MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUC
Ústav informatiky a aplikované matematiky

Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů

BAKALÁŘSKÁ PRÁCE

Erika Kopecká
Vedoucí práce: Ing. Lukáš Pavlík, Ph.D.

Olomouc 2020

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně a použila jen zdroje v seznamu literatury a použitých zdrojů.

Tištěná verze textu práce je shodná s textem práce na CD nosiči a elektronickou verzí vloženou do studijního systému IS/STAG.

Ve Vrbně pod Pradědem dne 17. 4. 2020

Erika Kopecká

PODĚKOVÁNÍ

Ráda bych poděkovala Ing. Lukáši Pavlíkovi, Ph.D., za odborné vedení bakalářské práce, ochotu při konzultacích a cenné rady. Také děkuji Mgr. Petru Vlkovičovi za podnětné připomínky a rady při zpracování bakalářské práce.

Moravská vysoká škola Olomouc
Akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Erika Kopecká**
Osobní číslo:	**M17039**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Podniková ekonomika a management**
Název tématu:	**Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů**
Téma anglicky:	**The Issue of GDPR and its Impact on Employers in the Field of Personal Data Protection**
Zadávající katedra:	**Ústav informatiky a aplikované matematiky**

Zásady pro vypracování:

1. Popiště základní problematiku legislativy GDPR.
2. Charakterizujte vybranou organizaci.
3. Proveďte komplexní analýzu vybrané organizace s důrazem na zavedení směrnice GDPR.
4. Vyhodnoďte výsledky provedné anylýzy a navrhněte vlastní způsob řešení.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: ANAG, 2017. Právo. ISBN 978-80-7554-097-3.
NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.
VOIGT, PAUL; VON DEM BUSSCHE, AXEL. The Eu General Data Protection Regulation: A Practical Guide. SPRINGER 2017. ISBN: 9783319579580.
NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 (tzv. GDPR).
KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v praktických příkladech. Praha: Bova Polygon, 2013, 168 s. ISBN 978-80-7273-173-2.
ZÁKON č. 101/2000 Sb., O OCHRANĚ OSOBNÍCH ÚDAJŮ.

Vedoucí bakalářské práce: Ing. Lukáš PAVLÍK
Ústav informatiky a aplikované matematiky

Datum zadání bakalářské práce: 24. května 2019
Termín odevzdání bakalářské práce: 31. března 2020

Podpis studenta: ..... Datum: 6.9.2019

Podpis vedoucího práce: ..... Datum: 24.6.2019

Mgr. Irena KOVAČIČINOVÁ
prorektorka

L.S.

Mgr. Veronika ŘÍHOVÁ, Ph.D.
manažer ústavu

V Olomouci dne 7. června 2019

Obsah

Úvod

Ochrana osobních údajů je téma, které se stalo velice diskutovaným v nedávné době, kdy Evropská unie přijala v dubnu 2016 dlouho chystanou právní úpravu této problematiky, tj. Obecné nařízení Evropského parlamentu a Rady o ochraně osobních údajů č. 2016/679. Běžně se používá zkratka GDPR podle anglického názvu nařízení General Data Protection Regulation, nebo také Obecné nařízení či jen Nařízení, proto i zde budou dále užívány tyto zkratky. Tato nová úprava ochrany osobních údajů nahradila dosavadní právní legislativy ve všech členských státech Evropské unie. Všechny subjekty, které zpracovávají osobní údaje fyzických osob, měly dva roky na to, aby se s novým nařízením seznámily a implementovaly ho do své organizace tak, aby v době účinnosti, tedy 25. května 2018, byly schopny se jím řídit.

Pro mnoho lidí je problematika ochrany osobních údajů v takovém rozsáhlém měřítku zbytečná, nepotřebná a nové nařízení podle nich přináší pouze více papírování. Ale současná doba ukazuje, že je potřeba chránit své osobní údaje, neboť riziko zneužití dat je obrovské. Také míra globalizace vyžaduje mít ucelenou právní legislativu pro celou Evropskou unii.

Za zmínku stojí fakt, že vydání GDPR inspirovalo například Kalifornii, která také přijala zákon na ochranu osobních údajů a od 1. ledna 2020 zde platí zákon na ochranu spotřebitelů.[1]

Hlavním cílem této bakalářské práce je zjistit, jaké jsou dopady GDPR po jeho zavedení do praxe pro vybraného zaměstnavatele. Mezi dílčí cíle patří pomocí rešerše vybrané literatury vymezit základní pojmy a problematiku legislativy GDPR, dále mezi dílčí cíle patří deskripce vybrané společnosti a v neposlední řadě také komplexní analýza vybrané společnosti s důrazem na implementaci GDPR tak, aby zjištěné výsledky umožnily vyhodnotit danou situaci ve vybrané firmě a pomohly navrhnout další způsob řešení.

Tato bakalářská práce bude rozdělena na čtyři části. První část tvoří úvod, po kterém bude následovat část teoretická, poté část praktická a na konci bude závěr.

V úvodu bakalářské práce proběhne seznámení s danou problematikou. Dále se uskuteční vymezení hlavního a dílčích cílů a v krátkosti bude představena základní struktura této práce.

Teoretická část bude rozdělena na kapitoly, popřípadě podkapitoly, které budou pojednávat o tématu práce, tedy o nařízení GDPR. Zachycena bude historie ochrany osobních údajů, definovány budou základní pojmy jako osobní údaj, zvláštní kategorie osobních údajů,

[1] OTEVŘEL, Richard a Vojtěch BARTOŠ. Havelpartners.blog. *Kalifornie přijala zásadní zákon na ochranu osobních údajů CCPA.* [online]. [cit. 2020-02-28]. Dostupné z: https://www.havelpartners.blog/blog/kalifornie-prijala-zasadni-zakon-na-ochranu-osobnich-udaju-ccpa/104#.

subjekt údajů, správce, zpracovatel, zpracování, profilování a pseudonymizace, další zaměření se bude týkat zásad a právních důvodů pro zpracování osobních údajů, dojde k vymezení práv subjektu údajů, proběhne seznámení s pojmem pověřenec pro ochranu osobních údajů a budou uvedeny i možné sankce a pokuty za neplnění nově vzniklých povinností. Pro úplnost zde bude také v krátkosti charakterizován doplňující zákon pro Českou republiku, zákon č. 110/2019 Sb., o zpracování osobních údajů.

V praktické části bude v dalších kapitolách a podkapitolách představena konkrétní firma, její organizační struktura, jednotlivé úseky a oddělení. Následovat bude popis implementace nařízení. Důležitou část práce bude tvořit vlastní průzkum. Jednak proběhne analýza osobních údajů a jejich toků jednotlivými úseky podniku i toků mimo podnik a v neposlední řadě se uskuteční krátký rozhovor s vybraným vzorkem zaměstnanců, který bude řízen pomocí vytvořeného checklistu. To vše bude podkladem pro vyhodnocení implementace nařízení GDPR, jeho dopadů a vyslovení konečného návrhu dalšího řešení.

V závěru budou shrnuty výsledky a cíle, kterých mělo být v rámci řešení bakalářské práce dosaženo.

Teoretická část

1 Historie ochrany osobních údajů

Lidé se o ochranu svého soukromí začali více starat v období, kdy se začalo s pronásledováním a vražděním osob, které vyznávaly odlišné náboženství nebo měly odlišné názory. Další popud k ochraně osobních údajů byla doba nacismu a rasová genocida. Vždyť také dnes mohou být údaje o náboženské či etnické příslušnosti rizikové. Od 70. let 20. st. se začala rozvíjet výpočetní technika, která jde stále kupředu, což přináší sice mnoho výhod, ale také hrozeb.[2]

Pravděpodobně první psaný právní rámec byla Deklarace práv člověka a občana z roku 1789. Následovala Všeobecná deklarace lidských práv z roku 1948.[3] V roce 1950 byla sjednána Evropská úmluva o ochraně lidských práv a základních svobod, která zaručovala právo na respektování rodinného a soukromého života. V lednu 1981 došlo k přijetí Úmluvy Rady Evropy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat. Tato úmluva poprvé definovala pojmy jako osobní údaj, správce, automatizované zpracování aj. Další právní akt byla 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. Inspirovala se předchozí Úmluvou, ale zpracování osobních údajů pojímala komplexně. Reakcí na moderní vývoj lidské společnosti je současné 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 o zrušení Směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů).[4]

Co se týče České republiky, ochrana osobních údajů začala být řešena až přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Ochrana osobních údajů při jejich zpracování se uzákonila 1. června 2000, kdy nabyl účinnosti zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.[5] Zákon vycházel ze Směrnice Evropského parlamentu a Rady 95/46/ES. Tento zákon byl zrušen a nahrazen přijetím nového zákona č. 110/2019 Sb., o zpracování osobních údajů, který vešel v účinnost 24. dubna 2019. O ochraně soukromí v širším pojetí pojednává i zákon č. 89/2012 Sb., občanský zákoník.

[2] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 26.
[3] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 27.
[4] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 13-16.
[5] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 18.

2 Nařízení Evropského parlamentu a Rady (EU) č. 2016/679

Celý oficiální název této právní legislativy zní Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. 4. 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).

Obecné nařízení představuje nový právní základ ochrany osobních údajů v Evropské unii, který má dopad na všechny, kdo určitým způsobem chtějí zpracovávat osobní údaje občanů Evropské unie. Důležitá je i právní forma tohoto legislativního aktu. Nejedná se o směrnici, nýbrž o nařízení, protože ta jsou pro členské státy závazná a přímo použitelná. Nemusí se tedy dále implementovat do právních řádů jednotlivých členských zemí. Nařízení je mimo jiné použitelné na Islandu, v Norsku a v Lichtenštejnsku. Jedná se o sjednocující právní normu. Více sjednocuje i evropský dozor.[6]

GDPR se skládá ze dvou částí. První část je tzv. Preambule, kterou tvoří recitály 1–173 (obsahující důvody přijetí nařízení a výklad, jak nové povinnosti chápat) a druhá část je vlastní text stanovující práva a povinnosti, kterou tvoří články 1–99 (obsahující pravidla pro zpracování osobních údajů).[7]

Základní zásady a principy GDPR se oproti původní směrnici neliší, spíše byly detailněji rozpracovány. GDPR je oproti původní směrnici založeno na dvou nových přístupech. Jedná se o princip odpovědnosti správce a o princip založený na riziku, od čehož se odvíjí nové povinnosti. Princip odpovědnosti znamená odpovědnost správce za dodržení zásad zpracování, které jsou uvedeny v článku 5 odst. 1 GDPR a zároveň v povinnosti správce tento soulad doložit. Přístup založený na riziku znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext, účel zpracování a musí přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu dále musí přizpůsobit i zabezpečení osobních údajů. K dokládání souladu mohou napomáhat záznamy o činnostech zpracování, kodexy, osvědčení, pověřenec pro ochranu osobních údajů. Jde o komplexní činnost, do které můžeme zařadit také zveřejňování informací, vyhotovení vnitřních předpisů nebo řádnou spolupráci s dozorovým úřadem.[8]

Působnost Obecného nařízení neboli vymezení rozsahu a realizace lze rozdělit na osobní, věcnou, místní a časovou.

---

[6] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 29-30.
[7] ŽŮREK, Jiří. *Praktický průvodce GDPR* Str. 23.
[8] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací.* Str. 29.

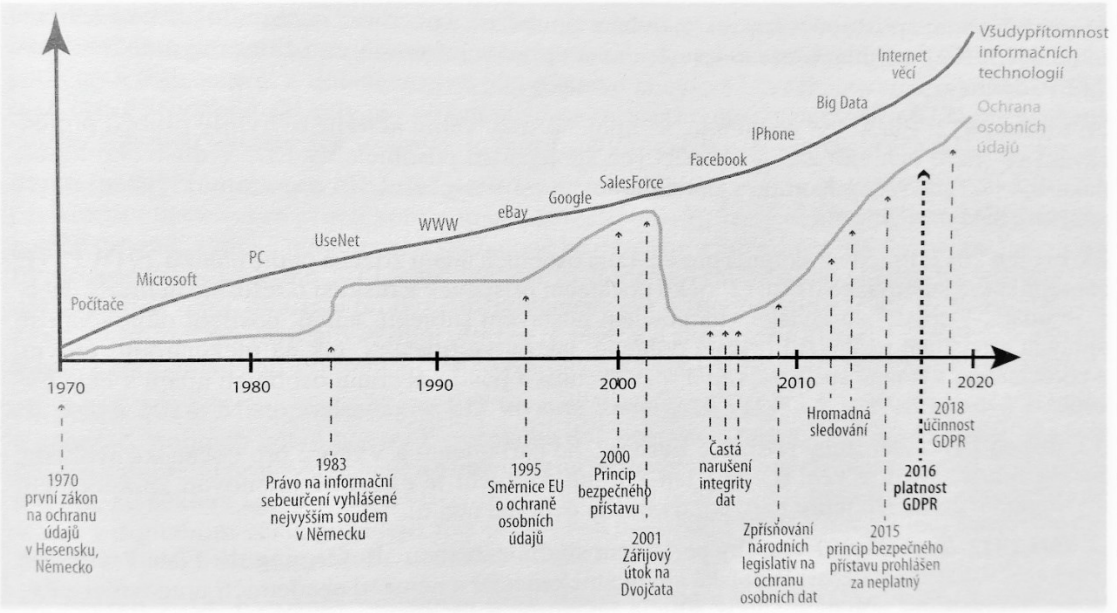
Osobní působnost určuje subjekty, na které se nařízení vztahuje. Zejména jde o správce, zpracovatele a subjekty údajů, ale i dozorové úřady a Sbor. Věcná působnost určuje, na které věcné oblasti či situace se nařízení vztahuje (pozitivní vymezení), a také nařízení obsahuje vymezení situací, na které se jeho věcná působnost nevztahuje (negativní vymezení). Dle pozitivního vymezení působnosti se nařízení vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Negativní vymezení vyjímá takové zpracování osobních údajů, které je výlučně osobní nebo domácí činností a dále takové zpracování, které je prováděné příslušnými orgány za účelem prevence, odhalování, vyšetřování a stíhání trestných činů. GDPR se nevztahuje na osobní údaje zesnulých osob. Místní působnost omezuje aplikaci nařízení na určité území, kde ho lze vymáhat prostřednictvím dozorových úřadů. V základní rovině se GDPR použije na zpracování osobních údajů, ke kterému dochází v souvislosti s činnostmi provozovny správce, zpracovatele v EU bez ohledu na to, zda samotné zpracování probíhá mimo EU. Časová působnost vymezuje dobu, po kterou je nařízení platné a účinné.[9]

Zjednodušeně jsou hlavní znaky (rozdíly) GDPR následující:

- je jednotně aplikovatelné v celé Evropské unii,
- zpřesňuje souhlas se zpracováním osobních údajů,
- vyžaduje vyšší technickou a organizační bezpečnost,
- v některých případech vyžaduje jmenování pověřence na ochranu osobních údajů,
- musí se vést záznamy o činnostech zpracování,
- při rizikových zpracování je vyžadována DPIA (analýza posouzení vlivu na ochranu osobních údajů),
- posiluje stávající práva subjektů údajů a zakládá nová práva jako právo být zapomenut a právo na přenositelnost údajů,
- závažné porušení ochrany osobních údajů musí být nahlášeno do 72 hodin subjektu údajů a dozorovému úřadu,
- zavádí vyšší sankce za porušení ochrany osobních údajů.[10]

[9] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 34-39.
[10] Ministerstvo průmyslu a obchodu. *GDPR.* [online]. [cit. 2018-12-04]. Dostupné z: https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/Podpurna-opatreni-mpo/2018/10/GDPR-V-KOSTCE-GDPR-je-prilezitost.pdf.

Cena informací ve světě neustále stoupá a osobní údaje se tak staly velmi cennou komoditou. Kybernetická bezpečnost je jedním z klíčových úkolů budoucnosti, protože krádež osobních údajů vystavuje občany EU významným rizikům. GDPR je reakcí na rychlou digitalizaci a kybernetizaci našeho prostoru.[11]



Obr. č. 1: Vývoj technologií v porovnání s vývojem legislativy[12]

Na přechozím obrázku číslo 1 je vidět, jak legislativní vývoj ochrany osobních údajů zaostává za vývojem technologickým, který je mnohem rychlejší a pružnější. Je důležité tedy, jaká je reakční doba právního systému na dané technologické změny.[13]

3 Definice základních pojmů

V Obecném nařízení je definice pojmů obsažena v článku 4 odst. 1. Mezi základní pojmy patří:

- osobní údaj,
- zvláštní kategorie osobních údajů,
- subjekt údajů,
- správce,
- zpracovatel,
- zpracování.

[11] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 14.
[12] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 15.
[13] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 14.

3.1 Osobní údaj

Osobní údaje jsou *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen "subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;“*[14] De facto jsou to veškeré údaje o subjektu údajů a důležitá je zde právě ta identifikovatelnost. Opakem jsou anonymní údaje, které se nedají vztáhnout k subjektu údajů, tím pádem nejsou osobními údaji. Anonymizaci je tedy možné použít jako druh výmazu osobních údajů.

3.2 Zvláštní kategorie osobních údajů

Do zvláštní kategorie osobních údajů patří tzv. citlivé údaje, které jsou taxativně vymezeny v článku 9 odst. 1.

Mezi citlivé údaje patří takové údaje, „*které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.“*[15]

Blíže se údaje o zdravotním stavu mohou specifikovat jako *„osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.“*[16]

Tato kategorie vyžaduje zvýšenou ochranu, neboť jsou takového charakteru, že mohou subjekt údajů poškodit ve společnosti nebo způsobit jeho diskriminaci.[17]

Zvláštní kategorie osobních údajů se nesmí zpracovávat. Jejich zpracování je povoleno pouze ve výjimečných případech uvedených v článku 9 odst. 2.

3.3 Subjekt údajů

Subjekt údajů je fyzická osoba, které se týkají osobní údaje. Právnická osoba subjekt údajů není, její údaje tedy nejsou osobními údaji.

---

[14] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/4.htm.
[15] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/9.htm.
[16] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/4.htm.
[17] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 35.

3.4 Správce

Správce je „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.*“[18] Správce zpracovává osobní údaje pro účely vyplývající z jeho činnosti, ale zpracovávat je může např. i pro své oprávněné zájmy, nepřevyšují-li je zájmy na ochranu základních práv a svobod fyzických osob.[19] Správce je ten, kdo primárně odpovídá za zpracování osobních údajů. Pro zpracování může využít zpracovatele.

3.5 Zpracovatel

Zpracovatel je „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.*“[20] Zpracovatel pro správce zpracovává pouze takové zpracovatelské činnosti, kterými jej správce pověřil.[21] Správce musí použít pouze ty zpracovatele, kteří poskytují dostatečné záruky, aby byla zajištěna ochrana práv subjektů údajů, a musí mít spolu uzavřenou smlouvu.[22] Zpracovatel může zpracovávat osobní údaje pro vlastní účely, v tom případě je ale správce.

3.6 Zpracování

Zpracování je „*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.*“[23]

Nařízení podléhají pouze činnosti, které naplňují podmínku zpracování a zároveň ke zpracování musí docházet zcela nebo částečně automatizovaně nebo prostřednictvím evidence

[18] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/4.htm.
[19] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 32.
[20] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/4.htm.
[21] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 32.
[22] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 99.
[23] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/4.htm.

a osobní údaje se týkají určité kategorie subjektů údajů. Příklad typického zpracování je personální agenda, zákaznické systémy aj.[24]

Pojem zpracování má stejný význam, jako měl v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých údajů.[25]

Důležité pojmy jsou také:

- profilování,
- pseudonymizace.

3.7 Profilování

Profilování znamená „*jakoukoli 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.“*[26] Jednoduše řečeno, jde o vytvoření profilu subjektu údajů, na základě kterého se dají analyzovat jeho postoje nebo preference, což umožňuje přiřadit ho do nějaké dané kategorie.

