPR

GDPR představuje evoluci v ochraně osobních údajů. Zřetelné stanovení práv subjektu údajů, nastavení povinností správců a zpracovatelů nebo dozorových úřadů, definování povinností ve spojitosti k zahraničí a mezinárodním institucím. To vše lze považovat za jeho přínos (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

GDPR je stavěno na modelu performance-based regulace, kde jsou povinnosti jen velmi obecně určeny právní úpravou a každý subjekt si sám stanoví postup, jakým dané povinnosti plní. Výhodu zmíněného modelu představuje možnost, aby si každý subjekt upravil řešení na míru vlastním požadavkům (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

1.4 Cíle GDPR

Cílem GDPR je asimilace právní regulace ochrany osobních údajů poměrům 21. století, integrace práva ochrany osobních údajů ve veškerých státech Evropské unie a v ostatní státech, na které dopadá. Jedním s dalších cílů je podpoření důvěryhodnosti Evropské unie a jejích členských států, států, na které GDPR dopadá a jiné státy, které mají zájem ve vývoji obchodu s Evropskou unií a s tím souvisícím svěřením osobních údajů mezi státy. Konečným cílem je podpora práv ve sféře ochrany osobních údajů všech osob, které jsou subjekty údajů a získat sjednoceného vysvětlení GDPR dozorovými úřady jednotlivých států Evropské unie (Navrátil a kol., 2018).

1.5 Nové přístupy

GDPR je stavěno na dvou nových přístupech, a to na principu odpovědnosti správce a přístupu založeném na riziku (Navrátil a kol., 2018).

Princip odpovědnosti správce

Tento princip zahrnuje odpovědnost správce za dodržení zásad zpracování osobní údajů a současně povinnosti správce tento soulad doložit. Doložení může proběhnout pomocí kodexu, osvědčení, certifikace nebo případně pomocí záznamů o činnostech zpracování (Navrátil a kol., 2018).

Přístup založený na riziku

V pojetí za účinnosti zákona č. 101/2000 Sb., o ochraně osobních údajů tento přístup představuje, že správce již od počátku prvního zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a vzít na vědomí nebezpečí pro práva a svobody fyzických osob a tomu přizpůsobit i zabezpečení osobních údajů (Úřad pro ochranu osobních údajů, 2017a).

V obecném nařízení navíc tento přístup znamená použití dodatkových aplikacích pro některé správce, kdy zpracování osobních údajů nebo porušení bezpečnosti představuje nebezpečí či vysoké nebezpečí pro práva a svobody fyzické osoby a je tedy důvod aplikovat tyto povinnosti. Nové povinnosti, o kterých nelze hovořit, že se plošně vztahují na všechny správce nebo zpracovatele řadíme zápisy o činnostech zpracování, označení pověřence pro ochranu osobních údajů, posouzení vlivu na ochranu osobních údajů a předcházející konzultace s dozorovým úřadem (Úřad pro ochranu osobních údajů, 2017a).

1.6 Nové povinnosti dle GDPR

Mezi nové povinnosti, které s sebou obecné nařízení o ochraně osobních údajů nese, lze zařadit vypracování a posouzení vlivu činností na ochranu osobních údajů, umožnění přenositelnosti osobních údajů od jednoho správce k jinému, povinnost určit pověřence ochrany a provádět přípravné konzultace s Úřadem pro ochranu osobních údajů. Dále pak sdělovat případy narušení bezpečí osobních údajů do 72 hodin od doby, kdy se o narušení osobních údajů správce dozví, a to na Úřad pro ochranu osobních údajů a také osobám, jejichž osobní údaje byly narušeny. Pro správce osobních údajů je také novou povinností vést o zpracování osobních údajů zápisy (Navrátil a kol., 2018).

2 Základní pojmy v souvislosti s osobními údaji

2.1 Osobní údaj

Každou informaci o identifikované nebo identifikovatelné fyzické osobě či subjektu údajů nazýváme osobním údajem. Tzv. identifikátorem či zvláštními prvky lze přímo či nepřímo identifikovat fyzickou osobu. Identifikátor představuje například jméno, bydliště, telefonní číslo či email. Zvláštními prvky pak rozumíme fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity dané fyzické osoby (Nezmar, 2017).

2.1.1 Zpracování osobních údajů

„Zpracování je jakákoli operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů 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.“ (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)., 2018).

Zpracování osobních údajů neodlišně souvisí s pojmem osobní údaj. Lze je tedy považovat za stejně podstatné, jelikož ke zpracování osobních údajů a k aplikaci určených pravidel dochází pouze za podmínky, že určitá činnost reprezentuje zpracování osobních údajů ve smyslu obecného nařízení (Žůrek, 2017).

2.1.2 Citlivý údaj

Citlivý údaj je zvláštní kategorií osobního údaje, které mohou subjekt údajů poškodit či způsobit diskriminaci. Na tento typ údajů je kladena zvýšená ochrana při jejich zpracování. Jedná se o údaj, který vypovídá o rasovém či etickém původu, náboženském vyznání či filozofickém přesvědčení, politických názorech, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci a genetické či biometrické údaje, které jsou zpracovávány za účelem identifikace fyzické osoby (Nezmar, 2017).

Citlivé údaje lze zpracovávat jen v některých případech, pokud například subjekt údajů udělil výslovný souhlas a z důvodu významného veřejného zájmu je zpracování

nevyhnutelné či zpracování je potřebné pro plnění povinností v oblasti pracovního práva, sociálního zabezpečení a sociální ochrany (Nezmar, 2017).

2.2 Subjekt údajů

Subjektem údajů je žijící fyzická osoba, ke které se osobní údaje vztahují. Na právnické osoby se toto nařízení nevztahuje. Vyplývá tak, že právnická osoba subjektem údajů není, tzn. údaje, které se ji týkají nejsou osobními údaji (Nezmar, 2017).

Pokud zaměstnanci právnické osoby využívají e-mailovou adresu ve formátu jmeno.prijmeni@nazevfirmy.cz, pak se již jedná o osobní údaj (Úřad pro ochranu osobních údajů, 2017b).

2.3 Správce

Správcem je subjekt, který stanoví účely a způsoby zpracování osobních údajů. Subjekt s libovolnou právní formou může být správcem, tedy i fyzická osoba. Správce zodpovídá za zpracování osobních údajů (Nezmar, 2017).

Správce zpracovává osobní údaje za účelem plynoucím z jeho působení, například z důvodu zákonem stanovené povinnosti, ze smluv či zpracování pro vlastní určené záměry, a to například pro své oprávněné zájmy (Úřad pro ochranu osobních údajů, 2017b).

2.4 Zpracovatel

Zpracovatel je subjektem, který provádí pro správce zpracovatelské operace spojené s osobními údaji. Tento subjekt zpracovává pouze takové operace, které mu správce svěří, nebo které vyplývají z činnosti, pro kterou byl správcem zpracovatel najatý (Nezmar, 2017).

Správce není zavázán si zpracovatele najmout, to znamená, že zpracovatel není povinným elementem při zpracování osobních údajů (Úřad pro ochranu osobních údajů, 2017b).

2.5 Pověřenec

Novým institutem, který GDPR přináší je pověřenec osobních údajů. Vystupují zde jako odborníci a jejich úkolem je napomáhat rozhodujícím způsobem při zajištění ochrany osobních údajů u fyzických či právnických osob, u kterých provozují svoji činnost. Pověřenci nesou odpovědnou za svoji odbornou práci a jsou hlavně zavázáni poskytovat svým zaměstnancům nebo klientům odbornou pomoc pro zajišťování plnění povinností

podle GDPR a lokálních nařízení. V případě, kdy na základě porušení předpisů vznikne fyzické či právnické osobě újma, za odčinění zodpovídá zaměstnavatel nebo klient pověřence. Až ten má možnost požadovat odškodnění od pověřence, ale pouze v situaci, kdy pověřenci prokáže zavinění vzniklé škody (Navrátil a kol., 2018).

2.6 Profilování

„Jde o formu automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu.“ (Úřad pro ochranu osobních údajů, 2017b).

S profilováním se můžeme setkat např. v oboru financí, kdy finanční subjekty profilují např. uchazeče o hypotéku, u kterého hodnotí schopnost splácet (Úřad pro ochranu osobních údajů, 2017b).

3 Zásady GDPR

3.1 Korektnost, transparentnost a zákonnost

Dostatečně korektní, specifické a transparentní musí být zákonné tituly, podle kterých je přijatelné provést veškerá zpracování osobních údajů. Tato zásada představuje předpoklad, že alespoň jeden z příčiny zpracování osobních údajů musí být uveden v Nařízení. V případě, kdy zákonný důvod neexistuje nebo pomine, je nevyhnutelné osobní údaj zlikvidovat (Janečková, 2018).

Popis zpracování, který odsouhlasil subjekt údajů v rámci GDPR charakterizuje korektnost (Nezmar, 2017).

Zřetelné a lehce přístupné s použitím srozumitelných jazykových prostředků, takové by dle zásady transparentnosti měly být informace, které subjekt osobních údajů dostává od správce nebo na něž má právo (Žůrek, 2017).

Transparentnost je splněna v případě, kdy je subjektu údajů oznámeno, jaké zpracování bude probíhat, a to ještě dříve, než začne shromažďování údajů nebo potencionální následující změny (Nezmar, 2017).

Hlavním potřebným předpokladem, aby bylo možné považovat zpracování osobních údajů za zákonné, je výskyt právního důvodu. Zpracování nesmí být protiprávní, tedy jeho účel nesmí být nelegální nebo nelegitimní. Protiprávní zákaz zpracování zahrnuje i právní řád obecně, který nesmí být porušen. V případě, že zpracování probíhá v souladu s Nařízením, ale například je v rozporu s občanským zákoníkem, zásada zákonnosti je porušena (Janečková, 2018).

3.2 Omezení účelem

Omezení účelem je možné označit za nejdůležitější zásadu zpracování osobních údajů. Tato zásada nejpodstatněji vymezuje rozsah, v jakém může správce s osobními údaji zacházet. Správce si stanoví důvod, kvůli kterému osobní údaje zpracovává. Po vymezení účelu může osobní údaje, až na výjimky, zpracovávat pouze za tímto účelem. Toto stanovení je důležité také proto, že se od něj odvíjejí následující zásady: minimalizace dat a omezení uložení (Nulíček, a kol. 2017).

Stanovení musí proběhnout nejpozději při shromáždění osobních údajů, pokud zákon neuvádí jinak. Účel musí splňovat tři charakteristiky, a to být určitý, výslovně vyjádřený a legitimní (Janečková, 2018).

3.3 Minimalizace dat

Osobní údaj podle Nařízení musí: „být *přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro která jsou zpracovávány (minimalizace) údajů.“* (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), 2018)

Splnění této zásady vyžaduje přesné definování minimálního rozsahu konkrétních údajů, které jsou pro naplnění stanoveného účelu skutečně nezbytné. Nutností je tak o každém osobním údaji prohlásit, zda je nebo není pro stanovený účel potřebný, popř. při kombinaci, s kterými údaji jsou potřebné. Záměrem této zásady je docílit stavu, kdy účelu zpracování bude docíleno s co nejmenší skupinou použitých osobních údajů (Janečková, 2018).

