VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV EKONOMIKY
INSTITUTE OF ECONOMICS

ANALÝZA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PODLE NAŘÍZENÍ GDPR

PERSONAL DATA PROCESSING ANALYSIS UNDER THE GDPR REGULATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Gabriela Slámová

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Viktor Ondrák, Ph.D.

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav ekonomiky
Studentka:	Bc. Gabriela Slámová
Studijní program:	Ekonomika a management
Studijní obor:	Podnikové finance a obchod
Vedoucí práce:	Ing. Viktor Ondrák, Ph.D.
Akademický rok:	2017/18

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Analýza zpracování osobních údajů podle Nařízení GDPR

Charakteristika problematiky úkolu:
Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska práce
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout systém ochrany osobních údajů.

Základní literární prameny:

BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v životě podnikatele: 103 řešení modelových situací. Olomouc: ANAG, 2013. ISBN 978-80-7263-811-6.

Evropský parlament a rada. Nařízení č. 679/2016 ze dne 14.4.2016: Obecné nařízení o ochraně osobních údajů (GDPR).

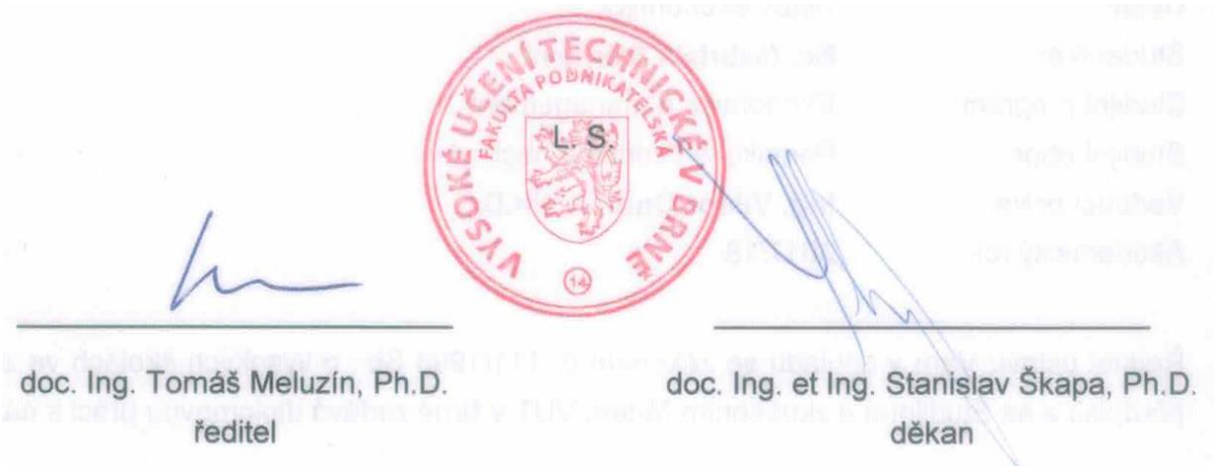
NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014. 484 s. ISBN 978-80-7478-665-5.

NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-765-3.

ÚZ 1209 Ochrana osobních údajů, GDPR. Ostrava: Sagit, 2017. 112 s. ISBN 978-80-7488-241-8.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018



doc. Ing. Tomáš Meluzín, Ph.D.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Diplomová práce se zabývá návrhem systému ochrany osobních údajům dle nařízení GDPR v organizaci Dentalife s.r.o. Návrh byl realizován na základě provedené analýzy současného stavu, která odhalila závažné nedostatky v souladu s nařízením GDPR. Na základě identifikace zjištěných nedostatků byl vypracován návrh doporučení, který v případě jeho následné implementace, povede k uvedení současného stavu do souladu s tímto nařízením. Téma diplomové práce bylo vybráno především z důvodu jeho aktuálnosti a chybějících materiálů, které by popisovaly a vysvětlovaly jednotlivé kroky celého procesu analýzy či implementace.

Klíčová slova

Ochrana osobních údajů, Obecné nařízení GDPR, Analýza současného stavu, mapa osobních údajů, GAP analýza

Summary

This diploma thesis deals with the proposal of a personal data protection system according to the General Data Protection Regulation in the organization Dentalife s.r.o.. The proposal was implemented on the basis of an analysis of the current situation which revealed serious shortcomings in line with the General Data Protection Regulation. Based on the identified deficiencies, a recommendation has been drawn up which, in the event of its subsequent implementation, will put the current situation into line with this Regulation. The theme of the diploma thesis was selected primarily because of its up-to-date and missing materials that would describe and explain the individual steps of the whole process of analysis and implementation.

Key words

Personal data protection, General Data Protection Regulation, analysis of the current situation, data map, GAP analysis

Bibliografická citace

SLÁMOVÁ, G. *Analýza zpracování osobních údajů podle Nařízení GDPR.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 98 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

.....

Podpis

V Brně dne 20. 5. 2018 Bc. Gabriela Slámová

OBSAH

SEZNAM SYMBOLŮ A ZKRATEK

Admin	administrátor
BOZP	bezpečnost a ochrana zdraví při práci
CRM	customer relationship management
ČR	Česká republika
DIČ	daňové identifikační číslo
e-shop	elektronický obchod
EPDB	Evropský sbor pro ochranu osobních údajů
EU	Evropská unie
GDPR	General Data Protection Regulation
IČO	identifikační číslo osoby
ISMS	Information Security Management Systém (systém řízení bezpečnosti informací)
IT	informační technologie
OSVČ	osoba samostatně výdělečně činná
PO	požární ochrana
PEDRO	účetní software
QMS	Quality Management Systém (systém řízení jakosti)
Teleshop	teleshopping
ÚOOÚ	úřad pro ochranu osobních údajů
URL	Uniform Resource Locator (jednotná adresa zdroje)
WP 29	Working Party (pracovní skupina 29)
WWW	Word Wide Web (celosvětový web)

Úvod

Ochrana osobních údajů, především se spojením s Obecným nařízením o ochraně osobních údajů (dále jen nařízení GDPR), se stala v poslední době velmi diskutovaným tématem. Stalo se tak především na základě masové medializace, která na sebe strhla velkou pozornost především hrozbami v podobě vysokých pokut za porušení povinností vyplývajících z Evropského nařízení. Doposud se subjekty fyzických a právnických osob v oblasti ochrany osobních údajů řídily zákonem č. 101/2000 Sb, o ochraně osobních údajů. Evropská unie však vydala novou legislativu, a to již zmíněné nařízení GDPR, které nahrazuje původní směrnici Evropského parlamentu a rady 95/46/ES.

Důvod, proč je nutné se ochranou osobních údajů zabývat stále intenzivněji, a proč se Evropská unie rozhodla posílit ochranu dat občanů, je vývoj informačních a telekomunikačních technologií, který je stále rychlejší a jejich podíl užívání v každodenním fungování společnosti neustále narůstá. Tato fakta doprovází i nárůst hrozeb v podobě neoprávněného nakládání s osobními údaji, a to až po jejich nezákonné zneužití.

Nařízení GDPR přináší pro subjekty, zpracovávající osobní údaje, nová práva a povinnosti. Jeho účinnost je připsána datu 25. května 2018. Od tohoto dne budou evropské úřady, zabývající se ochranou osobních údajů, oprávněny soulad s nařízením kontrolovat a jeho odchýlení pokutovat. V České republice bude soulad s nařízením GDPR kontrolovat Úřad pro ochranu osobních údajů (dále jen ÚOOÚ).

Spousta organizací vnímá Nařízení především jako administrativní a finanční zátěž, která nepřináší žádnou přidanou hodnotu pro organizaci. Nová pravidla lze ovšem vnímat i pozitivně. Organizace, která projde analýzou současného stavu, získá jasný přehled o osobních údajích, které vlastní. Eliminuje výskyt údajů, které spravuje neoprávněně. Zbaví se dat, která nepotřebuje a nastaví procesy, tak aby zabránila úniku dat a vzniku škod.

Nejsou to však jen organizace, které by se ochranou osobních údajů měly zabývat, ale i občané, kteří se stávají tzv. subjekty zpracování (tj. osobami jejichž osobní údaje jsou zpracovávány). Tyto subjekty zpracování, by měly zvýšit své povědomí v oblasti této problematiky a být obezřetnější při poskytování svých osobních údajů.

1 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Práce je zaměřena na provedení analýzy současného stavu, zpracování osobních údajů, ve společnosti Dentalife s.r.o., zhodnocení nesouladu vůči nařízení GDPR a vypracování návrhu na úpravy, které povedou k naplnění požadavků obsažených v obecném nařízení GDPR.

1.1 Cíl práce

Cílem této práce je vypracovat návrh doporučení jednotlivých opatření požadovaných nařízením GDPR. Tato doporučení po jejich implementaci povedou k uvedení organizace Dentalife s.r.o. do souladu s požadavky nařízení GDPR.

1.2 Dílčí cíl

Dílčím cílem je popsat průběh analýzy současného stavu zpracování osobních údajů, prováděné ve společnosti Dentalife s.r.o., včetně kroků, které analýze předcházejí.

1.3 Omezení práce

Samotná analýza současného stavu, bude prováděna na fiktivní společnosti, a to z toho důvodu, aby byly pokryty problémy, se kterými se nejčastěji setkává velké množství organizací. Vzhledem k oborové rozdílnosti organizací, není možné v obecné rovině definovat veškeré nesoulady, které mohou v rámci analýzy současného stavu nastat. Jedná se především o to, že organizace zabývající se prodejem zahradního nábytku, kde výskyt zpracování osobních údajů je minimální, bude řešit zabezpečení osobních údajů v jiném měřítku, než například nemocnice, která provádí rozsáhlé zpracování zvláštní kategorie osobních údajů. Zde budou kladeny mnohem větší nároky, a to jak na zabezpečení, tak na samotné zpracování osobních údajů.

Vzhledem k cíli a rozsahu dané práce dále není možné zabývat se hloubkovým zkoumáním všech článků nařízení GDPR a podrobně každý klasifikovat a vysvětlit jejich znění. Toto omezení se vztahuje i na ostatní legislativu vztaženou k problematice ochrany osobních údajů. Především se bude jednat o předpisy, které bude nutné synteticky začlenit při teoretickém výkladu implementace nařízení GDPR.

Vzhledem k rozsahu práce nebude provedena komparace nařízení GDPR vůči normě ISO/IEC 27001, ani její popis či implementace.

S přihlédnutím ke studijnímu oboru autora, práce nebude analyzovat ani navrhovat řešení v oblasti informačních technologií.

1.4 Použité metody

Za účelem naplnění stanoveného cíle diplomové práce bude v průběhu zpracování aplikováno několik obecných a empirických metod.

Diplomová práce „Analýza zpracování osobních údajů podle Nařízení GDPR“ bude vytvořena využitím metod, které odpovídají metodám řešení odborné práce. Při procesu tvorby práce budou použity následující metody řešení odborné práce.

Pro zpracování analýzy současného stavu v organizaci, budou použity především empirické metody prostřednictvím dotazníku a interview. Na základě této analýzy vznikne tzv. *mapa osobních údajů*, neboli jinak nazváno, *přehled zpracování osobních údajů*.

Pro teoretickou a návrhovou část bude použita rešerše dostupných materiálů, především odborných knih, dokumentů v elektronické podobě, zákonů a článků z internetu. Literární rešerše bude použita k vysvětlení problematiky obecného nařízení GDPR a k odůvodnění navrhnutých řešení.

Z obecných metod bude v návrhové části použita analýza, komparace, dedukce a syntéza. Bude vypracována diferenční analýza, která bude výsledkem komparace poznatků z provedené analýzy současného stavu v organizaci Dentalife s.r.o., s nařízení GDPR. Na základě dedukce a syntézy bude sestaven návrh doporučení jednotlivých opatření, které bude nutné implementovat proto, aby se organizace dostala do souladu s nařízením GDPR.

2 TEORETICKÁ VÝCHODISKA PRÁCE

Kapitola je věnována vymezení **zákona č. 101/2000 Sb. o ochraně osobních údajů** a **obecného nařízení GDPR**. Zákon č. 101/2000 Sb. o ochraně osobních údajů, jenž je v této kapitole popsán, vstoupil v účinnost dne 1. 6. 2000 a je stále platným legislativním předpisem. Dne 21. 3. 2018 byla vládou ČR schválena novelizace tohoto zákona, jenž bude doplňovat nařízení GDPR. Nařízení GDPR, jakož to nařízení EU má přednost před zákonem, je přímo aplikovatelné a závazné pro všechny členské státy EU, které nemají možnost nastavit si odlišná pravidla, pouze mohou nařízení doplnit v bodech, ve kterých jim to nařízení umožňuje. (1)

Zákon 101/2000 Sb. o ochraně osobních údajů je uváděn z důvodu, aby čtenář diplomové práce byl seznámen se zněním legislativy, která je aktuálně platná a podle které by se organizace měly řídit do doby, než nařízení GDPR nevyjde v účinnost a zároveň zaznamenal změny, jak v rozsahu, tak přístupu nové evropské legislativy. Následně bude v závěru práce zhodnoceno, zda organizace Dentalife s.r.o., prováděla zpracování osobních údajů podle doposud platné legislativy či nikoliv.

2.1 Zákon 101/2000 Sb. o ochraně osobních údajů

Zákon č. 101/2000 Sb. o ochraně osobních údajů nebyl první právním předpisem, zabývajícím se ochranou osobních údajů na území České republiky.

Ochrana osobních údajů na území České republiky, až do roku 1989 téměř neexistovala. Na vině byl vládnoucí komunistický režim, při němž nebylo žádoucí chránit soukromí občanů. Po rozpadu totalitního režimu došlo k ústavněprávní úpravě sepsáním Listiny základních práv a svobod. Tento dokument se stal prvním ústavním dokumentem, který zakotvil tradiční demokratická práva a svobody. Ochrana osobních údajů byla ustanovena článkem 10, který mimo jiné dává fyzickým osobám právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Po přijetí Listiny základních práv a svobod následovalo přijetí zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech (dále jen zákon o

ochraně osobních údajů v informačních systémech), který vycházel z Úmluvy Rady Evropy č. 108, ze dne 28. ledna 1981. Tato úmluva brala zřetel na automatizované zpracování osobních dat. Zákon o ochraně osobních údajů v informačních systémech byl po osmi letech své účinnosti zrušen. Stalo se tak na základě ucházení České republiky o členství v Evropské unii, kdy byla Česká republika vystavena kritice nedostačující právní ochrany, a bylo nutné uvést v účinnost zákon nový, který bude vycházet ze Směrnice Evropského parlamentu a Rady č. 95/46/ES, vydané v roce 1995. Tato směrnice se stala závaznou pro vstup České republiky do Evropské unie. V roce 2000 byl Parlamentem České republiky schválen zákon č. 101/2000 Sb., o ochraně osobních údajů (dále jen zákon o ochraně osobních údajů), jenž je dodnes platným právním předpisem České republiky, kompatibilní s právy Evropských společenství. (2) (3) (4) (5) (6) (7)

Zákon o ochraně osobních údajů vnáší zcela nový rozměr v rámci zpracování osobních údajů. Předcházející legislativa, zákon o ochraně osobních údajů v informačních systémech, se vztahoval pouze na ochranu osobních údajů a informací zpracovávané informačním systémem. Zákon o ochraně osobních údajů se zaměřuje na veškeré zpracování osobních údajů obecně. (4) (8)

S jeho účinností byly ustanoveny nové doposud neznámé pojmy, jako je *osobní údaj, zpracování osobních údajů, správce, zpracovatel, citlivý údaj, oznamovací povinnost* a mnoho dalších. (8)

Osobní údaj je zákonem o ochraně osobních údajů definován, jako jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. (8)

Zpracováním osobních údajů je, dle zákona o ochraně osobních údajů, jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních

údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace. Je zde nutné podotknout, že nahlížení, se dle zákona o ochraně osobních údajů, nepovažuje za zpracování, pokud ovšem informace je vyhledávána například informací umístěných na internetu, už se o zpracování osobních údajů jedná. (8) (9)

Správce, je zákonem definován, jako každý subjekt, který určuje účel a prostředky zpracování osobních údajů, zpracování provádí a odpovídá za něj. Těmto subjektům jsou ukládány povinnosti dle §5. Správce je povinen:

1) stanovit účel zpracování a zpracovávat tyto údaje pouze k vymezenému účelu;
2) stanovit prostředky a způsob zpracování;
3) zpracovávat pouze přesné osobní údaje;
4) shromažďovat osobní údaje pouze v rozsahu nezbytném k účelu;
5) uchovávat osobní údaje pouze dobu nezbytně nutnou k účelu. (8)

Následně jsou správci vymezena další omezení. **Správce může osobní údaje zpracovávat, pouze pokud je zpracování nezbytné pro**:

1) dodržení právní povinnosti správce;
2) pro plnění smlouvy, jejíž smluvní stranou je subjekt, nebo je jednáno o jejím uzavření,
3) ochranu životně důležitých zájmů subjektu;
4) zveřejnění osobního údaje v rámci zvláštního právního předpisu;
5) ochranu práv a právem chráněných zájmů správce či jiných dotčených osob;
6) uveřejnění osobních údajů o veřejně činné osobě, funkcionáři, či zaměstnanci veřejné správy, které vypovídá o jeho veřejné nebo úřední činnosti, o jeho funkčním nebo pracovním zařazením;
7) účely archivnictví dle zvláštního zákona. (8)

Pro veškerá zpracování, která neodpovídají výše uvedenému, je nutné opatřit si **souhlas subjektu údajů se zpracováním osobních údajů**, jehož náležitosti zákon o ochraně osobních údajů vymezuje. (8)

Výjimkou se stává zpracování osobních údajů, konkrétně jména, příjmení a adresy subjektu získaných z veřejného seznamu, a to za účelem nabízení obchodu nebo služeb tomuto subjektu. Tyto údaje je dále možné i za určitých podmínek předat jinému správci, který je využívá obdobným způsobem. Takové údaje je možné zpracovávat až do okamžiku vyslovení nesouhlasu subjektem. (8)

Novým pojmem se stávají **citlivé údaje**. Zákon je vymezuje jako osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu, sexuálním životě subjektu údaj, genetický údaj či genetický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. (8)

Takové osobní údaje lze zpracovávat zejména pouze pokud:

1) subjekt údajů dal ke zpracování výslovný souhlas;
2) zpracování je nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení nebezpečí hrozícího jejich majetku;
3) jedná se o zpracování při poskytování zdravotní služby, ochrany veřejného zdraví, zdravotního pojištění nebo výkon státní správy ve vymezených případech;
4) dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti;
5) zpracování se týká osobních údajů zveřejněných subjektem údajů;
6) a další nezmíněné, uvedené v §9. (8)

Správce má také povinnost v některých případech subjekt údajů **informovat** o prováděném zpracování osobních údajů. Je povinen sdělit informace o rozsahu a účelu zpracování, zda jsou osobní údaje poskytovány povinné či dobrovolné, dále o subjektech, které budou zpracování provádět a komu budou osobní údaje zpřístupněny a v neposlední řadě se jedná o poskytnutí informací o právech subjektu, konkrétně o právu na přístup a právu na opravu osobních údajů. (8)

Takové informace není správce povinen sdělovat především pokud:

1) zpracovává osobní údaje získané se souhlasem subjektu osobních údajů;
2) zpracovává osobní údaje, které jsou zveřejněny;
3) zpracování ukládá zvláštní zákon;
4) poskytnutí takových informací, by vyžadovalo neúměrné úsilí nebo nepřiměřeně vysoké náklady;
5) a další nezmíněné, uvedené v §11. (8)

Dále má správce povinnost sdělit některé informace všem subjektům, které využijí **práva na přístup k informacím**. Tedy těm, kteří zažádají o sdělení informací ohledně zpracování jejich osobních údajů. Správce je v takovém případě povinen subjektu sdělit:

1) účel zpracování osobních údajů;
2) výčet osobních údajů či kategorií osobních údajů, které jsou zpracovávány;
3) veškeré zdroje osobních údajů;
4) informace o příjemcích, případně kategorii příjemců;

Za tyto služby má správce oprávnění účtovat si přiměřenou úhradu.