3.8 Pseudonymizace

Pseudonymizace je „*zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.“*[27] To znamená, že místo osobního údaje se použije třeba nějaký kód, který se ale zpětně může spojit s daným osobním údajem. Protože se zpětně může spojit, musí se na pseudonymizované údaje pohlížet jako na osobní údaje. Přesto je to určitá ochrana pro subjekty údajů před zneužitím jejich dat.

[24] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 55.
[25] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 31.
[26] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/4.htm.
[27] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/4.htm.

4 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů má zkratku DPO, která vychází z anglického názvu Data Protection Officer. Dá se říci, že je to nezávislá osoba, která má chránit osobní údaje.

Organizace (správce) má povinnost jmenovat pověřence pro ochranu osobních údajů podle čl. 37 odst. 1 GDPR v těchto případech:

- zpracování provádí orgán veřejné moci či veřejný subjekt;
- hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.[28]

To znamená, že ne každá organizace musí mít pověřence, ale z hlediska přístupu k ochraně osobních údajů je lepší ho mít.

Není-li si organizace jistá, zda pověřence musí nebo nemusí jmenovat, je jí doporučeno, aby provedla interní analýzu ochrany osobních údajů, která ji dá odpověď. Závěr, že pověřence jmenovat nemusí, je důležité umět řádně zdůvodnit a vysvětlit všechny důležité faktory, na základě kterých k takovému závěru organizace dospěla. Tato analýza je součástí dokumentace k ochraně osobních údajů, která musí být pořízena dle zásady odpovědnosti a musí být průběžně aktualizována.[29]

Jeden pověřenec může pracovat pro více správců, ale je důležité, aby byl rychle dosažitelný. Také je důležité, aby byly dostupné jeho kontaktní údaje. Pověřenec může být zaměstnanec správce nebo u správce může působit externě.

Pověřenec musí být přímo podřízen vrcholovému managementu. Měl by mít přímý přístup k vedení organizace, aby při předávání informací nebyl mezi pověřencem a vedením další mezičlánek a pověřenec se tak na vedení organizace mohl kdykoliv obrátit v záležitostech ochrany osobních údajů.[30]

Nařízení říká, že „*pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti*

[28] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 103.
[29] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 248.
[30] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 41.

ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39.“[31] Pověřenec nemusí být vysloveně právník, ale musí mít dobrou znalost nejen právních přepisů o ochraně osobních údajů, ale mimo to také musí znát množství navazujících přepisů. Dále by měl znát praktickou stránku ochrany osobních údajů (od jejich získávání, přes zpracování až po likvidaci). Měl by mít dobrou znalost prováděných operací, informačních systémů, bezpečnosti dat. Nesmí mu chybět odpovídající osobní kvality.[32]

Mezi základní úkoly pověřence patří monitorování souladu zpracování s GDPR, zvyšování povědomí o ochraně osobních údajů a péče o odbornou přípravu zaměstnanců. Dalším úkolem je poskytování poradenství na požádání, pokud se jedná o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování. Role pověřence při posuzování vlivu je spíše poradní, přesto je jeho role při této činnosti významná a nezastupitelná. Dále pověřenec spolupracuje s dozorovým úřadem a působí jako kontaktní místo pro subjekty údajů. Také prošetřuje případné stížnosti.[33]

Pověřenec pro ochranu osobních údajů nenese osobní odpovědnost za neplnění GDPR. Zajistit soulad a dodržování nařízení má správce.[34]

5 Zásady zpracování osobních údajů

Zásady zpracování osobních údajů lze považovat za základní stavební kameny, na nichž je GDPR založeno, respektive za základy celé ochrany osobních údajů při jejich zpracování. Správce má povinnost dodržení souladu se zásadami doložit, což je už zmíněný princip odpovědnosti. Dokládání je nepřetržitým procesem.[35]

Činnosti zajišťování a prokazování souladu tedy jsou neustálým procesem plnění povinností správce, je to de facto komplex činností, nejedná se jen o jednu či několik izolovaných činností. Protože to pro správce znamená zvýšené nároky, existuje nástroje, které při zajišťování a dokládání souladu pomáhají. Jde zejména o záznamy o činnostech zpracování, kodexy chování, osvědčení a vnitřní politiku ochrany osobních údajů. Záznamy o činnostech zpracování jsou až na výjimky pro správce povinné, ostatní nástroje jsou dobrovolné.[36]

---

[31] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/37.htm.
[32] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 262-263.
[33] ŽŮREK, Jiří. *Praktický průvodce GDPR.* str. 111.
[34] GDPR.CZ. *DPO čili Pověřenec pro ochranu osobních údajů.* [online]. [cit. 2020-03-20]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/.
[35] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 58.
[36] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 155.

Nezbytným předpokladem k zajištění souladu zpracování je jeho zmapování. Je to první krok k tomu, aby správce zjistil, jaké zpracování provádí, jaké osobní údaje získává, jakým způsobem, v jakém formátu, jaké operace s nimi provádí, pro jaké účely, jaké k tomu má právní důvody aj. Na základě mapování může určit, jaké povinnosti se na něj vztahují a jaké konkrétní opatření má přijmout, zjistil-li nějaké nedostatky, a jak tedy dostat zpracování do souladu s GDPR.[37]

Správce musí vést záznamy o činnostech zpracování (do jisté míry je to náhrada za zrušení oznamovací povinnosti). Dá se říci, že tyto záznamy jsou jeden z výstupů mapování. Jak budou tyto záznamy vypadat, záleží na správci. Měly by seznámit s prováděnými operacemi a měly by obsahovat totožnost správce, účely zpracování, kategorie subjektů údajů a osobních údajů, příjemce, dobu zpracování, popis organizačních a technických opatření.[38]

V článku 5 obecného nařízení je možné najít 6 základních zásad zpracování osobních údajů:

- zákonnost, korektnost, transparentnost;
- účelové omezení;
- minimalizace údajů;
- přesnost;
- omezení uložení;
- integrita a důvěrnost.

5.1 Zákonnost, korektnost, transparentnost

Zákonnost znamená, že osobní údaje může správce zpracovávat, má-li alespoň jeden právní důvod, zpracování musí být prováděno zákonným způsobem. Zákonnost lze považovat za nejdůležitější zásadu. Je tedy základním předpokladem, aby bylo možné hovořit o zákonném zpracování osobních údajů. Korektností se dá nazvat poctivé zpracování osobních údajů. Správce nesmí zastírat účel, pro který osobní údaje zpracovává. Transparentnost předpokládá, že osobní údaje budou subjektu údajů snadno přístupné a srozumitelné, za použití jasných jazykových prostředků, že bude jasný účel zpracování.[39]

[37] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 156.
[38] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 157.
[39] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 59.

Subjektu údajů musí být sděleno, že má právo požadovat potvrzení a informaci o tom, které údaje jsou o něm zpracovány a musí být poučen o možných rizicích, předpisech a právech, které v souvislosti se zpracováním svých osobních údajů má a jak je může využít.[40]

5.2 Účelové omezení

Účelové omezení doplňuje zásadu transparentnosti a znamená, že účel zpracování osobních údajů musí být znám již při sběru dat.[41]

Jakékoli osobní údaje lze shromažďovat jen pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Za neslučitelné s původními účely se nepovažuje zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu nebo pro statistické účely.[42]

Správně definovaný účel musí být jasně specifikovaný, aby vymezil rozsah zpracování, musí být přesný, dostatečně jednoznačný a jasně vyjádřený a samozřejmě musí být zákonný.[43]

5.3 Minimalizace údajů

Osobní údaje lze zpracovávat pouze přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu ke stanovenému účelu, pro který jsou zpracovávány. Do jisté míry jde o bezpečnostní prvek, protože čím méně osobních údajů je zpracováváno, tím menší riziko hrozí subjektu údajů při jejich případném úniku.[44]

Správce by měl určit minimální množství osobních údajů, které potřebuje, tedy přesně tolik kolik potřebuje, ne více. Proto musí nejprve určit, proč osobní údaje má a k čemu je používá, protože se liší účel od účelu. Musí vzít v potaz kontext účelu pro každý subjekt údajů.[45]

5.4 Přesnost

Správce má povinnost zajistit správnost a přesnost osobních údajů. Osobní údaje musí být zpracovávány v přesné podobě a v případě potřeby musejí být aktualizované. Vždy musí jasné, co má záznam uvádět. Čím důležitější je přesnost osobních údajů, tím větší úsilí je třeba vynaložit na jejich zajištění. Organizace by měla ke splnění tohoto požadavku realizovat přiměřené kroky k zajištění přesnosti všech osobních údajů, také by měla zajistit, aby zdroj

[40] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 40.
[41] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 41.
[42] ŽŮREK Jiří. *Praktický průvodce GDPR.* Str. 60.
[43] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 55.
[44] ŽŮREK Jiří. *Praktický průvodce GDPR.* Str. 60-61.
[45] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 61.

osobních údajů byl jasný a nezpochybnitelný.[46] Neznamená to, že by správce sám musel aktivně vyhledávat nepřesné údaje a opravovat je. Musí je ale opravit na žádost subjektu údajů.

5.5 Omezení uložení

Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů po dobu ne delší, než je nezbytně nutné pro účely, pro které jsou zpracovávány. To znamená, že osobní údaje musejí být zlikvidovány v době, kdy pomine účel jejich zpracování.[47] Opět zde platí výjimka pro archivaci ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu a pro statistické účely.

Správce musí tedy kontrolovat dobu uchování osobních údajů a bezpečně zlikvidovat ty informace, které pro daný účel už nejsou potřebné. Dále musí aktualizovat, archivovat nebo bezpečně smazat informace, pokud jsou zastaralé. Pokud má informace, ke kterým není nutné přistupovat, ale je nutné je zachovat, ty by měly být bezpečně archivovány, což může vycházet ze zákona o archivnictví nebo třeba ze zákona o účetnictví. Dá se vycházet i ze skartačního řádu.[48]

5.6 Integrita a důvěrnost

Osobní údaje, které správce zpracovává, musejí být dostatečně zabezpečeny a chráněny pomocí vhodných technických nebo organizačních opatření před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.[49]

Každá organizace potřebuje jiné zabezpečení. Potřebná úroveň zabezpečení závisí na různých okolnostech, které ovlivňují zvolenou úroveň ochrany, například na okolnostech jejího vzniku, působení, pravidel, firemní kultuře, náhledu na bezpečnost, povaze služeb aj. Je potřeba mít na paměti, že porušení informační bezpečnosti může mít za následek způsobení škody. Je nutné posoudit informační riziko, zjistit jaká data jsou cenná, citlivá nebo důvěrná a co se může stát, pokud by došlo k porušení bezpečnosti a integrity dat.[50]

Důležitá jsou závazná podniková pravidla, která mají za cíl ochranu osobních údajů. Jedná se o pravidla technické povahy (řádné softwarové zabezpečení výpočetní techniky, automatické aktualizace), pravidla chování zaměstnanců, dodržování závazných právních předpisů, technických norem, bezpečnostních standardů aj.[51]

---

[46] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 62-64.
[47] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 62.
[48] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 67.
[49] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 63.
[50] NEZMAR, Luděk *GDPR: praktický průvodce implementací.* Str. 74-76.
[51] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 105.

V dnešním moderním světě jsou osobní údaje zpracovávány vesměs prostřednictvím počítačů a jiných elektronických zařízení, proto je nutné klást zvýšený důraz na jejich zabezpečení, vzhledem k rizikům, které digitalizace informací přináší. Řádné zabezpečení osobních údajů je nezbytným předpokladem pro dosažení souladu zpracování s GDPR.[52]

Vedení podniku musí v rámci své odpovědnosti za ochranu osobních údajů zajišťovat podmínky pro řádnou ochranu osobních údajů; musí zajišťovat průběžné vzdělávání zaměstnanců v této oblasti; odpovídá za personální zajištění ochrany osobních údajů; zajišťuje zdroje informací ke správné praxi; zajišťuje kontrolu činnosti při ochraně osobních údajů; zajišťuje realizaci svých vlastních opatření v oblasti ochrany osobních údajů, včetně kontroly znalosti povinností zaměstnanců, kteří přicházejí do kontaktu s osobními údaji.[53]

Zaměstnanci, kteří přicházejí do styku s osobními údaji, jsou povinní zpracovávat osobní údaje v souladu s GDPR; musí zachovávat mlčenlivost; zabránit neoprávněnému zpracovávání; při používání výpočetní techniky musí používat jen daný hardware a software, a to bezpečným způsobem a dodržovat zásady bezpečného používání výpočetní techniky.[54]

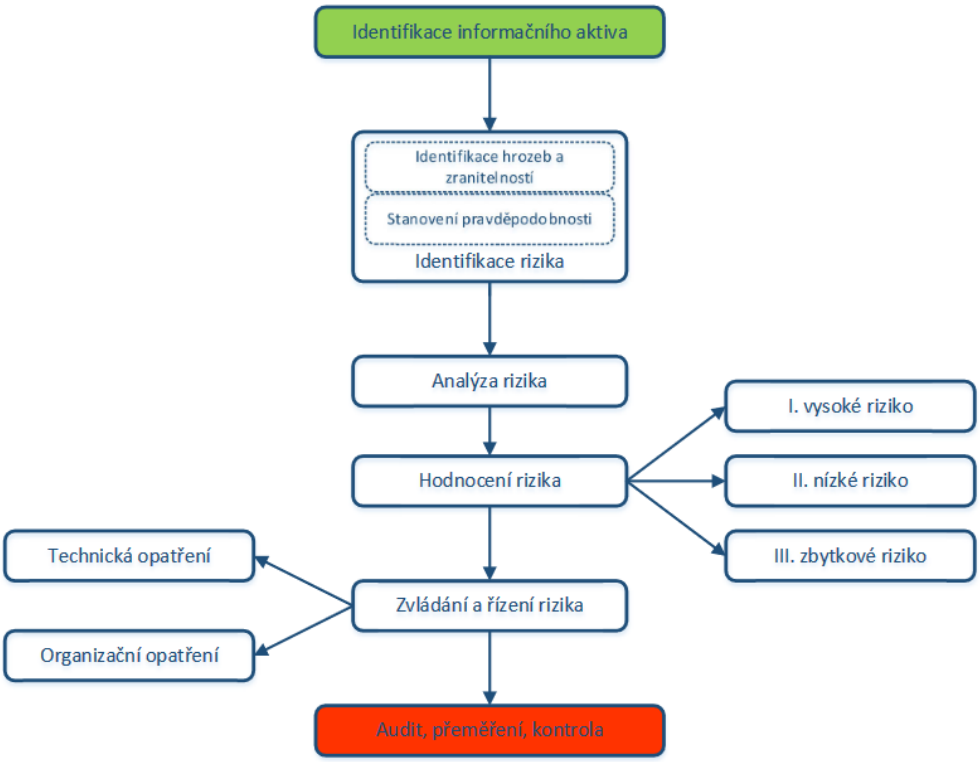
Zásada integrity a důvěrnosti uplatňuje přístup založený na riziku. Management rizika je pro organizace běžný a v současné době je potřeba ho doplnit o další důležitou oblast, a tou je právě ochrana osobních údajů.

5.6.1 Riziko pro ochranu osobních údajů

Je důležité posoudit rizika, kterým firma čelí, tím, že je shromažďuje, ukládá a jinak zpracovává, a to jednak riziko pro samotný subjekt údajů, riziko pro správce a vůbec rizika související s dodržováním předpisů. Všechna rizika by měla být posuzována a zmírňována tam, kde je to možné. Dá se říci, že riziko je hypotetický scénář, který popisuje, jak zdroj rizika (např. zaměstnanec či třeba konkurent) může zneužít zranitelnost aktiv osobních údajů v souvislosti s hrozbami a umožnit výskyt bezpečnostních incidentů na datech s osobními údaji a způsobit tak dopad na soukromí subjektů údajů. Úroveň možného rizika se stanovuje na základě závažnosti a pravděpodobnosti. Závažnost možného následku představuje míru významu rizika a pravděpodobnost míru možnosti vzniku rizika.[55]

Následující obrázek číslo 2 znázorňuje schéma, jak může probíhat práce s riziky.

[52] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 92.
[53] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 108.
[54] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 109.
[55] NEZMAR, Luděk *GDPR: praktický průvodce implementací.* Str. 114-116.



Obr. č. 2: Schéma toku rizika.[56]

5.6.2 Základní kroky hodnocení rizik

Hodnocení rizik je známé z managementu rizik, který předkládá následující možné základní kroky:

- kategorizace/klasifikace pracovních činností včetně jejich charakteristik;
- identifikace nebezpečí, tedy zvážení, kdo nebo co může být poškozeno a jak;
- stanovení rizika, jinak řečeno odhad rizika s uvedením plánovaných nebo stávajících bezpečnostních opatření;
- rozhodnutí o přijatelnosti rizika, posouzení, zda jsou bezpečnostní opatření dostatečná;
- příprava nápravných opatření ke snížení rizika;
- posouzení, zda plán nápravných opatření je odpovídající. Opětovné posouzení rizika, zda bylo sníženo na nejnižší dosažitelnou mez.[57]

[56] ÚZIS. Metodika implementace GDPR ve zdravotnictví. [online]. [cit. 2020-03-23]. Dostupné z: https://www.uzis.cz/index.php?pg=o-nas--ochrana-osobnich-udaju--gdpr-ve-zdravotnictvi
[57] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 120.

5.6.3 Vyhodnocení rizik

Jakou metodu vyhodnocení rizika si organizace zvolí, je zcela v jejích kompetencích. Existují různé metody a postupy. Důležité jsou výsledky, které určí naléhavost přijetí opatření ke snížení rizika a potřebu velikosti bezpečnostních opatření.

5.6.4 Míra rizika

Míru rizika lze rozdělit například do základních 5 stupňů. Od bezvýznamného rizika až po nepřijatelné riziko. Daný stupeň určuje, jaká opatření jsou potřebná udělat:

1. **Bezvýznamné či zanedbatelné riziko** – není vyžadováno žádné zvláštní opatření, ale určitě je nutné na něj upozornit.
2. **Akceptovatelné, méně významné riziko** – tady je nutné zvážit určité zlepšení nebo organizační opatření. Například školení nebo běžný dozor.
3. **Mírné riziko** – je nutné realizovat bezpečnostní opatření ve stanoveném časovém období.
4. **Nežádoucí riziko** – zde je nutné urychleně provést bezpečnostní opatření, které riziko sníží na přijatelnou úroveň.
5. **Nepřijatelné riziko** – znamená okamžité zastavení činnosti, dokud se neprovedou nezbytná opatření a riziko se nesníží.[58]

Správce musí provést vhodná technická a organizační opatření, aby byla zajištěna úroveň zabezpečení odpovídající danému riziku. To vše s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování. Zpracovávat osobní údaje by měla pověřená osoba a povinnost mlčenlivosti je u ní samozřejmost.

Není přípustné, aby například kartotéka s osobními údaji byla na chodbě mimo kancelář nebo aby kancelář měla nevhodné neuzamykatelné dveře.

Pokud nastane porušení zabezpečení osobních údajů, které je vysoce rizikové, má správce povinnost nahlásit to dozorovému úřadu, a to bez zbytečného odkladu, nejpozději do 72 hodin.

V rámci rizik je vhodné aspoň okrajově zmínit posouzení vlivu na ochranu osobních údajů neboli DPIA podle anglického Data Protection Impact Assessment. DPIA je novou povinností pro správce, a to ještě před zahájením zpracování a v případě, že je pravděpodobné, že zpracování bude mít za následek vysoké riziko pro práva a svobody subjektů údajů. Tedy zejména v následujících případech, kdy dochází k systematickému a rozsáhlému zpracování

[58] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Str. 127.

osobních údajů, které je založeno na automatizovaném zpracování, včetně profilování; je prováděno rozsáhlé zpracování zvláštních kategorií údajů nebo je prováděno rozsáhlé systematické monitorování veřejně přístupných prostorů.[59]

6 Právní důvody pro zpracování osobních údajů

Právní důvody poskytují právní základ pro možné zpracování a souvisí s účelem zpracování. Důvody si jsou rovny, zároveň může existovat více důvodů, které mohou různě vznikat a zanikat. Důležitá je likvidace osobních údajů po zaniknutí posledního právního důvodu.