3.4 Přesnost

Věrné, takové musí být podle zásady přesnosti zpracované údaje. Údaje mají odpovídat realitě a v situaci, kdy je to nezbytné musí být aktualizované. V případě nepřesného údaje musí správce tyto údaje opravit nebo odstranit pomocí všech rozumných opatření. Přesné údaje, však nemusejí vždy znamenat údaje pravdivé. Správce neodpovídá za nepřesnost údajů v momentě, kdy subjekt udá nepřesné údaje. Za nesprávné údaje považujeme údaje např. nepřesné z pohledu gramatických nebo výpočetních chyb či údaje, které v souvislosti s některou osobou nesvědčí o pravdě (Nulíček, a kol. 2017).

Princip přesnosti se prolíná také do práva subjektů údajů na opravu. V případě, kdy správce přijme od subjektu žádost je potřeba ověřit. Pokud nejsou soudobě přesné, měl by je obnovit (Nulíček, a kol. 2017).

Nezmar (2017) uvádí příklad významu slova přesnost, jak mu rozumí GDPR na zdravotnictví takto: Chybná diagnóza zdravotního stavu je ve složce záznamů pacienta uchována i poté, co je určena diagnóza správná, jelikož je významná při objasnění pacientovi léčení či příštích zdravotních problémech.

3.5 Omezení uložení

Osobní údaje musí být uschovány v podobě umožňující identifikace subjektu údajů po období ne delší, než je potřeba pro účely, za kterými jsou zpracovávány. V právní úpravě je tato zásada obsažena v § 5 odst. 1 písm. e), na základě, kterého je správce zavázán archivovat osobní údaje výhradně jen po období, které je potřebné k účelu jejich zpracování (Janečková, 2018).

Nařízení neurčuje minimální či maximální termíny, po které by měly být osobní údaje uchovány. Pro organizaci to v praxi znamená, že je její povinností sledovat dobu archivace osobních údajů, posoudit účel či účely, pro které uchovává informace při rozhodnutí, zda a jak dlouho si je uchová, spolehlivě smazat nebo zlikvidovat informace, které již pro stanovené účely jsou nepotřebné a obnovit, archivovat či bezpečně smazat informace, v případě, kdy jsou údaje zastaralé (Nezmar, 2017).

3.6 Integrita a důvěrnost

Osobní údaje musí být náležitě zabezpečeny před hrozbami zevnitř i zevně organizace, a to v podobě automatizovaného i papírového zpracování (Janečková, 2018).

Zařazením integrity a důvěrnosti do základních zásad Nařízení prohlašuje zabezpečení osobních údajů za povinnost klíčovou (Nulíček, a kol. 2017).

3.7 Zásada odpovědnosti

Odpovědnost za plnění všech přepisů stanovených GDPR je správce, který musí být schopen to vždy doložit. Tato zásada pro správce je novým elementem ve zpracování osobních údajů. Pro doložení zásady odpovědnosti je pro správce důležité zvolit vhodné technické a organizační opatření (Janečková, 2018).

4 Práva osob

4.1 Právo být informován

V případě práva být informován se jedná o povinnost správce osobních údajů sdělit informace o zpracování, které jsou pravdivé, a to zpravidla prostřednictvím zprávy o ochraně osobních údajů. V rámci toho práva je důležitá transparentnost při využívání osobních údajů. Informace, které jsou dány zpracováním osobních údajů, musí splňovat stručnost, jasnost, srozumitelnost, snadnou dostupnost, musí být psané jasným a srozumitelným jazykem a musí být poskytnuté zdarma, tedy bez jakýchkoliv poplatků (Nezmar, 2017).

Součástí povinnosti o informovanosti pro správce je i oznamovací povinnost, která vzniká v případě opravy, výmazu či omezení zpracování osobních údajů. Správce má za povinnost ohlásit jednotlivým adresátům, kterým jsou osobní údaje zpřístupněné, všechny opravy, výmazy či omezení zpracování osobních údajů. Výjimka je v případě, kdy se to projeví jako nemožné či to potřebuje nepřiměřené úsilí (Nezmar, 2017).

4.2 Právo na přístup k osobním údajům

Právo na přístup vyobrazuje subjektu údajů právo na potvrzení od správce, zda osobní údaje, které se k němu vztahují, jsou nebo nejsou zpracovány subjektem údajů. V případě, kdy údaje jsou zpracovány má subjekt údajů pravomoc získat k těmto osobním údajům přístup. Přístup v této situaci se váže například i k informacím ohledně účelu zpracování, plánovaného období, po které budou osobní údaje uloženy či právo předložit stížnost u dozorového úřadu (Janečková, 2018).

Nulíček, a kol. (2017) uvádí, že při zpracování značného počtu osobních údajů subjektu má správce údajů možnost požádat subjekt údajů o uvedení konkrétních informací, které žádá. Nicméně právo na přístup k osobním údajům nesmí být omezováno ani odmítnuto. V situaci, kdy subjekt údajů neupřesní svou prosbu o údajích, je nutné poskytnout informace v úplném rozsahu.

4.3 Právo na opravu

Právo na opravu souvisí se zpracováním přesných údajů, které je povinností správce osobních údajů a popisuje právo subjektu údajů, aby správce obnovil nepravdivé osobní údaje, které se k subjektu údajů vztahují, bez zbytečného odkládání (Janečková, 2018).

Podle práva na opravu má subjekt další právo, a to doplnění neúplných údajů. Toto právo se použije v případě, kdy chce subjekt správci poskytnout na základě vlastního rozhodnutí doplňkové osobní údaje. Doplnění neúplných údajů v praxi probíhá pomocí elektronického formuláře, ve kterém subjekt údajů vyplní jen vstupní pole, které jsou nepovinné. K doplnění může dojít také pomocí libovolného prohlášení určenému správci osobních údajů (Nulíček, a kol. 2017).

4.4 Právo na výmaz

Právo na výmaz či právo na vymazání je známé i jako „právo být zapomenut“. Podstatou tohoto práva, je poskytnout jednotlivci příležitost požádat o smazání či odstranění osobních údajů, nehledě na to, jestli existuje pro jeho následující zpracování některý přesvědčivý argument. Toto právo však nelze brát jako úplné „právo být zapomenut“. Osoba má právo na výmaz a zamezení zpracování jen za zvláštních okolností, které dále uvádí Nezmar (2017):

- pro účel, kvůli kterému byly osobní údaje prvotně shromážděny či zpracovány, jsou již nepotřebnými;
- při zrušení souhlasu jednotlivce, pokud se zpracování zakládá na souhlasu a pro zpracování neexistuje ani jeden další právní důvod;
- na zpracování je vznesena námitka a neexistuje ani jeden převládající argument pro zpracování osobních údajů;
- osobní údaje byly zpracovány nezákonně (tzn., že došlo k porušení GDPR);
- v případě, kdy ke zpracování osobních údajů dětí není dán rodičovský souhlas;
- k uspokojení právní povinnosti předepsané právem Unie či členského státu, které se týká správce, musí být osobní údaje vymazány.

Povinnost se neprosadí, jestliže je zpracování nevyhnutelné například při výkonu práva na svobodu vyjádření či informace, v oboru veřejného zdraví z důvodu veřejné účasti či ve veřejném zájmu se záměrem archivace (Janečková, 2018).

4.5 Právo na omezení zpracování

Nulíček, a kol. (2017) uvádí, že v následných případech má subjekt právo na to, aby správce údajů omezil zpracování:

- subjekt odmítá výstižnost osobních údajů, a to na dobu, která je pro správce údajů nezbytná k ověření přesnosti osobních údajů

- zpracování je nezákonné a subjekt neschvaluje výmaz osobních údajů, místo výmazu požaduje jen omezení použití osobních údajů
- osobní údaje jsou již pro správce nepotřebné vzhledem k účelu zpracování, ale subjekt je vyžaduje pro stanovení, výkon či obhajobu právních požadavků
- vznesením námitky subjektem proti zpracování, dokud nebude otestováno, jestli opodstatněné argumenty správce údajů převládají nad opodstatněnými argumenty subjektu.

Pokud bylo zpracování omezeno, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodu důležitého veřejného zájmu Unie nebo některého členského státu (Nulíček, a kol., 2017).

V případě, kdy bylo zpracování omezeno, mohou být omezené osobní údaje (Janečková, 2018).

4.6 Právo přenositelnosti

Získat osobní údaje, které se k subjektu vztahují a které poskytl správci, v čitelném formátu je dalším právem osob v oblasti GDPR. S tímto právem se váže i pravomoc, získané osobní údaje, svěřit jinému správci. Uplatnění tohoto práva je možné v případě, kdy zpracování je stavěno na souhlasu, na smlouvě nebo zpracování je prováděno automatizovaně (Navrátil a kol., 2018).

Účelem je snadný přenos osobních údajů a jejich opakované využití v různých službách. Záměrem toho práva je zlepšení přístupnosti k informacím (Nezmar, 2017).

4.7 Právo vznést námitku

Právo vznést námitku na zpracování osobních údajů, které se ho týkají, má subjekt údajů kdykoliv, a to včetně profilování. Zpracování musí být pozastaveno do doby, kdy správce údajů prokáže relevantní opodstatněné důvody pro zpracování, které převládají nad zájmy či pravomocemi a svobodami subjektu údajů (Janečková, 2018).

Existuje však námitka, které musí být vždy vyhověno. Jedná se o případ zpracování osobních údajů za účelem přímého marketingu. Zde má subjekt údajů také právo vznést námitku proti zpracování kdykoliv na údaje, kterého se ho pro daný marketing týkají (Navrátil a kol., 2018).

5 Aplikace GDPR

5.1 Kroky implementace GDPR

Implementace GDPR nepředstavuje nijak komplikovanou sadu opatření. Nejdříve je nezbytné zpracovat přehled všech typů osobních údajů, se kterými společnost pracuje, upřesnit důvody, proč tak činí, a dále definovat procesy a prostředky, kterými tak dělá (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018b).