Další povinností, která se vztahuje na správce, je **oznamovací povinnost** dle § 16. Doktor práv, pan Daniel Novák, ve své publikaci (10, s. 250), vydaném komentáři k zákonu o ochraně osobních údajů uvádí, že *oznamovací povinnost se vztahuje pouze na zcela nebo částečně automatizované zpracování, nebo souboru takového zpracování, které má stejný účel nebo účely související*. (8) (10)

Povinnosti správce se týkají i **zabezpečení osobních údajů**. Správce a zpracovatel[4], jsou dle §13, povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům. Tato povinnost platí i po ukončení zpracování osobních údajů. Zákon tedy nenařizuje přímo způsob, jakým by osobní údaje měly být chráněny, ale vybízí subjekty, aby zpracování řádně zabezpečily. (8)

[4] **Zpracovatele** vymezuje zákon o ochraně osobních údajů jako subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle zákona o ochraně osobních údajů. (8)

Jednou z posledních povinností správce nebo zpracovatele, je vypracování dokumentu, ve kterém budou obsaženy **informace o přijatých a provedených technicko-organizačních opatřeních**. Opět zákon nedefinuje formu ani míru detailu, ale vybízí subjekty, aby takový dokument zpracovaly. (8)

Nově byl zřízen, dle §2, **úřad pro ochranu osobních údajů**, jemuž byly svěřeny kompetence ústředního správního úřadu, jak v rámci české legislativy, tak kompetence stanovené mezinárodními smlouvami a předpisy Evropských společenství. Především se jedná o provádění dozoru nad dodržováním povinností stanovených zákonem a přijímání podnětů a stížností za porušení zákonné povinnosti, jejichž nedodržení má oprávnění pokutovat. (8)

Výše pokut je v právním předpisu členěna do 3 skupin dle závažnosti přestupku.

1) do výše 100 000 Kč
2) do výše 1 000 000 Kč
3) do výše 5 000 000 Kč (8)

První skupina, tedy pokuta v maximální výši 100 000 Kč, je udělena subjektům, jenž poruší povinnost mlčenlivosti dle §15. Druhá skupina, tedy pokuta v maximální výši 1 000 000 Kč, se týká především §5, jenž ukládá povinnosti správci. Pokuta může být udělena Správci nebo Zpracovateli, který například zpracovává osobní údaje bez souhlasu subjektu osobních údajů, nebo je uchovává po dobu delší než je nezbytně nutná k účelu, či neprovede opatření pro zajištění bezpečnosti jejich zpracování. Pokuta až do výše 5 000 000 Kč se týká především porušení povinnosti mlčenlivosti dle §15 spáchané tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí či jiným obdobně účinným způsobem. Dále se vztahuje na ohrožení většího počtu osob či porušení povinnosti pro zpracování citlivých údajů. (8)

2.2 Obecné nařízení GDPR

Nařízení GDPR (anglicky „*General Data Protection Regulation"*), neboli „*Obecné nařízení o ochraně osobních údajů",* je nařízení Evropské unie, jehož cílem je výrazně posílit ochranu osobních údajů občanů žijících v Evropské unii. Jedná se o nejvýznamnější legislativní počin v oblasti ochrany osobních údajů za posledních 20 let, jenž kromě zvýšené ochrany osobních údajů, přináší i vysokou míru právní nejistoty. (11) (12)

Nařízení bylo vyhlášeno v Úředním věstníku Evropské unie, ke dni 4. května 2016. Účinnost tohoto nařízení je stanovena na 25. května 2018, kdy začne v celé Evropské unii platit jednotně. (13)

V České republice, tak bylo nezbytné provést novelizaci zákona o ochraně osobních údajů, jejíž návrh byl ke dni 21. března 2018 schválen vládou. Novela bude pouze doplňovat obecné Nařízení, stejně jako tomu je nyní v případě směrnice 95/46/ES a současné podoby zákona o ochraně osobních údajů. (14)

2.2.1 Důvody vzniku Obecného nařízení GDPR

Evropská legislativa, kterou se státy doposud ohledně ochrany osobních údajů řídily, je zastaralá. Tato legislativa[5] vznikla v roce 1995, kdy nebyly sociální sítě, nebyla cloudová uložiště a mnoho dalších vyspělých informačních technologií. Bohužel i současné nařízení GDPR, které v roce 2018 vstoupí v platnost, zatím neřeší některé problémy, které se týkají pokroku těchto technologií. Dalším důvodem je množství osobních údajů, které jsou každodenně zneužívány. Řeč je především o tzv. obchodnících s osobními údaji, jejichž businessem se stalo odkupování databází osobních údajů od velkých společností a přeprodávání jich dále. Občan v dnešní době má minimální šanci dozvědět se o tom, kde všude se jeho osobní údaje nacházejí a především k čemu jsou využívány. Tato data jsou pak lehce zneužitelná. (11)

[5] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (11)

Na druhou stranu nařízení GDPR nepřináší zas tak zásadní změny. Velká většina ustanovení, které GDPR obsahuje, by měla být v organizacích zavedena již od roku 2000, a to s účinností zákona o ochraně osobních údajů. Nařízení GDPR, je i velmi podobné bezpečnostní normě ISO/IEC 27 001[6]. Dá se tedy říci, že pokud má podnik úspěšně nastavený systém podle této normy, či dodržuje ustanovení obsažená v české legislativě, tak jej čekají pouze malé změny. (15) (16)

Není to ovšem jen norma ISO 27 001 a zákon o ochraně osobních údajů, které osobní údaje chrání. Pokud není nakládáno správně s osobními údaji, tak je mimo jiné porušen zákon č. 89/2012 Sb., občanský zákoník *(§3 odst.2 písm. a) každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí)*, konkurence podnik může žalovat v rámci nekalé soutěže, problém s Českou obchodní inspekcí může nastat v rámci klamání spotřebitele a v neposlední řadě se může jednat o trestný čin při úniku osobních údajů. (17) (18)

2.2.2 Obecná ustanovení

Podkapitola se věnuje vysvětlení jednotlivých článků obsažených v nařízení GDPR. Nařízení GDPR obsahuje celkem 99 článků, které zaujímají, v české jazykové verzi, necelých 90 stran. Mohlo by se tedy zdát, že se jedná o dostatečný prostor, pro vysvětlení jednotlivých ustanovení a pojmů v nich obsažených. Opak je však bohužel pravdou. Nařízení provází velké množství nejasností, které je nutné následně upřesnit vydáním dalších oficiálních dokumentů. Konkrétně se jedná o výkladová stanoviska pracovní skupiny 29[7] (WP 29), která průběžně vydává a veřejně diskutuje materiály, které by měly sloužit k vysvětlení jednotlivých částí obecného nařízení. (19)

[6] ISO/IEC 27001 je mezinárodně platný standard, který definuje požadavky na systém managementu bezpečnosti informací. (16)

[7] Pracovní skupina 29 byla ustanovena článkem 29 směrnice 95/46/EC. Jde o nezávislý evropský poradní orgán na ochranu dat a soukromí. Je složena z vedoucích zástupců dozorových úřadů členských zemí Evropské unie. Účinností nařízení GDPR se změní v Evropský sbor pro ochranu osobních údajů (EPDB). Úkolem Sboru bude především zajišťování jednotného uplatňování Obecného nařízení a za tím účelem monitorovat jeho uplatňování a vydávat pokyny, doporučení a osvědčené postupy. (19)

2.2.2.1 Věcná a místní působnost

Nařízení GDPR se vztahuje na veškeré zpracování osobních údajů probíhající na území EU a mimo ni, pokud se jedná o zpracování osobních údajů občanů nacházejících se na území EU. V rámci vymezení místní působnosti, není česká verze nařízení příliš srozumitelná. Dle bodu 23[8] odůvodnění nařízení GDPR, se legislativa vztahuje na subjekty, které mají v úmyslu zpracovávat osobní údaje za účelem nabídky zboží nebo služeb občanů nacházejících se na území EU, aniž by proběhla platba. Je tedy nutné posoudit, zda se o takový záměr jedná či nikoliv. (20) (21)

Nařízení stanovuje pár výjimek, na které se nařízení nevztahuje, týká se:

- volného pohybu osobních údajů v souvislosti s činnostmi, které nespadají do působnosti práva Unie;
- činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, tedy bez jakékoliv souvislosti s profesní nebo obchodní činnosti;
- osobní údaje zesnulých osob;
- výkon činností členských států, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU;
- výkonů orgánů při provádění činností, které jsou prováděny za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestu, včetně ochrany před hrozbami pro veřejnou bezpečnost, a jejich předcházení. (20)

2.2.2.2 Vymezení základních pojmů

K porozumění GDPR je nutné znát základní pojmy, které provází celé nařízení. Uvedeny jsou pouze ty nejdůležitější. (20)

Osobní údaj

Nařízení GDPR osobní údaj definuje jako *veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou*

[8] Nařízení GDPR je doplněno 173 body, které blíže specifikují některá ustanovení. (20)

*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.* (20)

To znamená, pokud máme nějakou informaci, na základě které můžeme identifikovat osobu, a to i za pomocí technologií, sociálních sítí či dalších osob, tak se jedná o osobní údaj. Petra Dolejšová na své přednášce pro Hospodářskou komoru ČR (18, 2018), uvedla pomůcku, podle které je možné identifikovat, zda se jedná o osobní údaj či nikoliv. (20) (18)

O osobní údaj se jedná tehdy, pokud je FBI schopna, na základě této informace najít konkrétní osobu.

Osobním údajem je například fotografie, telefonní číslo, číslo účtu fyzické osoby, jméno a přímení pokud je možno ji spojit s informací, která odkazuje na konkrétní osobu. Klasifikovat tedy jako osobní údaj lze i pracovní či soukromý email nebo IP adresu. (18)

Zpracováním se rozumí 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 osobních údajů. Z uvedeného tedy vyplývá, že i pouhé nahlédnutí či vyhledávání osobních údajů podléhá nařízení GDPR. (20)

Správce je subjekt, který určuje účel zpracování osobních údajů. Může se tedy jednat jak o fyzickou, tak právnickou osobu, orgán veřejné moci či jiný subjekt. (20)

Zpracovatel může být fyzická či právnická osoba, orgán veřejné moci či jiný subjekt, který zpracovává osobní údaje pro správce. Z toho vyplývá, že nestanovuje účel zpracování, ale zpracovává osobní údaje dle pokynů správce. (20)

Je velice důležité si uvědomit, zda organizace zpracování provádí jako správce či zpracovatel. Je velice časté, že jedna organizace zpracovává některé osobní údaje v roli správce a jiné v roli zpracovatele. Na každou roli se váží jiné povinnosti, jak bude uvedeno a vysvětleno později. (20)

Pseudonymizace je takové zpracování, kdy není možné přiřadit osobní údaje ke konkrétní osobě, aniž bychom nepoužili dodatečné, účelně oddělené informace. Často se jedná o záměrnou ochranu osobních údajů, za pomocí jiných identifikátorů, například osobního čísla. (20)

Anonymizace je oproti preudonymizaci nevratné opatření ochrany osobních údajů. Neexistují data, na která by se dalo odkázat pro zosobnění těchto dat. Často se takové informace používají pro statistické účely. (20)

Profilování je jakákoliv forma automatizovaného zpracování, která slouží k hodnocení některých osobních aspektů, a na základě těchto aspektů zvýhodňuje či znevýhodňuje vybrané subjekty. Osobním aspektem může být nákupní chování, věk, lokalita, ekonomická situace a mnoho dalších. (20)

2.2.2.3 Zásady a zákonnost zpracování

Tato část se věnuje především výkladu článku 5 nařízení GDPR, které v této části uvádí zásady zpracování. Musí být dodržena zásada **korektnosti**, **zákonnosti** a **transparentnosti**. To znamená, že zpracovávané osobní údaje musí být aktuální, je tedy nutné v případě například změny bydliště tyto změny aktualizovat. Dále je nutné podávat co největší míru informovanosti a zpracovávat osobní údaje pouze na základě právních titulů uvedených v článku 6, který uvádí, že zpracování je zákonné, pouze pokud splňuje minimálně jednu podmínku z níže uvedených:

- subjekt údajů udělil souhlas pro jeden či více účelů;
- zpracování je nezbytné pro plnění smlouvy nebo vyjednávání o ní;
- zpracování je nezbytné pro splnění právní povinnosti správce;
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo

při výkonu veřejné moci, kterým je pověřen správce;

- zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, kdy nesmí být dotčeny základní práva a svobody subjektů údajů. (20)

Za zvýšenou pozornost stojí podmínka udělení **souhlasu** či **oprávněné zájmy** správce. Podmínkám **vyjádření souhlasu** se věnuje článek 7, který uvádí konkrétní náležitosti. Nařízení nepředepisuje formu, nýbrž uvádí, že správce musí být schopen souhlas doložit. Pokud se však správce rozhodne pro poskytnutí souhlasu písemnou formou, tak je nezbytné, aby takový souhlas byl jasně oddělen od jiných sdělení, srozumitelný, dobrovolný a kdykoliv snadno odvolatelný. V praxi to znamená, že souhlas nesmí být podmíněn čerpáním služby. I když subjekt nesouhlasí s udělením souhlasu se zpracováním, tak i tak mu musí být služba poskytnuta. Dále nesmí jít o slučování zpracování pro několik účelů. Pro každý účel musí být souhlas udělen zvlášť. Nařízení se nezmiňuje o délce trvání uděleného souhlasu. Pracovní skupina 29 vydala vodítka k udělení souhlasu, ve kterých uvádí doporučení, aby byl souhlas ve vhodných intervalech obnovován. Pokud správce či zpracovatel využívá ke zpracování souhlas, který nesplňuje podmínky nařízení GDPR, pak je souhlas neplatný. Správně napsaný souhlas je velice obtížné napsat na pár řádků, tak aby v něm byly obsaženy dostatečné a srozumitelné informace. Vzor souhlasu je uveden v příloze č. 1. (20) (22)

Oprávněný zájem bývá v praxi často využívaným pojmem. Jedná se o nejflexibilnější z právních titulů. Pokud se zájem správce dá považovat za oprávněný pak je možné osobní údaje zpracovávat, pokud nezasahuje do práv a svobod subjektů. Typickým příkladem by mohlo být monitorování prostor prodejny za účelem ochrany majetku. Při využívání tohoto právního titulu je vždy nutné důkladně posoudit jeho zákonnost. (20) (23)

Zásada účelového omezení, správci až na výjimky zakazuje zpracovávat osobní údaje za jinými účely, než za kterými byly shromážděny. To znamená, že pokud jsou zpracovávány osobní údaje pro účely plnění smlouvy, například v případě osobních

údajů z vytvořené objednávky na e-shopu, pak není možné tyto údaje využít pro cílený marketing[9]. (20) (24)

Zásada minimalizace udává rozsah zpracování osobních údajů, které by měly být minimální pro dosažení daného účelu, ke kterému jsou zpracovávány. (24)

Zásada integrity a důvěrnosti se týká zabezpečení, kdy je nezbytné, aby správce i zpracovatel přijali vhodná **technická a organizační opatření**. Tato povinnost je upřesněna v článku 32. Jedná se o další část nařízení, které není příliš konkrétní a jasné. Nařízení v článku 32 mimo jiné uvádí:

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. (20)

Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu. (20)

[9] Cílený marketing je forma marketingu, kdy se organizace snaží segmentovat trh a nabízet různé zboží různým segmentům potenciálních zákazníků. Nejedná se tedy o přímý marketing, na který nařízení GDPR nahlíží jako na oprávněný zájem, pokud není prováděno profilování. (25)

Pro rozhodnutí se, jak bude správce či zpracovatel osobní údaje chránit je nutné nejdříve posoudit rizika, která by mohla nastat při úniku či zneužití osobních údajů. Různé opatření pak stanoví organizace zabývající se pojištěním, kde hrozí únik informací subjektů údajů o výši jejich majetku, či zdravotním stavu. V tomto případě bude nutná implementace bezpečnostních technologií, které budou monitorovat a chránit osobní údaje. Organizaci zabývající se prodejem dentálních pomůcek pak postačí především zavedení organizačních opatření. Jedním takovým může být zakotvení mlčenlivosti a způsobu nakládání s osobními údaji do pracovních smluv či smluv s dodavateli, kteří taktéž přichází do kontaktu s osobními údaji zákazníků organizace. (26)

2.2.2.4 Zpracování zvláštních kategorií osobních údajů

Nařízení přikládá zpřísnění podmínek pro zpracování osobních údajů, které spadají do zvláštní kategorie. Vymezení podmínek se věnuje článek 9, který *zakazuje zpracování, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů*[10]*, biometrických údajů*[11] *za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.* Tento výrok ovšem neplatí, pokud například:

- subjekt údajů udělil výslovný souhlas pro takové zpracování a právo Unie mu zároveň toto udělení nezakazuje;
- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, a zároveň takové zpracování jiný předpis nezakazuje;
- subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas a zpracování je

[10] „genetickými údaji“ osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby. Příkladem může být DNA.