Právní důvod zpracování je jedním z nejdůležitějších prvků celého zpracování, protože legalizuje zpracování osobních údajů pro určité účely. Právní důvod je základním předpokladem, aby zpracování osobních údajů mohlo být považováno za legální. Zpracování se vždy děje za určitým účelem a právní důvod musí daný účel pokrývat. Je samozřejmé, že účelů může být stanoveno více, mohou se vyskytovat souběžně nebo mohou časem vznikat či zanikat. Pokud ale právní důvod zanikne a neexistuje už žádný jiný, osobní údaje musí být zlikvidovány.[60]

Zpracování osobních údajů je zákonné, pokud je splněna nejméně jedna z následujících podmínek:

- subjekt údajů udělil souhlas,
- zpracování je nezbytné pro splnění smlouvy,
- zpracování je nezbytné pro splnění právní povinnosti, která se vztahuje na správce,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
- zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, pokud před těmito zájmy nemají přednost zájmy nebo práva a svobody subjektu údajů, zejména dítěte.

[59] NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* Str. 101.
[60] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 65.

6.1 Souhlas subjektu údajů

Souhlas se zpracováním osobních údajů je jedinečný v tom směru, že jako jediný předpokládá aktivní činnost subjektu údajů.[61]

Souhlas subjektu údajů musí být svobodný, konkrétní, informovaný a jednoznačný. Subjekt údajů dává potvrzením své svolení ke zpracovávání svých osobních údajů. Účel zpracování musí být legitimní a právem nezakázaný. Subjekt údajů není povinen souhlas udělit a také má právo souhlas odvolat. Odvolání souhlasu musí být stejně snadné, jako jeho poskytnutí. Odvoláním souhlasu ale není dotčena zákonnost zpracování osobních údajů. Základním znakem souhlasu je dobrovolnost jeho udělení. Žádost o vyjádření souhlasu musí být jasně odlišitelná od jiných skutečností, musí být rozumným způsobem odlišen od ostatního textu, a správce musí být schopen souhlas doložit. Souhlas je udělován vždy konkrétnímu správci a účel zpracování by měl být v souhlasu jasný a zřetelný.[62]

Správce by měl vždy uvažovat nad použitím jiného právního titulu, než je souhlas subjektu údajů, a souhlas získat až ve chvíli, kdy je jasné, že jiný právní titul není možné použít.[63]

6.2 Plnění smlouvy

Osobní údaje lze správcem zpracovávat, pokud je to nutné pro splnění smlouvy a dále před uzavřením smlouvy, kdy má subjekt údajů jasný úmysl smlouvu uzavřít. Samozřejmě je nutné brát v potaz zásadu minimalizace osobních údajů a k předmětu plnění smlouvy zpracovávat jen ty nezbytně nutné.[64]

6.3 Právní povinnost

Právní povinnost správce by měla vyplývat ze zákona, případně z práva EU. Zákonem bývá správcům stanoven účel zpracování, taxativně i kategorie osobních údajů, které lze pro daný účel zpracovávat.[65]

6.4 Ochrana životně důležitých zájmů subjektu údajů

Zpracování osobních údajů je zákonné i případě, je-li nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby. Tento právní důvod se může použít pouze tehdy, nemůže-li být zpracování osobních údajů založeno na jiném právním základě. Zde

[61] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 66.
[62] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 69-75.
[63] NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář.* Str. 127.
[64] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 78.
[65] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 78.

se jedná například o zpracování nezbytné pro humanitární účely, včetně monitorování epidemií a jejich šíření.[66]

6.5 Plnění úkolu ve veřejném zájmu

Tento právní důvod cílí na činnost orgánů veřejné moci při výkonu jejich pravomoci. Velmi často dochází k souběhu tohoto právního důvodu s právním důvodem plnění právní povinnosti. Typicky může jít o obce či kraje, které plní širokou škálu činností ve veřejném zájmu a není to striktně stanovená povinnost.[67]

6.6 Oprávněné zájmy správce či třetí strany

Správce v tomto případě musí porovnávat jeho oprávněné zájmy se zájmy nebo základními právy a svobodami subjektu údajů (zejména pokud je subjektem údajů dítě). Tomuto poměřování se říká test proporcionality. Použití tohoto právního důvodu musí správce pečlivě zvážit a musí si ho umět obhájit, protože oprávněné zájmy mohou pro každého znamenat něco jiného. Jasným příkladem oprávněného zájmu je zpracování nezbytné pro účely zamezení podvodům.[68]

Podle dosud uskutečněných kontrol ÚOOÚ, který se zaměřil na kvalitu vypracování testu proporcionality, je nutné říci, že firmy si s touto problematikou zatím moc úspěšně neporadily a v rámci nesplnění této povinnosti padaly první pokuty.[69]

7 Práva subjektu údajů

Práva subjektu údajů vyvažují vztah mezi správcem a subjektem údajů, kdy subjekt údajů musí mnohdy zpracování osobních údajů strpět. Zajištění řádného výkonu práv subjektu údajů je nezbytnou podmínkou pro soulad zpracování jako celku s GDPR. Výkon práv subjektu údajů je vysoce chráněný zájem, jehož porušení je sankcionováno vyšší možnou sazbou pokuty.[70]

[66] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 79.
[67] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 79.
[68] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Str. 80.
[69] ITBIZ.CZ. *Pokuty za porušení GDPR přesáhly v Česku 7 milionů korun, kontroly odhalily neznalost balančního testu* [online]. [cit. 2020-03-23]. Dostupné z: http://www.itbiz.cz/clanky/pokuty-za-poruseni-gdpr-presahly-v-cesku-7-milionu-korun-kontroly-odhalily-neznalost-balancniho-testu/.
[70] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 124.

Subjekt údajů má následující práva:

- právo být informován,
- právo na přístup,
- právo na opravu a doplnění,
- právo na výmaz (být zapomenut),
- právo na omezení zpracování,
- právo přenositelnosti údajů,
- právo vznést námitku,
- právo nebýt předmětem automatizovaného individuálního rozhodování a profilování.

7.1 Právo být informován

Právo na informace je základní právo, které naplňuje zásadu transparentnosti zpracování. Subjektu údajů má zaručovat řádnou informovanost o zpracování jeho osobních údajů. Tuto povinnost musí správce plnit automaticky, a ne až na požádání subjektem údajů, a proto se jedná o aktivní povinnost správce. Nařízení rozlišuje obsah informací podle toho, zda správce získal osobní údaje přímo od subjektu údajů či nikoli. Obecně mezi základní poskytované minimum informací patří totožnost a kontaktní údaje správce, kontaktní údaje pověřence, je-li, dále účely a právní důvody zpracování, případný příjemce osobních údajů či úmysl předat osobní údaje do třetí země.[71]

7.2 Právo na přístup

Toto právo také úzce souvisí se zásadou transparentnosti. Subjekt údajů má právo získat od správce potvrzení, zda jsou jeho údaje zpracovávány. Pokud ano, má právo získat k těmto osobním údajům přístup a také má právo znát účel a ostatní informace. Pokud dochází k předání osobních údajů do třetí země, má subjekt údajů právo získat informace o použitých zárukách zabezpečujících ochranu těchto údajů.[72]

7.3 Právo na opravu a doplnění

Právo na opravu souvisí se zásadou přesnosti. Správce není povinen aktivně vyhledávat nepřesné údaje o subjektu údajů, ale pokud subjekt údajů požádá o opravu nepřesných osobních údajů či o jejich doplnění, musí tak učinit bez zbytečného odkladu s tím, že nejprve žádost

[71] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 126.
[72] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 129.

subjektu údajů prověří. V závislosti na kontextu a účelu zpracování může správce požádat subjekt údajů o kontrolu aktuálnosti.[73]

7.4 Právo na výmaz (být zapomenut)

Subjekt údajů má právo, aby jeho osobní údaje správce vymazal, a správce má povinnost osobní údaje vymazat bez zbytečného odkladu, je-li k tomu dán nějaký důvod. Mezi nejčastější důvody k výmazu patří naplnění účelu, pro který byly zpracovávány, dále odvolání souhlasu subjektem údajů nebo vznesení námitky proti zpracování. Správce má povinnost tak učinit, pokud už dané zpracování není nezbytné, například pro splnění právní povinnosti. Zpracovává tedy osobní údaje dále, dokud právní důvod nepomine.[74]

7.5 Právo na omezení zpracování

Omezení zpracování znamená označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu. Omezení zpracování je dočasné, čímž se liší od likvidace. Používá se například v případě, kdy subjekt údajů popírá přesnost osobních údajů a správce potřebuje nějaký čas k ověření přesnosti.[75]

7.6 Právo přenositelnosti údajů

Právo na přenositelnost údajů je zcela nové a umožňuje subjektu údajů získat své osobní údaje od správce ve strukturovaném, běžně používaném a strojově čitelném formátu a zároveň tyto údaje předat jinému správci. Účelem tohoto práva je snazší přechod subjektů údajů mezi správci jako poskytovateli určitých služeb, např. banky. Aby to bylo možné, musí být splněny kumulativně dvě podmínky. Zpracování je založeno na souhlasu či smlouvě a zpracování se provádí automatizovaně. Na jiné právní důvody se právo na přenositelnost nevztahuje.[76]

7.7 Právo vznést námitku

Subjekt údajů může ke konkrétní situaci zpracování osobních údajů vznést námitku proti zpracování jeho osobních údajů a správce údaje dále nesmí zpracovávat, dokud neprokáže závažné oprávněné důvody.[77]

[73] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Str. 131.
[74] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Str. 132.
[75] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Str. 132.
[76] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Str. 136.
[77] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Str. 140.

7.8 Právo nebýt předmětem automatizovaného individuálního rozhodování a profilování

Subjekt údajů má právo nebýt předmětem žádného automatizovaného zpracování, včetně profilování.[78]

8 Sankce, pokuty

Je logické, že za nedodržení jakékoliv právní normy hrozí nějaký postih. Platí to v případě GDPR. Před jeho zavedením v účinnost se správci, zpracovatelé obávali možné likvidace jejich podniku, když zjistili, jaké maximální pokuty jim hrozí. ÚOOÚ tuto paniku musel mírnit. Vysoké pokuty jsou stanoveny z jednoho prostého důvodu. Nařízení dopadá i na největší společnosti světa, na které by nízké pokuty neměly žádný dopad.

Ukládání správních pokut samozřejmě musí být účinné a odrazující, zároveň ale přiměřené. To znamená, že ne každé porušení znamená pokutu. Nejprve může být správce upozorněn na pravděpodobné porušení nařízení, může mu být uděleno napomenutí aj.[79]

Při rozhodování o správní pokutě se zohledňují různé okolnosti jako například kategorie dotčených údajů, délka trvání porušení, závažnost, úmysl či nedbalost, předchozí porušení, míra spolupráce s dozorovým úřadem aj.

Pokuty jsou rozděleny do dvou skupin, a to podle toho, jakého porušení se správce, zpracovatel dopustil.

Pokutu lze „*udělit až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší nebo až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.“*[80]

Rozdělení do dvou daných skupin je na základě míry porušených povinností. To znamená, že u vyšší sazby pokuty je očekávána vyšší míra zásahu do práv subjektu údajů. Jako příklad lze uvést porušení povinností upravujících zásady a zákonnost zpracování, porušení práv subjektu údajů. Do nižší sazby patří například porušení týkající se záznamů o činnostech zpracování, neprovedení posouzení vlivu.[81]

---

[78] ŽŮREK, Jiří. *Praktický průvodce GDPR.* Str. 141.
[79] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Str. 44.
[80] Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/83.htm.
[81] NEZMAR, Luděk *GDPR: praktický průvodce implementací.* Str. 44.

Počet nahlášených porušení zabezpečení osobních údajů ÚOOÚ je od začátku platnosti GDPR do 13. 11. 2019 celkem 638. Úřad celkem udělil 105 pokut za bezmála 7,5 mil. Kč.[82]

9 Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon č. 110/2019 Sb., o zpracování osobních údajů neboli tzv. Adaptační zákon vešel v platnost 24. dubna 2019. Tento zákon upravuje na vnitrostátní úrovni některé případy, které nejsou v rámci GDPR upraveny nebo jsou upraveny obecně. Zároveň s tímto zákonem byl také přijat další zákon, a to zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, tzv. Doprovodný zákon (ten dopadá pouze na orgány veřejné moci).[83]

Adaptační zákon tedy upřesňuje a upravuje nařízení, tak jak to samotné nařízení členským státům umožňuje. Adaptační zákon upřesňuje věkovou hranici u dětí, kdy jsou způsobilé k udělení souhlasu se zpracováním osobních údajů. Tuto hranici český zákon snížil na 15 let (GDPR říká 16 let). Také je upřesněna informační povinnost správce, kdy stačí zveřejnění potřebných informací na svých internetových stránkách. Zmírňuje povinnost vypracovat posouzení vlivu na ochranu osobních údajů při jejich rozsáhlém zpracování na základě zákonné povinnosti. Dále Adaptační zákon specifikuje zpracování osobních údajů na základě novinářské, akademické, umělecké, nebo literární licence a posuzování přiměřenosti takového zpracování. Rovněž došlo k omezení práva subjektu údajů na vznesení námitky proti zpracování osobních údajů. Co se týče přestupků, Adaptační zákon snížil horní hranice správních pokut. A v neposlední řadě došlo přijetím nového zákona k úpravě pozice Úřadu pro ochranu osobních údajů, kdy má jasně dané své pravomoci a úkoly.[84]

[82] ÚOOÚ. *Poskytnutí informací k dozorové činnosti.* [online]. [cit. 2020-03-23]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5842&n=poskytnuti%2Dinformaci%2Dk%2Ddozorove%2Dcinnosti.
[83] Ministerstvo průmyslu a obchodu. *GDPR.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.mpo.cz/cz/podnikani/ochrana-osobnich-udaju-gdpr/adaptacni-zakony-k-gdpr-byly-schvaleny-a-nabyly-ucinnosti---245652/.
[84] Epravo.CZ. *Nový zákon o zpracování osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html.

Praktická část

10 Charakteristika firmy Horské lázně Karlova Studánka

Horské lázně Karlova Studánka, dále uváděné také pod zkratkou HLKS, jak už název napovídá, se nacházejí v horské oblasti na úpatí nejvyšší hory Jeseníků, na úpatí hory Praděd. Leží v okrese Bruntál na severu Moravy. Lázně mají dlouholetou historii, ale jako státní podnik v současné podobě byly založeny 1. ledna 1991 Ministerstvem zdravotnictví České republiky. Do poloviny roku 2013 nesly jméno Státní léčebné lázně Karlova Studánka, státní podnik.

Obr. č. 3: Karlova Studánka – Pitný pavilon. (Zdroj: vlastní)

V Horských lázních Karlova Studánka se léčí nemoci onkologické, nemoci oběhového ústrojí, nemoci z poruchy výměny látkové a žláz s vnitřní sekrecí, netuberkulózní nemoci dýchacího ústrojí, nemoci nervové, nemoci pohybového ústrojí, duševní poruchy a nemoci kožní.[85]

Předmětem činnosti je zajišťování lázeňské péče pro pacienty ve stanovených indikacích podle příslušných předpisů v rozsahu stanoveném zakladatelem. Dále správa a využití přírodních léčivých zdrojů v součinnosti s Českým inspektorátem lázní a zřídel včetně jejich

[85] Portál HLKS – INDIKACE. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://www.horskelazne.cz/indikace.

ochrany. Předmětem podnikání lázní je také poskytování zdravotních služeb v oboru rehabilitační a fyzikální medicíny a dále lázně podnikají v následujících oborech:

- výroba tepelné energie,
- rozvod tepelné energie,
- distribuce plynu,
- výroba a distribuce elektřiny,
- obchod s plynem,
- obchod s elektřinou,
- hostinská činnost,
- výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona,
- masérské, rekondiční a regenerační služby,
- pronájem nemovitostí, bytů a nebytových prostor,
- prodej kvasného lihu, konzumního lihu a lihovin.[86]

Lázně nabízejí pro pojištěnce lázeňskou péči buď komplexní nebo příspěvkovou, dále nabízejí ambulantní rehabilitační péči a v neposlední řadě různé léčebné nebo rekreační pobyty. Pořádají se zde různé kongresy a akce. Pro širokou veřejnost je k dispozici bazénový komplex, sauny, whirlpool, solná jeskyně, fitness. Lázně provozují vlastní restauraci, cukrárnu, obchůdek i minimarket. Důležitá je služba Pošta Partner.

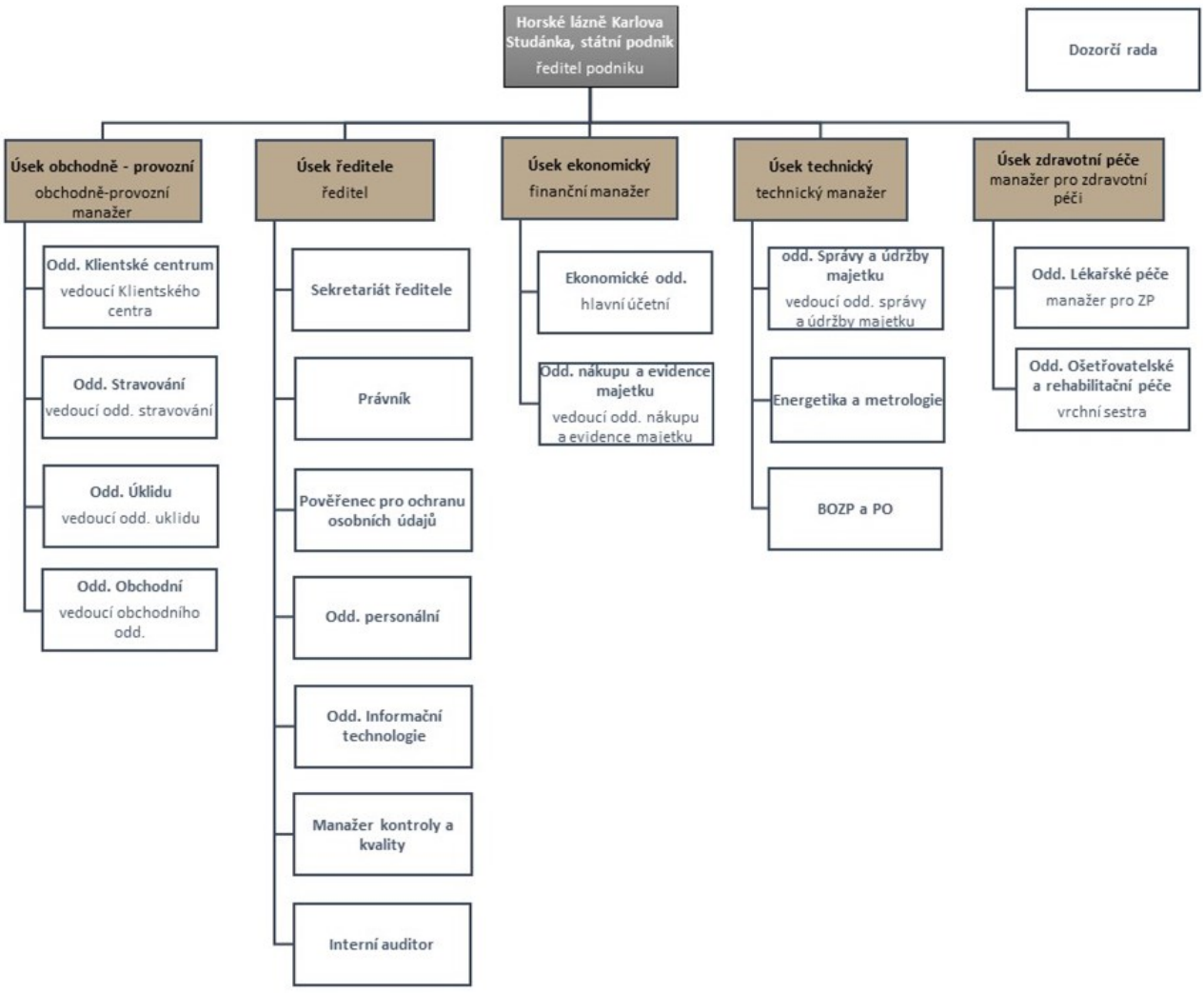
Statutárním orgánem lázní je ředitel podniku, který má tři zástupce. Státní podnik zřizuje jako kontrolní orgán dozorčí radu. Za podnik jedná ředitel a v jeho nepřítomnosti zástupce ředitele dle stanoveného pořadí. Vedení podniku tvoří ředitel, manažeři úseků a vedoucí oddělení. V hlavní lázeňské sezóně zde bývá zaměstnáno něco kolem 200 zaměstnanců. Ukázka celoročních průměrných počtů zaměstnanců za vybraná léta je znázorněna v následující tabulce.