Katalog osobních údajů

Katalog osobních údajů je prospěšný nástroj a vhodný první krok. V rámci, kterého dojde k revizi a kategorizaci veškerých osobních údajů, které správce zpracovává. V resortu zdravotnictví by se měly členit osobní údaje na standardní osobní údaje a zvláštní kategorii osobních údajů. Předem stanovená struktura, resp. forma pro katalog údajů není předepsána. Každý katalog by ale měl obsahovat upřesnění účelu a rozsah opodstatněného zájmu. Katalog osobních údajů by měl zároveň obsahovat jednotlivé informační systémy, ve který osobní údaje jsou shromažďovány a uchovány (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Katalog operací zpracování osobních údajů

Katalog operací může být součástí katalogu osobních údajů, ale i samostatným dokumentem. Katalog operací je přehledem zákroků, které se s údaji v provozu dělají (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Obsahem katalogu operací by měl především být příjemce, typy zpracování osobních údajů, osoby s přístupem k údajům, doba, po kterou jsou údaje uchovány či způsob likvidace. Stejně jako u katalogu osobních údajů je zde doporučeno přiřadit jednotlivé informační systémy, které budou při operacích využity (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Analýza souladu s GDPR

K vypracovanému katalogu procesu zpracování je potřeba dále přiřadit odpovídající povinnosti podle GDPR. Výsledkem přiřazení povinností je stav připravenosti na GDPR. Správce je povinen dodržet princip odpovědnosti správce a zároveň musí být způsobilý tento soulad prokázat. K doložení slouží kodexy vystupování, certifikace či případná

osvědčení nebo údaje o činnostech zpracování. Přístup ke zpracování údajů o činnostech zpracování lze prokázat různými způsoby. Podmínkou je však dodržet základní parametry, které GDPR nařídilo (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Analýza rizik

Přístup zakládaný na riziku je jedním ze dvou klíčových principů při implementaci GDPR, a to jak ze strany subjektu údajů, tak ze strany správce (případně zpracovatele údajů). Při analýze jsou důležitými kroky vyhodnocení rizika, které je potřeba následně posoudit a rozhodnout buď o přijmutí opatření, které povede ke snížení a eliminaci rizika či riziko přijmout (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018b).

Součástí analýzy rizik by mělo být stanovení pravděpodobnosti a rozsah rizika, a to v závislosti k charakteru, míře, kontextu a cíli zpracování. Stanoveno by mělo být také, zda zpracování tvoří riziko či vysoké riziko pro pravomoci a svobody subjektu osobních údajů. Vyhodnocení rizik a uplatnění souhrnných kontrol by mělo probíhat pravidelně (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Technická a organizační opatření

GDPR vyžaduje technické prostředky, které se zakládají na volbě vhodných technických opatření ochrany osobních údajů (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Organizační opatření by měla vyjít z podmínek konkrétního poskytovatele, který poskytuje zdravotní služby. Přesněji řečeno správce nebo poskytovatele. Jmenování pověřence je příkladem jednoho z hlavních organizační opatření pro ochranu osobních údajů, neméně důležitým je pak úprava systému interních normativních aktů (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Proškolení osob

Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR (2018b) uvádí, že je potřebné mít ideálně podepsané poučení, o řádném proškolení osobami, které mají přístup k osobním údajům a pracují s nimi, zejména v případě, kde takových osob je více a může nastat selhání lidského faktoru.

Pravidelná aktualizace a audit

Výše uvedeným krokům je potřeba se věnovat pravidelně, průběžně je hodnotit a aktualizovat. Pravidelnost průběžného hodnocení určují vnitřní normativní akty správce nebo zpracovatele. Časový rozvrh by měl obsahovat pravidelný termín pro audit a aktualizaci, a také ad hoc audity nebo aktualizace, například při porušení ochrany osobních údajů (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

5.2 Kontrola dodržení GDPR

Oprávněn ke kontrole splnění GDPR a plnění povinností s tím spojené je dozorový úřad. Dozorové úřady jsou segmentovány na vnitrostátní dozorový úřad a Evropský sbor pro ochranu osobní údajů (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Dozorový úřad

V České republice zodpovídá za kontrolu a dodržení GDPR Úřad pro ochranu osobních údajů (ÚOOÚ), který koná dozor nad dodržením zákonem určených povinnostech při zpracování osobních údajů, spravuje registr s povoleným zpracováním osobních údajů, přijímá výtky a návrhy občanů na přestoupení zákona či dává odborné konzultace v oblast ochrany osobních údajů (Úřad pro ochranu osobních údajů, 2017c).

„Dozorový úřad sestaví seznam zpracování, kde je posouzení vlivu na ochranu osobních údajů povinné a může sestavit seznam zpracování, kde posouzení vlivu není povinné.“ (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a). To charakterizuje novou povinnost, kterou Úřad pro ochranu osobních údajů s účinností GDRP dostává, s dopadem i do zdravotnictví.

K 30. březnu 2019 vyšel článek na serveru Novinky.cz, který píše, že za nedodržení GDPR by se sankce mohly teoreticky vyšplhat až na 20 milionů eur, tedy zhruba 512 milionů Kč. Úřad pro ochranu osobních údajů při zavedení GDPR uvedl, že v českých podmínkách chce udělit sankce nejvýše do deseti milionů korun. Pokutu považují až za poslední možnost, a to v případě kdy jsou všechny ostatní prostředky k nápravě vyčerpány. Úřad pro ochranu osobních údajů k 30. březnu 2019 pravomocně neudělil žádnou pokutu (www.novinky.cz, 2019).

Evropský sbor pro ochranu osobních údajů

Vedoucí jednoho dozorového úřadu z každé členské země a evropský kontrolor ochrany údajů či jejich zástupci utváří sbor pro ochranu osobních údajů. Jde o evropský orgán zajišťující jednotné použití GDPR uvnitř Evropské unie. Mezi povinnosti sboru z vlastního podnětu či případně na prosbu komise je zejména monitorování a zajištění správného uplatnění tohoto nařízení či v rámci mechanismu jednotnosti správa elektronického registru nařízení přijatých dozorovými úřady a soudy (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

6 Zdravotnictví

6.1 Specifika zdravotního trhu

Zdravotnictví je jedním z oboru národního hospodářství tzv. terciální sféry, na základě produkování zdravotnické služby (Gladkij, 2003).

Do odvětví zdravotnictví spadá veřejná ochrana zdraví, zdravotnické služby, lázeňské a relaxační služby, preventivní opatření, léky a léčiva aj. (Hejduková, 2015).

Klíčové funkce zdravotnických služeb lze definovat dle Gladkij (2003) jako:

- pomoc udržení zdraví a zabránění jeho poruch
- vracet lidi do běžného života pomocí diagnostiky a léčení poruch zdraví
- zdokonalovat kvalitu a délku života
- zajistit poskytnutí péče úměrně, hodnotně, úsporně a s potřebnou spravedlností.

Zdravotnické služby lze charakterizovat jako souhrn lidských činností, jejichž efekt praktičnosti se zakládá na práci. Mají povahu nehmotných činností provozovaných výhradně zdravotnickými pracovníky, a to zejména ve zdravotnických zařízení. Rozsah musí odpovídat odborné způsobilosti pracovníků (Durdisová, 2005).

Sítě zdravotnických zařízení tvoří zařízení státu, obcí, právnických a fyzických osob. Zdravotnická zařízení lze členit podle různých kritérií a to dle Durdisové (2005) na:

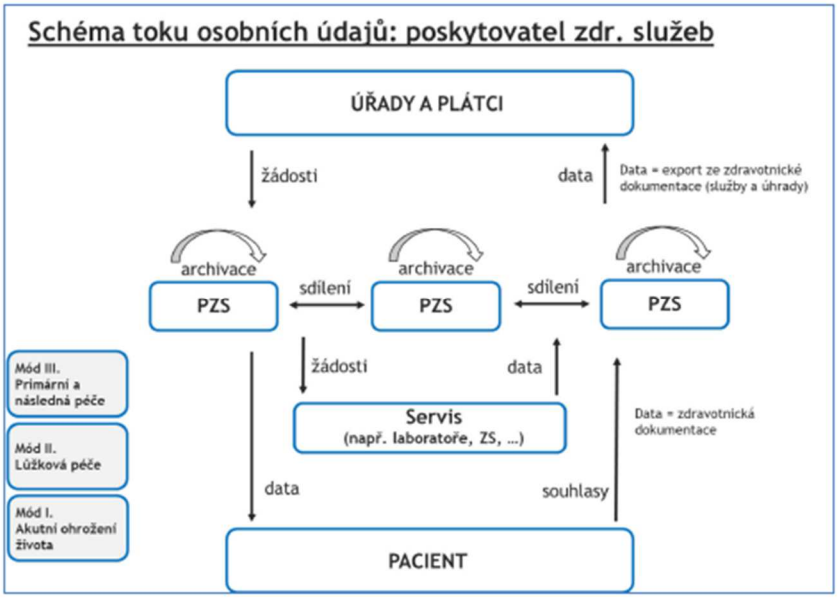
- státní a nestátní
- lůžková a ambulantní
- smluví a nesmluvní zařízení.

6.2 Specifika GDPR pro resort zdravotnictví

V oblasti zdravotnictví přineslo GDPR rozšíření práv pacientů, jakožto subjektu údajů a ve vztahu k těmto pravomocem se poskytovatelům zdravotních služeb rozšířily povinnosti, které musí respektovat. Analogické povinnosti s patřičnými úpravami se vztahují i na plátce, zřizovatele a správní úřady v resortu zdravotnictví (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

Ke specifikaci dochází, jelikož v resortu zdravotnictví jsou zpracovávány osobní údaje a zvláště citlivé osobní údaje, které se vážou k zdravotnímu stavu pacientů.

Obrázek 1 Tok osobních údajů při poskytování zdravotnických služeb



Zdroj: Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a

Osobní údaje, které poskytovatelé zdravotních služeb zpracovávají, je možné rozdělit do následující skupin:

- pacientovo údaje, kdy primárním zdrojem dat je zdravotnická dokumentace,
- údaje týkající se zaměstnanců, zdrojem jsou osobní spisy,
- dodavatelské údaje, návazně na smlouvy o zpracování údajů.

Zpracování osobních údajů v resortu zdravotnictví je ve vztahu k pacientům, zaměstnancům či dodavatelům. Ve vztahu k pacientům je poskytnutí informací o zpracování údajů i v situaci, kdy je zpracování konáno na základě zákona bez souhlasu pacienta nebo pro splnění právnických povinností, také v situaci poskytnutí „nadstandartních služeb“ nebo v rámci marketingového oslovení s pacientovo souhlasem. Ve vztahu k zaměstnancům se jedná o tok zpracování osobních údajů především ve spojení s plněním právnických povinností, zde je důležité rozlišení, kdy je potřebný a kdy nepotřebný souhlas se zpracováním osobních údajů. U dodavatelů se jedná o používání osobních údajů obousměrně a musí zde být zakotvena ochrana osobních údajů (Ministerstvo zdravotnictví ČR a Ústav zdravotnických informací a statistiky ČR, 2018a).

7 GDPR na příkladu konkrétního subjektu

7.1 Představení vybraného subjektu

Vybraným subjektem je společnost TrenDent s. r. o. Vznikla a do obchodního rejstříku byla zapsána v roce 2016 se sídlem v Praze. Ve společnosti TrenDent s. r. o. působí 3 lékaři, 3 sestry a 1 recepční pro podnik toto složení představuje cílový stav. Jedná se o malou praxi, která je nově založená a jejím cílem je nabrat nové pacienty. Společnost se zabývá výrobou, obchodem a službami neuvedenými v přílohách 1 až 3 živnostenského zákona a od června 2018 i poskytováním zdravotních služeb. Zubní klinika provádí preventivní prohlídky, dentální hygienu, ošetření dětí, výplně, endodontické a reendodontické ošetření, zubní implantáty, chirurgické krytí krčků a mnoho dalších.