[11] „biometrickými údaji“ osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje na fotografii.

nutné pro ochranu životně důležitých zájmů jeho či jiných subjektů;
- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství. (20)

Důvodem zvláštního režimu je možnost ohrožení základních práv subjektu na jeho soukromí, které vychází již ze samotné povahy zpracovávaných osobních údajů. Nejčastěji se jedná o osobní údaje zpracovávané v pracovním lékařství. Běžná společnost se se zpracováním této kategorie spíše nesetká. Článek sice pojednává o zpracování fotografií, aby se ovšem jednalo o zvláštní kategorii, musela by fotografie v případě zpracování projít speciální technikou, která dokáže určit identifikaci osoby, například při automatické identifikaci zaměstnanců při vstupu do budovy. O zvláštní kategorii se také nejedná v podobě lékařských prohlídek uložených ve složce zaměstnance, které klasifikují zdravotní stav jako způsoben, nezpůsoben, způsoben s omezením. (44)

2.2.3 Práva subjektu údajů

Práva subjektu údajů jsou v nařízení GDPR vymezena v kapitole III. Jedná se především o práva:

- právo být informován;
- právo na přístup k osobním údajům;
- právo na výmaz;
- právo na opravu;
- právo na omezení zpracování;
- právo na přenositelnost;
- právo vznést námitku;
- právo nebýt předmětem automatizovaného rozhodnutí. (20)

Právo být informován

Subjekt údajů má právo dostat informace o zpracování jeho osobních údajů. Výčet poskytnutých informací je uveden v článcích 13 a 14, ve kterých se na náležitosti poskytnutých informací pohlíží ve dvou odlišných případech. První případ uděluje právo získat informace od správce, kterému byly osobní údaje sděleny přímo subjektem

údajů. Druhý případ se týká správce, jenže zpracovává osobní údaje subjektu, které ovšem nebyly od tohoto subjektu přímo získány. Mohlo tedy dojít o předání osobních údajů jiným správcem nebo zpracovatelem. Takového předání může nastat například v případě využití zprostředkovatelů. Příkladem může být autonehoda ve voze, jehož majitelem je leasingová společnost. V takovém případě subjekt z pravidla zasílá veškeré dokumenty leasingové společnosti. Ta se následně spojí s pojišťovnou, které předá získané dokumenty a pojistnou událost s ní uzavře. (20)

V prvním případě je správce povinen sdělit informace o zpracování osobních údajů a to **v okamžik jejich získání**. Znamenalo by to, že leasingová společnost by ihned po obdržení příslušných dokumentů k autonehodě měla obratem zaslat subjektu informace o zpracování osobních údajů. Tuto skutečnost správce nemusí plnit, pokud subjekt informace již získal, například pokud se nejedná o první pojistnou událost, nebo pokud subjekt informace získal například při uzavření smlouvy. (20)

Správce poskytne dle článku 13 následující informace:

- *totožnost a kontaktní údaje správce a jeho případného zástupce;*
- *případně kontaktní údaje případného pověřence pro ochranu osobních údajů;*
- *účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;*
- *oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na oprávněném zájmu zpracování*
- *případné příjemce nebo kategorie příjemců osobních údajů;*
- *případný úmysl správce předat osobní údaje*
- *doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;*
- *existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;*
- *pokud je zpracování založeno na udělení souhlasu, tak bude uvedena existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;*

- *existence práva podat stížnost u dozorového úřadu;*
- *skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;*
- *skutečnost, že dochází k automatizovanému rozhodování, včetně profilování*
- *pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu* (20)

Informace, dle článku 12, mohou být podány písemně nebo jinou formou. Nařízení umožňuje i ústní formu, v tomto případě ovšem správce musí být schopen doložit uskutečnění a obsah předaných informací. Nařízení klade důraz především na stručnost, transparentnost a srozumitelnost sdělení. Informace dále musí být podány bezplatně. Správce má i právo nevyhovět žádosti vůbec nebo si za ni účtovat přiměřený poplatek ale pouze v případě, kdy by se jednalo o opakované, nedůvodné nebo nepřiměřené žádosti subjektu. Vzor informační povinnosti je uvede v příloze č 2. (20)

Ve druhém uvedeném případě, kdy osobní údaje nejsou získány přímo od subjektu, správce poskytne informace o zpracování:

- *v přiměřené lhůtě, nejpozději však do jednoho měsíce nebo;*
- *nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace nebo;*
- *nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému správci.* (20)

Lhůta pro poskytnutí osobních údajů, je jedním z rozdílů, mezi výše uvedenými dvěma případy. Dále má subjekt údajů krom výčtu uvedených informací, uvedených v prvním případě i další dvě práva, a to právo získat informaci o kategoriích dotčených osobních údajů a zdroji, ze kterého osobní údaje pocházejí. (20)

Možnosti, jak lze informace poskytovat jsou různé. Vždy ovšem správce či zpracovatel musí myslet na prokázání předání těchto informací a dodržet včasnost daného sdělení. V případě vypsání výběrového řízení je možné tyto informace umístit přímo pod vypsaný inzerát, kdy žadatel zaškrtne pole, ve kterém stvrzuje seznámení se s poskytnutými informacemi. Banka může dané informace poskytnout prostřednictvím přihlášení se na internetové bankovnictví nebo prostřednictvím bankomatu. Je možné i informace zakomponovat přímo do smlouvy nebo je poskytnout za pomocí přiloženého dokumentu, jehož seznámení subjekt stvrdí svým podpisem.

Právo na přístup

Subjekt údajů má právo získat potvrzení o tom, zda jeho osobní údaje jsou zpracovávány, informace o zpracovávaných osobních údajích a také získat přístup k těmto informacím. Informace musí být poskytnuty do 1 měsíce s možností prodloužit tuto dobu o další dva. Subjekt má také právo získat bezplatně jednu kopii zpracovávaných osobních údajů. (20)

V praxi to znamená, že pokud subjekt zašle žádost o poskytnutí informací o zpracovávaných osobních údajích, pak by měl obdržet v rámci práva na přístup informace o:

- účelu zpracování;
- kategoriích dotčených osobních údajů;
- příjemci nebo kategoriích příjemců osobních údajů;
- plánované době zpracování;
- existenci práv subjektu (právo na výmaz, právo vznést námitku a další);
- právu podat stížnost u dozorového úřadu;
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování;
- pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách podle článku 46;
- měl by mít přístup k osobním údajům například přes webové rozhraní;
- má právo na jednu bezplatnou kopii (např. výpis hovorů, lékařské zprávy). (20)

Subjekt údajů také může konkretizovat, o které osobní údaje má zájem, pokud však tuto skutečnost správci nesdělí, pak má subjekt právo získat kompletní informace. (20) (26)

Toto právo může být omezeno v zájmu správce, zpracovatele nebo třetí strany. Správce může omezit poskytnuté informace v zájmu ochrany obchodního tajemství, duševního vlastnictví nebo autorského práva. Typickým omezením může dojít při poskytnutí kamerového záznamu, na kterém jsou zachyceny i třetí osoby. (20) (45)

Důležité je sdělit, že v případě uplatnění práva na přístup, se poskytnuté informace vztahují jak na osobní údaje poskytnuté subjektem tak na ty které vznikly bez činnosti subjektu. Právo se tedy vztahuje na všechny zpracovávané osobní údaje. (20)

Právo na opravu

Subjekt údajů má právo na to, aby doplnil neúplné osobní údaje či na to, aby správce opravil nepřesné osobní údaje. Příkladem může být změna trvalé adresy, telefonního čísla, emailu. V takovém případě má subjekt právo na to, aby správce tyto údaje opravil. (20)

Právo na výmaz („právo být zapomenut“)

Právo na výmaz, nebo-li právo být zapomenut, dává subjektům právo, za určitých podmínek, aby správce zlikvidoval jeho osobní údaje a dále je neuchovával. Za určitých podmínek znamená, že zpracovávané osobní údaje již nejsou potřebné pro účel, pro který byly původně zpracovávány. Musíme zde ovšem myslet i na jiné právní předpisy, které naopak dávají správci povinnost osobní údaje dále uchovávat. Příkladem může být zákon č. 563/1991 Sb., o účetnictví, který dává správci povinnost uchovávat účetní doklady po dobu 5ti let, mzdové listy je nutné uchovávat dle zákona č. č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení až po dobu 30ti let, jiné dokumenty je nutné uchovávat kvůli záruční době. Tyto skutečnosti musí správce vždy respektovat, a pokud subjekt zažádá o právo na výmaz, pak ne vždy bude možné takovému požadavku vyhovět. (20)

Dle článku 17, osobní údaje musí být vymazány pokud:

- *osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány*
- *subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;*
- *subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;*
- *osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje;*
- *osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti*. (20)

Správce na základ oprávněné žádosti na výmaz následně musí informovat všechny ostatní správce, jimž osobní údaje poskytl, aby jej zlikvidovali a dále neuchovávali. (20)

Právo na omezení zpracování

Subjekt údajů má právo na to, aby správce omezil zpracování, pokud si to subjekt údajů přeje a to především v případech kdy:

- subjekt údajů popírá přesnost zpracovávaných osobních údajů, a přeje si omezit zpracování do doby, než správce jejich přesnost ověří;
- zpracování je protiprávní a subjekt požaduje omezení jejich zpracování;
- správce osobní údaje již nepotřebuje, ale subjekt si nepřeje jejich výmaz pouze omezení z důvodů výkonu právních nároků;
- subjekt údajů vznesl námitku proti takovému zpracování. (20)

Aby došlo k omezení zpracování osobních údajů, musí subjekt údajů, s výjimkou jejich uložení, vyjádřit souhlas. Správce musí následně subjekt údajů informovat o zrušení takového omezení. (20)

Právo na přenositelnost

Skupina 29 vydala k ustanovení zachycující právo subjektu na přenositelnost osobních údajů, uvedeny v článku 20 nařízení GDPR, vodítka, ve kterých podrobněji vysvětluje

uplatnění daného práva. Právo na přenositelnost dává subjektu právo získat osobní údaje, jež **poskytl** správci, a předat tyto osobní údaje správci jinému. Zároveň ovšem nesmí být nepříznivě dotčena práva a svobody jiných osob. (20) (46)

Z výše uvedeného plyne, že správce je povinen poskytnou subjektu pouze osobní údaje, které on poskytl. Právo se tedy nevztahuje na osobní údaje, které byly vytvořeny bez činnosti subjektu. Druhou podmínkou je, že zpracování musí být prováděno na základě **smlouvy** nebo **souhlasu**, aby subjekt tohoto práva mohl využít, a zároveň musí jít o **automatizované zpracování**. Příkladem může být přenesení informací z aplikace kalendář při přechodu na jinou aplikaci nabízející stejné služby. Subjekt tak může zažádat o předání informací z jeho staré aplikace, aby poskytovatel tyto údaje předal jemu samotnému nebo novému poskytovateli. Správce by tedy měl předat krom jména, příjmení a emailové adresy subjektu, také informace o zaznamenaných schůzkách či poznámkách. Problém, na který by subjekt mohl narazit, je ta skutečnost, že nařízení GDPR nedává správci povinnost tyto osobní údaje přijmout. (20) (46) (27)

Lhůta pro poskytnutí osobních údajů správcem se řídí článkem 12, který uvádí jeden měsíc s možností prodloužit tuto dobu o další dva měsíce. (20)

Článek 20 nařízení se dále zmiňuje o podmínkách technického provedení předání těchto osobních údajů. Osobní údaje by měly být poskytnuty ve strukturovaném, běžně používaném a strojově čitelném formátu, přesný typ formátu ovšem nezmiňuje vzhledem k různorodosti jednotlivých odvětví. Bod 68 nařízení GDPR objasňuje tuto skutečnost výrokem, že formát by měl být interoperabilní, což znamená schopný toku informací, které umožňují vzájemnou výměnu dat. Skupina 29 uvádí jako příklady vhodných formátů, formáty XML, JSON nebo CVS. (20) (28)

Právo vznést námitku

Právo vznést námitku uděluje subjektu oprávnění vyjádřit se proti zpracování, které v případě, že bude námitka oprávněná, přikazuje správci přestat zpracovávat osobní údaje daného subjektu. (20)

Toto právo lze ovšem uplatnit pouze pokud zpracování bude probíhat na základě:

- oprávněného zájmu správce;
- zpracování nezbytného pro účely veřejného zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
- zpracování pro účely přímého marketingu;
- zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely. (20)

Jako jediné absolutní právo z výše uvedených, je právo vznést námitku proti zpracování pro účely přímého marketingu[12]. V tomto případě musí správce ihned přestat takové osobní údaje zpracovávat. U ostatních případů, má možnost správce prokázat jejich nutnost zpracování. (20)

Automatizované individuální rozhodování, včetně profilování

Posledním právem subjektu údajů, je obsaženo v článku 22, nařízení GDPR. Jedná se o právo subjektu, nebýt předmětem žádného zpracování, které je založeno na automatizovaném individuálním rozhodování, včetně profilování. (20)

Příkladem takového zpracování může být aplikace banky, která na základě vložených a zjištěných informací dokáže vyhodnotit poskytnutí či neposkytnutí úvěru danému subjektu. Toto právo má však své výjimky. (20)

Zpracování založené na automatizovaném zpracování lze využít v případech, kdy k tomu dal subjekt údajů výslovný souhlas, zpracování je nezbytné pro plnění nebo uzavření smlouvy, nebo je takové zpracování povoleno jiným právem (právem Unie nebo členského státu). (20)

[12] Přímý marketing je způsob marketingové komunikace, při které se oslovují zákazníci přímým adresním oslovením (např. e-mailem, poštou, telefonicky nebo i osobně). (29)

2.2.4 Obecné povinnosti správce a zpracovatele

Nařízení GDPR, v článcích 24-39 stanovuje **povinnosti správce a zpracovatele**. Jedná se především o povinnosti zabezpečení, vedení záznamů o činnostech zpracování, jmenování pověřence na ochranu osobních údajů či zapojení dalšího správce nebo zpracovatele. Nařízení také vymezuje rozsah jejich odpovědnosti. (20)

Odpovědnost správce

Odpovědnost za zpracování nese správce. Pokud účely zpracování určí společně dva nebo více správců, pak se stávají správci společnými a je nezbytné stanovit si mezi sebou podíly jejich odpovědnosti. (20)

Příkladem může být společný portál, který si zřídil hotel společně s poskytovatelem wellness. Oba poskytovatelé mají přístup na portál, tudíž i k objednávkám hostům. Příkladem, kdyby se nejednalo o společné správce, by byla situace, kdy by na portálu sice bylo možné objednat hotelové služby i wellness, ovšem poskytovatel wellness by neměl k osobním údajům přístup přímo přes portál, ale poskytovatel hotelových služeb by zasílal objednávky poskytovateli wellness. V tomto případě by se hotel stal správcem osobních údajů a wellness zpracovatelem.