Tab. č. 1: Průměrné počty zaměstnanců. (Zdroj: výroční zprávy[87])

Vybraný rok	2001	2007	2010	2013	2015	2017	2018
Průměrný počet zaměstnanců	121	139	156	125	141	166	167

[86] Veřejný rejstřík a sbírka listin. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://or.justice.cz/ias/ui/vypis-sl-firma?subjektId=214034.
[87] Veřejný rejstřík a sbírka listin. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://or.justice.cz/ias/ui/vypis-sl-firma?subjektId=214034.

Nejvíce zaměstnanců pracuje na úseku obchodně-provozním, dále na úseku zdravotní péče, následuje úsek technický, úsek ředitele a nejméně zaměstanců je na úseku ekonomickém. Každý úsek má různý počet oddělení, jak ukazuje organizační schéma na následujícím obrázku.



Obr. č. 4: Organizační schéma podniku HLKS[88]

10.1 Úsek obchodně-provozní

Klientské centrum stojí na samém začátku a vlastně i konci pobytu klienta (pacienta či rekreanta). Na základě došlého návrhu na lázeňskou péči, který posílá do lázní zdravotní pojišťovna, se klientské centrum domlouvá s pacientem (telefonicky, písemně), jak tato péče bude probíhat, sjednávají spolu veškeré požadavky (lázní i pacienta). Klientské centrum je tedy oddělení, které zpracovává i zvláštní kategorii osobních údajů, a to zdravotní stav pacienta. Co

[88] Portál HLKS. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://www.horskelazne.cz/organizacni-schema.

se týče rekreantů, zpracovávají se pouze standardní osobní údaje. Po příjezdu do lázní jsou klienti odbaveni na recepci, ta zpracovává pouze jejich základní údaje.

Oddělení stravování zpracovává osobní údaje o tom, jakou stravu klient požaduje, zda je na nějaké jídlo alergický nebo vyžaduje určitou dietu, zda má celodenní stravu či polopenzi. Tyto údaje do kuchyně předává nutriční terapeut souhrnně za všechny přítomné hosty. Obsluha klienta usazuje ke stolu, u kterého se klient stravuje celý svůj pobyt. Na stole má kartičku se svým jménem, dobou trvání stravy a popřípadě s daným stravovacím omezením. K tomuto oddělení patří také sklad potravin, který zpracovává osobní údaje pouze z odběratelsko-dodavatelských vztahů, stejně tak externí provozy (restaurace a cukrárna).

Na následujícím obrázku je jedna z jídelen, kde se stravují pacienti, tzv. Velká jídelna. Kuchyně a jídelny se nacházejí v lázeňském domě Libuše.

Obr. č. 5: Velká jídelna na Libuši.[89]

Oddělení úklidu provádí úklid skrz celé lázně, na starosti má veškeré provozy. To znamená, že obstarávají také úklid na pokojích, kde jsou hosté ubytovaní. Celkově mají lázně k dispozici 468 lůžek v jedno a dvoulůžkových pokojích v 8 lázeňských domech. Pokojské se o klientovi, který je na pokoji ubytovaný, dozvědí jméno, příjmení a délku pobytu, to znamená, jen základní údaje.

[89] Portál HLKS – FOTOGALERIE. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://www.horskelazne.cz/libuse.

Obchodní oddělení má na starosti marketing, kongresy, rekreologii a lázeňské obchody. Toto oddělení zpracovává osobní údaje subjektu údajů na základě smluvní dohody mezi klientem a lázněmi a dále na základě odběratelsko-dodavatelských vztahů, tedy pouze standardní osobní údaje.

10.2 Úsek ředitele

Úsek ředitele, to je **právník, pověřenec pro ochranu osobních údajů, interní auditor, manažer kontroly a kvality**. Běžně se setkávají se standardními osobními údaji.

Dále tady patří **sekretariát ředitele a podatelna**, která vede spisovou službu, evidenci smluv a vnitropodnikovou dokumentaci. Spisová služba zahrnuje evidenci veškeré pošty, příchozí a odchozí, to znamená třeba i návrhů na lázeňskou péči, kde jsou osobní údaje ze zvláštní kategorie (zdravotní stav). Po zaevidování ji předává oddělení, kterému je určena.

K úseku ředitele patří také **oddělení informačních technologií**, které má na starosti servis a údržbu informačních systémů, včetně aktualizace, zálohování a přenosu dat. Dále IT oddělení řídí přístupová práva uživatelů, přiřazuje uživatelům IP adresy. Na starosti má také kamerový systém. Zpracovává standardní osobní údaje.

Poslední a podstatné oddělení tohoto úseku je **oddělení personální a mzdové**, které zpracovává osobní údaje o zaměstnancích podniku pro řádné plnění pracovně-právního vztahu. Zaznamenává všechny osobní údaje přijatého zaměstnance k dalšímu zpracování jako vytvoření povinných hlášení příslušným úřadům, vytváření statistik, generování příslušných potvrzení pro peněžní ústavy, vytváření ročního zúčtování daně, rozhodnutí o dočasné pracovní neschopnosti, zdravotní a sociální pojištění aj. Mimo jiné se jedná i o zvláštní kategorii osobních údajů, kterou představuje v tomto případě členství v odborové organizaci.

10.3 Úsek ekonomický

Pod úsek ekonomický spadá **finanční účtárna**, která zpracovává účetní doklady, faktury. Finanční účtárna dostává podklady potřebné pro účetnictví z ostatních oddělení. Jedná se tedy o vnitropodnikové podklady a dokumentaci, ale zejména se zde zpracovávají osobní údaje týkající se odběratelsko-dodavatelských vztahů. K ekonomickému úseku patří také **oddělení nákupu, sklad MTZ a evidence majetku**. Oddělení nákupu eviduje dokumentaci k veřejným zakázkám a eviduje smlouvy ve veřejném registru smluv. Sklad MTZ zpracovává vnitropodnikovou dokumentaci, kterou představují výdejky a dodavatelskou dokumentaci, jako faktury a dodací listy. Evidence majetku má na starosti ubytovny, byty a nebytové prostory, které pronajímá. To znamená, že vede osobní údaje na základě smluvního vztahu.

10.4 Úsek technický

Oddělení správy a údržby majetku zajišťuje řádný chod lázní. Provádí údržbu, opravy. Osobní údaje má pouze z odběratelsko-dodavatelských vztahů, stejně jako **oddělení energetiky a metrologie**. **BOZP a PO** vykonává externí pracovník na základě smluvního vztahu s lázněmi.

10.5 Úsek zdravotní péče

Úsek zdravotní péče je pro lázně ten nejdůležitější. Rozděluje se na dvě oddělení, a to **oddělení lékařské péče** a **oddělení ošetřovatelské a rehabilitační péče**. Na tomto úseku stojí veškerá léčebná a rehabilitační péče. Lékaři, fyzioterapeuti, zdravotní maséři, zdravotní sestry a ostatní zdravotní personál přicházejí do styku se subjekty údajů a jejich osobními údaji, zejména se zvláštní kategorií osobních údajů, která je prezentována zdravotním stavem. Je důležité znát tyto osobní údaje, aby léčba a rehabilitace probíhala správným směrem, pomohla a neuškodila.

Obr. č. 6: Provoz balneoterapie Letní lázně – vany.[90]

Na předchozím obrázku je ukázka provozu balneoterapie, kterou pacienti navštěvují. Jde o jednu z možných koupelí.

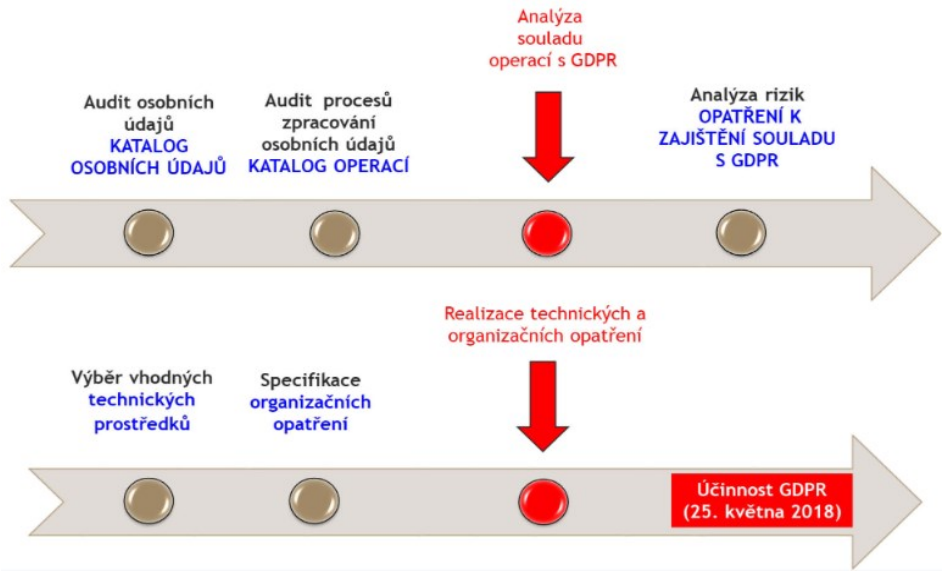
[90] Portál HLKS – FOTOGALERIE. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://www.horskelazne.cz/letni-lazne.

11 Postup implementace GDPR

Na podzim roku 2017 se v médiích začalo každý den skloňovat GDPR a ochrana osobních údajů. Nařízení se najednou začalo řešit ve velkém a mnoho firem dostalo strach, že nestihnou GDPR do řádného termínu implementovat. Řešit se to začalo i v lázních. Proto na příkaz ředitele byla ustanovena pracovní skupina k ochraně osobních údajů, která měla za úkol implementovat GDPR do podniku a zároveň ho vnést do povědomí zaměstnanců. Jako vedoucí skupiny byl ustanoven právník podniku, který měl za úkol řídit a metodicky vést ostatní členy pracovní skupiny tak, aby bylo vše ve stanovený čas v souladu s GDPR. Členy pracovní skupiny byli zvoleni vybraní zaměstnanci z jednotlivých oddělení.

Na začátku požadované implementace GDPR bylo potřeba, aby se všichni členové pracovní skupiny seznámili se základními informacemi a dokumenty, které s nařízením souvisí. Tedy kdo je správce/zpracovatel; co je to osobní údaj/citlivý osobní údaj, co je to zpracování, jaké jsou právní důvody zpracování, jaké práva má subjekt údajů, kdo je pověřenec pro ochranu osobních údajů aj. K dispozici dostali několik materiálů jako například Obecné nařízení nebo dokument s názvem Metodika implementace GDPR ve zdravotnictví, který je dostupný mimo jiné na stránkách Ministerstva zdravotnictví České republiky.

První schůzka byla víceméně seznamovací. Šlo o všeobecnou diskuzi, aby všichni pochopili význam GDPR a také jeho jednotlivé definice a samozřejmě také, aby se vedoucí skupiny ujistil, že celá skupina má představu o tom, co bude následující týdny řešeno. Už na začátku bylo důležité znát dobře problematiku ochrany osobních údajů, aby následně všichni mohli řádně plnit úkoly potřebné ke sladění požadavků s GDPR. Mimo jiné členové pracovní skupiny dostali za úkol seznamovat kolegy na svých oddělení s činností této pracovní skupiny, měli jim předávat poznatky o GDPR a průběhu implementace, tak aby sami zaměstnanci byli schopni a ochotni se do implementace zapojit a aby pochopili její význam. Vedoucí skupiny postupně seznamoval ostatní členy s tím, jak by celý proces měl probíhat, jaký konkrétní postup implementace by byl vhodný a co tedy bude kdy následovat. Názorně je to představeno na následujícím obrázku.



Obrázek č. 7: Postup implementace GDPR[91]

11.1 Mapování

Po tomto úvodním seznámení se mohlo začít. Nejprve bylo potřeba zmapovat situaci týkající se osobních údajů v rámci celého podniku. Každý člen pracovní skupiny za své oddělení a se svým oddělením v součinnosti. Probíhalo to tím způsobem, že se do rukou vzal každý dokument, který se v podniku zpracovává a sepsalo se, jaké obsahuje osobní údaje standardní, popřípadě osobní údaje zvláštní kategorie. Cílem bylo zjistit, jaké množství osobních údajů se vlastně shromažďuje, jaký je rozsah jejich zpracování, jaká je doba jejich uložení a v neposlední řadě, jak jsou tato data dostupná. Vše se průběžně zapisovalo do katalogu osobních údajů. Katalog se postupně rozrůstal a rozpracovával, protože se k němu následně přiřazovaly účely a právní důvody zpracování. Nakonec se ke všem osobním údajům musely přiřadit jednotlivé informační systémy, ve kterých jsou dané osobní údaje shromažďovány.

Tento úvodní katalog sloužil k vytvoření 3 druhů číselníků společných pro všechna oddělení podniku, a to pro kategorii osobních údajů, pro právní důvody zpracování a pro operace zpracování.

[91] ÚZIS. Metodika implementace GDPR ve zdravotnictví. [online]. [cit. 2020-03-23]. Dostupné z: https://www.uzis.cz/index.php?pg=o-nas--ochrana-osobnich-udaju--gdpr-ve-zdravotnictvi.

11.2 Operace zpracování

Po vytvoření společných druhů číselníků se přistoupilo k vytvoření katalogu operací zpracování. Opět každé oddělení samo za sebe a až po následné diskuzi pracovní skupiny se operace, které se vyskytly u více oddělení, přiřadily k jednomu určitému, proto aby se nezpracovávaly zbytečně duplicitně. Byla vytvořena tabulka, do které se k procesu zpracování vepisovaly nosiče, tedy prostředky zpracování. Dále se podle vytvořených číselníků doplňoval účel zpracování, právní důvod a kategorie osobních údajů. Nechyběly operace zpracování, zdokumentování procesu, poznámka či komentář a jako poslední se přidala kolonka subjekt. Prakticky je proces zpracování (skupiny činností) například účetnictví. Nosičem v elektronické podobě je program, ve kterém se účetnictví zpracovává, v papírové podobě se jedná o faktury, daňové doklady, pokladní doklady aj. Účelem zpracování je vedení a evidence z důvodu plnění smlouvy a na základě právní povinnosti. Dále se do procesu zpracování vypsali z už dříve vytvořených číselníků vybrané kategorie osobních údajů, které je zde možné najít a operace zpracování, které se s nimi provádějí. Zdokumentování procesu účetnictví je uvedeno ve směrnicích ekonomického úseku. V poznámce jsou vypsané zákony, kterých se proces zpracování účetnictví a jeho evidence týkají. Nechybí typ subjektu údajů, kterými jsou zaměstnanec a smluvní strana. V případě kontroly jde o třetí osobu.

11.3 Analýza souladu s GDPR

Katalog zpracování se následně opět více rozpracoval ve formuláři popisu procesů zpracování. To znamená, že do vytvořeného formuláře se napsal název činnosti, ke které se dále doplnily popis a náležitosti procesu, celkem 13 bodů. Konkrétně se jednalo o stručný obsah procesu srozumitelně formulovaný; o kategorie subjektu údajů rozdělené na klíčové, doplňkové; o typ agendy zpracování, zda se jedná o manuální či automatizované; o účel zpracování, jaký je hlavní účel a jsou-li nějaké vedlejší; o právní důvody; pokud je oprávněný zájem, tak jaký, v čem spočívá; pokud je právní povinnost, tak jak je podložena, jakým právním předpisem; dále jsou zde zaznamenána místa uložení osobních údajů, jak v elektronické podobě tak v listinné, ať jde o originály či kopie; zdroj těchto údajů, zda je to subjekt údajů sám nebo někdo jiný, potom kdo; dále kdo ze zaměstnanců má oprávnění zpracovávat osobní údaje; jaká je doba uchování, tedy lhůta pro výmaz; jsou-li zpracovatelé, tak jejich bližší specifikace; nechybí kategorie příjemců v ČR popřípadě mimo ČR, datum vyhovení zápisu a kdo tento zápis vypracoval.

Co se týče zpracovatelů, zde vyvstala otázka, kdo je zpracovatel lázní, pro koho jsou zpracovatelé lázně a zda s někým lázně nejsou společnými správci. Nebylo to vždy

jednoznačné, proto se členové pracovní skupiny dotazovali příslušných firem a žádali stanovisko, zda se považují za zpracovatele či správce. Šlo o to pochopit správně význam zpracovatele, správce a jejich činností.

Tyto formuláře se následně použily při zhodnocení naplnění požadavku nařízení, kdy se prováděla analýza souladu s GDPR, která znamenala vypracování dalších 3 dokumentů, a to minimalizace údajů, účelové omezení a zpracovatelé.

Minimalizace údajů a účelové omezení obsahují kolonky název procesu; zhodnocení, jestli vyhovuje či nikoli; popis případného nedostatku a návrh opatření, je-li potřeba. Co se týče zpracovatelů, tato tabulka obsahovala opět název procesu, jméno zpracovatele, předmět plnění, zhodnocení, jestli vyhovuje či nikoli; popis případného nedostatku a návrh opatření, je-li potřeba.

11.4 Analýza rizik

Ke každému procesu zpracování bylo potřeba vytvořit analýzu rizika. K tomuto nelehkému kroku prováděné implementace byl přizván manažer kvality a kontroly, který má dostatečné zkušenosti s problematikou tvorby rizik a mohl pracovní skupině pomoct a objasnit základní principy tvorby této analýzy. Pracovní skupina se po této konzultaci s manažerem kvality a kontroly shodla, že využije nejjednodušší analýzu rizika, která spočívala v určení pravděpodobnosti rizika a dopadu rizika, kdy jejich následným vynásobením se určuje míra možného rizika. Za prvé se musely identifikovat možné hrozby (lidský faktor, pracovní prostředí, technické zabezpečení aj.) a následně určit pravděpodobnost výskytu rizika. Pro pravděpodobnost výskytu se použila stupnice od jedné (která představuje nejnižší pravděpodobnost) do pěti (která představuje jistotu výskytu). Pokračovalo se hodnocením dopadu rizika. Opět byla stanovená stupnice od jedné (což znamená zanedbatelný dopad) do pěti (což je kritický dopad). Na základě dané matice se určila míra rizika. Míra rizika mohla být vysoká, nízká nebo zbytková, právě podle vypočítaného skóre. Hodnoty skóre rizika 1–3 znamenaly zbytkové riziko, hodnoty 4–12 nízké riziko a hodnoty 13–25 riziko vysoké.

Dalším úkolem bylo zjištěné míry rizika vyhodnotit a adekvátně na ně reagovat. To znamená, že zvýšené míry rizik se musely snížit na určitou mez, což se provedlo v rámci dalších kroků implementace.

11.5 Výběr vhodných technických a organizačních opatření

Vzhledem k době, po kterou lázně fungují a vzhledem k předchozí právní úpravě regulující nakládání s osobními údaji, lázně měly již řadu organizačních a technických opatření

zavedených. Bylo potřebné tato opatření místy upřesnit či doplnit. Některá opatření bylo nutné nově zavést tak, aby odpovídala konkrétním rizikům.