7.2 Postup implementace GDPR

Před získáním licence potřebné k poskytování zdravotních služeb společnost neměla žádné zaměstnance, a zpracovávala tak pouze údaje o dodavatelích a odběratelích. S prvními zaměstnanci, kteří jsou ve společnosti od května 2018, a novým Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů bylo potřeba zpracovat vhodnou směrnici, dodržující základní zákonné povinnosti Nařízení. Společnost TrenDent s. r. o. se pro splnění povinností GDPR rozhodla pro nabídku od plzeňské společnosti VIS. Tato společnost poskytuje unikátní soubor prostředků zahrnující komentované Nařízení EU 2016/679, metodiku pro zavedení GDPR, vzorovou směrnici GDPR, předlohu pro vytvoření, lehkou aktualizaci směrnice pro konkrétní organizaci, příklady spolu s předlohami pro všechny potřebné dokumenty (např. vzor souhlasu, vzor smlouvy s pověřencem pro ochranu osobních údajů či informační štítky), databázi častých dotazů a jejich odpovědi. Společnost VIS poskytuje výše zmíněné služby na základě webové aplikace. TrenDent s. r. o. zmíněnou cestu ke splnění povinností GDPR zvolil na základě osobní znalosti dodavatele, doporučení od společnosti pro externí zpracování účetnictví a daní Moore Stephens s. r. o., ale také kvůli ceně, která je na základě následného vlastního zpracování společnosti nízká. GDPR se zabývá jeden ze tří jednatelů společnosti TrenDent s. r. o. v rámci své statutární činnosti a veškerý čas věnovaný GDPR je pro jednatele bez finanční odměny.

Školení

Úvodního školení na téma GDPR od společnosti VIS se zúčastnili dva jednatelé společnosti pro případnou zastupitelnost. Školení probíhalo v Plzni a bylo rozděleno na dvě části. První část byla spíše obecná, druhá poté konkrétní se zaměřením na zdravotnictví za přítomnosti odborníku z resortu. Jednatelé absolvované školení považují za kvalitní a velmi užitečné, jelikož zde byli zaškoleni i na zpracování souborů, které jim společnost VIS poskytla. Proškolení ostatní zaměstnanců společnosti TrenDent s. r. o. probíhá interně od externě proškolených jednatelů. Školení bude probíhat při změnách v legislativě či při nástupu nových zaměstnanců.

Analýza rizik

Analýza rizik byla zpracována interně jednatelem společnosti podle předlohy od společnosti VIS. Agendy, ve kterých společnost zpracovává osobní údaje a bylo u nich potřeba zhodnotit míru rizika jsou uvedené níže:

- Personalistika a mzdy
- Mzdy
- Evidence přístupových prostředků
- Účetní doklady obsahující osobní údaje
- Zálohy dat
- Provoz webových stránek
- Elektronická komunikace, evidence e-mailů a telefonních hovorů
- Fotografie
- Evidence dodavatelů
- Evidence odběratelů
- Evidence pracovních úrazů zaměstnanců
- Evidence docházky
- Evidence žádostí subjektů údajů
- BOZP a PO
- Řešení pohledávek
- Zdravotnický informační systém

Nejprve byly zhodnoceny okolnosti ovlivňující míru rizika v rámci agendy. Zde bylo rozhodnuto, že ve společnosti dochází ke zpracování citlivých osobních údajů, subjekty

údajů jsou i osoby mladší 18 let a dochází k předávání osobních údajů v rámci České republiky. Naopak nedochází k předávání osobních údajů do zemí Evropské unie, Evropského hospodářského prostoru ani k předávání osobních údajů do ostatních zemí. Pravděpodobnost výskytu rizika bezpečnostního incidentu rozděluje analýza rizik na čtyři následující možné úrovně:

- Nikdy se nestalo a není důvod si myslet, že se někdy stane.
- Je možné, že by se mohlo stát, ale pravděpodobně se to nestane.
- Je pravděpodobné, že se riziko stane.
- Je vysoce pravděpodobné, že za současných okolností k riziku dojde.
- Stává se pravidelně, nebo existuje důvod domnívat se, že je bezprostřední.

Zde společnost TrenDent s. r. o. zvolila pro své agendy úroveň 1 – nikdy se nestalo a není důvod si myslet, že se někdy stane.

V rámci analýzy rizik bylo důležité i zvolit úroveň objektivního hodnocení možných dopadů z následujících možností:

- Dopad je v omezeném časovém období, malého rozsahu a nesmí být katastrofický. Představuje dopad na subjekty údajů se závažným zásahem do jejich práv a svobod postihujícího nejvýše 5 % osob z celkového počtu, jejichž osobní údaje jsou v rámci agendy zpracovávány.
- Dopad je v omezeném rozsahu a v omezeném časovém období. Představuje dopad na subjekty údajů se závažným zásahem do jejich práv a svobod postihujícího více než 5 % osob z celkového počtu, jejichž osobní údaje jsou v rámci agendy zpracovávány.
- Dopad je omezeného rozsahu, ale je trvalý. Představuje dopad na subjekty údajů se závažným zásahem do jejich práv a svobod bez ohledu na jejich počet.
- Dopad je plošným rozsahem, trvalý. Představuje dopad na subjekty údajů se závažným zásahem do jejich práva svobod bez ohledu na jejich počet.

Zpracování osobních údajů ve společnosti TrenDent s. r. o. je charakterizováno úrovní 1 - dopad je v omezeném časovém období, malého rozsahu a nesmí být katastrofický. Představuje dopad na subjekty údajů se závažným zásahem do jejich práv a svobod postihujícího nejvýše 5 % osob z celkového počtu, jejichž osobní údaje jsou v rámci agendy zpracovávány.

Analýza rizik mimo jiné hodnotí i stávající zabezpečení prostoru s řízeným přístupem, zabezpečení osobních údajů v listinné podobě a zabezpečení osobních údajů v elektronické podobě. Prostor s řízeným přístupem je ve společnosti TrenDent s. r. o. zabezpečený zámkem s bezpečnostní vložkou, vstupní dveře jsou vybaveny elektronickým, nebo mechanickým zavíracím řízením a prostor je chráněn elektronickým zabezpečovacím systémem. Pro větší zabezpečení osobních údajů by společnost ve svých prostorách mohla mít bezpečnostní dveře, bezpečnostní skla či bezpečnostní fólie v oknech, bezpečnostní mříže na oknech, monitorovat prostor kamerovým systémem či využít služeb fyzické ostrahy. Osobní údaje v listinné podobě jsou plně zabezpečeny, jelikož jsou uloženy v prostorách s řízeným přístupem a k uložení osobních údajů v prostorách jsou využity uzamykatelné skříně. I osobní údaje v elektronické podobě jsou bezpečně zpracovávány, jelikož jsou uloženy na vlastním uložišti v prostorách organizace s řízeným přístupem, na vlastním nebo pronajatém uložišti v zabezpečeném datovém centru, na lokálním zařízení v prostorách organizace. Zařízení pro přístup k osobním údajům je umístěno v prostorách s řízením přístupem, připojuje se k uložišti s osobními údaji metalickou nebo optickou sítí, zabezpečenou bezdrátovou sítí a přístup k osobním údajům je zabezpečený heslem. Společnost TrenDent s. r. o. nemá osobní údaje uložené v zašifrované podobě.

Zaměstnanci společnost TrenDent s. r. o. byli zvyklí dodržovat všechna bezpečností pravidla již před zavedením GDPR, proto s novým Nařízením nebylo potřeba si zvykat či nově upravovat zabezpečení osobních údajů.

Z pohledu pacienta při úniku jeho citlivých osobních údajů dojde do porušení lékařského tajemství a pacient může být na základě úniku zneužit. Může nastat společenské ponížení, krádež identity či vznik podvodů.

Směrnice GDPR

Samostatnou směrnici GDPR zpracoval jednatel společnosti, který se problematikou zabývá, dle zakoupené šablony. Po analýze rizik bylo důležité udělat přehled osobních údajů, které společnost zpracovává, tedy běžné a citlivé. Další potřebnou činností bylo vyobrazit agendy, ve kterých společnost zpracovává osobní údaje.

Katalog osobních údajů

Ve společnosti TrenDent s. r. o. dochází ke zpracování běžných údajů, které jsou uvedené níže:

- jméno a příjmení, titul zobrazené osoby
- jméno a příjmení, titul
- rodné příjmení
- datum narození
- rodné číslo
- adresa trvalého pobytu
- adresa přechodného pobytu
- korespondenční adresa
- státní příslušnost
- místo narození
- telefonní číslo
- e-mailová adresa
- zdravotní pojišťovna
- dokumentace z pracovně – lékařských prohlídek a posouzení zdravotní způsobilosti zaměstnanců k vykonané práci
- identifikace přiděleného přístupového prostředku
- pracovní zařazení
- pracoviště
- vztah zástupce k subjektu údajů
- dodavatelem uvedená adresa
- dodavatelem uvedený obchodní název
- odběratelem uvedená adresa
- odběratelem uvedený obchodní název
- IČO
- DIČ
- navštívená místa v rámci pracovních cest
- navštěvovaná osoba nebo organizace
- datum návštěvy
- obchodní název

- vztah subjektu údajů ke správci osobních údajů
- výše pohledávky

Vybraný subjekt TrenDent s. r. o. je z oblasti zdravotnictví, je tedy zřejmé, že společnost zpracovává i citlivé osobní údaje. Mezi zvláštní (citlivé) osobní údaje, které v zubní klinice zpracovávají, patří:

- informace o pracovních úrazech zaměstnanců
    - datum a čas úrazu
    - místo úrazu
    - vykonávaná činnost při vzniku úrazu
    - zraněná část těla
    - popis úrazového děje
    - příčina úrazu
- zdravotní omezení s ohledem na typ vykonávané práce
- zdravotní dokumentace
    - anamnéza
    - nálezy vlastních objektivních klinických vyšetření
    - operační protokoly z vlastních provedených operačních výkonů
    - obrazová dokumentace a slovní popisy provedených přístrojových vyšetření
    - hodnoty z uskutečněných laboratorních vyšetření
    - diagnostické rozvahy, epikrízy a diagnostické závěry
    - navržená doporučení (léčba, režimová opatření)
    - lékařské zprávy z jiných zdravotnických zařízení
        - nálezy odborných a konsiliárních vyšetření
        - lékařské zprávy z hospitalizací
    - posudky o zdravotním stavu
    - žádanky o vyšetřená
    - vystavené recepty na léky a poukazy na zdravotnické prostředky
    - vystavená rozhodnutí o dočasné pracovní neschopnosti a rozhodnutí o potřebě ošetřování (péče)
    - ostatní zdravotnická dokumentace
    - dokumentace o komunikaci s Policií ČR, se soudy a s orgány sociální péče týkající se zdravotního stavu klientů

- dokumentace o komunikaci s komerčními pojišťovnami týkající se zdravotního stavu klientů ve věci náhrad a pojistných plnění

Katalog operací zpracování osobních údajů

Jelikož společnost TrenDent s.r.o. má zaměstnanců méně než 250, není nutné dle platné legislativy vést záznamy o činnostech zpracování. Nicméně s ohledem na skutečnost, kdy všechny osobních údaje v agendách společnosti jsou zpracovávaný systematicky, a ne pouze příležitostně, záznamy o činnostech zpracování společnost vede.