Odpovědnost zpracovatele

Správce má možnost využít pro zpracování i jiného zpracovatele (viz. kapitola 2.2.2.2 Vymezení základních pojmů). Zpracovatel nestanovuje účely zpracování, ale pouze se řídí pokyny správce, které musí být vymezeny ve **zpracovatelské smlouvě** nebo jsou řízeny jiným právním aktem. Tato smlouva nebo jiný právní akt stanovuje:

- předmět zpracování;
- dobu trvání zpracování;
- povahu a pokyny zpracování;
- účel zpracování;
- typ osobních údajů a kategorie osobních údajů;
- povinnosti a práva správce;
- závazek mlčenlivosti;
- zabezpečení zpracování osobních údajů;

- dodržení podmínek zapojení dalšího správce či zpracovatele;
- právo správce provést inspekci či audit u zpracovatele;
- povinnost zpracovatele nahlásit správci pokyny, které jsou protiprávní. (20)

Pokud zpracovatel poruší nařízení GDPR tím, že sám určí účely nebo prostředky zpracování, pak se automaticky stává správcem, a vztahuje je na něj i plná odpovědnost za takové zpracování. (20)

Nařízení GDPR stanovuje formu zpracovatelské smlouvy nebo právního aktu, a to jedině písemnou, která může představovat i elektronickou podobu. (20)

Pro mnohé toto ustanovení bude znamenat revidovat smlouvy se svými zpracovateli nebo vůbec nějakou vytvořit, pokud tak zatím neučinili. Důležité bude především vymezit rozsah a pokyny zpracování. Zpracovatelé by tedy měli naléhat na své správce, aby smlouva byla co nejpřesnější a stanovila i způsob sběru dat. V praxi se můžeme setkat se smlouvami, opravňující zpracovatele ke sjednání smluv s novými klienty. Smlouva už ovšem nestanovuje náležitosti, jakým způsobem je možné nové či stávající klienty oslovovat. Ze smlouvy tak není jisté, zda zvolený způsob stanovil správce či zpracovatel. (20)

Důležité je také sdělit, že nařízení GDPR nestanovuje, kdo by měl vytvoření smlouvy iniciovat, zda správce nebo zpracovatel. Vzhledem k faktu, že za zpracování je zodpovědný správce, tak by právě ten, měl být hlavním iniciátorem. (20)

Povinnosti správce a zpracovatele

Povinnosti stanovuje nařízení GDPR buďto na správce tak zpracovatele stejné, nebo povinnosti vztahující se pouze na správce. (20)

Povinnosti vztahující se na zpracovatele:

- zabezpečení zpracování (viz kapitola 2.2.2.3. Zásady a zákonnost zpracování);
- vedení záznamu o činnostech zpracování;

- jmenování pověřence pro ochranu osobních údajů (viz kapitola 2.2.2.2. Vymezení základních pojmů);
- spolupracovat s dozorovým úřadem;
- doložení souladu s pokyny správce. (20)

Povinnosti vztahující se pouze na správce:

- vyhovění práv subjektů uvedených v nařízení GDPR (viz kapitola 2.2.3. Práva subjektu údajů);
- zabezpečení zpracování (viz kapitola 2.2.2.3. Zásady a zákonnost zpracování);
- vedení záznamu o činnostech zpracování;
- jmenování pověřence pro ochranu osobních údajů;
- spolupracovat s dozorovým úřadem;
- ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu;
- oznámení případů porušení zabezpečení osobních údajů subjektu údajů;
- provedení posouzení vlivu na ochranu osobních údajů;
- doložení souladu s nařízením GDPR. (20)

Povinnost vést záznamy o činnostech zpracování

Jedná se o povinnost, uvedenou v článku 30 nařízení GDPR, která spadá jak na správce tak zpracovatele. Tyto záznamy musejí být vedeny v případě, pokud zpracování osobních údajů splňuje nejméně jednu z níže uvedených podmínek:

- organizace zaměstnává více než 250 zaměstnanců;
- zpracování, které organizace provádí, představuje riziko pro práva a svobody subjektu údajů;
- zpracování zahrnuje zvláštní kategorii osobních údajů;
- zpracování není příležitostné
- zpracovávané osobní údaje se týkají rozsudků v trestních věcech a trestných činů. (20)

Záznamy zpracování vedené **správcem**, popřípadě jeho zástupcem, musejí poskytovat, dle článku 30 nařízení GDPR, všechny níže uvedené informace:

- *jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;*
- *účely zpracování;*
- *popis kategorií subjektů údajů a kategorií osobních údajů;*
- *kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny*
- *informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci;*
- *je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;*
- *je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.* (20)

Záznamy zpracování vedené **zpracovatelem**, popřípadě jeho zástupcem, musejí poskytovat, dle článku 30 nařízení GDPR, všechny níže uvedené informace:

- *jméno a kontaktní údaje zpracovatele nebo zpracovatelů;*
- *jméno a kontaktní údaje správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele;*
- *jméno a kontaktní údaje pověřence pro ochranu osobních údajů;*
- *kategorie zpracování prováděného pro každého ze správců;*
- *informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci*
- *je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.* (20)

V praxi se využívá tabulka, která nese veškeré výše uvedené informace. Veškeré údaje v tabulce obsažené má správce či zpracovatel povinnost uchovávat aktuální.

Povinnost jmenovat pověřence pro ochranu osobních údajů

Povinnost jmenovat pověřence pro ochranu osobních údajů nebo-li DPO (anglicky Data Protection Officer), mají dle článku 37 jak správce, tak zpracovatel, a to v případech, kdy zpracování provádí orgány státní správy s výjimkou soudu. Povinnost se dále

vztahuje na organizace, jejichž **hlavní činností** je **rozsáhlé**, **systematické monitorování fyzických osob** nebo **rozsáhlé zpracování zvláštních kategorií údajů**, či osobních údajů týkajících se rozsudků v trestních věcech a trestných činů. (20)

Často kladené dotazy znějí, co znamená **rozsáhlé**, a co si představit pod pojmem **systematické**. Pracovní skupina 29 vydala stanovisko k těmto pojmům. Skupina uvedla, že do skupiny, která bude mít povinnost, jmenovat vlastního DPO jsou především nemocnice, banky, pojišťovny či poskytovatelé telefonních služeb. Naopak zdravotní ordinace praktického lékaře, tuto povinnost mít nebude, jelikož nezpracovává zvláštní kategorii osobních údajů v tak rozsáhlém měřítku. (30)

Další pojem, který klade otázky je **monitorování chování**. Nařízení GDPR tento pojem objasňuje v bodě 24, který uvádí:

Aby se určilo, zda může být činnost zpracování považována za monitorování chování subjektu údajů, mělo by být zjištěno, zda jsou fyzické osoby sledovány na internetu, včetně případného následného použití technik zpracování osobních údajů, které spočívají v profilování fyzické osoby, zejména za účelem přijetí rozhodnutí, která se jí týkají, nebo za účelem analýzy či odhadu jejích osobních preferencí, postojů a chování. (20)

Pokud organizace není schopna rozklíčovat, zda se na ni povinnost jmenování pověřence vztahuje či nikoli, měla by na základě doporučení pracovní skupiny 29, provést interní analýzu, a tou následně dokládat dozorovému úřadu své rozhodnutí. (30)

Naopak je doporučováno nějakého pověřence ve společnosti mít, i když nařízení tuto povinnost neukládá. V tomto případě se ovšem na tyto dobrovolně jmenované pověřence pohlíží stejně jako na zákonem nařízené. Jsou na ně tedy kladeny stejné povinnosti. Pracovní skupina 29 ovšem doplňuje, že pokud organizace nechce nedobrovolně jmenovat pověřence tak může najmout interního zaměstnance nebo externí konzultanty, kteří sice nebudou v postavení pověřence, ale budou zastávat úkoly související s ochranou osobních údajů. V takovém případě by ovšem mělo být interním

zaměstnancům i veřejnosti sděleno, že taková osoba není v roli pověřence pro ochranu osobních údajů. (30)

V rámci úkolů, které na DPO spadají, jde především o monitorování souladu s nařízením, dále bude mít na starosti řízení činnosti interní ochrany dat (např. přípravu směrnic), bude školit pracovníky, kteří přicházejí do styku s osobními údaji, a v neposlední řadě bude v roli auditora. (20)

Nařízení GDPR uvádí, že v roli pověřence by měla stát osoba, která musí disponovat znalostmi v oblasti ochrany osobních údajů, a musí být schopna plnit úkoly stanovené v článku 39 nařízení GDPR. Úroveň odborných znalostí by se měla odvíjet od složitosti prováděných operací a od druhu a množství zpracovávaných osobních údajů. Nařízení tedy přímo nestanovuje konkrétní požadavky na odbornost pověřenců. Pracovní skupina 29 však uvádí, že pověřenec by měl také rozumět prováděným operacím zpracování, oboru podnikání a informačním technologiím. (20) (31)

Článek 38 nařízení GDPR dále uvádí, že DPO je osoba, která je přímo podřízena nejvýše postavené osobě ve společnosti, a správce ani zpracovatel nesmí této osobě v rámci výkonu činnosti DPO zadávat jakékoliv úkoly. DPO dále nenese zodpovědnost za nesoulad s nařízením a nesmí být v rámci plnění svých úkolů správcem ani zpracovatelem sankciován nebo propuštěn. V praxi to znamená, že DPO může být sankciován i propuštěn ale na základě jiné skutečnosti, například v rámci závažného porušení povinnosti na základě zákona č. 262/2006 Sb. zákoníku práce. (20)

DPO nesmí být v konfliktu zájmu. To znamená, že nesmí vykonávat roli implementátora ochrany osobních údajů, ale může s touto osobou diskutovat o tom jak být v souladu a co pro to musí udělat. To znamená, že to například nemůže být vedoucí IT oddělení, jelikož DPO je osoba, která by jej měla kontrolovat. (32)

Může se jednat i o tým složený z několika DPO či o outsorcovanou službu. Avšak pro účely kontaktní osoby pro dozorový úřad bude vybráno pouze jedno jméno, jako role zástupce DPO pro danou společnost. Nařízení umožňuje i naopak zvolit jednoho

pověřence pro více správců. Takový případ by se právě týkal pověřence dodávaného jako služba externím dodavatelem. (20)

Ohlášení případů porušení zabezpečení

Tato povinnost se týká správce, který má povinnost ohlásit porušení zabezpečení, jehož následkem by mohlo dojít k ohrožení práv a svobod fyzických osob. Správce takovou skutečnost musí ohlásit dozorovému úřadu do 72 hodin, od doby, kdy se o takové události dozvěděl. Ohlášení, tedy nemůže být nepřiměřeně zdržováno činností, která prověřuje, zda k porušení skutečně došlo. Správce musí tedy nakládat s takovou skutečností, že k porušení došlo až do jeho prokázání že k porušení zabezpečení nedošlo. (20) (33)

Pokud je pravděpodobné, že porušení zabezpečení bude vysokým rizikem pro práva a svobody fyzických osob, pak je povinností správce tuto skutečnost oznámit i subjektu údajů a to bez zbytečného odkladu. (20) (33)

Obecné podmínky pro ukládání správních pokut

Nařízení GDPR neponechává pravomoc určení stropních hranic sankcí jednotlivým členským státům, stropní hranice určuje centrálně, tedy pro všechny členské státy rovnocenně. Článek 83, nařízení GDPR, rozděluje udělení výše sankcí do dvou kategorií, a to podle závažnosti incidentu. Nižší výše hranice je vyčíslena na hodnotu do 10 000 000 EUR, nebo 2% celkového ročního obratu, podle toho, která hodnota je vyšší. Vyšší hranice je stanovena na hodnotu do 20 000 000 EUR, nebo 4% celkového ročního obratu, taktéž podle toho, která hodnota je vyšší. Články, které se k těmto sankcím vztahují, jsou ustanoveny v článku 83, nařízení GDPR. Za příklad nejzávažnějšího porušení je považováno porušení zákonnosti zpracování, zásad zpracování či nedodržení náležitostí udělení souladu. (20)

Hranice jsou opravdu vysoké. Článek 83, nařízení GDPR, odst. 1, avšak také uvádí tu skutečnost, že sankce udělované dozorovým úřadem, mají být udělovány tak, aby byly účinné, přiměřené a odrazující nikoliv likvidační. (20)

Členské státy mají pravomoc určit vlastní pravidla toho, zda je možné pokutovat orgány veřejné moci a veřejné subjekty, popřípadě do jaké míry. (20)

2.3 Zhodnocení obecného nařízení GDPR

Nařízení GDPR oproti původní legislativě, zákona o ochraně osobních údajů, znamená pro českou legislativu jisté zpřísnění pravidel a zavádí několik nových povinností, které se na správce a zpracovatele vztahují. Nařízení GDPR v prví řadě rozšiřuje pojem osobní údaj, kdy například výslovně stanovuje, že se může jednat v některých případech o IP adresu nebo využívání protokolu http cookies[13]. Nové právo pro subjekty představuje především právo na přenositelnost osobních údajů či právo být zapomenut. Novou povinností pro správce je hlášení bezpečnostních incidentů do 72 hodin. Novou povinností, jenž se vztahuje pouze na některé správce, se stává jmenovaní pověřence pro ochranu osobních údajů, či provedení posouzení vlivu na ochranu osobních údajů. Výraznou změnou také prošly výše sankcí, které mohou být úřadem pro ochranu osobních údajů uloženy. (1)

[13] http cookie je protokol, který posílá data o uživatelích WWW serveru na jejich prohlížeč. Prohlížeč při opětovném navštívení WWW serveru data posílá zpět. Cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládají se do nich uživatelské předvolby apod. Prostřednictvím cookie je možné postupně zjišťovat zájmy konkrétního návštěvníka, proto představují hrozbu pro soukromí subjektu. (34)

3 ANALÝZA SOUČASNÉHO STAVU

Kapitola se zabývá provedením analýzy současného stavu v organizace Dentalife s.r.o., v oblasti zpracování osobních údajů. V úvodu bude popsáno, jak analýza současného stavu probíhá v praxi při využití externího dodavatele, a jaké činnosti vypracování samotné analýzy předchází. Dále bude popsáno, jaké osobní údaje organizace zpracovává, a budou uvedeny oblasti, ve kterých organizace nezpracovává osobní údaje dle nařízení GDPR.

3.1 Předprojektová fáze

Ke zpracování analýzy současného stavu, dochází na základě poptávky dané organizace. Vytvoření poptávky organizací je aktuálně podporována marketingovými kampaněmi.

V současné době je možné na trhu nalézt různá školení, marketingové kampaně a konference na téma ochrany osobních údajů, které mohou rovněž sloužit organizacím, jako zdroj informací, na základě kterých lze identifikovat nedostatky v zabezpečení osobních údajů.

Možnosti využití zdrojů pro dosažení souladu s nařízením GDPR:

- svépomocí, při využití interních zaměstnanců organizace
- dodáním služby externím dodavatelem

Vzhledem k rozsáhlému výběru různých druhů dostupných materiálů, je možné úspěšnou implementaci nařízení GDPR provést svépomocí, a to při využití interních zaměstnanců. Dané řešení disponuje jak svými výhodami, tak nevýhodami. Výhodou může být ušetření nákladů, které může, ale nemusí být zásadní. Náklad organizace v takovém případě znamená čas pověřeného zaměstnance a vynaložené finanční prostředky na školící kurzy. Další výhodou je znalost interního prostředí organizace a otevřená komunikace s ostatními zaměstnanci v organizaci. Nevýhodou naopak může být organizační slepota, či nedostatečné odborné znalosti, které mají za následek přehlédnutí nebo nevěnování dostatečné pozornosti důležitým oblastem.

Dodání služby analýzy a implementace nařízení GDPR externím dodavatelem je možno realizovat několika odlišnými způsoby. Jedna z možností zahrnuje oslovení dodavatele, který se zákazníkem spolupracuje již delší dobu v oblasti informační bezpečnosti. Jinou možností může být získání dodavatele přes výběrová řízení. V takovém případě jsou kladeny na dodavatele nároky v podobě dodání seznamu referenčních projektů, v oblasti analýzy či implementace nařízení GDPR. Dodavatelské společnosti ovšem ne vždy disponují referencemi na projekty ochrany osobních údajů. Tento fakt je způsoben inovací ze strany EU v oblasti ochrany osobních údajů a časovou náročností obdobných projektů, které dle velikosti organizace mohou dosahovat až k měsíčním časovým horizontům.

Využití externího dodavatele taktéž disponuje výhodami i nevýhodami. Hlavní výhodou je především odbornost pracovníků zabývající se problematikou v oblasti ochrany osobních údajů. Organizace, tak může být obohacena o informace, které by složitě zjišťovala. Jak již bylo řečeno, aktuálně je na trhu mnoho materiálů věnující se danému tématu, ovšem ne vždy jsou uvedeny praktické poznatky celého procesu implementace či analýzy. Jinou výhodou, může být ušetřený čas zaměstnanců dané organizace. Jako nevýhodu je možné uvést neznalost prostředí dané organizace a jejího okolí, kdy je nezbytné znát legislativu, kterou se organizace musí řídit. Jiná nevýhoda by mohla být neochota zaměstnanců poskytnout úplné informace o probíhajících procesech v organizaci a poslední uvedenou bude cena, která může být pro organizaci vysoká.

Následným krokem, po vybrání vhodného dodavatele, je sestavení nabídky. Základní kámen nabídky tvoří cena a termín dodání. Pokud je společnost pro dodavatele nová, je zapotřebí zjistit aktuální stav ochrany osobních údajů v organizaci, z důvodu adekvátního nacenění celého projektu. Jedna z možností je sestavit sadu kontrolních otázek, na které zákazník odpoví. Struktura otázek může vypadat následovně:

- V jakém sektoru se pohybujete? (veřejný sektor, energetika, obchod …)
- Co je předmětem podnikání vaší organizace?
- Jak velká je vaše organizace - její organizační struktura, počet zaměstnanců, počet uživatelů informačního systému?

- Jaký je počet poboček (lokalit)?
- Z kolika právních subjektů se vaše organizace skládá?
- Má některý ze subjektů sídlo mimo EU?
- Zabývali jste se již někdy v minulosti informační bezpečností?
- Existuje popis interních procesů?
- Jaký je objem businessu s fyzickými osobami (řádově počet klientů)?
- Máte zákaznickou linku, online obchodní kanál (eshop, tel. prodej, teleshop…), callcentrum interní/externí?
- Je organizace certifikována dle mezinárodních standardů, případně jakých? ISMS, QMS, …
- Používá vaše organizace externí dodavatele, případně pro jaké účely (správa IT, bezpečnost, externí callcentrum, archiv, …) ?
- Předáváte osobní údaje do zahraničí? Do EU nebo mimo EU?

Akceptací nabídky ze strany zákazníka, se uzavírá předprojektová část a začíná analýza současného stavu.

3.2 Postup analýzy současného stavu

Průběh analýzy bývá ve většině případů obdobný, co se liší, jsou výstupy analýzy. Vzhledem k odlišnosti organizací je možné konstatovat rozdílnou výslednou strukturu analýzy, nicméně v obecné rovině je možné doporučení zde uvedená aplikovat v každém prostředí organizace. Jelikož se prostředí organizace neustále vyvíjí v čase, je nezbytné, aby se analýza zpracování osobních údajů rovněž časem aktualizovala, což inklinuje k cykličnosti celého procesu analýzy.