V této fázi jako první začali členové pracovní skupiny oslovovat zpracovatele osobních údajů, aby doložili, že přijali adekvátní technická a organizační opatření k zajištění řádné ochrany osobních údajů, a tedy, že jsou u nich dány dostatečné záruky řádného provádění zpracování, kterými jsou pověřeni lázněmi. Lázně se odkazovaly na článek 28 odst. 1 GDPR, který povoluje jen zpracovatele, kteří splňují požadavky nařízení. Proto si zpracovatelé museli sami vyhodnotit a lázním v určené době předložit, jaké mají technické zabezpečení, IT zabezpečení a nakonec, jaké mají organizační a smluvní zajištění. Jednoduše byli požadovány záruky spolupráce. Smluvní vztahy se upravovaly, popřípadě se uzavíraly nové smlouvy.

V HLKS se také řešilo fyzické umístění všech dokumentů obsahujících jakékoliv osobní údaje. Kde a jak jsou uložené. Zda v uzamykatelných skříních či kartotékách, v kancelářích či archivech. Kdo má do jednotlivých kanceláří a archívů přístup. Jaké je zabezpečení jednotlivých budov. Celé lázně se procházely a vyhodnocovalo se, nakolik je fyzická bezpečnost v pořádku, kde a jak je potřeba udělat určitá opatření.

Podstatným organizačním opatřením bylo zavedení pověřence pro ochranu osobních údajů a jeho zavedení do organizační struktury podniku, do úseku ředitele. Další organizační opatření řeší jednotlivé směrnice. Tak aby byly popsány jednotlivé pracovní činnosti zaměstnanců. Je důležité, aby bylo jasně dané, jak mají vypadat jednotlivé kroky všech činností, aby nebylo možné se odchýlit od zavedené praxe.

Nedílnou součástí byla kontrola informačních systémů. Tu měli na starosti převážně pracovníci IT oddělení. Jen jim manažeři a vedoucí všech oddělení sepsali, které systémy využívají jednotliví zaměstnanci, které potřebují a kterými disponují nad rámec svých povinností. Podle toho se omezovala nebo rozšiřovala jednotlivá přístupová práva. Zavedla se kontrola zálohování a aktualizace, nastavila se určitá doba, kdy se musí měnit hesla, která mají stanovenou minimální délku a doporučilo se užití velkých a malých písmen, číslic a ostatních znaků. Samozřejmostí byla a jsou nadále unikátní přístupová hesla, která zaměstnanci spolu nesdílí. Není povoleno do firemních počítačů vkládání vlastních nosičů dat. Při nepoužívání se počítač automaticky uzamkne. Pokud zaměstnanec odchází od svého počítače, musí ho uzamknout sám.

11.6 Zpracování informací pro pacienty a ostatní klienty

Pro subjekty údajů byly sepsány informace o zpracování osobních údajů, zvlášť pro pacienty a zvlášť pro ostatní klienty, protože v některých bodech se mírně liší. Základní

struktura informačního dokumentu je v obou případech stejná. Lázně jako správce informuje subjekty údajů, jaké osobní údaje zpracovává; na jakém základě, za jakým účelem a jak dlouho; co se stane s údaji po uplynutí oprávněného uchování; komu jsou osobní údaje zpřístupněny či předávány; jaké mají práva a kontakt na pověřence pro ochranu osobních údajů. Tyto informace jsou mimo jiné zveřejněny i na webových stránkách lázní.

11.7 Školení

Zaměstnanci HLKS byli proškolování průběžně členy pracovní skupiny. Každý člen měl za úkol plnit příslušné požadavky v součinnosti se svými kolegy. Ti proto museli být seznámeni se vším, co pracovní skupina řešila na svých poradách.

11.8 Aktualizace a audit

V den nabytí účinnosti nařízení měli lázně splněnou základní implementaci. Ustanovili pověřence pro ochranu osobních údajů z řad vlastních zaměstnanců, protože v danou chvíli se to jevilo jako nejlepší možné řešení. Samozřejmě toto datum neznamenalo, že by činnost pracovní skupiny byla u konce a dále neměla co na práci. Ta je pověřena stále (jen průběžně dochází k různým personálním změnám), protože jak už bylo několikrát zmíněno, ochrana osobních údajů je neustálý nikdy nekončící proces. A také je potřeba provádět opakovaně aktualizace vytvořených dokumentů.

Pokud se zavádí nový informační software nebo cokoliv nového, musí se to nejprve zkonzultovat s pověřencem pro ochranu osobních údajů. Již při plánování, nejpozději při zahájení nové činnosti, musí být pracovní postupy a technické prostředky nastaveny tak, aby garantovaly plnění základních zásad a povinností nařízení.

12 Rozdělení osobních údajů

Z provedené implementace GDPR vyplývá, jaké osobní údaje se v HLKS zpracovávají, proč a na základě jakého právního důvodu. Tyto osobní údaje se dají rozdělit do čtyř základních kategorií. Osobní údaje pacientů, osobní údaje ostatních klientů (rekreantů a uživatelů volnočasových aktivit), další kategorií jsou osobní údaje zaměstnanců a poslední čtvrtou kategorií jsou osobní údaje z odběratelsko-dodavatelských vztahů (kam je možné zařadit také odběratele energií a nájemce bytových a nebytových prostor). Osobní údaje subjektů údajů se nezpracovávají pouze na jednom úseku či oddělení, ale obvykle se prolínají více úseky.

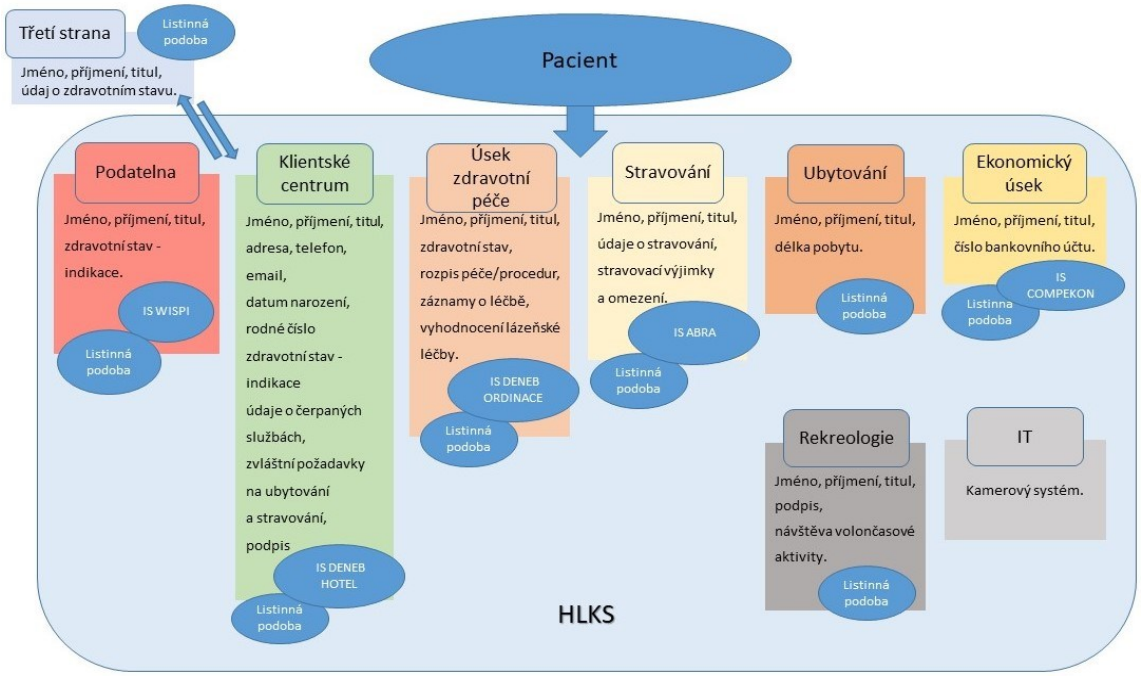
12.1 Osobní údaje pacientů

Lázně zpracovávají údaje, které jim o subjektu údajů zaslala zdravotní pojišťovna a údaje od samotného subjektu údajů, tedy pacienta. Jde o jméno, příjmení, titul, datum narození, rodné číslo, adresu, telefonní číslo, údaje o zdravotní pojišťovně a zdravotním stavu nebo léčebné indikaci, údaje o rodinném stavu, informace o důchodu a zaměstnání, kontakty na rodinné příslušníky. Osobní údaje slouží ke zpracování požadavku na lázeňskou péči, pro komunikaci s pacientem, pro poskytnutí služeb zdravotní péče, pro ubytování či stravování, dále pro vyúčtování poskytnuté péče, v neposlední řadě pro evidenci, a nakonec pro archivaci. Právním základem pro zpracovávání osobních údajů je nezbytnost pro plnění smluvního vztahu o poskytování zdravotní péče a dále plnění právních povinností, které se na lázně vztahují. Jmenovitě jde především o zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, dále o vyhlášku č. 98/2012 Sb., o zdravotnické dokumentaci, nebo třeba o zákon č. 48/1997 Sb., o veřejném zdravotním pojištění.

Do lázní přichází návrh na lázeňskou péči v listinné podobě, který přebírá podatelna. Podatelna návrh zapíše do informačního systému a předá dál oddělení klientského centra. Klientské centrum zkonzultuje návrh s lékařem, podle toho se poté obrací na samotné pacienty a domlouvá s nimi nástup do lázní a vše potřebné. Poté co pacient přijede a zapíše se na recepci, dostane ubytovací a stravovací kartičku, kterou odevzdá na pokoji a na jídelně. Po konzultaci s lékařem mu časovací kancelář následně načasuje rozpis léčby a jednotlivých procedur, který má pacient po celou dobu strávenou v lázních u sebe a na každé proceduře se s ním prokazuje. Po proběhlém léčení se tento rozpis ukládá do chorobopisu pacienta, který je archivován v lázních. Část návrhu na lázeňskou péči doplněný o průběh léčby se vrací zpět do zdravotní pojišťovny. Ubytovací a stravovací kartička se na příslušném oddělení skartuje. Ekonomický úsek zpracovává osobní údaje, tedy jméno, příjmení, titul a číslo bankovního účtu pouze v případě, že pacient z nějakého důvodu (většinou zkrácení pobytu) požaduje vrácení poplatku či doplatku. Tyto údaje získá účetní od klientského centra. Oddělení rekreologie zpracovává jméno a příjmení, popřípadě podpis v případě, že se pacient účastní nějaké volnočasové aktivity, kde je například omezený počet návštěvníků a je potřeba být nahlášen. Některé prostory jsou v lázních monitorované kamerovým systém, proto je pravděpodobné, že na těchto záznamech je zachycen i pacient. Na následujícím obrázku je znázorněno v jednoduché formě schéma výskytu osobních údajů pacientů během jejich pobytu v HLKS.

Znázorněné schéma ukazuje, že třetí strana, kterou tvoří zdravotní pojišťovna či revizní lékař, a následně i samotný pacient, předávají lázním spoustu osobních údajů. Tok osobních

údajů je samozřejmě obousměrný. V případě pacientů jde také o zvláštní kategorii osobních údajů. Je zde vidět, že každý úsek zpracovává jiné údaje. V každém případě jen ty, které opravdu potřebuje, nikdo nezpracovává nic navíc. Také je vidět, že každý úsek má svůj vlastní informační systém, do kterého se potřebná data zadávají.

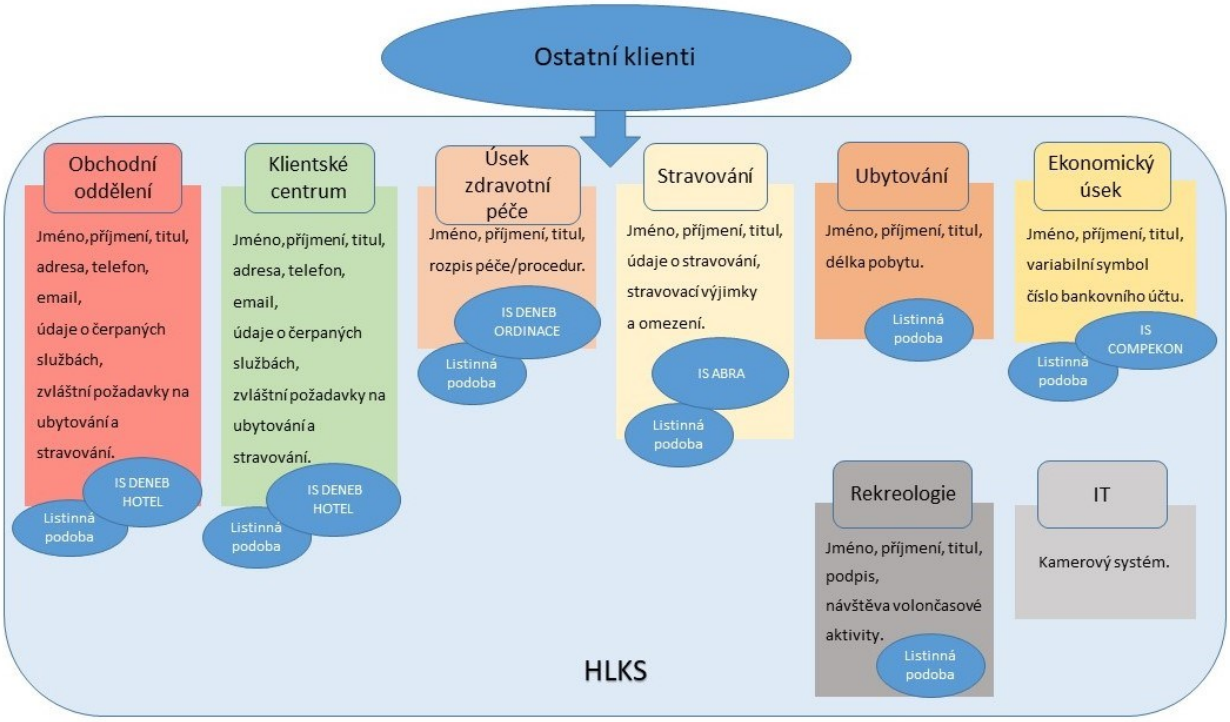


Obr. č. 8: Schéma výskytu osobních údajů pacientů. (Zdroj: vlastní)

12.2 Osobní údaje ostatních klientů

Ostatní klienti jsou ti, kteří využívají lázně k rekreaci, účasti na kongresu nebo navštěvují volnočasové aktivity, které lázně pořádají.

Jedná se primárně o obchodní oddělení, které zpracovává osobní údaje na základě objednávkového listu nebo dané poptávky po službách lázní a údaje osobně předložené klientem na místě. Jedná se o osobní údaje jako jméno, příjmení, titul, datum narození, adresa, telefon, e-mail, podpis, v případě cizinců jsou údaje vyžadované ze zákona pro hlášení pobytu cizinců (státní občanství a číslo cestovního pasu), přesněji dle zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů; dále jsou to údaje o využitých službách či údaje o úhradě služeb. Osobní údaje slouží ke zpracování požadavků na poskytnutí služeb, uzavření a evidování smluvního vztahu. Smluvní vztah je právní důvod zpracování. Podle toho, s jakými požadavky klienti do lázní přicházejí, se jejich osobní údaje vyskytují v daných informačních systémech daných oddělení. Neznamená tedy, že každé oddělení vždy zpracovává osobní údaje ostatních klientů, ale ta možnost zde je, a proto jsou na následujícím obrázku znázorněna všechna oddělení, kde se osobní údaje objevit mohou.



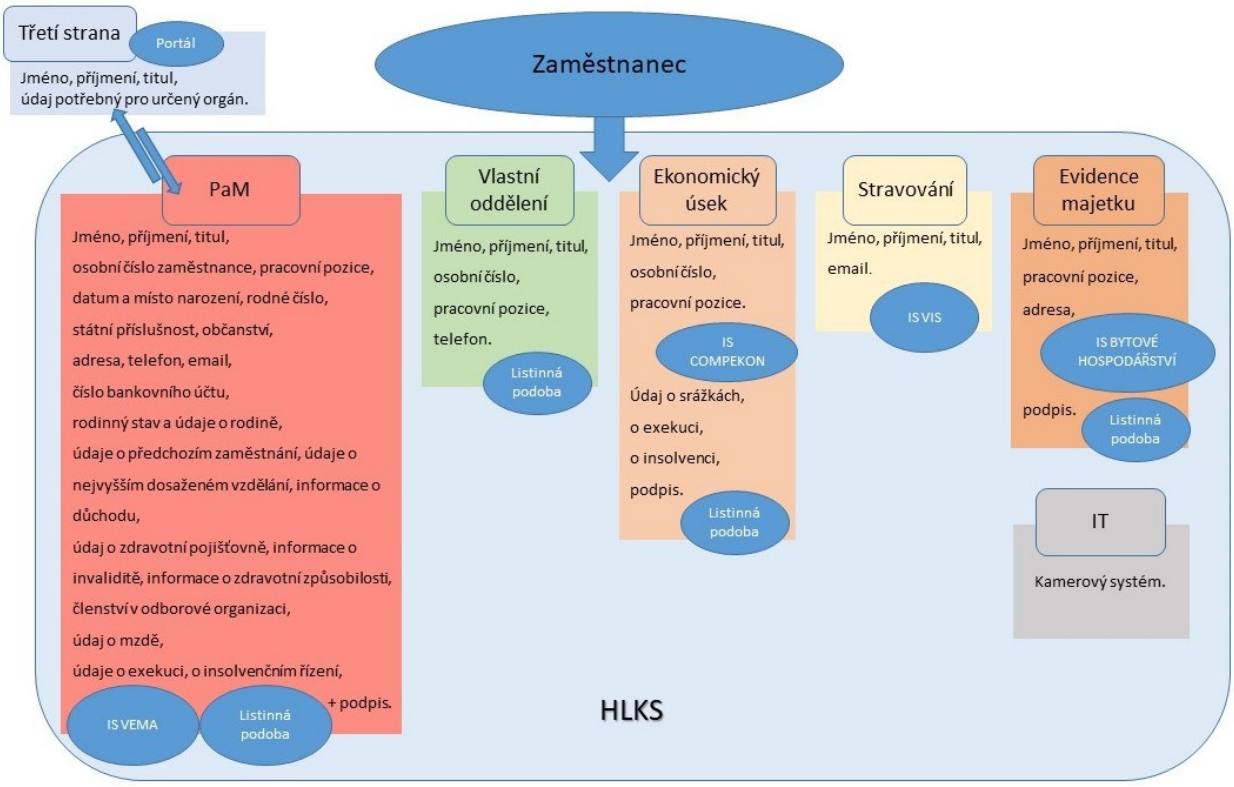
Obr. č. 9: Schéma výskytu osobních údajů ostatních klientů lázní. (Zdroj: vlastní)

12.3 Osobní údaje zaměstnanců lázní

Osobní údaje zaměstnanců HLKS zpracovává v první řadě oddělení personální a mzdové. Začíná to přijetím uchazeče o zaměstnání. Nekončí to výstupem z pracovního poměru, nýbrž až skartací po době dané zákonem. Zpracovávají se osobní údaje jako jméno, příjmení, titul, datum narození, rodné číslo, údaj o zdravotní pojišťovně, údaje o rodině a dětech, o rodinném stavu, číslo bankovního účtu, údaje o předešlém zaměstnání, o nejvyšším dosaženém vzdělání a další. Oddělení personální a mzdové zpracovává také zvláštní kategorii osobních údajů, a to členství v odborové organizaci. Osobní údaje zaměstnanců jsou zpracovávány na základě několika zákonů. Jedná se o zákon č. 262/2006 Sb., zákoník práce a zákon č. 89/2012 Sb., nový občanský zákoník. Na základě dalších zákonů se osobní údaje zpracovávají, přijímají od třetí strany a předávají třetí straně, což jsou další samostatní správci osobních údajů. Zahrnout se zde mohou následující zákony: zákon č. 586/1992 Sb., o daních z příjmu; zákon č. 48/1997 Sb., o veřejném zdravotním pojištění; zákon č. 155/1995 Sb., o důchodovém pojištění, dále zákon č. 187/2006 Sb., o nemocenském pojištění, exekuční řád zákon č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti; nebo také např. insolvenční zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení.