Zodpovědný za zpracování osobních údajů v agendách jsou všichni jednatelé společnosti. Povinná mlčenlivost osob, kteří přicházejí do kontaktu s osobními údaji je součástí pracovní smlouvy. K činnostem souvisejícími se zpracováním osobních údajů v rámci organizace dochází v níže uvedených agendách:

Personalistika a podklady pro mzdy

V této agendě společnost zpracovává běžné osobní údaje a z citlivých údajů jen obecný údaj o kategorii osob se zdravotním postižením a posudek lékaře o schopnosti vykonávat práci na určité pozici, případně o pracovních omezeních, které plynou ze zdravotního stavu. Agenda personalistiky a podkladů pro mzdy je zpracována za účelem organizace v souladu s pracovně – právními předpisy pro potřeby personální práce organizuje a vyhodnocuje výběrové řízení a zpracovává osobní údaje uchazečů o konkrétní pozici, připravuje některé podklady pro výpočet mezd a zakládá osobní spisy nových zaměstnanců. Zde společnost TrenDent s. r. o. vystupuje v roli správce osobních údajů. Roli subjektů osobních údajů zastávají zaměstnanci organizace a uchazeči o zaměstnání v organizaci. Dokumenty s osobními údaji, které se v rámci personalistiky a podkladů pro mzdy zpracovávají, je osobní dotazník, životopis, zápočtový list z předchozího zaměstnání a ostatní personální dokumentace. Subjekt může svůj souhlas se zpracováním osobních údajů dát formou listinné podoby nebo v podobě elektronické. Souhlas může být odvolaný kdykoli a společnost je v takovém případě bez zbytečného odkladu, nejpozději do 5 pracovních dnů, přestat jeho osobní údaje v uvedeném rozsahu zpracovávat. Osobní údaje se uchovávají v agendě personalistiky a podkladů pro mzdy ve společnosti po dobu výběrového řízení a lhůty pro odvolací řízení, pokud uchazeč nedá souhlas s delším zpracováním a po dobu trvání pracovněprávního vztahu. Aktualizace osobních údajů proběhne na základě informací přímo od zaměstnanců při změně, která se vztahuje k pracovněprávnímu vztahu. Osobní údaje jsou likvidovány u neúspěšných

uchazečů po skončení lhůty pro odvolací řízení, případně po skončení doby udělení souhlasu se zpracováním osobních údajů, u zaměstnanců po ukončení pracovního poměru ve společnosti TrenDent s. r. o. a doběhnutí ochranné lhůty. Nízké riziko charakterizuje agendu personalistiky a podkladů pro mzdy, je tedy minimální hrozba úniku osobních údajů a jejich zneužití.

Mzdy

Rozsah zpracovaných osobních údajů je u agendy mezd totožný s agendou personalistiky a podkladů ke mzdám, jsou tedy zpracovávány běžné osobní údaje a z citlivých údajů obecný údaj o kategorii osob se zdravotním postižením a posudek lékaře o schopnosti vykonávat práci na konkrétní pozici, případně o pracovních omezeních, které plynou ze zdravotního stavu. Společnost zpracovává osobní údaje v souladu s pracovně - právními předpisy a vede osobní spisy zaměstnanců a provádí výpočet mezd pro vlastní zaměstnance. TrenDent s. r. o. v agendě mezd vystupuje jako správce osobních údajů. Roli subjektů osobních údajů zastávají zaměstnanci organizace. Mezi dokumenty v rámci, kterých společnost zpracovává osobní údaje v agendě mezd patří pracovní smlouva včetně všech dodatků, mzdové výměry, prohlášení poplatníka daně ze závislé činnosti, zápočtový list z předchozího zaměstnání, osobní dotazník zaměstnance, potvrzení Okresní správy sociálního zabezpečení o výkonu samostatně výdělečné činnosti, potvrzení o absolvovaném školení BOZP a PO, dokumenty týkající se rodinných příslušníků (např. kopie rodných listů dětí uplatňovaných jako vyživované, potvrzení o výši příjmu manžela, manželky, apod.), změny zdravotní pojišťovny, rozhodnutí Okresní správy sociálního zabezpečení o přiznání OZZ nebo invalidity, dokumentace ze vstupních, průběžných a výstupních zdravotních prohlídek, souhlas zaměstnance prováděním srážek ze mzdy, mzdové listy, evidenční listy důchodového pojištění, rozhodnutí o exekucích, rozsudky o svěření do péče, smlouvy o penzijním pojištění nebo životním pojištění, prohlášení o seznámení se zásadami používání programů v organizaci, potvrzení o zdanitelných příjmech ze závislé činnosti, vydaná potvrzení o výši příjmů, posudek při ukončení pracovního poměru a zápočtový list při ukončení pracovního poměru. Osobní údaje jsou ve společnosti TrenDent s. r. o. uchovány po dobu trvání pracovněprávního vztahu a po dobu ochranné lhůty. Společnost získává osobní údaje převzetím v rámci organizace nebo přímo od subjektů údajů. Jejich aktualizuje je možná na základě informací přímo od zaměstnanců při kterékoli změně, která se vztahuje

k pracovně-právní vztahu. Ochrana osobních údajů odpovídá v agendě mezd nízkému riziku, kdy je minimální hrozba úniku osobních údajů a jejich zneužití.

Evidence přístupových prostředků

Tato agenda zpracovává pouze běžné osobní údaje společnosti, konkrétně jméno a příjmení, titul, pracovní zařazení, osobní číslo, identifikace přiděleného přístupového prostředku, datum a čas využití přiděleného přístupového prostředku. Organizace v souladu se svým oprávněným zájmem eviduje adresné přidělení jednotlivých přístupových prostředků a eventuálně informace o jejich využití z důvodů ochrany majetku. Společnost zde také vystupuje v roli správce osobních údajů. V roli subjektu údajů jsou fyzické osoby, kterým jsou přístupové prostředky přiděleny. S touto agendou jsou spojené dokumenty jako předávací protokol, evidence přidělených přístupových prostředků a záznamy o využití přístupových prostředků z elektronických zámků, otvíračů a dalších obdobných zařízení. Získání osobních údajů probíhá přímo od subjektů údajů. K jejich aktualizaci dochází pří faktickém provedení změny. Osobní údaje v rámci agendy evidence přístupových prostředků jsou uchováván po dobu přidělení přístupového prostředku. Ochrana osobních údajů v rámci této agendy odpovídá nízkému riziku a je tedy je minimální pravděpodobnost úniku osobních dat a jejich zneužití.

Účetní doklady obsahující osobní údaje

Agenda zpracovává běžné osobní údaje v rozsahu jméno a příjmení, titul, dodavatelem uvedený obchodní název, dodavatelem uvedená adresa, IČO, DIČ, identifikace soukromého vozidla zaměstnance použitého k pracovní cestě, navštívená místa v rámci pracovních cest a telefonní číslo. Společnost v agendě zastupuje roli správce osobních údajů a dotčenými subjekty údajů jsou zaměstnanci organizace a dodavatelé – fyzické osoby. Mezi dokumenty, které zpracovávají osobní údaje této agendy společnost řadí vystavené a přijaté účetní a daňové doklady, cestovní příkazy a vyúčtování cestovních náhrad a kopie účetních a daňových dokladů zaměstnanců, kterými prokazují oprávněnost nárokování přiznaných náhrad. Společnost TrenDent s. r. o. získá zpracovávané osobní údaje přímo od subjektu údajů a na základě informací přímo od subjektu vzniká jejich aktualizace. Osobní údaje jsou uchovány po dobu archivace z hlediska platné legislativy (Zákonu o účetnictví, Zákon o dani z přidané hodnoty, Zákon o dani z příjmu apod.) Minimální hrozba úniku osobních údajů a jejich zneužití, tedy nízké riziko charakterizuje agendu účetních dokladů obsahující osobní údaje.

Zálohy dat

Zálohy dat společnost realizuje u počítačových systémů periodickou zálohou dat z důvodu zajištění dostupnosti těchto systému v případech poruch, havárií či jiných výpadků dostupnosti systému a ztráty dat. V rámci této agendy jsou zpracovávány osobní údaje všech ostatních agend, které společnost ve směrnici GDPR uvádí. I zde společnost vystupuje v roli správce osobních údajů a dotčenými subjekty jsou veškeré fyzické osoby, jejich osobní údaje jsou zpracovávány v agendách společnosti. Aktualizace probíhá zcela nebo částečně automatizovaně dle nastavené doby a čestnosti zálohování. Záloha je automaticky přepisována na zálohu novější. Agenda zálohy dat představuje minimální hrozbu úniku osobních údajů a jejich zneužití, tedy nízké riziko.

Provoz webových stránek

Společnost TrenDent s. r. o. v souladu se svým oprávněným zájmem provozuje vlastní webové stránky za účelem prezentace sebe, své činnosti, nabídky zboží a služeb. Na základě provozu webových stránek společnost zpracovává osobní údaje – jméno a příjmení, titul zobrazené osoby, jméno a příjmení, titul, pracovní zařazení, skupinové fotografie a individuální fotografie. Společnost zastupuje správce osobních údajů, dotčené subjekty údajů jsou fyzické osoby zachycené na skupinových či individuálních fotografiích. Získání osobní údajů probíhá přímo od subjektu údajů a k aktualizaci dochází na základě žádosti o provedení změny přímo od subjektu údajů. Uchování osobních údajů je ve společnosti TrenDent s. r. o. na webových stránkách po celou dobu zaměstnání zaměstnance. Po uplynutí doby uchování jsou data vymazány. Nízkým rizikem je charakterizována i tato agenda, tedy minimální hrozbou úniku osobních údajů a jejich zneužití.

Elektronická komunikace, evidence e-mailů a telefonních hovorů

Společnost v rámci svého oprávněného zájmu používá hlasové služby a systémy elektronické komunikace jako běžné kanály komunikace se zaměstnanci, obchodními partnery, orgány státní moci a dalšími subjekty a eviduje využití těchto kanálu. V agendě elektronické komunikace, evidence e-mailů a telefonních hovorů jsou zpracovávány osobní údaje – jméno a příjmení, titul, obchodní název, e-mailová adresa, telefonní číslo, datum a čas využití komunikačního kanálu. Tato agenda obsahuje dokumenty e-mailové dokumentace a evidence příchozích a odchozích e-mailů, které zpracovávají osobní údaje. Osobní údaje jsou uchovávány po dobu 1 roku od uskutečnění komunikace. Jsou

získány přímo od subjektu údajů a k aktualizaci dochází na základě žádosti o provedení změny přímo od subjektu údajů. TrenDent s. r. o. zastupuje roli správce a dotčenými subjekty jsou fyzické osoby, se kterými organizace komunikuje prostřednictvím hlasové služby nebo systému elektronické komunikace. Elektronická komunikace, evidence e - mailů a telefonních hovorů je vyhodnocena nízkým rizikem pro hrozbu úniku a jejich zneužití.