Po předprojektové fázi, kdy dojde k akceptaci nabídky ze strany zákazníka, je z pravidla uskutečněna úvodní schůzka se zákazníkem. Na této schůzce jsou sděleny informace sloužící k bližšímu poznání organizace. Na základě těchto informací je v první řadě sestaven harmonogram jednotlivých dílčích činností prováděné analýzy. Jednou z těchto činností je provedení interview sloužících primárně ke zhodnocení současného stavu v organizaci. Interview slouží k tomu, aby jednotliví pracovníci sdělili dodavateli, jakým způsobem probíhá zpracování osobních údajů na jejich oddělení. Aby dodavatel

získal správné informace, je doporučováno provést úvodní školení všech zúčastněných respondentů. Pokud by byl tento krok vynechán, mohlo by dojít k neúplnému sdělení informací směrem od pracovníka, a tím pádem i k neúplné analýze současného stavu.

Jednotlivá Interview probíhají po jednotlivých odděleních. Důvodem je návaznost probíhajících procesů a vnesení řádu do průběhu analýzy. Interview se účastní z pravidla vedoucí zaměstnanec, který má přehled o probíhajících procesech.

Na základě zjištěných informací z interview bude vypracován dokument, nesoucí informace o přehledu zpracování osobních údajů, který po jeho odsouhlasení organizace bude sloužit jako jeden z podkladů pro vytvoření rozdílové analýzy a návrhu opatření, které bude nutné uskutečnit, pro realizaci stavu, slučujícího se s požadavky nařízení GDPR.

Následující obrázek č. 1 zobrazuje řetězec navzájem navazujících činností a výstupů z nich, které je nutné provést pro zjištění současného stavu ochrany osobních údajů v organizaci, při využité externího dodavatele.

Obrázek č. 1: Řetězec činností provázejících analýzu současného stavu

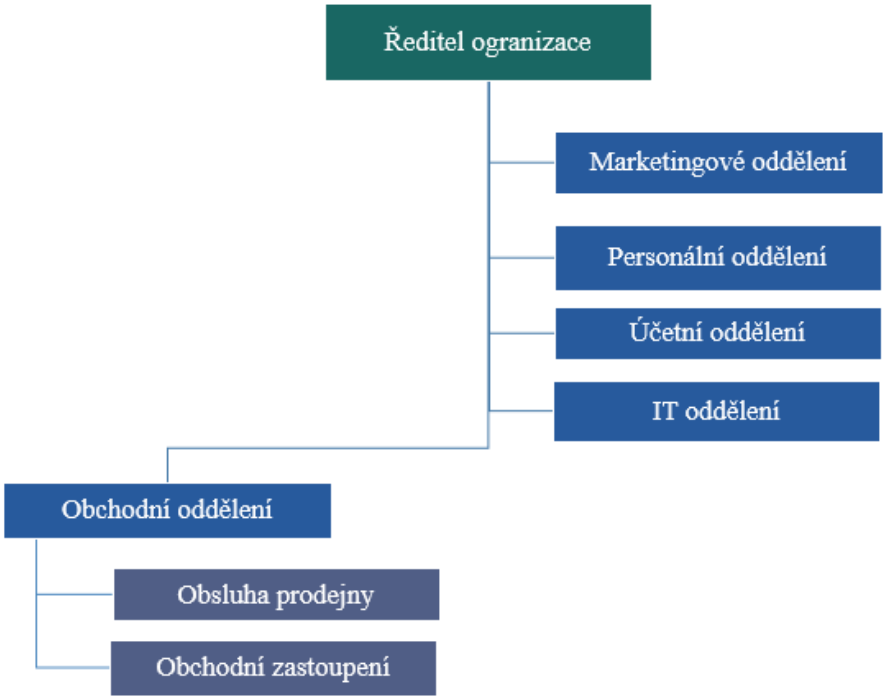
(Zdroj: vlastní zpracování)

3.3 Analýza současného stavu v organizaci Dentalife s.r.o.

Podkapitola se věnuje provedením analýzy současného stavu v organizaci Dentalife s.r.o.. Budou zde zachyceny veškeré procesy, u kterých dochází ke zpracování osobních údajů. Organizace se rozhodla pro provedení analýzy současného stavu, využít služeb externího dodavatele. Interview budou probíhat po jednotlivých odděleních s vedoucími pracovníky, z důvodů přehlednosti a systematičnosti celé analýzy. Dále budou jednotlivá interview realizována pouze na Brněnské pobočce, jelikož se zde nacházejí veškeré procesy, které probíhají i na ostatních pobočkách stejně.

3.3.1 Charakteristika organizace

Společnost Dentalife s.r.o. se zabývá prodejem zboží pro zubaře a dentální hygienisty. V rámci této služby má zavedený e-shop. Sídlo společnosti funguje jako možnost kontaktního místa, kde je možné některé produkty si vyzkoušet. Ordinace dentálních pracovníků navštěvuje obchodní zástupce v rámci nabídky za cílem zvýšení prodeje. Společnost zaměstnává celkem 20 zaměstnanců na 3 pobočkách. Organizační struktura organizace je znázorněna následujícím schématem.



Obrázek č. 2: Organizační schéma organizace Dentalife s.r.o.

(Zdroj: vlastní zpracování)

Personální obsazení jednotlivých poboček, ve společnosti Dentalife s.r.o. je následující:

Pobočka Brno

Brněnská pobočka je organizačně složena z jednatele společnosti, marketingového manažera, asistentky prodeje, personalisty, pracovníka účtárny, Brněnská pobočka je organizačně složena z , IT specialisty (admin[14]).

Pobočka Praha

Pražská pobočka je organizačně složena z asistentky prodeje, tří obchodních zástupců a dvou pracovníků obsluhy prodejny.

Pobočka Plzeň

Plzeňská pobočka je organizačně složena ze dvou obchodních zástupců a jednoho zaměstnance, pracujícího na pozici obsluha prodejny.

3.3.2 Personální oddělení

Společnost Dentalife s.r.o. provádí v rámci personálního oddělení níže uvedené aktivity:

- Vyhledávání a nábor zaměstnanců
- Kopírování a zpracování dokumentů
- Školení řidičů, BOZP a PO
- Přidělení benefitů zaměstnancům
- Monitorování služebních počítačů a služebních vozů
- Provozování kamerových systémů

Vyhledávání a nábor zaměstnanců

Vyhledávání zaměstnanců je realizováno prostřednictvím několika různých technik, se společným cílem, a to přijetí nového zaměstnance. Tento soubor technik, může být

[14] Administrátor nebo-li admin je osoba, která spravuje počítačovou síť, servery, síťové tiskárny, a jiné síťové prvky.

dále rozšířen o specifické techniky vyhledávání, jako jsou cílené oslovování potenciálních zaměstnanců na základě doporučení.

Pro nábor zaměstnanců společnost využívá:

- Webový portál LinkedIn.com
- Webový portál Jobs.cz
- Své vlastní webové stránky
- Doporučení interních zaměstnanců
- Personální agenturu

Webový portál LinkedIn

Kandidáty na tomto portálu, personální pracovník organizace, aktivně vyhledává. Personalista si ukládá odkazy vhodných kandidátů na server společnosti. Vybrané kandidáty kontaktuje přímo přes server LinkedIn.

Webový portál Jobs.cz

Uchazeči se sami ozývají na zveřejněné telefonní číslo či pošlou životopis na email personalisty, ze kterého nejsou mazány. Firemní email má personalista pouze jeden. Souhlas se zpracováním osobních údajů není vyžadován. Vybrané životopisy se ukládají na interní server, kde jsou uloženy po různě dlouhou dobu.

Personální agentura

Personální agenturu společnost využívá jen při výjimečných případech. Pokud se tak už stane, dochází k podepsání smlouvy o zprostředkování vyhledání zaměstnance.

Personální agentura pro vyhledávání nových potenciálních zaměstnanců využívá svoji databázi klientů, či profesní portály jako je Jobs nebo LinkedIn. Personální agentura na základě požadavků společnosti zasílá nejdříve životopis, na jehož základě se personalista organizace rozhoduje, zda si kandidáta pozve na pohovor.

Životopisy nepřijatých kandidátu jsou uloženy ve složce na interním serveru, kde jsou uloženy neomezeně, pro případ že by organizace opět hledala podobného kandidáta.

U všech výše uvedených technik personalista organizace přeposílá získané životopisy uchazečů, kteří budou přizváni na pohovor, řediteli organizace prostřednictvím firemního emailu. Při fyzickém pohovoru si pak životopis vytiskne a použije jej pro psaní poznámek při fyzickém setkání s uchazečem, a založí si jej do vlastní složky, odkud se údaje nemažou. V případě přijetí uchazeče, pak jeden výtisk založí do jeho osobní složky. Dokument v elektronické podobě je uložen na serveru ve složce personalisty, kam mají přístup všichni zaměstnanci. Dokumenty se z této složky nevymazávají. S personální agenturou má společnost podepsaný kontrakt, kde se zavazuje použít informace uchazeče pouze pro účely náboru.

Kopírování a zpracovávání dokumentů

V rámci procesu přijetí nových zaměstnanců, personalista vyžaduje po zaměstnanci dokumenty, které následně zakládá do jeho osobní složky. Obsah složky je následující:

- kopie občanského průkazu
- vyplněný osobní dotazník (obsahuje informace o zaměstnanci)
- profesní životopis
- kopie dokladu o dosaženém vzdělání
- zápočtový list od předchozího zaměstnavatele
- lékařský posudek o zdravotní způsobilosti

Do této složky pak zakládá dokumenty, které vznikají již při trvání pracovního poměru:

- mzdový výměr
- pracovní smlouva
- prohlášení poplatníka
- odpovědnost za svěřené věci (počítač, telefon)
- školení řidičů
- školení PO a BOZP

Personalista výše uvedené dokumenty zakládá do složky zaměstnance, která je v papírové podobě uložena v pořadači na účetním oddělení. Fyzická složka se nachází v zamčené plechové skříni na účetním oddělením. Do této skříně mají přístup pouze účetní společnosti. Účetní oddělení je dále zabezpečeno uzamykatelnými dveřmi, které

jsou v době nepřítomnosti zaměstnanců uzamčeny. Přístup do těchto prostor mají účetní, asistentka, a uklízečka. Samotná účtárna se dále nachází za zamčenými hlavními dveřmi společnosti, které je možné odemknou čipovou kartou nebo fyzicky klíčem. Od těchto dveří mají kartu všichni zaměstnanci společnosti, uklízečka a správce/majitel budovy. Složky se nelikvidují. Ve skříni jsou složky všech bývalých i přítomných zaměstnanců.

Odpovědnost zaměstnance ohledně ochrany osobních údajů není formálně definována ani ustanovena.

Bezpečnost práce, požární ochrana a školení řidičů

BOZP, PO a školení řidičů společnost provádí prostřednictvím agentury. Společnost má nainstalovaný software, přes který se provádí školení. Software zaměstnanci vygeneruje potvrzení o uskutečnění školení, které podepíše, a odnese personalistovi. Personalista následně založí dokument do složky zaměstnance. Jednou ročně prostory navštěvuje pracovník agentury, který se aktivně zajímá o bezpečnost práce a zkoumá pracovní podmínky.

Benefity

Organizací jsou zaměstnancům poskytnuty následující benefity:

- multisport karta
- služební mobilní telefon
- služební mobilní tarif
- služební počítač

Zaměstnanec, pokud má zájem čerpat benefit v podobě multisport karty, ohlásí tuto skutečnost personalistovi organizace. Personalista se po té domluví s agenturou, která karty poskytuje. Agentura po společnosti požaduje jméno, příjmení a datum narození zaměstnance. Poskytnutí informací probíhá prostřednictvím firemního emailu. Následně agentura vydá kartu a zašle ji poštou na brněnskou pobočku. Účetní sepíše se zaměstnancem nový mzdový výměr, jelikož kartu společnost hradí jen z části, a kartu mu následně předá.

Dále mají pracovníci možnost využít služební mobilní telefony se služební SIM kartou a počítače. Pracovníci využívají firemní tarif. V rámci vyúčtování, je využíváno elektronické zasílání výpisů hovorů všech firemních čísel. Se zaměstnancem je při předání podepsán předávací protokol, který je založen do jeho osobní složky.

Monitoring

Organizace realizuje provozní a bezpečnostní monitoring prostřednictvím softwarových a hardwarových nástrojů. Tyto nástroje jsou dodávány a spravovány externí společností, která se na daný typ monitoringu specializuje. V rámci organizace je použit následující monitoring:

- monitoring firemních počítačů
- monitoring služebních vozů
- kamerový systém

Monitoring firemních počítačů

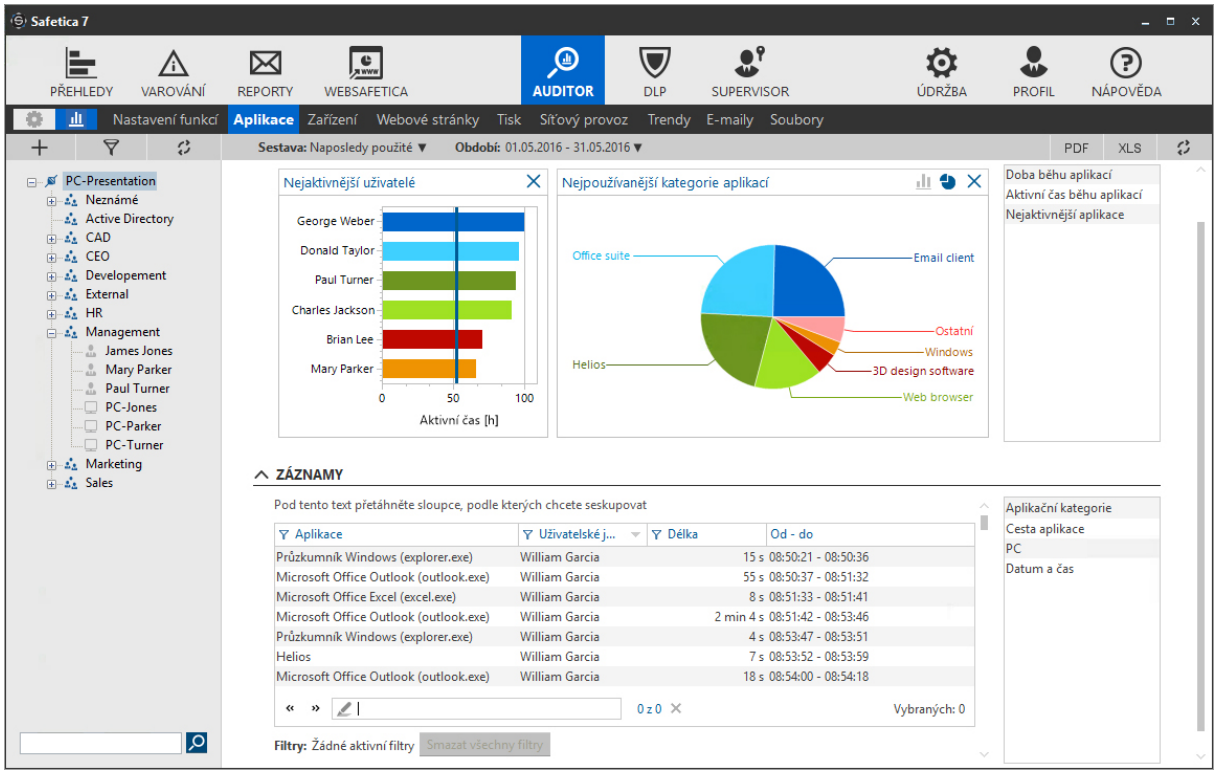
Společnost monitoruje **činnost na firemních počítačích svých zaměstnanců**. Pro tuto činnost používá software Auditor od společnosti Safetica. Tento software monitoruje činnosti zaměstnanců na webových stránkách, aplikacích, tiskárnách, poskytuje informace o přijatých a odeslaných emailech či souborech. Společnost se v rámci využívání daného softwaru, snaží sledovat produktivitu zaměstnanců ve své organizaci a mít přehled nad pohybem firemních dokumentů. Zároveň společnost uvádí informaci, že svým zaměstnancům dala svolení pro užívání počítače a telefonu pro soukromé účely. Zaměstnanci o provádění monitoringu nejsou informováni.

Program v rámci prohlížení internetových stránek poskytuje informace o jménu uživatele, čísle zařízení, doméně, titulku stránky, URL, délce návštěvy a čase ve formě od-do. Tyto získané údaje, jsou dále vyhodnocovány zaměstnanci oddělení IT.

V případě tisku dokumentů na firemní tiskárně, program poskytuje informace o jménu uživatele, celém názvu dokumentu, celkový počet stran, barvu tisku, velikost papíru,

název zařízení, aplikaci, datum a čas tisku. Sledování tisku, je zřízeno pro účely řízení materiálových kapacit.

Přístup do programu má ředitel organizace a IT oddělení. Ředitel prostřednictvím daného nástroje kontroluje produktivitu svých zaměstnanců. Monitoring služebních vozů byl zařazen pod personální oddělení, jelikož se jedná o monitoring činnosti lidských zdrojů.