Základní osobní údaje zaměstnance předává oddělení personální a mzdové dalším úsekům lázní. V první řadě se jedná o úsek a oddělení, kde zaměstnanec vykonává svou pracovní činnost. Zaměstnanec má možnost závodního stravování. V tom případě své údaje předá na úsek stravování. Pokud mu lázně poskytují přechodné ubytování, dává své údaje na oddělení evidence majetku. Důležitý úsek, který zpracovává osobní údaje zaměstnance, je úsek ekonomický. Oddělení personální a mzdové dostává od výše zmíněných oddělení osobní údaje zaměstnance zpět, například aby proběhly srážky za jídlo či ubytování, z vlastního úseku je předávána docházka či mimořádné ohodnocení. A i zaměstnanec je zachycován kamerovým systém, pokud prochází místy, kde jsou kamery umístěny.

Opět následuje schéma výskytu osobních údajů tentokrát zaměstnanců znázorněné ve zjednodušené formě na obrázku č. 10.



Obr. č. 10: Schéma výskytu osobních údajů zaměstnanců lázní. (Zdroj: vlastní)

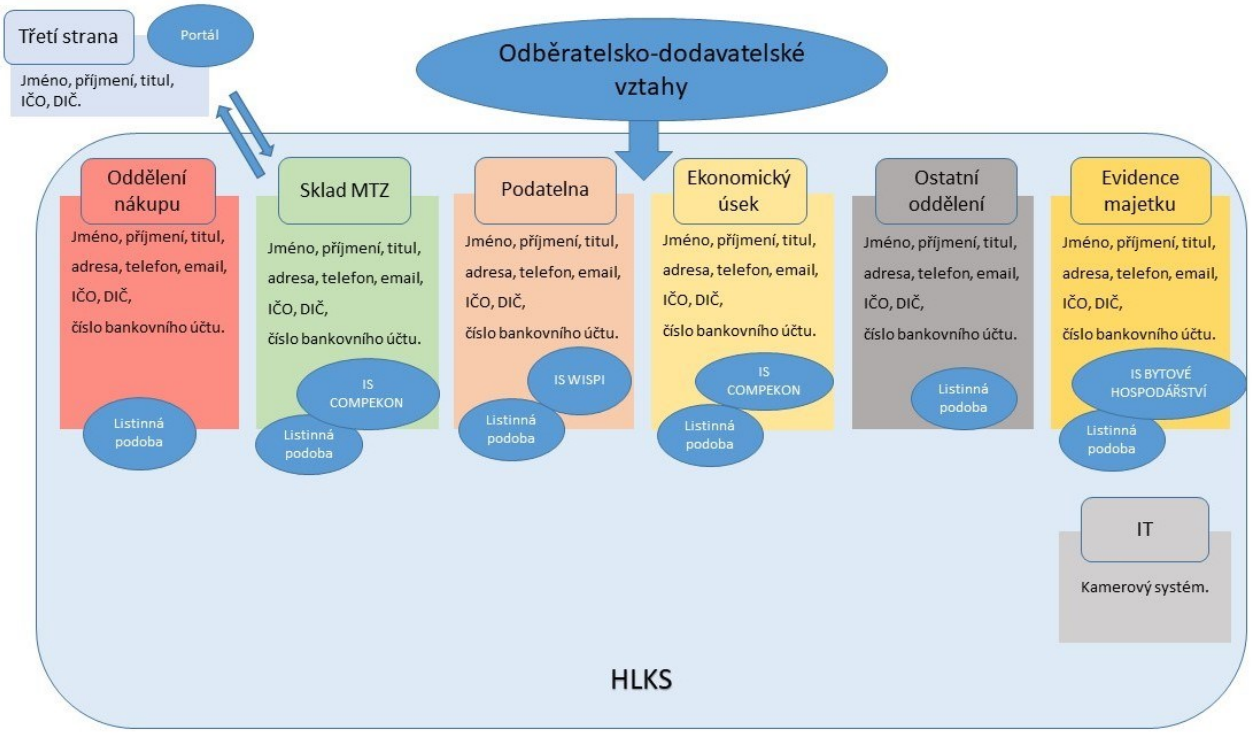
12.4 Osobní údaje v odběratelsko-dodavatelských vztazích

V první řadě údaje z odběratelsko-dodavatelských vztahů řeší oddělení nákupu. Jako státní podnik mají lázně povinnost vyhlašovat výběrová řízení a provádět veřejné zakázky dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek. Uzavřené smlouvy se musí zveřejňovat ve veřejném registru smluv, což řeší zákon č. 340/2015 Sb., o registru smluv.

Sklad MTZ nakupuje drobný materiál přes internetové nebo kamenné obchody v okolí. Veřejné zakázky i drobný nákup se dokládá daňovým dokladem nebo fakturou. Faktury se evidují na podatelně, která je následně předá na oddělení nákupu, kde se k fakturám přidávají žádanky, objednávky či smlouvy. Odtud putují na finanční účtárnu, kde se zaúčtují. Před zaplacením je ke kontrole dostane ten úsek, který zadal požadavek k nákupu. V těchto případech je možné zmínit celou řadu zákonů. Výběrem je to například zákon č. 77/1997 Sb., o státním podniku; zákon č. 563/1991 Sb., o účetnictví; zákon č. 320/2001 Sb., o finanční kontrole; zákon č. 235/2004 Sb., o dani z přidané hodnoty; zákon č. 500/2004 Sb., správní řád; zákon č. 16/1993 Sb., o dani silniční; zákon č. 338/1992 Sb., o dani z nemovitých věcí; zákon č. 89/1995 Sb., o státní statistické službě aj. Třetí stranu zde tvoří kontrolní orgány, jako např. finanční úřad.

Do této kategorie osobních údajů jsou také zahrnuty osobní údaje z oddělení evidence majetku, které se stará o bytové a nebytové prostory. Tyto bytové a nebytové prostory lázně různě pronajímají na základě smluvního vztahu. Lázně prodávají také na základě smluvního vztahu energie.

I v tomto případě lze uvést kamerový záznam, jelikož dodavatelé vozí své zboží a materiál do lázní nebo v lázních vykonávají požadovanou službu, tudíž se na kamerovém záběru mohou objevit.



Obr. č. 11: Schéma výskytu osobních údajů v odběratelsko-dodavatelských vztazích. (Zdroj: vlastní)

Na obrázku č. 11 je znázorněné schéma výskytu osobních údajů v odběratelsko-dodavatelských vztazích. V tomto případě projde všem oddělením rukama faktura, to znamená, že zpracovávají stejné osobní údaje.

13 Vlastní průzkum mezi zaměstnanci

V HLKS byla provedena implementace GDPR. Na jejím základě bylo provedeno několik opatření a změn. Důležitou otázkou ale je, jak dopady implementace nařízení vnímají samotní zaměstnanci, zda ji vůbec vnímají. Proto byl sestavený základní checklist, který byl podkladem pro krátký rozhovor s vybraným vzorkem zaměstnanců z každého oddělení a který je uveden v následující tabulce.

Tab. č. 2. Checklist pro zaměstnance lázní. (Zdroj: vlastní)

1.	Byli jste řádně seznámeni s GDPR?	ANO / NE
2.	Byli jste poučeni, jak nakládat s osobními údaji?	ANO / NE
3.	Zpracováváte osobní údaje zvláštní kategorie (citlivé údaje)?	ANO / NE
4.	Vznikly Vám po zavedení GDPR nové povinnosti?	ANO / NE
5.	Navýšila se Vám po zavedení GDPR administrativní činnost?	ANO / NE
6.	Víte, kdo v lázních vykonává funkci pověřence pro ochranu osobních údajů?	ANO / NE

Zaměstnanci lázní byli pro tento výzkum rozděleni do dvou skupin. V každé skupině bylo 15 respondentů. První skupinu tvořili manažeři úseků, vedoucí všech oddělení a zaměstnanci z kanceláří. Druhá skupina byla tvořena zaměstnanci z jednotlivých provozů, jmenovitě kuchaři a pomocným personálem, obsluhou, pokojskými a uklízečkami, zdravotním personálem (maséry, obsluhou van a inhalací, fyzioterapeuty) a zaměstnanci technického úseku.

13.1 První skupina

1. Byli jste řádně seznámeni s GDPR?

Na tuto otázku všichni dotázaní odpověděli kladně. Zkratka GDPR jim je známá, věděli, na co odpovídají. Pracovní skupina zpracovávala své úkoly právě v součinnosti se zaměstnanci z první skupiny a seznamovala je s nabytými vědomostmi ohledně nařízení.

2. Byli jste poučeni, jak nakládat s osobními údaji?

Opět všichni dotázaní odpověděli kladně. Zároveň dodávali, že už před GDPR věděli, jak nakládat se zpracovávanými osobními údaji. Poučeni byli v rámci své pracovní pozice při nástupu do pracovního poměru.

3. Zpracováváte osobní údaje zvláštní kategorie (citlivé údaje)?

Cílem této otázky bylo zjistit, zda zaměstnanci umí rozlišit mezi standardními osobními údaji a zvláštní kategorii osobních údajů. Přesto že byli řádně seznámeni s GDPR, ne vždy si byli jistí, co do které kategorie patří. Například do citlivých údajů přiřazovali rodné číslo, (hlavní účetní dávala příklad, kdy OSVČ dostávali přidělené číslo IČO podle rodného čísla, což už se nedělá). Na druhou stranu pro ně nebylo citlivým údajem členství v odborech, náboženské vyznání nebo rasový původ. Mzdová účtárna členství v odborech musí znát, aby mohla provádět srážky apod., a protože s těmito údaji pracuje, nepřijdou ji citlivé. Zdravotní stav za citlivý považují všichni dotázaní.

4. Vznikly Vám po zavedení GDPR nové povinnosti?

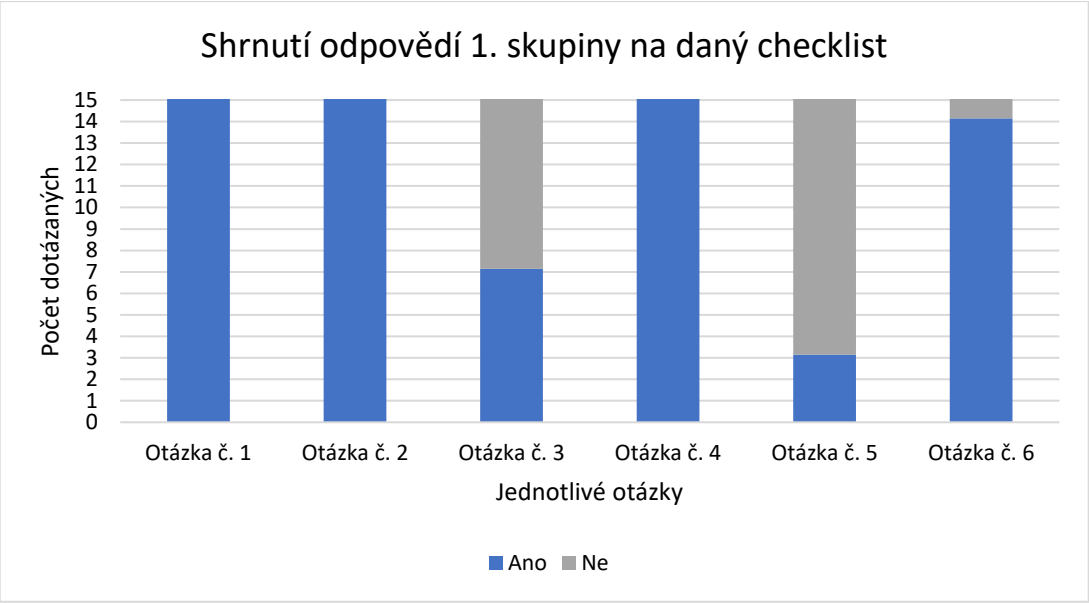
Tato otázka přinesla nejvíce diskuzí. Někteří se neuvědomovali, že by měli nějaké nové povinnosti, ale při bližším pohledu na věc si uvědomili, že nové povinnosti jim vznikly. Mají je už ale tak zažité za necelé dva roky praxe nařízení, že si je neuvědomují. Nejvíce změn bylo v oblasti informačních technologií, kde se nejhůře všem zvykalo na uzamykání svých počítačů, když od něj odcházejí. Někde se mírně změnil pracovní postup při zpracování osobních údajů, některé osobní údaje se přestaly po subjektu údajů vyžadovat. Nejvíce je tato změna vidět na oddělení personálním.

5. Navýšila se Vám po zavedení GDPR administrativní činnost?

Kladně na tuto otázku odpověděli pouze zaměstnanci klientského centra a blíže specifikovali, že se jedná o jeden list papíru (tzv. registrační kartu), který musí vytisknout navíc a předložit klientovi k podpisu. Tedy nic, co by je nějak zatěžovalo. Ostatní dotázání dlouze přemýšleli, nakonec odpověděli záporně. Na mzdové účtárně například administrativy ubylo (nepřeposílají se výplatní pásky).

6. Víte, kdo v lázních vykonává funkci pověřence pro ochranu osobních údajů?

Na poslední otázku také všichni odpověděli kladně. Jen v jednom případě ke správnému jménu pověřence byla ještě navíc přidána celá pracovní skupina.



Graf č. 1: Shrnutí odpovědí ano/ne 1. skupiny na daný checklist. (Zdroj: vlastní)

Na předchozím grafu je souhrnně znázorněno, jak respondenti 1. skupiny odpovídali na jednotlivé otázky.

13.2 Druhá skupina

1. Byli jste řádně seznámeni s GDPR?

Nikdo z dotázaných nevěděl, co znamená GDPR. Po následném vysvětlení odpovídali, že asi seznámeni byli. Jedna odpověď zněla, že byla seznámena v předchozím zaměstnání a jedna odpověď zněla striktně ne.

2. Byli jste poučeni, jak nakládat s osobními údaji?

Jen jeden dotázaný odpověděl záporně. Následně doplnil, že ho nikdo nepoučil, jak nakládat s osobními údaji, přesto to ví a chová se podle toho. Jinak všichni ostatní poučeni byli a ví, co a jak mají dělat.

3. Zpracováváte osobní údaje zvláštní kategorie (citlivé údaje)?

Pro pracovníky z provozů je to bezpředmětná otázka, protože takové osobní údaje nezpracovávají, přesto proběhla všeobecná diskuze o tom, co to osobní údaje jsou, a zda tedy vůbec nějaké zpracovávají a co s nimi dělají.

4. Vznikly Vám po zavedení GDPR nové povinnosti?

Tady opět proběhla diskuze. Z těch, kteří osobní údaje zpracovávají, jsou například pokojské, které dostávají papír se jménem klienta a dobou pobytu, tento papír vrací vedoucí ke

skartaci, dříve ho likvidovali sami. Stejně tak obsluha na jídelně informace o klientovi vrací své vedoucí, která je po ukončení pobytu klienta skartuje. Zdravotní personál do ruky dostává rozpis procedur od pacienta a ten mu také po poskytnuté proceduře vrací zpět, zde se nic nezměnilo. Technický úsek osobní údaje nezpracovává.

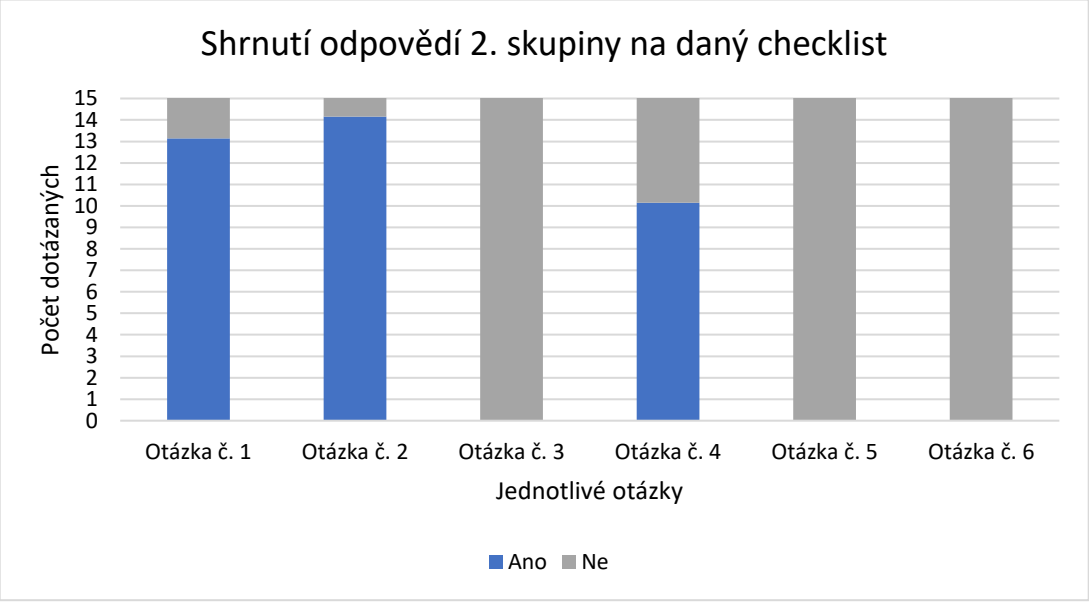
5. Navýšila se Vám po zavedení GDPR administrativní činnost?

Tato otázka přinesla záporné odpovědi. Zaměstnanci z provozů moc administrativní činnosti nevykonávají.

6. Víte, kdo v lázních vykonává funkci pověřence pro ochranu osobních údajů?

Stejně jako u první otázky, kdy muselo nejdříve dojít k vysvětlení, co GDPR vlastně znamená, i tady bylo potřeba nejdřív vysvětlit, kdo je to pověřenec pro ochranu osobních údajů a jaký je jeho úkol ve firmě. Ani jeden z dotázaných správnou odpověď neznal, všichni odpověděli tedy záporně. Následně jméno pověřence znát chtěli.

Na následujícím grafu je opět vidět souhrnné shrnutí odpovědí, tentokrát 2. skupiny respondentů.



Graf č. 2: Shrnutí odpovědí ano/ne 2. skupiny na daný checklist. (Zdroj: vlastní)

13.3 Vyhodnocení

Z výsledku rozhovorů s vybraným vzorkem zaměstnanců vyplynulo, že je potřeba, aby lázně na informovanosti ohledně GDPR zapracovaly. Zaměstnanci, kteří pracují v kancelářích, jsou informováni poměrně dobře. Na druhou stranu získané vědomosti pomalu ztrácejí, protože neprobíhají žádná další školení. O poznání hůř jsou na tom zaměstnanci z provozů. Do

implementace zapojeni nebyli, tudíž nezískali žádné kompletní informace o GDPR. Pouze byli seznámeni s novými povinnostmi, které si neuměli přiřadit k danému novému nařízení.

Je nezbytné podotknout, že nejdůležitější a nejrizikovější jsou pro lázně osobní údaje pacientů, které nejvíce zpracovává oddělení klientského centra. Pacienti zde začínají i končí. To je důvod, proč by toto oddělení mělo mít nejlepší vědomosti o GDPR. Z provedeného výzkumu vyplývá, že tomu tak skutečně je a toto oddělení je z celých lázní nejerudovanější v oblasti ochrany osobních údajů.

13.4 Návrhy na zlepšení

Z provedené analýzy vyplývá, že v lázních byla provedena implementace nařízení řádně, v řádném termínu. Je to dáno tím, že ochrana osobních údajů pro zaměstnance lázní nebyla ničím novým ani převratným. Přeci jenom jsou lázně zdravotnické zařízení, kde ochrana osobních údajů byla vždy důležitá. Druhým důvodem byla samozřejmě existence předešlého českého zákona č. 101/2000 Sb., o ochraně osobních údajů, který se musel dodržovat. Vlastní vnitřní předpis měly lázně vytvořený i před GDPR, pouze tento předpis nebyl tak obsáhlý, jak vyžaduje současné nařízení. Lázně také komunikovaly s Úřadem pro ochranu osobních údajů, například když zaváděly do provozu kamerový systém. Přesto byla jmenovaná pracovní skupina, která musela dát vše do souladu. Bylo provedeno několik opatření, aby byl soulad zajištěn, jak organizačních, tak technických, každopádně nejvíce opatření a změn proběhlo na úseku informačních technologií. Byl ustanoven pověřenec pro ochranu osobních údajů, zveřejnily se informace pro klienty na webových stránkách lázní.