Evidence pracovních úrazů zaměstnanců

Agenda eviduje údaje o vzniklých pracovních úrazech zaměstnanců v souladu s platnou legislativou. Evidence pracovních úrazů zaměstnanců obsahuje osobní údaje – jméno a příjmení, titul, datum narození, datum a čas úrazu, místo úrazu, vykonávaná činnosti při vzniku úrazu, zraněná část těla, popis úrazového děje a příčina úrazu. Zmíněné osobní údaje jsou použity v knize úrazu a záznamu o úrazu. Osobní údaje jsou uchovávány po dobu stanovenou platnou legislativou. Získání osobních údajů probíhá přímo od subjektu údajů a případně od svědků úrazu. K aktualizaci těchto údajů nedochází. Společnost zde vystupuje v roli správce a dotčenými subjekty pro zpracování osobních údajů jsou zaměstnanci společnosti. Agenda evidence pracovních úrazů zaměstnanců představuje minimální hrozbu úniku osobních údajů a jejich zneužití.

Evidence docházky

V rámci této agendy jsou zpracovány jména a příjmení, tituly a osobní čísla zaměstnanců. Společnost agendou evidence docházky plní zákonnou povinnost evidovat docházku do zaměstnání. Zpracované osobní údaje pro evidenci docházky jsou obsaženy v měsíčních záznamech docházky v listinné podobě, které jsou uchovávány po dobu stanovené platné legislativy. Společnost vystupuje v roli správce osobních údajů a dotčenými subjekty jsou zaměstnanci organizace. I zde společnost vyhodnotila agendu s nízkým rizikem pro minimální hrozbu úniku osobních údajů a jejich zneužití.

Evidence žádostí subjektů údajů

Společnost TrenDent s. r. o. v souladu se svým oprávněným zájmem vede evidenci přijatých žádostí o poskytnutí informací o zpracovaných osobních údajích subjektu údajů, případně jejich zmocněnců a opatrovníků. Agenda zpracovává běžné osobní údaje, a to jména a příjmení, titul, adresu trvalého pobytu, vztah subjektu údajů ke správci osobních údajů, obchodní název, sídlo, datum narození, telefonní číslo, e-mailovou adresu a vztah

zástupce k subjektu údajů. I v této agendě společnost vystupuje v roli správce, dotčenými subjekty jsou fyzické osoby žádající o poskytnutí informací a jejich zástupci. Osobní údaje jsou získávané přímo od subjektů údajů a k jejich aktualizaci v rámci agendy evidence žádosti subjektů údajů nedochází. Nízkým rizikem hrozby úniku osobních údajů a jejich zneužitím je charakterizována i tato agenda.

BOZP a PO

Bezpečnost a ochrana zdraví při práci společně s požární ochranou zpracovává běžné osobní údaje, konkrétně jména a příjmení, titul, adresa trvalého pobytu, datum narození, pracoviště a pracovní zařazení. Prezenční listy z absolvovaného školení, seznam zaměstnanců a jejich zařazení do kategorií, zaměstnanci podepsané vnitřní předpisy k bezpečnosti a ochraně zdraví při práci a požární ochranou a poukazy na lékařské vyšetření, to jsou dokumenty, které obsahují zpracované osobní údaje. Společnost zastupuje roli správce osobních údajů a zaměstnanci organizace jsou dotčenými subjekty. K získání osobních údajů dochází přímo od subjektů údajů, od posudkových lékařů provádějící požadované zdravotní prohlídky a jejich aktualizaci dochází při změně pracovně - právního vztahu nebo na žádost subjektů údajů při změnách adresy trvalého bydliště. Ochrana osobních údajů v této agendě odpovídá nízkému riziku, kdy je minimální hrozba úniku osobních údajů a jejich zneužití.

Řešení pohledávek

Společnost na základě svého oprávněného zájmu eviduje pohledávky u odběratelů i zaměstnanců a řeší jejich vymáhání. Zpracované osobní údaje jako jména a příjmení, titul, adresu trvalého pobytu, odběratelem uvedený obchodní název, odběratelem uvedená adresa, datum narození, IČO, DIČ a výše pohledávek. Zpracované osobní údaje obsahuje kniha pohledávek společnosti. Způsobem, kterým společnost TrenDent s. r. o. získává osobní údaje z evidence plateb a jejich aktualizace probíhá při změně v evidenci tržeb. Společnost je v roli správce osobních údajů a dotčenými osobami jsou odběratelé a zaměstnanci společnosti. Nízké riziko charakterizuje také agendu řešení pohledávek.

Zdravotnický informační systém

Zdravotnický informační systém slouží ve společnosti pro evidenci pacientů, zápis provedených výkonů, vyúčtování výkonů zdravotním pojišťovnám a pro vedení předepsané zdravotnické dokumentace. Společnost v rámci této agendy zpracovává

běžné osobní údaje (například jména a příjmení, titul, rodné příjmení, datum narození, rodné číslo, adresa trvalého pobytu apod.), ale také osobní údaje citlivé (informace o kategoriích osob se zdravotním postižením či zdravotnická dokumentace). Společnost zde vystupuje v roli správce a dotčenými osobami jsou evidovaní pacienti zdravotního zařízení. Pacienti svůj souhlas se zpracováním potvrdí v listinné podobě a mohou svůj souhlas kdykoliv odvolat. Společnost je v takovém případě povinna bez zbytečného odkladu, nejpozději do 5 pracovních dnů, přestat osobní údaje v uvedeném rozsahu zpracovávat. Společnost TrenDent s. r. o. získá osobní údaje přímo od subjektu údajů a aktualizuje údajů probíhá na žádost subjektu údajů. Minimální hrozbou úniku osobních údajů a jejich zneužitím je charakterizována i tato agenda společnosti.

Dalšími agendami, které společnost zpracovává jsou fotografie zaměstnanců umístěných na webových stránkách společnosti, evidence dodavatelů a evidence odběratelů. Zde jsou zpracovávány běžné osobní údaje, a to pouze interně.

8 Zatížení spojené s GDPR pro vybraný subjekt

8.1 Uložení dat

Společnost zpracovává osobní údaje pacientů pomocí stomatologického programu XDENT, který poskytuje zdravotní dokumentaci, léčebné plány i elektronické podpisy. Data společnosti jsou v programu zálohována v reálném čase a jsou zabezpečena a zašifrovaná totožnou technologií jako používají bankovní společnosti. Společnost TrenDent s. r. o. používá webové uložiště Dropbox. Přes cloudové uložiště Dropbox společnost sdílí soubory a složky s ostatními uživateli, a to pomocí synchronizace souborů. Na Dropboxu má společnost uložené podklady pro účetnictví a mzdy. Společnost TrenDent s. r. o. využívá také účetní aplikaci iDoklad, který je propojený s účetní programem Money. S daty společnosti kromě zaměstnanců přichází do kontaktu i externí mzdová pracovnice, laboratoře, účetní a daňová firma. Se všemi subjekty má společnost uzavřenou smlouvu o ochraně osobních údajů.

8.2 Pověřenec

Společnost TrenDent s. r. o. by musela jmenovat pověřence v případě, kdyby byla orgánem veřejné moci, veřejným subjektem či kdyby v rámci hlavní činnosti bylo vyžadováno rozsáhlé pravidelné a systematické monitorování subjektu údajů nebo by hlavní činnost spočívala ve zpracování běžných nebo citlivých osobních údajů týkajících se rozsudků v trestních věcech. TrenDent s. r. o. pověřence pro ochranu osob nemá, a to na základě školení od společnosti VIS, kde bylo zřejmým závěrem, že malé praxe mít pověřence nemusí.

8.3 Aktualizace

Společnost VIS, která nabízí soubory ve formě webové aplikace, za poplatek jednoduše aktualizuje či upravuje směrnici společnosti TrenDent s. r. o. v případě legislativních změn. Kontrolu dodržování z důvodu absence pověřence ve společnosti provádí jednatel, který má obecně GDPR pod dohledem.

8.4 Řešení případného porušení práv osob

V rámci informační povinnosti správce bylo potřeba z hlediska práv osob vypracovat postup pro poskytování informací o zpracování osobních údajů subjektům. Společnost zveřejnila a v případě potřeby aktualizuje prostřednictvím vlastních webových stránek zubní kliniky nebo prostřednictvím vývěsné desky v objektu sídla organizace či případně

prostřednictvím obojího pokyny subjektům údajů, které se týkají poskytování informací o zpracování osobních údajů. Zde společnost musí vyhovět všem právům osob, tedy žádosti o informace o zpracovávaných osobních údajích, žádosti na opravu zpracovávaných osobních údajů, žádosti o výmaz zpracovávaných osobních údajů, žádosti o předání zpracovávaných osobních údajů třetí straně či námitce proti zpracovávání osobních údajů. TrenDent s. r. o. tyto žádosti a námitky přijímá formou osobní či písemného podání na adresu společnosti či prostřednictvím elektronické pošty na emailovou adresu společnosti. Jelikož se jedná o osobní údaje, společnost vždy ověří totožnost žadatele. Při osobním podání je žadatel ověřen na základ platného dokladu totožnosti, tedy občanským průkazem nebo cestovním pasem. V případě písemného podání doručeného poštou musí být podpis žadatele na žádosti úředně ověřen. Společnost TrenDent s. r. o. je zavázána poskytnout odpověď na žádost do jednoho měsíce ode dne podání této žádosti. V situaci, kdy se jedná o složitější případ je možné prodloužení lhůty až na tři měsíce, je ale potřeba žadatele do jednoho měsíce o prodloužení informovat. V případě, kdy je podání vyhodnoceno za nedůvodné, nepřiměřené, nebo šikanózní, může společnost rozhodnout o zpoplatnění poskytnutí informace o zpracování osobních údajů ve výši administrativních nákladů na zpracování a předání, odeslání odpovědi či odmítnout poskytnutí informací o zpracovávaných osobních údajích.

8.5 Náklady spojené se zavedením GDPR

Nákladem pro společnost TrenDent s. r. o. bylo zakoupení předloh GDPR ve výši 3 000 Kč. Školení dvou jednatelů za 2 000 Kč a náklady vynaložené na cestu 2 000 Kč. Součástí je také roční poplatek společnosti VIS ve výši 300 Kč, který poskytuje aktualizaci a úpravu souborů.

Jednatel se GDPR zabývá v rámci své pozice statutárního jednatele bez finanční odměny. Ve společnosti TrenDent s. r. o. jsou zaměstnáni 3 lékaři, 3 sestry a 1 recepční. Jedná se o cílový plný stav, který se průběžně odchyluje podle aktuální situace (např. nástupy nových zaměstnanců, odchody zaměstnanců či zaměstnankyň na mateřské dovolené). Z níže uvedených sazeb, které jsou stanovené společností lze vypočítat zisk, kterého by společnost dosáhla kdyby nebylo potřeba řešit GDPR a dodržovat jeho náležitosti.