Obrázek č. 3: Náhled monitorovacího nástroje

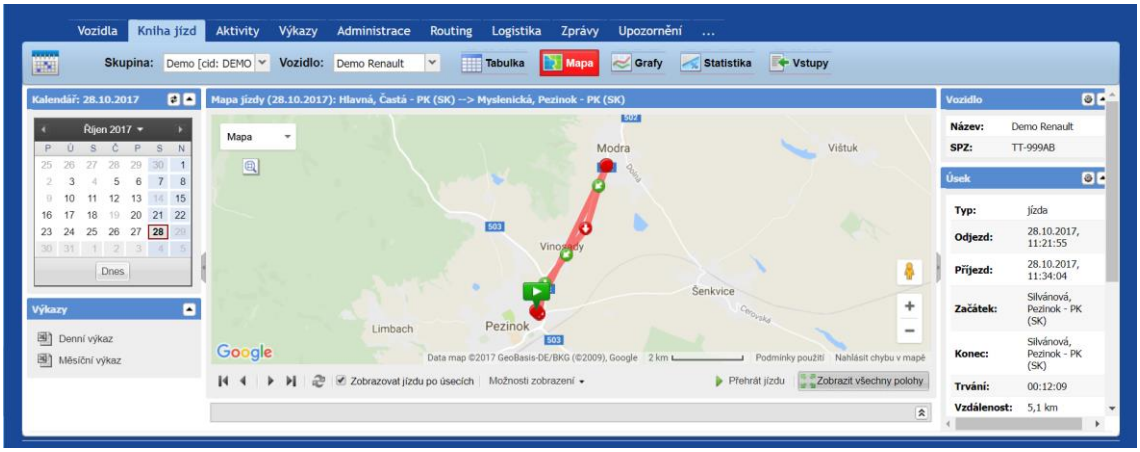
(Zdroj: Upraveno autorem, 34)

Obrázek náhled monitorovacího nástroje znázorňuje ukázku monitorovacího programu od společnosti Safetica, zavedený ve společnosti Dentalife s.r.o.. Tento monitorovací program dokáže vygenerovat veškeré činnosti subjektů na jejich počítačích.

Monitoring služebních vozů

Společnost provádí monitoring **pohybu služebních vozů**. Každý obchodní zástupce má svůj vlastní služební vůz, který používá i pro své soukromé účely. Zaměstnanci jsou

o monitorování vozidel informováni ve smlouvě a mají možnost si sledování vypnout při užití vozu pro soukromé účely. Společnost tak činní, z důvodu neustálého přehledu o nákladech na své podnikání a kontrolu nad výkazem pouze služebních cest.



Obrázek č. 4: Ukázka zobrazení monitorovacího programu

(Zdroj: vlastní úprava, 35)

Kamerové systémy

Společnost využívá na všech svých pobočkách **kamerové systémy**, konkrétně v prostoru skladu, prodejny, a v prostorách před budovou. Činní tak především, z důvodů předcházení krádežím ze strany zaměstnanců či zlodějů. Jelikož se jedná o drahé dentální přístroje, vyslovila pojišťovna při pojištění prostor podmínku, že prostory musí být monitorovány. Zaměstnanci jsou ústně informováni o všech kamerách, které v prostoru jsou. Kamery nejsou registrovány ani označeny.

3.3.3 Účetní oddělení

Účetní oddělení je umístěno v budově společnosti v Brně. Místnost je oddělena dveřmi a veškeré doklady jsou při nepřítomnosti účetních zamčené v plechové skříni, do nichž má přístup pouze účetní organizace. Klíče od účtárny vlastní účetní, asistentka prodeje a uklízečka.

V kanceláři účetní se nachází osobní složka zaměstnance, kam účetní zakládá listiny vzniklé na základě její činnosti. Konkrétně se jedná o pracovní smlouvu, mzdový výměr

a prohlášení poplatníka. Dále do složky zakládá ostatní dokumenty, které jí poskytne personální pracovník. Do této složky má přístup pouze účetní. Dokumenty se v této složce nelikvidují.

Účetní oddělení má na starosti jak veškerou mzdovou agendu, tak i samotné vedení účetnictví celé organizace.

Účetní v rámci zpracování mezd využívá online docházkový systém, ve kterém zaměstnanec vyplní dny, kdy byl přítomen na pracovišti, popřípadě si přes něj může zažádat o dovolenou. Účetní následně obdrží informace o odpracovaných dnech. K těmto informacím se dostane po přihlášení do systému. Konkrétně se zobrazuje jméno, příjmení, interní číslo a počet odpracovaných dnů za předcházející měsíc. Osobní údaje v daném programu jsou aktuálně uloženy po dobu tří let, jedná se o dobu, po kterou organizace software využívá. Přístup ke zmiňovanému výstupu ze systému má pouze účetní.

Účetní dále odvádí zákonné pojistné zdravotním pojišťovnám a správě sociálního zabezpečení. Odvádí daň z příjmu sociálnímu úřadu, popřípadě uskutečňuje další srážky ze mzdy (multisport karta, půjčky...).

V rámci vedení účetnictví účetní vydává a přijímá faktury. Tyto faktury se nacházejí v uzamčených skříních na daném oddělení. Aktuálně jsou zde uloženy veškeré faktury od založení společnosti, tedy 7 let. Faktury se vystavují na základě informací z účetního softwaru PEDRO, vytvořeného podniku na míru. Účetní zde vidí informace o objednávkách, na základě kterých vystavuje faktury a rozesílá je emailem klientům. Ručně pak mění stav na nezaplacen/zaplacen. Do systému má neomezený přístup. Vidí tedy jméno, příjmení, emailovou adresu, adresu doručení, fakturační adresu, číslo účtu, částku, datum platby, datum objednávky, stav objednávky, množství, název zboží, kód zboží, způsob dopravy, poznámky. Informace z PEDRA se nemažou. Faktury jsou generovány automaticky. Systém disponuje automatickým zasíláním faktur, nicméně tato funkcionalita není využívána. Zasílání faktur probíhá se součinností účetního, který povolí odeslání zálohové faktury, nebo daňového dokladu. V době nepřítomnosti účetní má tato práva obchodní asistentka a ředitel společnosti.

3.3.4 Obchodní oddělení

Společnost Dentalife s.r.o., se zabývá prodejem vybavení pro zubní ordinace. V rámci prodeje je zastupována obchodníky, kteří jsou fyzicky přítomni na prodejnách a obchodními zástupci, kteří se věnují klientům přímo v jejich ordinacích či na jiných pracovištích.

Obsluha prodejny

Pracovníci, pracují na prodejnách, jsou zaměstnanci na hlavní pracovní poměr. Jejich náplní práce je péče o příchozí zákazníky na prodejnu a mimo jiné, i vyřizování objednávek, reklamací, řízení skladových zásob či komunikace s dodavateli a odběrateli.

Pro práci využívají software PEDRO, se kterým pracuje i účetní oddělení v rámci fakturace objednávek. Tento systém obchodníkům umožňuje:

- vedení databáze zákazníků;
- řízení objednávek;
- řízení reklamací;
- řízení skladových zásob.

Vedení databáze zákazníků

Vedení databáze zákazníků je realizováno prostřednictvím softwaru PEDRO. Software umožňuje shromažďovat, třídit a zpracovávat údaje o zákaznících, především jejich kontakty, probíhající obchodní procesy a dosahované tržby. V evidenci je zaznamenáno (jméno, příjmení, IČO, DIČ, sídlo či trvalá adresa, email, telefonní kontakt, přidělený obchodní zástupce, výše nastavené slevy, možnost nákupu na fakturu). Osobní údaje zákazníků ze softwaru nejsou mazány.

Řízení objednávek

Obsluha prodejny má v rámci softwaru PEDRO přístup k veškerým informacím o nákupech zákazníka (jméno, příjmení, fakturační adresa, adresa doručení, kontaktní informace, IČO, DIČ, druh objednaného zboží, množství, cena, číslo bankovního účtu, stav objednávky čeká na platbu/ zaplaceno/ odesláno/ reklamace/ změna). Osobní údaje

zákazníků a informace o jejich nákupech nejsou ze softwaru mazány.

Objednávku je možné zaplatit předem na bankovní účet, dále při převzetí zboží na prodejně či dopravní společnosti. Poslední možností je platba na fakturu se 14cti denní splatností.

V případě nezaplacení, software automaticky vygeneruje a zašle připomínkový email objednavateli. Pokud se jedná o platbu předem, objednávka se automaticky stornuje po uplynutí deseti pracovních dní od vytvoření objednávky. Pokud se jedná o nezaplacenou platbu na fakturu, řeší ji následně obchodník osobně.

Řízení reklamací

Reklamace jsou řízeny obsluhou prodejny. Zboží je možné vrátit do 14cti dní od jejich doručení zákazníkovi. Pokud k takové reklamaci dojde, pak jsou zákazníkovi automaticky vráceny peníze, z pravidla do tří pracovních dnů. Postup je takový, že zákazník vyplní reklamační formulář (obsahuje jméno, příjmení, adresu, číslo objednávky, číslo zboží, název zboží, počet kusů, popis vad) který najde na webu organizace a zašle elektronicky jeho scan či jej pošle poštou zároveň se zbožím. Z pravidla jej zákazníci posílají i elektronicky i v papírové podobě. Formuláře jsou oscanovány a nahrány do systému k objednávce. Fyzicky se zakládají do šanonu. Nic ze systému se nemaže ani neskartuje v případě papírové formy. Pokud je na zboží nějaká vada, kterou je nutné řešit s výrobcem, pak obsluha prodejny kontaktuje výrobce a problém s ním řeší. Veškerá zjištění se zapisují opět do poznámek k objednávce. Zákazník je kontaktován emailem či telefonem o stavu reklamace.

Řízení skladových zásob

Software PEDRO je přímo navázán na e-shop. To znamená, že pokud objednané zboží není k dispozici, uvidí to jak zákazník na e-shopu tak obchodník v systému PEDRO. Pokud se však stane, že zákazník vytvoří objednávku nedostupného zboží, pak systém automaticky zašle informaci ohledně nedostupnosti. Zároveň však dojde toto upozornění obsluze prodejny, která zákazníka kontaktuje emailem či telefonem o možnostech nákupu jiného zboží či dostupnosti již objednaného zboží. Veškeré

poznámky se zaznamenávají do systému k objednávce.

Objednávky od dodavatelů jsou do programu PEDRO zadávány ručně obsluhou prodejny. Obsluha prodejny má na starosti expedici zboží a přijímání plateb na prodejně. Obsluha prodejny potenciální zákazníky neoslovuje.

Obchodní zástupci

Obchodní zástupci nejsou zaměstnanci společnosti. Jsou to osoby samostatně výdělečně činné (OSVČ). Sami oslovují potenciální zákazníky.

Kontakty vyhledávají na internetu. Ve většině případů se jedná o webové stánky ordinace nebo zubního specialisty či internetové databáze nabízející informace o specialistech dle lokalit. Kontakty následně oslovují, ve většině případů telefonicky. Oslovení zákazníci, u nichž se nepodařilo prodej uskutečnit, jsou zaznamenáváni do softwaru PEDRO, aby se nestalo, že zákazník bude osloven vícekrát v krátkém časovém horizontu. O těchto subjektech je vedena databáze, která obsahuje informace o osobě, která subjekt kontaktovala, osobní údaje subjektu (jméno, příjmení, jméno organizace, adresa, adresa, IČO, DIČ, telefonní kontakt) a poznámky.

Do systému PEDRO mají přístup všichni zaměstnanci a obchodní zástupci organizace. Všichni mají stejný náhled. Systém je zaveden od roku 2012. Od jeho zavedení se z něj nic nemazalo. Fyzicky jsou drženy reklamační formuláře, které jsou umístěny v kanceláři, v poličce. Nachází se tam všechny, které za dobu existence organizace vznikly, nic se neskartuje. Veškeré faktury se nachází na účetním oddělení.

3.3.5 Marketingové oddělení

Společnost zaměstnává jednoho manažera, který má na starosti veškerou marketingovou činnost. Jeho hlavní činností je editace na webu společnosti, jehož součástí je e-shop. Webové stránky mají aktivní http cookie, jenž si ukládá informace ohledně přihlášení uživatele, historii zobrazených produktů a nákupní košík. Návštěvník webových stránek je o využívání http cookie informován při vstupu na www stránky. Sledování http cookie nemá možnost odmítnout, pouze přijmout.

Dáje je prováděn přímý marketing, kdy manažer rozesílá zákazníkům emailem pozvánky v rámci promoakcí, upozornění na slevy, novinky, bestsellery. Jako podklad pro tvorbu přímého marketingu využívá program PEDRO a informace z http cookie. O této skutečnosti nejsou zákazníci informováni.

V rámci organizace promo akcí, jsou rozesílány emailové pozvánky subjektům, které určí obchodníci, obsluha prodejny či ředitel společnosti. Může se jednat, jak o stále zákazníky, tak potenciální nové. Manažer subjektům zašle pozvánku a poprosí o potvrzení účasti. Účast subjektů na promo akcích je zaznamenávána do excel tabulky umístěné po neomezenou dobu na serveru organizace. Organizace nedisponuje dokumentem, který by uděloval souhlas se zpracováním pro takovou činnost.

3.3.6 Vedení organizace

Ředitel organizace má neomezené přístupy na server organizace, do systému PEDRO, monitorovacích programů a ke kamerovým záznamům.

3.4 Zhodnocení současného stavu v organizaci Dentalife s.r.o.

Na základě poznámek z provedené analýzy vznikl dokument, který poskytuje informace o současných činnostech zpracování. Níže je uveden ve zkrácené verzi (Tabulka č. 1). Plná verze je obsažena v příloze č. 3. Účelem dokumentu je na jednom místě přehledně identifikovat účely zpracování, zákonnost zpracování, tedy z jakého právního titulu organizace zpracovává osobní údaje dle nařízení GDPR. Dále identifikuje, jaké konkrétní osobní údaje jsou o subjektu sbírány (dataset), jednotlivé kategorie subjektů údajů, dobu zpracování či identifikuje možné příjemce osobních údajů. Dokument, je jednou z povinností uvedených v nařízení GDPR, které organizace musí vést a udržovat aktuální. (20)

Tabulka č. 1: Záznam o činnostech zpracování

Účel zpracování	Zákonnost zpracování/ právní titul	Dataset	Subjekty zpracování	Doba zpracování
Nábor zaměstnanců	Smlouva	Jméno, příjmení, trvalá adresa, datum narození, email, telefon, vzdělání, pracovní zkušenosti	Uchazeč o zaměstnání	Neomezená
Vedení personální agendy	Smlouva	Jméno, příjmení, trvalá adresa, datum narození, email, telefon, vzdělání, pracovní zkušenosti, místo narození, rodné číslo, číslo účtu,	Zaměstnanec	Neomezená
Provedení školení	Zákon	Jméno, příjmení, společnost	Zaměstnanec	Neomezená
Poskytnutí benefitu zaměstnanci	Smlouva	Jméno, příjmení, datum narození, trvalá adresa, telefonní číslo	Zaměstnanec	Neomezená
Zpracování mezd, výplata mezd	Zákon Oprávněný zájem	Jméno, příjmení, adresa trvalého bydliště, rodné číslo, variabilní symbol od sociálního úřadu, datum narození, pohlaví, občanství, zdravotní pojišťovna, počet dětí a jejich rodné číslo, bankovní spojení	Zaměstnanec	Neomezená
Srážky ze mzdy za zdravotní a sociální	Zákon	Jméno, příjmení, adresa trvalého bydliště, rodné číslo, variabilní symbol od sociálního úřadu, datum narození, pohlaví, občanství, zdravotní pojišťovna, počet dětí a jejich rodné číslo, bankovní spojení	Zaměstnanec	Neomezená
Zpracování cestovních příkazů	Zákon	Jméno, příjmení	Zaměstnanec	Neomezená

Zpracování účetních dokladů, zpracování podkladů pro fakturaci	Zákon	Jméno, příjmení, trvalá adresa, IČO, DIČ, rodné číslo	Zaměstnanec Zákazník Dodavatel	Neomezená
Archivace účetních dokladů	Zákon	Jméno, příjmení, trvalá adresa, IČO, DIČ, rodné číslo, datum narození	Zaměstnanec Zákazník Dodavatel	Neomezená
Objednávka	Smlouva Oprávněný zájem	Jméno, příjmení, společnost, trvalá adresa, telefonní kontakt, email	Zákazník Oslovený potenciální zákazník Dodavatel	Neomezená
Marketing	x	Jméno, příjmení, společnost, email	Zákazník Potenciální zákazník	Neomezená
Registrace	Oprávněný zájem	Jméno, příjmení, email, společnost, trvalá adresa, telefonní kontakt	Zákazník Potenciální zákazník	Neomezená
Monitoring	x	Jméno, příjmení	Zaměstnanec	Neomezená

(Zdroj: vlastní zpracování)

V průběhu provedení analýzy současného stavu, byly také zaznamenány oblasti, ve kterých organizace nedodržuje náležitosti jak ustanovené v zákoně o ochraně osobních údajů, tak náležitosti uvedené v nařízení GDPR. V režimu poznámek vznikl seznam oblastí, které bude nutné uvést do souladu s nařízením GDPR. Seznam nálezů a poznámky z interview jsou nositelem informací pro sestavení diferenční analýzy (GAP analýzy), která bude uvedena v návrhové části práce.

Při analýze současného stavu, prováděné na **personálním oddělení**, byly zjištěny následující nedostatky:

Tabulka č. 2: Seznam nálezů na personálním oddělení

Nález
• Uchazeči o zaměstnání nejsou řádně informováni o zpracování osobních údajů.
• Dokumenty obsahující osobní údaje jsou zpracovávány po delší dobu, než je potřebné k jejich účelu.
• Chybí zákonnost zpracování v rámci uchovávání životopisů uchazečů o zaměstnání.
• Nejsou dodrženy zásady zpracování při uchovávání životopisů uchazečů o zaměstnání.
• K životopisům uchazečů o zaměstnání mají přístup neoprávněné osoby.
• Není řádně podepsána zpracovatelská smlouva se zpracovateli osobních údajů.
• Je prováděno nezákonné kopírování občanských průkazů.
• Není provedeno organizační opatření při zpracování osobních údajů.
• Zaměstnanci nejsou informováni o prováděném monitoringu služebních počítačů.
• Organizace není schopna prokázat informovanost zaměstnanců v rámci využití kamerových systémů, monitoringu služebních počítačů či vozů.
• Monitoring služebních počítačů je prováděn v rozsahu, ve kterém postrádá zákonnost zpracování.
• S obchodními zástupci nejsou podepsány pracovní smlouvy, které by obsahovaly náležitosti uvedené v nařízení GDPR.
• V pracovních smlouvách chybí náležitosti týkající se organizačních opatření, na základě kterých by došlo k předcházení incidentů v rámci nakládání s osobními údaji.