Ochrana osobních údajů je v lázních prováděna dle nařízení. Přesto je stále v této oblasti na čem pracovat. Každá organizace, tudíž i tato, je živý organismus, ve kterém se mohou měnit zaměstnanci nebo třeba zavedený software, vytvářejí se nová pravidla, stará se ruší aj. a proto je potřeba neustále přemýšlet nad tím, zda není možné dělat něco lépe. K tomu mohou dopomoct následující návrhy.

13.4.1 Školení

Jednoznačně je potřeba proškolit zaměstnance v oblasti GDPR. Tato oblast se podcenila. Vhodným doporučením je školení provádět po úsecích, protože každý úsek, respektive oddělení má jiné potřeby a musí se zaměřit na jiné zpracování. Každý zpracovává jiné osobní údaje, používá k tomu jiný software. Důležité je také školení opakovat každoročně. Z průzkumu vyplývá, že opakování je žádoucí. V tomto případě není možné zvolit samostudium bez zpětné vazby.

13.4.2 Vnitropodniková dokumentace

Jednotlivé směrnice daných úseků obsahují informace i o ochraně osobních údajů, je v nich popsáno, jak s nimi při konkrétní činnosti nakládat, jak je zpracovávat. Nicméně je určitě vhodné a praktické mít samostatnou směrnici k této problematice, kde lze najít ucelený přehled toho kdo, kde a jak osobní údaje zpracovává a kde je vysvětleno, proč se tak děje.

13.4.3 Fyzická bezpečnost

Budovy lázní jsou zajištěny bezpečnostním systémem, kanceláře mají uzamykatelné dveře. Potřeba je pouze ještě v některých kancelářích vyměnit otevřené regály či volně přístupné skříně za uzamykatelný nábytek, tak aby přístup k daným osobním údajům měla pouze pověřená osoba.

Dále je potřeba zaměstnance upozornit, že k fyzické bezpečnosti patří také čistý pracovní stůl. To znamená, že při odchodu z kanceláře by neměly zůstávat dokumenty s osobními údaji na pracovním stole, zejména ne po skončení pracovní doby.

13.4.4 Personál

Nesmí se zapomínat na prevenci úniku dat, který může způsobit lidský faktor, tedy zaměstnanec osobně. Je žádoucí popřemýšlet o určité motivaci zaměstnanců, aby se zvýšila loajalita k firmě. Také je nezbytné, aby firma disponovala pouze lidskými zdroji s příslušnou kvalifikací. Určitě je možné dělat namátkové kontroly a v neposlední řadě je důležité zařadit kontrolu GDPR do činnosti interního auditora.

Závěr

V dubnu 2016 došlo k přijetí Obecného nařízení, které v současné době musí akceptovat všichni ti, kteří chtějí zpracovávat osobní údaje občanů Evropské unie. Předložená bakalářská práce představila tuto základní problematiku GPDR a ve zjednodušené formě ukázala, jak lze nařízení implementovat do organizace, aby bylo v souladu s touto právní legislativou. Samotná implementace není jednoduchá, a proto je nezbytné zmapovat všechny procesy, které v organizaci probíhají. Zavedení do praxe ale už není nic mimořádného. Je důležité si uvědomit, že ochrana osobních údajů bude s narůstající technikou více a více vyžadována, proto je důležité se tímto tématem zabývat.

Hlavním cílem této bakalářské práce bylo zjistit, jaké jsou dopady GDPR po jeho zavedení do praxe pro vybraného zaměstnavatele. Mezi dílčí cíle této práce patřilo vymezení základních pojmů a vysvětlení problematiky legislativy GDPR, dále mezi dílčí cíle patřila deskripce vybrané společnosti a v neposlední řadě také komplexní analýza vybrané společnosti s důrazem na implementaci GDPR. Zjištěné výsledky umožnily vyhodnotit danou situaci a navrhnout další řešení.

V teoretické části byla popsána historie ochrany osobních údajů, byly definovány základní pojmy jako osobní údaj, zvláštní kategorie osobních údajů, subjekt údajů, správce, zpracovatel, zpracování, profilování a pseudonymizace, dále došlo k seznámení se zásadami a právními důvody pro zpracování osobních údajů, došlo k vymezení práv subjektu údajů, bylo vysvětleno, kdo je pověřenec pro ochranu osobních údajů a jaká je jeho funkce ve firmě, dále jaké jsou možné sankce a pokuty při nedodržení plnění právních povinností, a nakonec byl představen doplňující český zákon k nařízení, a to zákon č. 110/2019 Sb., o zpracování osobních údajů.

V praktické části byla představena konkrétní firma, její organizační struktura, jednotlivé úseky a oddělení. Následně byla popsána implementace nařízení v dané společnosti. Důležitou část práce tvořil vlastní průzkum, kdy byl analyzován tok osobních údajů v podniku i mimo podnik a proběhly také krátké rozhovory s vybraným vzorkem zaměstnanců za pomoci vytvořeného checklistu.

Výstupem této bakalářské práce bylo shrnutí a vyhodnocení implementace nařízení v daném podniku. Byl také představen možný návrh dalšího řešení.

Použitá literatura a zdroje

GDPR.CZ. *DPO čili Pověřenec pro ochranu osobních údajů.* [online]. [cit. 2020-03-20]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/.

CHLEBUS Tomáš a Jakub DOSTÁL. Nový zákon o zpracování osobních údajů. *Epravo.cz.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html.

ITBIZ.CZ. *Pokuty za porušení GDPR přesáhly v Česku 7 milionů korun, kontroly odhalily neznalost balančního testu* [online]. [cit. 2020-0**3**-23]. Dostupné z: http://www.itbiz.cz/clanky/pokuty-za-poruseni-gdpr-presahly-v-cesku-7-milionu-korun-kontroly-odhalily-neznalost-balancniho-testu/.

Ministerstvo průmyslu a obchodu. *GDPR.* [online]. [cit. 2018-12-04]. Dostupné z: https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/Podpurna-opatreni-mpo/2018/10/GDPR-V-KOSTCE-GDPR-je-prilezitost.pdf.

Ministerstvo průmyslu a obchodu. *GDPR.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.mpo.cz/cz/podnikani/ochrana-osobnich-udaju-gdpr/adaptacni-zakony-k-gdpr-byly-schvaleny-a-nabyly-ucinnosti---245652/.

NAVRÁTIL, Jiří a kolektiv. *GDPR pro praxi.* 1. vyd. Plzeň: Aleš Čeněk. 2018, s. 339. ISBN 978-80-7380-689-7.

NEZMAR, Luděk. *GDPR: Praktický průvodce implementací.* 1. vyd. Praha: Grada Publishing. 2017, s. 304. ISBN 978-80-271-0668-4.

NULÍČEK, Michal, Josef DONÁT, František NONNEMANN, Bohuslav LICHNOVSKÝ, Jan TOMÍŠEK a Kristýna KOVAŘÍKOVÁ. *GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář.* 2. aktual. vyd. Praha: Wolters Kluwer ČR, 2018, s. 580. ISBN 978-80-7598-068-7.

OTEVŘEL, Richard a Vojtěch BARTOŠ. Havelpartners.blog. *Kalifornie přijala zásadní zákon na ochranu osobních údajů CCPA.* [online]. [cit. 2020-02-28]. Dostupné z: https://www.havelpartners.blog/blog/kalifornie-prijala-zasadni-zakon-na-ochranu-osobnich-udaju-ccpa/104#.

Portál HLKS – FOTOGALERIE. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://www.horskelazne.cz.

Portál HLKS – INDIKACE. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://www.horskelazne.cz/indikace.

Portál HLKS. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://www.horskelazne.cz/organizacni-schema.

Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/4.htm.

Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/9.htm.

Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/37.htm.

Privacy Regulation. *EU Obecné nařízení o ochraně osobních údajů.* [online]. [cit. 2020-02-23]. Dostupné z: https://www.privacy-regulation.eu/cs/83.htm.

ÚOOÚ. *Poskytnutí informací k dozorové činnosti.* [online]. [cit. 2020-03-23]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5842&n=poskytnuti%2Dinformaci%2Dk%2Ddozorove%2Dcinnosti.

ÚZIS. *Metodika implementace GDPR ve zdravotnictví*. [online]. [cit. 2020-03-23]. Dostupné z: https://www.uzis.cz/index.php?pg=o-nas--ochrana-osobnich-udaju--gdpr-ve-zdravotnictvi.

Veřejný rejstřík a sbírka listin. *Horské lázně Karlova Studánka* [online]. [cit. 2020-03-04]. Dostupné z: https://or.justice.cz/ias/ui/vypis-sl-firma?subjektId=214034.

ŽŮREK, Jiří. *Praktický průvodce GDPR.* 1. vyd. 2. dotisk. Olomouc: Anag. 2017, s. 224. ISBN 978-80-7554-097-3.

Seznam zkratek

BOZP a PO	Bezpečnost a ochrana zdraví při práci
ČR	Česká republika
DPIA	Posouzení vlivu na ochranu osobních údajů
DPO	Pověřenec po ochranu osobních údajů
EU	Evropská Unie
EUR	Měna euro
GDPR	Obecné nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/45/ES
HLKS	Horské lázně Karlova Studánka, státní podnik
IČO	Identifikační číslo osoby
IT	Informační technologie
OSVČ	Osoba samostatně výdělečně činná
Sklad MTZ	Sklad materiálového a technického zásobování
ÚOOÚ	Úřad pro ochranu osobních údajů

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam příloh

Číselníky z Katalogu osobních údajů a procesů zpracování

Katalog procesu zpracování – vzor

Popis procesu zpracování

Analýza souladu – zpracovatelé

Informační dokument – zdravotní péče

ČÍSELNÍKY

KATEGORIE OSOBNÍCH ÚDAJŮ

ČÍSLO	ÚDAJ	POZNÁMKA, KOMENTÁŘ
1	jméno	
2	příjmení	
3	titul	
4	datum narození	
5	rodné číslo	
6	IČO	
7	DIČ	
8	e-mailová adresa	
9	adresa - trvalý pobyt/bydliště	
10	adresa - sídlo/místo podnikání	
11	podpis	Vlastnoruční nebo elektronický.
12	ID datové schránky	
13	telefonní číslo	
14	registrační značka vozidla	
15	podobizna nebo fotografie	Potřeba zohlednit míru, ve které fotografie identifikuje subjekt údajů a ve které může zasahovat do jeho soukromí.
16	uživatelské jméno	
17	číslo bankovního účtu	
18	IP adresa	Síťový identifikátor. Statická i dynamická IP.
19	číslo ŘP	
20	číslo OP	
21	číslo cestovního dokladu	
22	údaj o odsouzení za trestný čin	Citlivý údaj ve smyslu ZOOÚ (§ 4 písm. b). Není zvláštním OÚ dle GDPR.
23	údaje o zdravotním stavu.	Zvláštní OÚ (čl. 9 GDPR) - stav pacienta při přijetí, anamnéza, indikace, diagnóza, medikace. Kategorie č. 23 je zpracovávána především při procesech souvisejících s poskytováním zdravotní péče.
24	údaj o zdravotní pojišťovně	
25	místo narození	
26	rodinný stav	
27	informace o důchodu	
28	informace o invaliditě	Zvláštní OÚ (čl. 9 GDPR) - konkrétněji vypovídá o zdravotním stavu subjektu údajů (než č. 41). Kategorie č. 28 je zpracovávána především při při procesech souvisejících s pracovněprávní problematikou.
29	údaje o exekuci	
30	údaje o insolvenčním řízení	
31	nejvyšší dosažené vzdělání	
32	údaje o předchozím zaměstnání	
33	pracovní pozice, funkce nebo členství v orgánu	
34	členství v odborové organizaci	Zvláštní OÚ (čl. 9 GDPR). Kategorie je zpracována při procesu zpracování mezd.
35	osobní číslo zaměstnance	
36	státní příslušnost, občanství	
37	informace o rodinných příslušnících	
38	datum úmrtí	GDPR se nezvtahuje na zpracování údajů zesnulých osob. Údaj je zpracováván v souvislosti s poskytováním rekreačních a léčebných pobytů.
39	údaj o mzdě	
40	spisová značka, číslo jednací - soudní nebo správní řízení	
41	zdravotní způsobilost uchazeče o zaměstnání nebo zaměstnance	Není zvláštní kategorií OÚ dle čl. 9 GDPR, proto byla vyčleněna z kategorie č. 23. Sama informace o zdravotní způsobilosti (41) není konkrétní informací o zdravotním stavu. Jde pouze o závěr vyhodnocení zdravotní způsobilosti k práci.
42	IMEI SIM karty	
43	MAC adresa	Síťový identifikátor.
44	číslo pacienta	číselné označení pacienta - IS DENEB

KATEGORIE OPERACÍ ZPRACOVÁNÍ

ČÍSLO	OPERACE	POZNÁMKA/KOMENTÁŘ
1	shromáždění, získání	
2	zaznamenání	
3	uspořádání	vč. zkompletování
4	strukturování	vč. třídění, kategorizace
5	uložení	

6	zálohování	
7	přizpůsobení, pozměnění, aktualizace	
8	vyhledání	
9	nahlédnutí	
10	použití	
11	přenos, odeslání	e-mail, pošta, přenosná média, apod.
12	šíření	zveřejnění, webové stránky, apod.
13	skenování, kopírování, tisk	
14	seřazení	
15	zkombinování	
16	omezení	
17	výmaz, zničení, skartace	
18	předání k archivaci	oblastní archiv

PRÁVNÍ DŮVODY ZPRACOVÁNÍ				
ZKRATKA	ČLÁNEK GDPR	PRÁVNÍ DŮVOD	PRACOVNÍ ZKRATKA	KOMENTÁŘ
A	čl. 6 odst. 1 písm. a)	Subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů.	souhlas	Souhlas je jedním z právních důvodů zpracování a měl by být brán jako základ zpracování pouze tehdy, není-li naplněn jiný právní důvod zpracování.
B	čl. 6 odst. 1 písm. b)	Zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů.	plnění smlouvy	
C	čl. 6 odst. 1 písm. c)	Zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje.	právní povinnost	Povinnost stanovená právním přespisem ČR a EU.
D	čl. 6 odst. 1 písm. d)	Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.	životně důležité zájmy	
E	čl. 6 odst. 1 písm. e)	Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.	úkol ve veřejném zájmu nebo výkon veřejné moci	Pro HLKS není relevantní - nepoužije se.
F	čl. 6 odst. 1 písm. f)	Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.	oprávněné zájmy	Jen pokud mají přednost před zájmy nebo základními právy a svobodami subjektů, které vyžadují ochranu osobních údajů; zvlášť když je subjektem údajů dítě!

TYPY SUBJEKTŮ ÚDAJŮ			
ZKRATKA	TYP SUBJEKTU ÚDAJŮ		POZNÁMKA/KOMENTÁŘ
Z	zaměstnanec nebo člen orgánu podniku		Zahrnuje i studenty na praxi.
S	smluvní strana		Smluvní strana jiná než zaměstnanec a pacient (dodavatel, odběratel/klient, jiná smluvní strana).
P	pacient		Komplexní, příspěvková péče. Ambulantní péče.
T	třetí osoba		Úřední osoba, kontrolor, jiná třetí osoba.

PROCES ZPRACOVÁNÍ (SKUPINA ČINNOSTÍ)	NOSIČ	ÚČEL ZPRACOVÁNÍ	PRÁVNÍ DŮVOD	KATEGORIE OÚ STANDARTNÍ	KATEGORIE OÚ ZVLÁŠTNÍ	OPERACE ZPRACOVÁNÍ	ZDOKUMENTOVÁNÍ PROCESU	POZNÁMKA, KOMENTÁŘ	TYP SUBJEKTU
Administrace veřejných zakázek (objednávky, smlouvy)	výzva k podání nabídky ve veřejné zakázce	administrace veřejné zakázky, evidence	C	1,2,3,8,10,13,33		1,2,3,5,8,9,10,11,12, 13,17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	Z,S
	zadávací dokumentace veřejné zakázky	administrace veřejné zakázky, evidence	C	1,2,3,8,10,13,33		1,2,3,5,8,9,10,11,12, 13,17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	Z
	seznam dodavatelů k oslovení/ známých	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,13,33		1,2,3,5,8,9,10,11,13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	T,S
	Nabídka uchazeče, vč. návrhu smlouvy	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11,13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	T,S
	seznam podaných nabídek	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11,12, 13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	T,S
	protokol o otevírání, hodnocení a posouzení nabídek	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11,12, 13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	T,S,Z
	rozhodnutí o výběru nejvhodnější nabídky	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11,12, 13,17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	T,S,Z
	oznámení o výběru nejvhodnější nabídky	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11,12, 13,17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	T,S,Z
	prohlášení o neexistenci střetu zájmů členů komise	administrace veřejné zakázky, evidence	C	1,2,3,11,33		1,2,3,5,8,9,10,11,13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	Z
	smlouva	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11,12, 13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	S,Z
	objednávka	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11,12, 13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	S,Z
	Tendermarket	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11,12, 13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	T,S,Z
	Tenderaréna	administrace veřejné zakázky, evidence	C	1,2,3,6,7,8,10,11,13,17,3 3		1,2,3,5,8,9,10,11, 12, 13, 17	OS4_Pravidla nákupu	zákon č. 134/2016 Sb., o zadávání veřejných zakázek. V přípravě nová směrnice.	T,S,Z

POPIS PROCESŮ ZPRACOVÁNÍ

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

Zákon č. 101/2000 Sb., o ochraně osobních údajů (ZOOÚ)

Správce:	Horské lázně Karlova Studánka, státní podnik
Odpovědný úsek - útvar:	Zvolte položku.

- Prosím každého z členů pracovní skupiny, abyste za Vám svěřený útvar podniku ve spolupráci s Vašimi kolegy vyplnili níže uvedené údaje pro každý z procesů zpracování dle katalogu (verze 4.9. dostupné ve složce GDPR uložené na Public)
- Prosím zkopírujte níže uvedenou tabulku tolikrát, aby v dokumentu byla 1 pro každý z procesů.
- Číslujte procesy dle pořadí v katalogu. Uveďte název procesu dle katalogu.
- Vyplňujte tabulku dle otázek a instrukcí v jednotlivých bodech.
- V případě pochybností uveďte doplňující informace, ze kterých vycházíte.
- Po vyplnění odstraňte červený text

1.	**NÁZEV PROCESU**
Popis a náležitosti procesu	
a) Stručný obsah procesu: [Nevynechejte ani i to, co osobně považujete za samozřejmé. Formulujte to tak, aby to pochopil běžný člověk, který, nezná Vaši práci a který nepracuje v našem podniku.]	Nyní nedoplňujte.
b) Kategorie subjektů údajů: [Viz katalog: Pacient, zaměstnanec, smluvní strana, třetí osoba. Rozčleňte na klíčové a doplňkové. Např. ve zdravotnické dokumentaci jsou klíčové údaje údaj o lékaři a jeho podpisu má doplňkový nebo provozní význam. Pokud jde jen o provozní charakter dokumentace (např. evidence majetku, seznam, podpisový arch), pak vyplňte do skupiny doplňové zaměstnance)]	Klíčové: ▪ Pacient Doplňkové: ▪ zaměstnanec (podpis lékaře, ředitele)
c) Typ agendy zpracování: [manuální, automatizovaná, kombinace; Zpracování může být manuální-ruční (např. přepis údajů z papíru do el. evidence/databáze) nebo automatické (zpracování například provádí informační systém bez potřeby lidského zásahu). Je možné, že jde o kombinaci obou způsobů; pak prosím, abyste uvedli, že je jde o kombinaci manuálního a automatického zpracování a které převažuje (z hlediska množství úkonů – operací zpracování).]	▪ Manuální agenda zpracování ▪ Automatizovaná agenda zpracování ▪ Kombinace manuálního a automatizovaného zpracování – převažuje manuální/automatizované *Dále uveďte cokoliv, co považujete za potřebné zmínit.*
d) Účel zpracování: [Zde prosím vepište účely z katalogu – prosím každý na zvláštní řádek. Na prvním místě uveďte obecný-společný účel, který shrnuje podstatu daného procesu zpracování jako celku. Pak vypište případné další účely, tak jak jsou uvedeny u jednotlivých nosičů/zdrojů.]	Hlavní (společný) účel: Příklad na procesu Poskytování lázeňské péče ▪ Poskytování lázeňské léčebně rehabilitační péče Další účely: ▪ Vyúčtování lázeňské péče ▪ Evidence zdravotnické dokumentace
e) Právní důvody [Zde vepište právní důvody zpracování z katalogu – prosím každý na zvláštní řádek]	▪ Souhlas (A) ▪ Smlouva (B) ▪ Právní povinnost (C) ▪ Životně důležitý zájem (D) ▪ Oprávněný zájem (F)
f) Oprávněný zájem (F)	Vyplňte, jen pokud je právním základem zpracování oprávněný zájem (F).