Tabulka 1 Sazby zaměstnanců

Pozice	**sazba**
Lékař	2 700 Kč
Sestra	1 500 Kč
Recepční	1 000 Kč

Zdroj: Vlastní zpracování, 2019

Ušlý zisk společnosti vznikl během školení jednatelů, zpracování směrnice včetně analýzy podmínek a systémů, aktualizací dodavatelských smluv, proškolením zaměstnanců a tvorbou formuláře souhlasu pacientů se zpracováním osobních údajů.

Tabulka 2 Kalkulace zavedení GDPR

Popis činnosti	**Počet lidí**	**Počet hodin**	**Sazba**	**Celkem**
Školení jednatelů	2	4	2 700 Kč	**21 600 Kč**
Zpracování směrnice	1	20	2 700 Kč	**54 000 Kč**
Aktualizace dodavatelských smluv	1	10	2 700 Kč	**27 000 Kč**
Proškolení zaměstnanců – lékař	1	1	2 700 Kč	**2 700 Kč**
Proškolení zaměstnanců – zdravotní sestra	3	1	1 500 Kč	**4 500 Kč**
Proškolení zaměstnanců – recepční	1	1	1 000 Kč	**1 000 Kč**
Formulář souhlasu pacienta se zpracováním osobních údajů	1	1250[1]	1 000 Kč	**12 500 Kč**

Zdroj: Vlastní zpracování, 2019

Společně s vynaloženými skutečnými náklady a ušlým ziskem společnost TrenDent s. r. o. vyšlo nové Nařízení Evropského parlamentu a Rady (EU) č. 2016/679

[1] Cílem společnosti TrenDent s. r. o. je nabírání nových pacientů, jedná se o údajů k 03/2019, kdy společnost má 2 500 pacientů. Zdravotní sestra přibližně 0,5h řeší s pacientem formulář souhlasu se zpracováním osobních údajů. V budoucnu se tedy předpokládá růst této dílčí částky.

ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů na 123 300 Kč. Pro společnost se nejedná o malou částku. Výběr této varianty zavedení GDPR do společnosti byl zvolen na základě doporučení od účetní a daňové společnosti Moore Stephens s. r. o., který měl kvalitu společnosti VIS ověřenou.

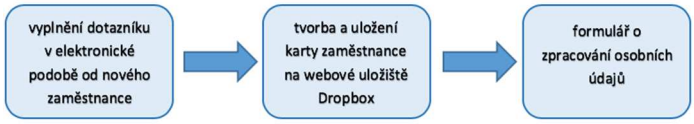
8.6 Návrh metodických postupů pro zpracování osobních údajů

Ve společnosti TrenDent s. r. o. se řídí postupy při zpracování osobních údajů, které nejsou pevně stanoveny formou vizuálního metodického postupu. Navrhovala bych tyto postupy ve společnosti dodržovat. Bude tak docíleno přesného a správného zabezpečení ochrany osobních údajů z pohledu zpracovatele. Při nástupu nových zaměstnanců tyto návody poslouží k rychlejšímu a snadnějšímu zapracování ve společnosti TrenDent s. r. o. Pro společnost budou navrhnuty procesní karty zobrazující postup při nástupu nového zaměstnance, přijetí nového pacienta a postup po absolvování externího školení. Ke každému metodického postupu budou vytvořené formuláře, které po zpracování osobních údajů budou podepsány pověřeným zaměstnancem.

Nový zaměstnanec

V situaci, kdy společnost přijme nového zaměstnance pro svou zubní kliniku získá jeho osobní údaje pomocí vyplněného dotazníku v elektronické podobě. K vyplnění dotazníku používá společnost TrenDent s. r. o. tabulkový procesor Microsoft Excel. Poté je karta zaměstnance uložena a archivována na webovém uložišti Dropbox. Založení karty a změny osobních údajů pracovníků společnosti doporučuji, aby měla na starost recepční, která změnu pečlivě a správně provede. Následně informace o provedené změně potvrdí formulářem, který bude k těmto účelům sloužit. Při odchodu zaměstnance společnost postupuje na základě skartačního a archivačního řádu.

Obrázek 2 Metodický postup při přijetí nového zaměstnance



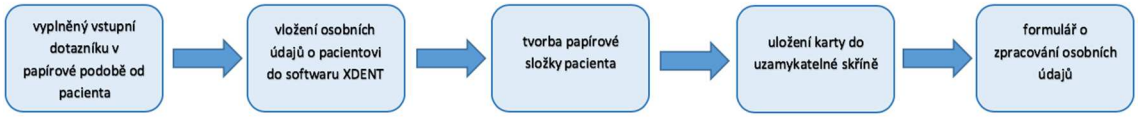
Zdroj: Vlastní zpracování, 2019

Nový pacient

Společnost TrenDent s. r. o. má za cíl nabrat nové pacienty. Proto by tento metodický postup byl hojně využíván. Při první návštěvě v zubní klinice pacient vyplní vstupní

dotazník. Ten obsahuje mimo jiné i jméno, příjmení, bydliště, rodné číslo a pojišťovnu. Dále je nutné vložit osobní údaje o pacientovi do stomatologického softwaru XDENT, který poskytuje mimo jiné zdravotní dokumentaci a léčebné plány. Osobní údaje pacienta jsou zde archivovány. Doporučuji, aby recepční následně vytvořila a založila kartu pacienta do kartotéky. Jako kartotéka ve společnosti TrenDent s. r. o. slouží uzamykatelné skříně na recepci. Zpracování vstupních osobních údajů pacienta by mělo být podložené podepsaným formulářem. Za změny v osobních údajích zaměstnanců bych navrhovala, aby zodpovídala recepční společnosti TrenDent s. r. o. přesně dle směrnice. Při odchodu pacientů k jinému lékaři či úmrtí pacienta společnost jedná dle skartačního a archivačního řádu.

Obrázek 3 Metodický postup při přijetí nového pacienta

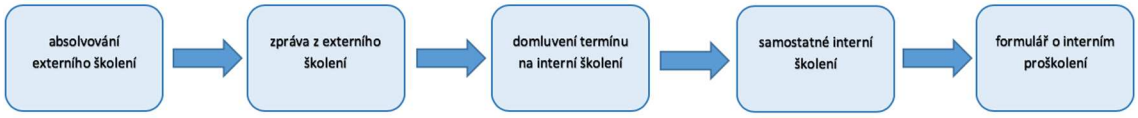


Zdroj: Vlastní zpracování, 2019

Školení

Zaměstnanci se pravidelně zúčastňují několika školení. Například školení odborného, o bezpečnosti práce a požární ochrany či zaměřeného na GDPR od společnosti VIS, kterého se zúčastňují vždy dva jednatelé pro případnou zastupitelnost. Navrhuji po absolvování školení zpracovat zprávu ze školení, kterou proškolený uloží na cloudové uložiště. Důležité je domluvit s recepční společnosti vhodný termín pro interní zaškolení všech zaměstnanců, a to nejpozději do 10 pracovních dnů. Na základě komentáře k vypracované zprávě poté může probíhat interní školení pro ostatní zaměstnance. Přikládám i návrh hromadného formuláře, kde zaměstnanci svým podpisem stvrzují účast na školení.

Obrázek 4 Metodický postup pro školení zaměstnanců

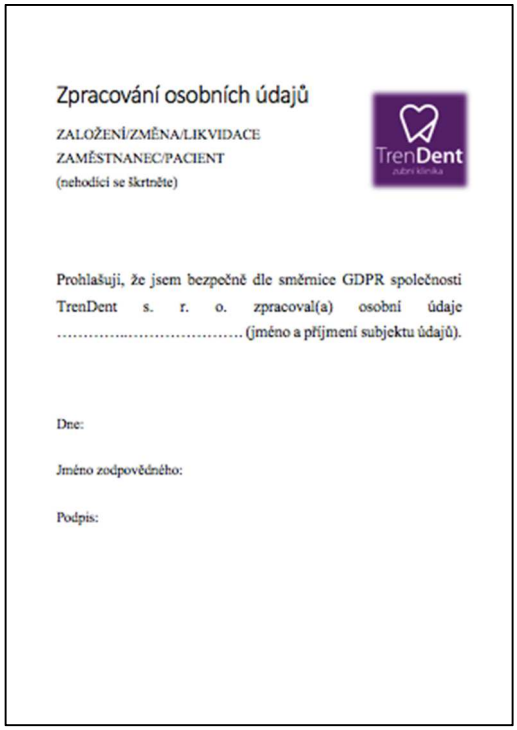


Zdroj: Vlastní zpracování, 2019

Formuláře k metodickým postupům

Oba formuláře slouží k doložení správného provedení zpracování osobních údajů a evidenci, kdy a kdo tak učinil. Doporučuji tyto interní doklady plně využívat a archivovat je v uzamykatelné skříni na recepci.

Obrázek 5 Formulář o zpracování osobních údajů



Zpracování osobních údajů

ZALOŽENÍ/ZMĚNA/LIKVIDACE
ZAMĚSTNANEC/PACIENT
(nehodící se škrtněte)

TrenDent zubní klinika

Prohlašuji, že jsem bezpečně dle směrnice GDPR společnosti TrenDent s. r. o. zpracoval(a) osobní údaje ……(jméno a příjmení subjektu údajů).

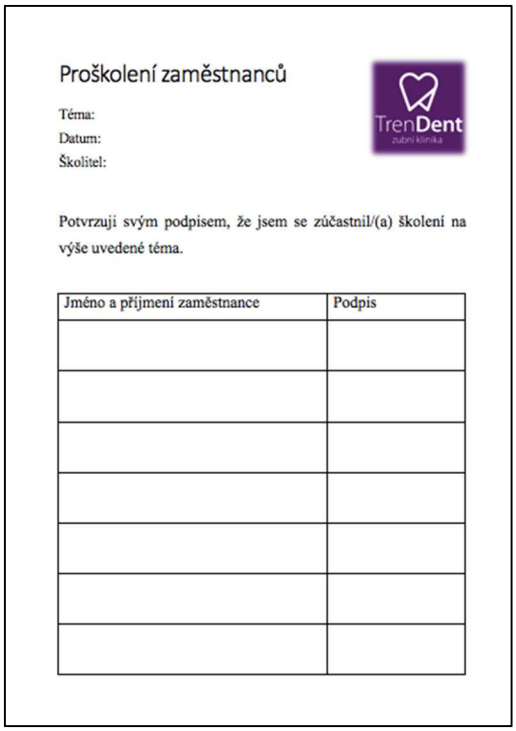
Dne:

Jméno zodpovědného:

Podpis:

Zdroj: Vlastní zpracování, 2019

Obrázek 6 Formulář k proškolení zaměstnanců



Proškolení zaměstnanců

Téma:
Datum:
Školitel:

TrenDent zubní klinika

Potvrzuji svým podpisem, že jsem se zúčastnil/(a) školení na výše uvedené téma.