(Zdroj: vlastní zpracování)

Při analýze současného stavu, prováděné na **účetním oddělení**, byly zjištěny následující nedostatky:

Tabulka č. 3: Seznam nálezů na účetním oddělení

Nález
• Osobní údaje obsažené na účetních, mzdových a daňových dokladech jsou zpracovávány po dobu delší, než je nezbytně nutná k jejich účelu.

(Zdroj: vlastní zpracování)

Při analýze současného stavu, prováděné na o**bchodním oddělení**, byly zjištěny následující nedostatky:

Tabulka č. 4: Seznam nálezů na obchodním oddělení

Nález
• **Zpracovávané osobní údaje obsaženy v systému PEDRO, emailové komunikaci pracovníků a na listinných dokumentech, jsou zpracovávány po dobu delší, než je nezbytně nutná k jejich účelu.**
• **Pracovníci disponují širšími právy přístupu, než je nezbytné pro výkon jejich pracovní náplně.**
• **Zákazníci nejsou řádně informování o zpracování osobních údajů.**
• **S obchodními zástupci nejsou podepsány pracovní smlouvy, které by obsahovaly náležitosti uvedené v nařízení GDPR.**

(Zdroj: vlastní zpracování)

Při analýze současného stavu, prováděné na **marketingovém oddělení**, byly zjištěny následující nedostatky:

Tabulka č. 5: Seznam nálezů na marketingovém oddělení

Nález
• Organizace nedisponuje udělenými souhlasy v rámci provádění profilování, na základě kterého jsou zasílány informace o produktech

• Organizace zpracovává databáze svých zákazníků po neomezeně dlouhou dobu
• Subjekty nejsou řádně informováni o zpracování osobních údajů na základě funkce http cookies
• Subjekty nejsou řádně informování o zpracování osobních údajů v rámci odeslané objednávky

(Zdroj: vlastní zpracování)

Při analýze současného stavu, prováděné v organizaci Dentalife s.r.o., byly zjištěny, krom již výše uvedených, následující nedostatky:

Tabulka č. 6: Seznam nezačleněných nálezů v organizaci

Nález
• Organizace nemá zavedené procesy, které by vedly k plnění práv subjektů údajů (právo na přístup, právo na výmaz, právo na opravu, právo na omezení zpracování, právo na přenositelnost, právo vznést námitku)
• Organizace nemá zavedené procesy, na jejichž základě by byla připravena reagovat na případná narušení bezpečnosti osobních údajů, dle požadavků nařízení GDPR.
• Zaměstnanci organizace nejsou dostatečně seznámeni s legislativou, pravidly a postupy v oblasti ochrany osobních údajů.
• Není zajištěno udržování souladu s nařízením GDPR (do budoucna) ve společnosti

(Zdroj: vlastní zpracování)

4 VLASTNÍ NÁVRHY ŘEŠENÍ

Kapitola je věnována konkrétním návrhům řešení, jednotlivých nálezů, které byly identifikovány na základě analýzy současného stavu. Nálezy zde budou popsány a také bude uveden možný návrh či návrhy jejich řešení. Následně bude vybráno jedno konkrétní řešení a odůvodněno, proč bylo zvoleno právě ono včetně jeho časové a finanční náročnosti. Kapitola bude členěna dle oddělení a činností zpracování stejně jako tomu bylo v analýze současného stavu. Důvodem je zachování stejné struktury celé práce.

4.1 Personální oddělení

Podkapitola se věnuje širšímu rozvoji nálezů, které byly identifikovány v analýze současného stavu na personálním oddělení a návrhům jejich možného řešení včetně výběru finálního doporučení a jeho odůvodnění.

Nálezy v oblasti vyhledávání a nábor zaměstnanců

Organizace v rámci činnosti vyhledávání nových zaměstnanců, není v souladu s nařízení GDPR, hned v několika jeho částech. Životopisy nepřijatých uchazečů jsou zpracovávány po dobu delší, než je potřebná k jejich účelu, jenž byl nábor nového zaměstnance. Pokud by si organizace chtěla životopisy nepřijatých uchazečů ponechat, pro účely vypsání podobné pozice v budoucnu a oslovení daného kandidáta, pak by takové zpracování možné bylo, ale pouze po dobu ne delší než půl roku. Jedná se o dobu, která odpovídá účelu daného zpracování a zároveň není porušena zásada přesného a aktualizovaného zpracování. Jedná se o dobu, ve které je velmi pravděpodobné, že daný uchazeč již práci našel, proto není nutné takové osobní údaje dále uchovávat. Pokud by ovšem organizace přesto chtěla životopisy kandidátů uchovávat po dobu delší, musela by si opatřit pro takové zpracování souhlas, aby byla splněna zákonnost zpracování. Je také nezbytné podniknou opatření, na základě kterého se nebude stávat, že životopisy budou uloženy v emailových schránkách pracovníků a nebudou z emailů mazány. V takovém případě lze životopisy, v případě nutného rozesílání mezi zaměstnance organizace, umístit na server organizace a zasílat pouze

odkaz na uložiště. Organizace tak získá kontrolu nad prováděným zpracováním a nebude muset periodicky upozorňovat zaměstnance, aby si promazaly své emailové schránky.

Organizace má velké nedostatky především v organizačních opatřeních zabezpečení zpracování. Zaměstnanci disponují neomezenými přístupy k osobním údajům, především k životopisům uchazečů o zaměstnání a také s nimi není řádně podepsána mlčenlivost v rámci ochrany osobních údajů subjektů.

Uchazeči o zaměstnání nejsou řádně informování o zpracování jejich osobních údajů dle nařízení GDPR. Je nutné vypracovat dokument, který bude obsahovat informace obsažené v článku 13, nařízení GDPR, v němž budou definovány účely zpracování, doba zpracování či kontaktní údaje správce. Tyto informace je nutné předat v okamžiku získání osobních údajů od subjektu. Je tedy možné informace přímo umístit pod daný inzerát, nebo zasílat tyto informace emailem. Je nutné zajistit prokazatelnost předaných informací, té by bylo dosaženo, pokud by pod inzerátem byla možnost potvrzení přečtení v podobě procesu opt-in[16].

Organizace (správce) využívá zpracovatele pro zpracování osobních údajů. Konkrétně se jedná o využívání služeb personální agentury. Poskytovatel služby je v roli zpracovatele a organizace v postavení správce, jelikož určuje účely zpracování osobních údajů. Je tedy nutné, aby mezi organizací a zpracovatelem byla řádně podepsána smlouva, jenž odpovídá požadavkům nařízení GDPR. Budou v ní tedy obsaženy informace o účelech zpracování, rozsah zpracování či závazek mlčenlivosti. Organizace sice disponuje podepsanou smlouvou o poskytování služeb, nicméně je nutné ji doplnit dodatkem či podepsat novou smlouvu, která již bude vyhovovat požadavkům nařízení GDPR.

[16] opt-in je označení procesu, kdy se subjekt přihlašuje k odběru nějaké služby, nebo si nějakou službu aktivuje/zapíná. Opakem je opt-out, kdy je subjektu předdefinován souhlas a subjekt se následně musí aktivně zajímat o možnost zrušení takového zpracování. (37)

Doporučení

Na základě výše uvedených nálezů a možností řešení doporučuji smazat životopisy nepřijatých uchazečů z emailů všech pracovníků organizace a skartovat vytištěné. Životopisy nepřijatých uchazečů ukládat na server organizace a nezpracovávat je tímto způsobem déle jak půl roku, popřípadě si opatřit pro takové zpracování souhlas. Dále doporučuji odepřít přístupy neoprávněným zaměstnancům do složky na interním serveru organizace, která obsahuje osobní údaje uchazečů o zaměstnání. Je také nutné vytvořit dodatky k pracovním smlouvám, které budou vázat pracovníky mlčenlivostí v rámci zpracování osobních údajů.

Doporučuji sepsat dokument, nesoucí informace obsažené v článku 13, který bude umístěn přímo pod inzerátem, umístěným na webovém portále s přidanou funkcionalitou zaškrtnutí pole procesem opt-in, bez kterého nebude možné osobní údaje odeslat. Důvod takového řešení je usnadnění práce personálnímu pracovníkovi, který nebude nucen odesílat informace o zpracování všem kandidátům jednotně.

Doporučuji také přidat k inzerátu zaškrtávací pole, prostřednictvím kterého budou uchazeči souhlasit se zpracováním osobních údajů po dobu dvou let a to pouze pro účely náboru. Pole bude v režimu opt-in, a bude možné osobní údaje zaslat i bez jeho zaškrtnutí. Řešení je zvoleno opět pro zefektivnění práce personálního pracovníka, který tak bude moci uchovávat některé životopisy po delší dobu a nebude nutné žádat o souhlas zvlášť. Dvouletá doba platnosti souhlasu byla zvolena z důvodu časem se snižující pravděpodobnosti nástupu daného uchazeče, která navazuje na možnou odůvodnitelnou dobu zpracování v případě kontroly dozorovým úřadem. V případě, kdy osobní údaje nebudou obdrženy prostřednictvím inzerátu, doporučuji uchazeči odeslat email, prostřednictvím kterého bude splněna informační povinnost správce.

Dále bude nutné vyhotovit zpracovatelskou smlouvu s personální agenturou, která stojí v roli zpracovatele vůči organizaci a jenž bude vyhovovat požadavkům nařízení GDPR a s obchodními zástupci organizace jenž pracují jako osoby výdělečně činné.

Nálezy v oblasti kopírování a zpracovávání dokumentů

Organizace provádí kopírování občanských průkazů svých zaměstnanců. V tomto případě je ovšem takové zpracování nezákonné. Zákon č. 328/1999 Sb., o občanských průkazech, zakazuje jakékoliv kopírování občanských průkazů bez souhlasu občana, jemuž náleží, pokud jiný předpis nestanoví jinak. Vzhledem k tomu, že jiný zákonný předpis zaměstnavateli vytvářet kopie neumožňuje, není možné takové zpracování bez souhlasu subjektu provádět. Pro účel ověření totožnosti zaměstnance postačí fakt, že dokumenty zkontrolovala pověřená osoba, popřípadě zapsala číslo dokladu se svým podpisem do spisu zaměstnance. (38)

Životopisy zaměstnanců jsou uchovávány v personální složce zaměstnance. Pro takové zpracování ovšem chybí, dle nařízení GDPR, legitimní účel zpracování.

Organizace uchovává personální spisy bývalých zaměstnanců po dobu delší než je nezbytná k jejich účelu. Spis zaměstnance je možné uchovávat i po odchodu zaměstnance z organizace, je však nutné jej zpracovávat pouze s informacemi nezbytně nutnými k jejich účelu, tedy bez osobních údajů členů jeho rodiny, jiných osob či nadbytečných informací nevtahujících se k účelu zpracování. Ve většině případů se v rámci zpracování jedná o ochranu zaměstnavatele proti občansko-právnímu sporu. Doba archivace je doporučována nejméně po dobu tří let. Po tuto dobu trvá, dle zákona č. 89/2012 Sb. občanský zákoník, subjektivní promlčecí lhůta[17]. Maximální doba zpracování by byla obhájitelná před dozorovým orgánem po dobu deseti let, jenž je objektivní lhůta promlčení[18] dle stejného zákona. Následně je nutná likvidace takového zpracování. (39)

[17] Subjektivní promlčecí lhůta, dle § 629 odst. 1 NOZ, běží ode dne, kdy právo mohlo být uplatněno poprvé. Právo může být uplatněno poprvé, pokud se oprávněná osoba dozvěděla o okolnostech rozhodných pro počátek běhu promlčecí lhůty, anebo kdy se o nich dozvědět měla a mohla. (39)

[18] Objektivní promlčecí lhůta, začíná běžet nezáviste na subjektivní promlčecí lhůtě a počíná v den vzniku škody. (39)

Není řádně podepsána zpracovatelská smlouva se zpracovatelem osobních údajů poskytující multisport karty. Poskytovatel je v roli zpracovatele a organizace z postavení správce určuje účely zpracování osobních údajů. Je tedy nutné, aby mezi organizací a zpracovateli byla řádně podepsána smlouva, jenž odpovídá požadavkům nařízení GDPR. Organizace sice disponuje podepsanou smlouvu o poskytování služeb, nicméně je nutné ji doplnit dodatkem či podepsat novou smlouvu, která již bude vyhovovat požadavkům nařízení GDPR.

Doporučení

Na základě výše uvedeného odůvodnění doporučuji životopisy zaměstnanců fyzicky předat zaměstnanci nebo jej smazat či skartovat. Doporučuji také skartovat kopie občanských průkazů umístěných v personální složce zaměstnance. Personální složky bývalých zaměstnanců doporučuji omezit na nezbytný rozsah a po uplynutí čtyřleté doby skartovat. Doporučená čtyřletá doba je stanovena na základě subjektivní promlčecí lhůty, která zohledňuje i fakt, že žaloba může být žalovanému zaměstnavateli doručena i několik měsíců po uplynutí promlčecí lhůty.

Dále doporučuji vyhotovit zpracovatelskou smlouvu, jenž bude v souladu s požadavky nařízení GDPR. Smlouvu bude nutné uzavřít s poskytovatelem služeb v rámci multisport karet, jenž je zpracovatelem osobních údajů.

Nálezy v oblasti monitorování zaměstnanců

Zpracování na základě, kterého je prováděn monitoring služebních počítačů, není prováděn dle požadavků nařízení GDPR. Zároveň je porušován Zákon č. 262/2006 Sb., zákoník práce, §316, který zakazuje zaměstnavateli narušovat soukromí zaměstnanců a je povinen je informovat o rozsahu kontroly a způsobech jejího provádění. (32)

Účelem monitorování služebních počítačů je sledování produktivity zaměstnanců. Takové zpracování je oprávněným zpracováním správce, pokud je prováděno v přiměřeném rozsahu k jeho účelu. Pro sledování produktivity postačí zobrazení domény navštívené stránky, nikoliv titulku stránky, adresy URL či obsahu stránky. Důležité je, aby v rámci monitoringu nebylo zasahováno do soukromí subjektů údajů,

kteří používají zařízení i pro soukromé účely. Je důležité, aby obsah sledovaných informací byl omezen na nezbytný rozsah vzhledem ke svému účelu. Sledování názvu dokumentů v rámci tisku dokumentů je v pořádku, organizace ovšem nesmí sledovat jejich obsah, zde by docházelo k narušení svobod subjektu. Pro zvýšení ochrany osobních údajů subjektů je možné využívat osobních čísel místo jmen subjektů. Jedná se o prevenci při nakládání s osobními údaji neoprávněnými osobami. Ovšem ideálním řešením v rámci monitoringu pohybu zaměstnanců na webových stránkách, je neprovádět monitoring vůbec a zavést jiná opatření, například zablokování některých stránek nebo zřídit v prostorách podniku zařízení, které pracovníci mohou využívat internet pro své soukromé účely, aniž by je kdokoli monitoroval

Na základě zákona č. 262/2006 Sb., zákoníku práce, §316, je nutné subjekty o prováděném monitoringu informovat. Informovanost lze provést několika způsoby, vždy je ovšem nutné, v případě prováděné kontroly dozorovým úřadem, předání informací prokázat. Je tady možné nechat zaměstnance podepsat dokument s obsaženými informacemi či informace zakomponovat do interní směrnice.

Sledování polohy služebních vozů je v pořádku, pokud je sledování možné vypnout pro soukromé účely a zaměstnanci jsou o prováděném monitoringu informování, což organizace splňuje.

Sledování prostor kamerovými systémy je taktéž v pořádku, pokud není zasahováno do soukromí subjektů. Organizace sleduje pouze prostory, které je nezbytné sledovat k účelu případných krádeží. Organizace ovšem musí subjekty o prováděném monitoringu opět informovat a to jak interní pracovníky, tak návštěvníky prodejny. Ideálním řešením je označení prostor informací o prováděném monitoringu.

Doporučení

Na základě výše uvedených nálezů a možností řešení doporučuji informovat pracovníky organizace o prováděném monitoringu prostřednictvím směrnice, která bude přístupná všem pracovníkům na serveru organizace. Řešení je zvoleno na základě dostatečné formy poskytnutí informací, vycházejících z požadavků nařízení GDPR. Směrnice bude

obsahovat informace o účelech, rozsahu, době uložení, zákonnosti zpracování či právech subjektu. Tento rozsah je přímo definován nařízením GDPR. V rámci předání informací veřejnosti o sledování prostor kamerovým systémem je nezbytné umístit cedule u vchodu do budovy s informací, že prostor před budovou a uvnitř budovy je monitorován. Jedná se o řešení, které dostatečně pokrývá požadavky nařízení GDPR.

Doporučuji omezit rozsah zpracování v rámci monitoringu firemních počítačů, který bude přiměřený k jeho účelu. Konkrétně se jedná o omezení rozsah sledovaných informací o prohlížených webových stránkách na název domény a v rámci tisku nezobrazovat jméno uživatele ale využívat osobních čísel zaměstnanců. Jedná se o řešení, které zpracovává minimu osobních údajů potřebných k naplnění jejich účelu.

4.2 Účetní oddělení

Podkapitola se věnuje širšímu rozvoji nálezů, které byly identifikovány v analýze současného stavu na účetním oddělení a návrhům jejich možného řešení včetně výběru finálního doporučení a jeho odůvodnění.