[Pokud je právním základem zpracování oprávněný zájem podniku (F), pokuste se slovně vyjádřit, v čem spočívá a čím převyšuje zájem na ochraně soukromí fyzické osoby.]			
g) Právní povinnost (C) [Pokud je právním základem zpracování právní povinnost (F), uveďte konkrétní právní předpis – viz katalog.]	Vyplňte, jen pokud je právním základem zpracování právní povinnost (C).		
h) Místa uložení osobních údajů [uveďte, kde jsou uloženy osobní údaje v elektronické a listinné/fyzické podobě – vyberte z nabídky, případně prosím upřesněte]	El. dokumenty: ▪ PC – počítač zaměstnance (dokumenty uložené na místním úložišti v PC) ▪ e-mailový klient – MS Outlook (+archiv + zálohy na serveru) ▪ el. spisová služba (WISPI) ▪ server HLKS – sdílené uložiště (R,S,W,T...) ▪ server HLKS – osobní uložiště zaměstnance (H) ▪ IS [*uveďte název IS dle katalogu*] – databáze IS na serveru HLKS ▪ IS [*uveďte název IS dle katalogu*]– databáze IS uložená mimo server HLKS ▪ přenosná média (externí disk, USB flash disk, DVD..) ▪ Jiné umístění elektronického dokumentu – upřesněte: Listinné/fyzické dokumenty (originály i kopie): ▪ jiné fyzické umístění – upřesněte: ▪ příruční spisovna ▪ centrální spisovna *Dále uveďte cokoliv, co považujete za potřebné zmínit.*		
i) Zdroj údajů:	Křížkem zvolte platnou možnost: ☐ údaje získané od subjektu údajů. ☐ údaje získané z jiného zdroje: upřesněte V případě, že některé údaje jsou získávány od subjektu údajů a některé ne, upřesněte.		
j) Oprávnění zaměstnanců zpracovávat osobní údaje [uveďte, kdo je oprávněn v rámci procesu zpracovávat osobní údaje, třeba jen na ně nahlížet. Tzn. pracovat s dokumentací a přistupovat k IS...]	Nosiče a zdroje osobních údajů mimo IS: ▪ Pracovní pozice ▪ Pracovní pozice IS [*uveďte název IS dle katalogu*]: ▪ Pracovní pozice ▪ Pracovní pozice Přístupová práva uživatelů (zaměstnanců) do IS (výše) – křížkem zvolte platnou možnost: ☐ jsou jasně definována: ve směrnici XY ☐ nejsou definována *Dále uveďte cokoliv, co považujete za potřebné zmínit.*		
k) Doba uchování (Lhůty pro výmaz) [Uveďte konkrétní doby zpracování osobních údajů; rozčleňte, pokud jsou doby uchování různé, podle okolností. Pozn. osobní údaje lze uchovávat jen po dobu, která je nezbytná pro plnění daného účelu zpracování. Pokud je právním základem zpracování právní povinnost, pak tato doba vyplývá z konkrétního právního předpisu. U zpracování na základě oprávněného zájmu, plnění smlouvy nebo souhlasu může být nápomocný spisový řád - srov. skartační lhůty].			
l) Zpracovatelé: [viz úkol: Analýza souladu – zpracovatelé. Jen zrekapitulujte, vymezte, v čem spočívá zpracování a kategorii subjektu údajů. Pokud v daném procesu nevystupuje zpracovatel, pak	Název/Jméno, příjmení	Předmět zpracování (případně i název IS, pokud jde o dodavatele IS)	Kategorie subjektu údajů

<table>
<tr><td rowspan="3">uveďte, že není žádný zpracovatel. Zpracovatele uveďte vždy, i když]

[Řádek v tabulce lze přidat přidáním pod předposlední řádek.]</td><td>A</td><td>A</td><td>A</td></tr>
<tr><td>B</td><td>B</td><td>B</td></tr>
<tr><td>C</td><td>C</td><td>C</td></tr>
<tr><td>m) Kategorie příjemců:
[Komu jsou osobní údaje podnikem předávány? Pokud ano, uveďte příjemce. Uvedeny jsou některé příklady.]</td><td colspan="3">V ČR:

▪ Praktický lékař pacienta
▪ Revizní lékař
▪ Zdravotní pojišťovna
▪ Ministerstvo zdravotnictví
▪ Krajský úřad
▪ Obecní úřad
▪ Celní správa
▪ Cizinecká policie
▪ Finanční úřad
▪ Okresní správa sociálního zabezpečení
▪ …
▪ …
Mimo ČR:
▪ Žádný příjemce</td></tr>
<tr><td>Datum</td><td colspan="3"></td></tr>
<tr><td>Zpracoval(i):</td><td colspan="3"></td></tr>
</table>

ANALÝZA SOULADU
Zpracovatelé

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

Zákon č. 101/2000 Sb., o ochraně osobních údajů (ZOOÚ)

Správce:		Horské lázně Karlova Studánka, státní podnik
Úsek:		Zvolte položku.
Zákonný požadavek:		Použití pouze takových zpracovatelů, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky GDPR a aby byla zajištěna ochrana práv subjektu údajů.
GDPR	Čl. 4 odst. 8	Zpracovatelem se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
	čl. 28 odst. 1	Pokud má být zpracování provedeno pro správce, využije správce pouze ty zpracovatele, kteří poskytují **dostatečné záruky** zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.
	Čl. 28 odst. 3	Zpracování zpracovatelem se řídí **smlouvou** nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt **zejména stanoví**, že zpracovatel: a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu; b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti; c) přijme všechna opatření požadovaná podle článku 32; d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4; e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III; f) je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici; g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů; h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje. Pokud jde o první pododstavec písm. h), informuje zpracovatel neprodleně správce v případě, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy Unie nebo členského státu týkající se ochrany údajů.
	Čl. 28 odst. 9	Smlouva nebo jiný právní akt podle odstavců 3 a 4 musí být vyhotoveny písemně, v to počítaje i elektronickou formu.

ZOOÚ	§ 4 písm. k)	Zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.
	§ 6	Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.
Vymezení úkolu:		1) Zhodnocení, zda zpracovatel vyhovuje výše uvedeným zákonným požadavkům, tj. zda zpracovatel poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření, zda se zpracování řídí smlouvou a zda smlouva obsahuje stanovené náležitosti („*zhodnocení*“). 2) Popis případného zjištěného nedostatku („*nedostatek*“). 3) Návrh opatření v případě nedostatku („*návrh opatření*“).

NÁZEV PROCESU	ZPRACOVATEL	PŘEDMĚT PLNĚNÍ	1) ZHODNOCENÍ	2) NEDOSTATEK	3) NÁVRH OPATŘENÍ
(Název procesu dle katalogu – dříve skupina činností)	*(Název procesu dle katalogu – dříve skupina činností)*	*Uvést obecně plnění, při jehož poskytování zpracovatel zpracovává OÚ pro HLKS*	Zvolte položku.	*(Uvést, co konkrétně je v rozporu se zákonným požadavkem)*	*(Uvést, jak napravit nedostatek)*
Účetnictví	COMPEKON s.r.o.	Užívání informačního systém COMPEKON	VYHOVUJE		*Uzavřít smlouvu o zpracování*
			Zvolte položku.		
			Zvolte položku.		

Datum:

Zpracoval(i):

KARLOVA STUDÁNKA
Horské lázně

INFORMACE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ
Zdravotní péče

Vážení klienti,

z platné právní úpravy na ochranu osobních údajů pro nás vyplývá řada povinností týkajících se ochrany Vašich osobních údajů. Věřte, že na jejich plnění klademe maximální důraz a přinášíme Vám následující informace týkající se zpracování Vašich osobních údajů.

Horské lázně Karlova Studánka, státní podnik, IČO: 14450216, se sídlem č. p. 6, Karlova Studánka, PSČ: 793 24 (dále také jen „*lázně*" nebo „*my*") zpracovávají Vaše osobní údaje a mají postavení správce Vašich osobních údajů.

1. Jaké Vaše údaje zpracováváme?

Pokud jste **pacientem (klientem) lázní**, který má předepsánu **komplexní nebo příspěvkovou lázeňskou léčbu**, zpracováváme tyto Vaše osobní údaje obsažené v návrhu na lázeňskou péči, který nám zaslala Vaše zdravotní pojišťovna nebo údaje, které získáme od Vás po příjezdu nebo při telefonickém či písemném předjednání Vámi požadovaných služeb:

- kontaktní a identifikační osobní údaje:
  - jméno, příjmení, titul, datum narození a rodné číslo, adresa, telefonní číslo,
- údaje o Vaší zdravotní pojišťovně, rodinný stav,
- informace o důchodu, údaje o předchozím zaměstnání a o druhu práce,
- informace o kontaktech na rodinné příslušníky (pro případnou nutnost předání informací),
- identifikační číslo pacienta v interním informačním systému,
- údaje o Vašem zdravotním stavu:
  - stav při přijetí, anamnéza, diagnóza, medikace, stupeň mobility.

Pokud jste **pacientem (klientem) lázní**, který má **předepsánu ambulantní rehabilitační léčbu**, zpracováváme tyto Vaše osobní údaje obsažené v žádance na rehabilitační (fyzioterapeutickou nebo ergoterapeutickou) péči nebo údaje, o jejichž sdělení Vás požádáme před poskytnutím výkonu:

- kontaktní a identifikační osobní údaje:
  - jméno, příjmení, titul, datum narození a rodné číslo, adresa, telefonní číslo,
- údaje o Vaší zdravotní pojišťovně, rodinný stav,
- informace o důchodu, údaje o předchozím zaměstnání a o druhu práce,
- informace o rodinných příslušnících (pro případnou nutnost předání
- informací),
- údaje o Vašem zdravotním stavu:
  - stav pacienta při přijetí, anamnéza, diagnóza, medikace, stupeň mobility.

Bez získání a zpracování výše uvedených údajů nelze poskytnout zdravotní péči.

2. Na základě čeho, za jakým účelem a jak dlouho Vaše osobní údaje zpracováváme?

Vaše údaje požadujeme a využíváme především proto, abychom mohli:
- zpracovat požadavek na lázeňskou péči (tedy rozhodnout o přijetí k lázeňské léčbě nebo o odmítnutí z kapacitních důvodů),
- komunikovat s Vámi ohledně Vašich požadavků na poskytnutí služeb a Vašich specifických požadavků,
- ověřit si Vaši totožnost při příjezdu a zaevidovat si Vás v interním ubytovacím systému a interním zdravotním systému,
- poskytnout Vám zdravotní péči a případné související služby jako je ubytování a stravování,
- vyúčtovat zdravotní péči Vaší zdravotní pojišťovně nebo vyúčtovat Vám případné doplatky za nadstandardní služby a poplatky za další sjednaná plnění,
- evidovat stav úhrady zdravotní péče,
- evidovat doklady o poskytnuté péči pro účely kontroly poskytnutí služeb ze strany zdravotní pojišťovny,
- archivovat zdravotní dokumentaci.

Právním základem zpracování Vašich osobních údajů k výše uvedeným účelům je nezbytnost pro plnění smluvního vztahu o poskytování zdravotní péče a dále plnění právních povinností, které se na nás vztahují (především zákon č. zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění).

Údaje pro tyto účely uchováváme po dobu léčby a Vašeho pobytu v lázních a dále po dobu nezbytně nutnou, nejdéle po dobu 10 let od ukončení léčby a po dobu, po kterou je zdravotní pojišťovna na základě obecně závazných právních předpisů oprávněna provést kontrolu poskytnutých hrazených služeb a jejich vyúčtování. Obdobně v případě příspěvkové péče, či v případě péče hrazené samoplátcem zpracováváme osobní údaje po dobu, v níž je samoplátce oprávněn zpochybnit poskytnutí péče.

Účetní a daňové doklady, kterými poskytnutou péči vyúčtováváme, obsahují též některé osobní údaje (jméno a příjmení klienta, rodné číslo, údaj o zdravotní pojišťovně, datum vystavení dokladu, typ poskytnuté služby). Tyto doklady uchováváme pouze pro účely splnění povinností stanovených relevantními účetními a daňovými právními předpisy. Údaje pro tyto účely uchováváme po dobu stanovenou účetními a daňovými předpisy.

Ve výjimečných případech, vznikne-li mezi námi spor týkající se našich vzájemných závazků nebo dojde ke zpochybnění poskytnutých služeb zdravotní pojišťovnou, můžeme Vaše údaje případně využít při řešení tohoto sporu, a to i v soudním nebo správním řízení a dále za účelem evidence jeho průběhu a výsledku, a to z důvodu našeho oprávněného zájmu, kterým je uplatňování nebo bránění našich práv. V takovém případě jsou údaje uchovávány a předány k archivaci nejdéle po 20 letech od ukončení sporu.

3. Co se stane s Vašimi údaji poté, co uplyne doba pro jejich oprávněné uchování?

Chceme Vás ujistit, že Vaše údaje zpracováváme pouze k účelům, které jsou uvedeny v tomto dokumentu a pouze po dobu, po kterou je takové zpracování pro daný účel nezbytné. Po uplynutí doby pro oprávněné uchování a zpracování Vašich osobních údajů probíhá automatický výmaz Vašich údajů z informačních systémů podniku, probíhá výmaz Vašich údajů z jiných prostředků zpracování. Dokumentace v listinné podobě podléhá skartačnímu a archivačnímu řízení podle platných právních předpisů.

4. Komu Vaše osobní údaje zpřístupňujeme či předáváme?

Vaše osobní údaje standardně předáváme, v nezbytně nutném rozsahu:
- Vaší zdravotní pojišťovně, případně Vašemu ošetřujícímu (registrujícímu) lékaři,
- dalším poskytovatelům zdravotních služeb pro zajištění specializovaných zdravotních výkonů, vyžaduje-li takový postup Vaše léčba.

Ve výjimečných případech může být dočasný přístup k některým údajům, které se Vás mohou týkat povolen našim smluvním partnerům, kteří pro nás provádějí servisní práce na informačních systémech a databázích.

Vaše osobní údaje nepředáváme do států EU ani do jiných zemí.

5. Jaká jsou Vaše práva dle platné právní úpravy?

Rádi bychom Vás též informovali, že dle platné právní úpravy ochrany osobních údajů máte následující práva:

- právo na potvrzení, zda zpracováváme Vaše osobní údaje a právo přístupu k osobním údajům, které ve Vašem případě zpracováváme,
- právo na opravu Vašich osobních údajů v případě, že by byly v kterémkoli směru nesprávné, či nepřesné,
- v případě, že byste zjistili, nebo se domnívali, že provádíme zpracování Vašich osobních údajů, které je v rozporu s ochranou Vašeho soukromého a osobního života nebo v rozporu se zákonem, zejména pokud by Vaše osobní údaje byly nepřesné s ohledem na účel jejich zpracování, máte právo požádat nás o vysvětlení a také požadovat, abychom odstranili takto vzniklý stav (např. blokováním, provedením opravy, doplnění nebo likvidací Vašich osobních údajů),
- právo požadovat výmaz osobních údajů, popřípadě omezení jejich zpracování,
- právo vznést námitku proti zpracování za účelem posouzení, zda došlo k porušení povinností uložených nám platnou právní úpravou,
- máte právo odvolat souhlas v případě, kdy Vaše osobní údaje zpracováváme na základě Vámi uděleného souhlasu,
- podat stížnost u dozorového úřadu, kterým je Úřad pro ochranu osobních údajů se sídlem Pplk. Sochora 27, 170 00 Praha 7,
- máte též právo na přenositelnost těch údajů, které jste nám poskytl a které zpracováváme automatizovaně, je-li zpracování založeno na Vašem souhlasu nebo na nezbytnosti pro plnění smlouvy. V případě, kdy byste měli zájem předat tyto údaje jinému správci, Vám umožníme získat Vaše osobní údaje

ve strukturovaném, běžně používaném a strojově čitelném formátu, případně, bude-li to technicky proveditelné, je přímo předáme jinému správci.

Své žádosti a dotazy k otázce zpracování Vašich osobních údajů můžete zasílat na adresu námi určeného pověřence pro ochranu osobních údajů:

Horské lázně Karlova Studánka, státní podnik
Pověřenec pro ochranu osobních údajů
č. p. 6
793 24 Karlova Studánka
e:mail: osobni.udaje@horskelazne.cz

ANOTACE

Bibliografický údaj: Kopecká, Erika. *Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů.* Olomouc 2020. Bakalářská práce. Moravská vysoká škola Olomouc. Vedoucí práce: Ing. Lukáš Pavlík, Ph.D.

Název práce: Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů

Autor: Erika Kopecká

Ústav: Ústav informatiky a aplikované matematiky

Vedoucí práce: Ing. Lukáš Pavlík, Ph.D.

Abstrakt: Tato bakalářská práce se zaměřuje na ochranu osobních údajů a její právní legislativu Obecné nařízení Evropského parlamentu a Rady o ochraně osobních údajů č. 2016/679, neboli GDPR, která byla přijata v dubnu 2016 a je závazná pro všechny, kteří chtějí zpracovávat osobní údaje subjektu údajů z jakéhokoliv členského státu Evropské unie. Je důležité si uvědomit, že ochrana osobních údajů bude s narůstající technikou více a více vyžadována, proto je důležité se tímto tématem zabývat. Teoretická část této práce pojednává o základních pojmech a je v ní charakterizována problematika GDPR. V praktické části je popsána implementace nařízení ve vybraném podniku, tak aby praxe byla v souladu s danou právní legislativou, je také analyzován výskyt osobních údajů a vlastním průzkumem formou krátkého rozhovoru s vybranými zaměstnanci je popsán současný stav organizace. To vše ukazuje, jaký je dopad implementace v podniku a dává podklad pro návrh na zlepšení.

Klíčová slova: GDPR, ochrana osobních údajů, osobní údaj, subjekt údajů, implementace.

Title: The Issue of GDPR and its Impact on Employers in the Field of Personal Data Protection

Author: Erika Kopecká

Department: Department of Computer Science and Applied Mathematics

Supervisor: Ing. Lukáš Pavlík, Ph.D.

Abstract: This bachelor thesis focuses on the protection of personal data and its legislation General Regulation of the European Parliament and the Council on the protection of personal data No. 2016/679, or GDPR, which was adopted in April 2016 and is binding for all who want

to process data from any Member State of the European Union. It is important to recognize that the protection of personal data will be more and more required as technology grows, so it is important to address this issue. The theoretical part of this work deals with basic concepts and explains the characteristics of GDPR. The practical part describes the implementation of the regulation in the selected company, so that the practice is in accordance with the legal legislation, the occurrence of personal data is analyzed and the actual survey in the form of a short interview with selected employees is analyzed the actual situation in the organization. All this shows the impact of implementation in the company and gives the basis for the proposal for improvement.

Keywords: GDPR, Protection of personal data, personal data, data subject, implementation.