Jméno a příjmení zaměstnance	Podpis

Zdroj: Vlastní zpracování, 2019

8.7 Shrnutí GDPR ve vybraném subjektu

Zavedení GDPR ovlivnilo společnost TrenDent s. r. o. při administrativě, a to většími nároky. Dále i ušlým ziskem a náklady, které bylo potřeba obětovat pro splnění Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Společnosti GDPR z důvodu původní dobré praxe u lékařů, která byla velmi podobná této stávající, která je platná od 25. května 2018, nebylo potřeba velkých změn. Pouze zpracovat směrnici GDPR, která charakterizuje agendy, ve kterých dochází ke zpracování osobních údajů. Společnost TrenDent s. r. o. vnímá jako největší ztrátu při zavedení GDPR čas, který mohla věnovat povinnostem, které v rámci zubní kliniky zaměstnanci vykonávají.

Vzhledem k tomu, že GDPR mělo silnou mediální podporu, obecná povědomost lidí je dobrá a téměř každý ví, o co se jedná a co se pro to má dělat, společnost nemá zatím žádné pozitivní ani negativní zkušenosti s přístupem pacientů na GDPR.

Z důvodu absence pověřence bude kontrolu dodržování provádět jednatel, který se GDPR ve společnosti zabývá a následně podle změn v legislativě budou za poplatek společnosti VIS aktualizovány soubory pomocí webové aplikace a proběhne školení, buď interní vedené jednatelem, v případě nástupu nového zaměstnance či externě při změně legislativy od společnosti VIS pro dva jednatele, kteří pak interně zaškolí ostatní zaměstnance zubní kliniky TrenDent s. r. o.

Společnosti doporučuji sledovat případné změny v oblasti GDPR, průběžně školit zaměstnance, aktualizovat dle potřeb směrnici a osobní údaje stále správně zabezpečovat a chránit, aby nemohlo dojít k úniku údajů, které jsou v resortu zdravotnictví opravdu citlivé. Společnost TrenDent s. r. o. tak nevzniknou zbytečné nepříjemnosti s tímto Nařízením.

Závěr

V prvních kapitolách byla zpracována východiska k problematice ochrany osobních údajů. Byla charakterizována právní úprava, vývoj ochrany osobních údajů v České republice, rysy GDPR, cíle GDPR, nové přístupy a nové povinnosti dle GDPR. Dále byly definovány základní pojmy v souvislosti s osobními údaji jako osobní údaj, subjekt údajů, správce, zpracovatel, pověřenec a profilování. Následovala charakteristika zásad GDPR, kterými jsou korektnost, transparentnost a zákonnost, omezení účelem, minimalizace dat, přesnost, omezení uložení, zásada odpovědnosti, integrita a důvěrnost. Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů nově přineslo i práva osob být informován, na přístup k osobním údajům, na opravu, na výmaz a právo vznést námitku. Další kapitola byla zaměřena na aplikaci GDPR, která obsahuje kroky implementace a kontrolu dodržení GDPR. Implementace je doporučena v sedmi krocích, a to zpracování katalogu osobních údajů, katalogu operací zpracování osobní údajů, analýzy souladu s GDPR, analýzy rizik, technickými a organizačními opatřeními, proškolením osob, pravidelnou aktualizací a auditem. Kontrolu dodržení GDPR provádí dozorový řád uvnitř státu a vně státu Evropský sbor pro ochranu osobních údajů. V závěru první části bylo charakterizováno zdravotnictví jako resort a vymezena jeho specifika z důvodu vybraného subjektu, kterým je zubní klinika.

Kapitola GDPR na příkladu konkrétního subjektu na začátku představila vybraný subjekt TrenDent s. r. o. Cílem práce bylo zabývat se problematikou GDPR ve vybraném subjektu, zhodnotit dopady implementace a stanovit doporučení pro danou společnost. Po představení subjektu byl popsán postup implementace, školení, analýza rizik, směrnice dat, kde byly charakterizovány osobní údaje běžné a citlivé, agendy v rámci, kterých společnost zpracovává osobní údaje. Bylo řešeno i téma uložení dat, pověřence, aktualizace souborů pro ochranu osobních údajů, práva osob a vyčíslení nákladů spojených se zavedením GDPR. Pro společnost TrenDent s. r. o. byl vypracován metodický postup při přijetí nového zaměstnance či nového pacienta a postup po absolvování externího školení.

Společnost TrenDent s. r. o. musela na zakoupení souborů se šablonami pro zavedení GDPR a školením s dopravou vynaložit 7 000 Kč. Z pohledu ušlého zisku přišla

společnost o 123 300 Kč. Společnost zpracovávala osobní údaje na stejném principu již před začátkem GDPR. Před 25. květnem, kdy GDPR vešlo v platnost, bylo potřeba zpracovat směrnici, zaškolit zaměstnance a získat souhlasy o zpracování osobních údajů od pacientů zubní kliniky. Fyzicky zabezpečené osobní údaje byly již před zavedením Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, a to pomocí uzamykatelných skříněk, uživatelským jménem a heslem do počítačů ve společnosti. Pro zubní kliniku navrhuji pro zlepšení zpracování osobních údajů využívat navrhnuté metodické postupy pro nového zaměstnance, nového pacienta a školení. Pro větší zabezpečení osobních údajů navrhuji společnosti TrenDent s. r. o. zvážit zavedení kamerového systému na recepci.

Seznam použité literatury

Knižní a monografické publikace

DURDISOVÁ, Jaroslava. *Ekonomika zdraví.* Vyd. 1. Praha: Oeconomica, 2005. 228 s. ISBN 80-245-0998-9

GLADKIJ, Ivan a kol. *Management ve zdravotnictví.* Vyd. 1. Brno: Computer Press, 2005. xii, 380 s. Praxe manažera. ISBN 80-7226-996-8

HEJDUKOVÁ, Pavlína. *Veřejné finance: teorie a praxe*. Vydání první. Praha: C.H. Beck, 2015. xii, 252 stran. Beckovy ekonomické učebnice. ISBN 978-80-7400-298-4

JANEČKOVÁ, Eva. *GDPR: Praktická příručka implementace*. Vydání první. Praha: Wolters Kluwer, 2018. xiii, 119 stran. ISBN 978-80-7552-248-1

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Praha: Verlag Dashöfer, [2018]. ISBN 978-80-87963-54-8

NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 339 stran. Pro praxi. ISBN 978-80-7380-689-7

NEZMAR, Luděk. *GDPR: Praktický průvodce implementací.* První vydání. Praha: Grada Publishing, 2017. 301 stran. Právo pro praxi. ISBN 978-80-271-0668-4

NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. xvii, 559 stran. Praktický komentář. ISBN 978-80-7598-068-7

VOIGT, Paul a BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR): a practical guide*. Cham: Springer, [2017], ©2017. ix, 383 stran. ISBN 978-3-319-57958-0

ŽŮREK, Jiří. *Praktický průvodce GDPR*. 1. vydání. Olomouc: ANAG, 2017. 223 stran. Právo. ISBN 978-80-7554-097-3

Elektronické zdroje

Ministerstvo zdravotnictví ČR (2018a).*GDPR metodika implementace ve zdravotnictví* [online]. Praha [cit. 17.4.2019]. Dostupné z: http://www.mzcr.cz/Legislativa/dokumenty/metodika-implementace-gdpr_14864_3805_11.html

Ministerstvo zdravotnictví ČR (2018b).*GDPR metodika implementace ve ambulantní* sféře [online]. Praha [cit. 17.4.2019]. Dostupné z: http://www.mzcr.cz/Legislativa/dokumenty/metodika-implementace-gdpr-v-ambulantni-sfere_15782_3805_11.html

Novinky.cz (2019). *Obavy z GDPR byly zbytečné, pokuta za něj zatím nepadla* [online]. Praha [cit. 17.4.2019]. Dostupné z: https://www.novinky.cz/internet-a-pc/499998-obavy-z-gdpr-byly-zbytecne-pokuta-za-nej-zatim-nepadla.html

Úřad pro ochranu osobních údajů (2017). *GDPR (obecné nařízení)* [online]. Praha [cit. 17.4.2019]. Dostupné z: https://www.uoou.cz/gdpr/ds-3938/p1=3938

Úřad pro ochranu osobních údajů (2017a). *Nové přístupy a povinnosti* [online]. Praha [cit. 17.4.2019]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=27268&n=2-nove-pristupy-a-povinnosti

Úřad pro ochranu osobních údajů (2017b). *Nejdůležitější pojmy* [online]. Praha [cit. 17.4.2019]. Dostupné z: https://www.uoou.cz/3-nejd-lezit-jsi-pojmy/d-27293

Úřad pro ochranu osobních údajů (2017c). *Dozorová činnost* [online]. Praha [cit. 17.4.2019]. Dostupné z: https://www.uoou.cz/dozorova-cinnost/ds-1277/p1=1277

Seznam tabulek

Seznam obrázků

Seznam použitých zkratek

BOZP	Bezpečnost a ochrana zdraví při práci
ČR	Česká republika
DIČ	Daňové identifikační číslo
EU	Evropská unie
GDPR	General Data Protection Regulation
IČO	Identifikační číslo osoby
OZZ	Osoby zdravotně znevýhodněné
PO	Požární ochrana

Abstrakt

VAŠÁKOVÁ, Aneta. *Problematika GDPR ve vybraném subjektu.* Plzeň, 2019. 54 s. Bakalářská práce. Západočeská univerzita v Plzni. Fakulta ekonomická.

Klíčová slova: ochrana osobních údajů, Nařízení, GDPR, problematika, zdravotnictví

Cílem této bakalářské práce je zhodnocení dopadů GDPR na příkladu konkrétního subjektu a stanovit doporučení pro další působení Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů v malé zubní klinice z resortu zdravotnictví. První kapitoly jsou zaměřeny definování základních pojmů, zásad, práv osob související s problematikou GDPR a doporučené kroky implementace dle metodiky vydané Ministerstvem zdravotnictví České republiky. Následně je provedena deskripce problematiky GDPR ve vybrané zubní klinice TrenDent s. r. o. Po zhodnocení dopadů této problematiky je zřejmé, že pro společnost se jedná o značný ušlý zisk i přesto, že osobní údaje byly správně chráněné již před platností Nařízení. Pro malou společnost TrenDent s. r. o. bylo potřeba zpracovat směrnici, která zahrnuje agendy zpracovávající osobní údaje, proškolit zaměstnance a připravit souhlasy se zpracováním osobních údajů pro pacienty zubní kliny.

Abstract

VAŠÁKOVÁ, Aneta. *The issue of GDPR in selected entity.* Pilsen, 2019. 54 s. Bachelor Thesis. University of West Bohemia. Faculty of Economics.

Key words: protection of personal data, Regulation, GDPR, the issue, health service

The aim of this bachelor thesis is to evaluate the impact of GDPR on the example of a specific subject and to make recommendations for further action Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and free movement these data in a small dental clinic from the health sector. The first chapters are focused on definitions basic concepts, principles, rights of persons related to GDPR and recommended steps of implementation according to methodology issued by the Ministry of Health of the Czech Republic. Subsequently, the description of GDPR in the selected dental clinic TrenDent s. r. o. After assessing the impact of this issue, it is clear that the company is a significant loss of profit even though personal data have been properly protected before the Regulation. For a small company, TrenDent s. r. o., It was necessary to develop a directive which includes agendas processing a personal data, train employees, and prepare personal data processing consent for dental patients.