Nálezy

Zpracování osobních údajů na účetním oddělení, není prováděno dle nařízení GDPR. Organizace zpracovává osobní údaje, které umožňují identifikaci subjektů údajů po dobu delší než je nezbytně nutná k účelu. Doby uchování, přímo se vztahující k účetním, daňovým a mzdovým dokladům se řídí následující legislativou: (40) (41) (42) (43)

Zákon č. 563/1991 Sb., o účetnictví
Zákon č. 235/2004 Sb., zákon o dani z přidané hodnoty
Zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení
Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení

Pro uchovávání dokladů po dobu delší, než je stanovena výše uvedenými zákony, musí existovat oprávněný zájem správce. V opačném případě se jedná o porušení nařízení

GDPR. Oprávněným zájmem správce, může být délka záruční doby zboží. Pokud společnost nakoupí zboží, které má delší záruční dobu než je zákonem stanovená archivační lhůta, stanovuje se na toto zboží v rámci doby zpracování, délka poskytnuté záruční doby.

Doporučení

Na základě výše uvedených nálezů a legislativy doporučuji vypracovat skartační řád, kterým se bude účetní oddělení a ostatní pracovníci v organizaci řídit. Po uplynutí stanovené doby bude nutné dokumenty v listinné podobě skartovat a smazat je i z elektronického zpracování, tedy z účetního programu a softwaru PEDRO. Doby uchování, které doporučuji (Tabulka č. 7), přímo vycházejí z výše uvedené platné legislativy.

Tabulka č. 7: Zákonné lhůty po archivaci účetních dokumentů

Typ dokumentu	**Zákonná doba archivace**	**Zákonný předpis**
Účetní závěrka	10 let	Zákon č. 563/1991 Sb., o účetnictví
Výroční zpráva	10 let	Zákon č. 563/1991 Sb., o účetnictví
Účetní doklady	5 let	Zákon č. 563/1991 Sb., o účetnictví
Účetní knihy	5 let	Zákon č. 563/1991 Sb., o účetnictví
Odpisové plány	5 let	Zákon č. 563/1991 Sb., o účetnictví
Inventurní soupisy	5 let	Zákon č. 563/1991 Sb., o účetnictví
Účtový rozvrh	5 let	Zákon č. 563/1991 Sb., o účetnictví
Přehledy	5 let	Zákon č. 563/1991 Sb., o účetnictví
Účetní záznamy	5 let	Zákon č. 563/1991 Sb., o účetnictví
Daňové doklady	10 let	Zákon č. 235/2004 Sb., zákon o dani z přidané hodnoty
Účetní záznamy pro stanovení odvodu pojistného	10 let	Zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení
Evidenční listy	3 roky	Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení

Mzdové listy	30 let	Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení
Mzdové listy pro uživatele starobního či invalidního důchodu	10 let	Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení
Účetní záznamy o údajích potřebných pro účely důchodového pojištění	30 let	Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení

(Zdroj: vlastní zpracování (40) (41) (42) (43))

Informace vedené jako podklad pro výpočet mzdy, tedy informace uvedené v softwaru, na základě kterého dochází k výpočtu odpracovaných hodin, doporučuji smazat po uplynutá čtyřleté doby. Doporučená čtyřletá doba je stanovena na základě subjektivní promlčecí lhůty, která zohledňuje i fakt, že žaloba může být žalovanému zaměstnavateli doručena i několik měsíců po uplynutí promlčecí lhůty (například v případě neproplacené práce přes čas).

4.3 Obchodní oddělení

Podkapitola se věnuje širšímu rozvoji nálezů, které byly identifikovány v analýze současného stavu na obchodním oddělení a návrhům jejich možného řešení včetně výběru finálního doporučení a jeho odůvodnění.

Nálezy

Zpracování osobních údajů na obchodním oddělení, není prováděno dle nařízení GDPR. Osobní údaje zákazníků jsou uchovávány po neomezeně dlouhou dobu. Osobní údaje subjektů jsou obsaženy v elektronické podobě v programu PEDRO a emailech pracovníků organizace. V rámci využívání softwaru je možným řešením kontaktovat dodavatele, který dodá verzi softwaru, která umožňuje nastavení doby, po které budou osobní údaje ze softwaru automaticky smazány. V listinné podobě se osobní údaje

subjektů nacházejí na reklamačních formulářích, které zákazníci organizaci zasílají. Pro takové zpracování je nutné nastavit dobu, po které budou osobní údaje ze všech nosičů odstraněny. Objednávka je účetním dokladem, na něž se vztahuje, dle zákona č. 563/1991 Sb., o účetnictví, pětiletá povinná archivační doba. Reklamační formuláře je možné uchovávat v případě nutného doložení dokumentu při možném občansko-právním sporu, jehož subjektivní promlčecí doba je tříletá.

Organizace vede databázi svých zákazníků i subjektů, kteří vyslovili požadavek, nebýt již v budoucnu oslovováni. Účelem vedení databáze je získání přehledu o objednávkách jednotlivých zákazníků, zefektivnění práce s programem, možnost oslovení zákazníka v případě vyřízení objednávky a pro účely provádění přímého marketingu. Je tedy nutné dobu zpracování určit na základě těchto účelů. Vedení databáze subjektů, kteří si nepřejí býti osloveni je v pořádku, pokud rozsah zpracování osobních údajů je minimální vzhledem k jeho účelu, jenž je v daném případě minimální rozsah informací, na základě kterých lze identifikovat subjekt. Pro tyto účely postačí jméno, příjmení subjektu, organizace a adresa, IČO ostatní údaje nejsou potřebné.

Zpracování není prováděno způsobem, který náležitě zabezpečuje osobní údaje. Pracovníci organizace mají přístup k více informacím, než by bylo nezbytné pro výkon jejich pracovní náplně. Je tedy nutné zavést organizační opatření, která povedou ke zvýšení zabezpečení osobních údajů před možným únikem, poškozením či náhodnou ztrátou. Pracovníci mají přístup k číslu bankovního účtu subjektu, což je osobní údaj, jenž k výkonu své práce nepotřebují mít přístup.

Organizace neinformuje zákazníky o zpracování osobních údajů dle nařízení GDPR. V okamžiku přijetí osobních údajů prostřednictvím objednávky je nutné subjekt údajů informovat o účelech zpracování, kontaktních údajích správce, doby zpracování či ostatních náležitostech obsažených v článku 13 nařízení GDPR.

Obchodní zástupci kontaktují s nabídkou produktů zubní ordinace a dentální hygienisty. Takové oslovení zákazníka je v pořádku, je ovšem nezbytné sepsat s pracovníky smlouvu o zpracování, vzhledem k faktu, že tito pracovníci stojí v postavení

zpracovatele. Ve smlouvě bude nutné především stanovit přesné pokyny, kterých se pracovníci musí držet v rámci zpracování a oslovení potenciálních zákazníků organizace.

Doporučení

Na základě výše uvedených nálezů doporučuji vypracovat skartační řád, který bude nosičem informací, určující doby zpracování jednotlivých dokumentů. Objednávky doporučuji zpracovávat po dobu, ne delší pěti let od jejich vzniku. Doba je shodná s minimální dobou uchování dle zákona č. 563/1991 Sb., o účetnictví. Reklamační formuláře doporučuji zpracovávat maximálně po dobu čtyř let. Doporučená čtyřletá doba je stanovena na základě subjektivní promlčecí lhůty, která zohledňuje i fakt, že žaloba může být organizaci doručena i několik měsíců po uplynutí promlčecí lhůty. Je také nutné osobní údaje smazat z emailové komunikace pracovníků organizace. Doporučuji vytvořit v emailu složky, podle účelu komunikace (objednávka/reklamace/ žádost o nezpracovávání osobních údajů), do nichž bude komunikace přesunuta. Komunikaci ve složkách doporučuji smazat po uplynutí jejich účelu.

Databázi zákazníků, doporučuji smazat po uplynutí pěti let, kdy byla jimi vytvořena poslední objednávka, provedena registrace či proběhla jiná účelná komunikace. Jedná se o dobu, po jejíž uplynutí je velice nepravděpodobné, že by subjekt zareagoval na nabídku, na základě přímého marketingu, či jiné pobídky, pokud dosud tak neučinil. Doba je nastavena také z důvodu, že organizace nabízí speciální přístroje, které specialista obměňuje po delším časovém intervalu. V rámci delšího zpracování, se také riziko nedodržení podmínky zásady zpracování, jenž ukládá správci povinnost zpracovávat přesné osobní údaje.

Databázi subjektů, kteří si nepřejí býti osloveni, doporučuji zpracovávat v rozsahu, jenž zaručí minimalizaci potřebných informací vzhledem k účelu zpracování. Doporučuji zpracovávat pouze jméno, příjmení, název organizace, IČO. Jedná se minimální rozsah informací, na základě kterého, nedojde k mylné identifikaci subjektu. Zpracování telefonního kontaktu a DIČ je pro účel nadbytečný.

Je dále nezbytné vytvořit pravidla pro přístup, pracovníků organizace k osobním údajům. Tyto pravidla je nezbytně nutné aplikovat v softwaru PEDRO. Konkrétně doporučuji zrušit přístup k bankovnímu účtu zákazníka, všem pracovníkům, vyjímaje účetní. Jedná se o osobní údaj, který pracovníci, k výkonu pracovní náplně nepotřebují znát.

Dále doporučuji přepracovat pracovní smlouvy s obchodními zástupci. Do smluv je nezbytně nutné zakomponovat náležitosti, které předepisuje nařízení GDPR v článku 13. Smlouva bude obsahovat přesné pokyny zpracování osobních údaje s důrazem na způsob vyhledávání a kontaktování potenciálních zákazníků, kdy bude uvedeno, že obchodní zástupci nesmí oslovovat přímo fyzickou osobu, která nebude uvedena jako kontaktní údaj dané ordinace či specialisty. Ve smlouvě bude také uveden závazek mlčenlivosti, závazek zabezpečení osobních údajů, závazek součinnosti a dodržení pokynů správce, závazek dodržení podmínek pro zapojení dalšího zpracovatele a v neposlední řadě závazek doložení informací prokazujících plnění náležitostí dané smlouvy. Takové doporučení je stanoveno z důvodu, aby se organizace zprostila odpovědnosti při nedodržení pokynů obsažených ve smlouvě.

4.4 Marketingové oddělení

Podkapitola se věnuje širšímu rozvoji nálezů, které byly identifikovány v analýze současného stavu na marketingovém oddělení a návrhům jejich možného řešení včetně výběru finálního doporučení a jeho odůvodnění.

Nálezy

Zpracování není v souladu nařízení GDPR. Organizace využívá protokol http cookie. O této skutečnosti jsou sice subjekty osobních údajů informováni, ovšem ne podle náležitostí nařízení GDPR. Data jsou sbírány jak pro fungování webu, tak pro provádění profilování. Využívat protokol http cookie pro fungování webových stránek je možné, zároveň je ale nezbytné subjekty o této skutečnosti řádně informovat. Informační povinnost je možné umístit do lišty či odkazu k informaci o používání http cookie. Provádět profilování je možné pouze na základě získaného souhlasu, jehož náležitosti

nařízení GDPR stanovuje. Souhlas musí být umístěn separátně, nelze ho tedy umístit například do obchodních podmínek. Je ovšem možné umístit jej do registračního formuláře.

Doporučení

Na základě výše uvedených nálezů doporučuji umístit do okna, které informuje návštěvníky webu o využívání služeb http cookie, také informace, které budou splňovat náležitosti ustanovené v článku 13, nařízení GDPR. Informace bude možné zobrazit za pomocí odkazu. Doporučení je uděleno na základě faktu, že organizace zpracovává IP adresy návštěvníků webu a nevyužívá tyto informace pro marketingové účely ale pouze pro fungování webu, s nímž souvisí uložení obsahu nákupního košíku.

Do formuláře, kterým návštěvník webové stránky provádí registraci, doporučuji umístit:

- souhlas pro provádění profilování;
- souhlas pro využívání marketingu na základě http cookie;
- informační povinnost správce o zpracování osobních údajů.

Uvedené dva souhlasy musí být od sebe odděleny a musí být uděleny na základě opt-in. Pokud subjekt souhlas neudělí, pak organizace nesmí osobní údaje pro tyto účely zpracovávat. Dobu zpracování doporučuji stanovit dvouletou. Jedná se o dobu, po kterou pokud subjekt neprovedl objednávku, která byla podpořena marketingem, pak je velmi malá pravděpodobnost, že tak subjekt učiní i v budoucnu. Pokud se jedná o zákazníka, který zboží objednává pravidelně, pak bude nezbytné, aby souhlas po dvou letech udělil znovu opět na dobu dvou let. Jedná se o dobu, která je obhájitelná pro provádění profilování před dozorovým úřadem. Těsně pod formulář doporučuji umístit informaci o používání http cookie, kterou bude možné pro získání více informací rozkliknout pomocí odkazu. Formulář tak nebude vypadat chaoticky a zároveň bude splňovat nařízení GDPR.

Pokud zákazník neprovede registraci ale přímo objednávku, pak doporučuji stejné náležitosti, jako byly obsaženy v registračním formuláři umístit pod objednávkový formulář.

Pokud uživatel udělil souhlas, pak doporučuji tyto funkcionality pro příští nákup odstranit z objednávkového formuláře. Subjekt již informace má a proto není nutné mu je znovu poskytovat. Je ovšem nutné informace o zpracování a uděleném souhlasu umístit na jiné místo na webových stránkách organizace. Doporučuji vytvořit na webových stránkách odkaz, který bude nositelem stejných informací, které byly poskytnuty při registraci nebo při vytvoření objednávky.

Doporučuji databázi, která nese informace o účastnících na promoakcích uchovávat pouze po dobu maximálně tří let. Zohledňuji při takovém rozhodnutí fakt, že se jedná o drahé speciální přístroje, kdy se specialista může rozhodovat pro nákup takového přístroje delší dobu a organizace potřebuje sledovat vynaložené náklady na potenciálního zákazníka.

4.5 Obecná doporučení

Podkapitola se věnuje širšímu rozvoji nálezů, které byly identifikovány v analýze současného stavu, která se ovšem nevztahují k jednotlivým oddělením ale k celé organizaci obecně. Následně budou opět navržena jejich řešení.

Nálezy

Organizace nemá nastavené procesy tak, aby mohla vykonávat práva subjektů údajů dle nařízení GDPR. Je tedy nezbytně nutné, aby organizace nastavila procesy a sepsala dokumentaci, která bude nositelem informací, podle kterých, by měli pracovníci organizace postupovat, při uplatnění těchto práv. Mapa osobních údajů organizaci pomůže si uvědomit, kde všude se osobní údaje nacházejí.

Organizace nemá zavedené procesy, které by vedly k výkonu povinnosti správce ohlašovat případy porušení zabezpečení osobních údajů, dle nařízení GDPR. Organizace musí své procesy nastavit tak, aby byla schopná se o incidentu včas dozvědět a nahlásit tuto skutečnost nejpozději do 72 hodin dozorovému úřadu či přímo subjektu údajů, pokud by to povaha incidentu vyžadovala.

Zaměstnanci organizace nejsou dostatečně seznámeni s legislativou, pravidly a postupy v oblasti ochrany osobních údajů. Je tedy nezbytné provést opatření, která povedou k seznámení zaměstnanců o tom, jak by měly osobní údaje zpracovávat.

V organizaci není stanovena osoba, která by vykonávala kontrolu nad zpracováním osobních údajů. Organizace sice nespadá do povinnosti jmenovat pověřence pro ochranu osobních údajů, nicméně by měla být stanovena osoba, která tuto činnost bude provádět.

Doporučení

Na základě výše uvedených nálezů doporučuji vypracovat dokumentaci, například v podobě směrnice, jenž bude nést informace o tom, jak by měli zaměstnanci postupovat v případě případů porušení zabezpečení osobních údajů. Dokument doporučuji umístit na server organizace.

Je také nezbytně nutné zavést pravidla na výkon práv subjektů. Doporučuji zvolit jednu pověřenou osobu, která se stane kontaktním místem, jak pro interní potřeby, tak pro subjekty osobních údajů vně organizace. Tato osoba v případě požadavků subjektů údajů bude vykonávat jeho práva v rámci nařízení GDPR. Aby byl proces účinný, doporučuji zaškolit veškeré pracovníky, kteří v případě zaznamenání požadavku subjektu (například prostřednictvím emailové či ústní komunikace) předal požadavek zvolené pověřené osobě. Pro ulehčení výkonu práv doporučuji kontaktovat dodavatele softwarů, jenž organizace využívá, aby dodali verzi, která umožňuje tyto práva uplatnit. Pověřená osoba bude také vykonávat periodické kontroly nad dodržováním nařízení GDPR v organizaci. Navrhuji, aby tyto činnosti vykonávala asistentka prodeje, která bude disponovat podporou ze strany vedení organizace.

Doporučuji provést školení, které seznámí zaměstnance s náležitostmi nařízení GDPR. Školení doporučuji opakovat jednou ročně a dokumentovat prostřednictvím prezenční listiny. Organizace nese odpovědnost za nakládání s osobními údaji, proto je v jejím zájmu proškolit své zaměstnance a také disponovat dokumentem, který při případné kontrole prokáže, že organizace poskytla kroky potřebné k tomu, aby předešla možným bezpečnostním incidentům.

4.6 GAP analýza

Organizaci Dentalife s.r.o., byl dodavatelskou organizací dodán dokument, který popisuje jednotlivé nedostatky, které byly během interview identifikovány s odkazem na články nařízení GDPR, které jsou v konkrétním případě porušeny. Dokument je taktéž doplněn o návrh řešení jednotlivých nálezů a prioritu jejich implementace.

Priority byly zvoleny na základě několika faktorů. Prvním faktorem je závažnost porušení dle nařízení GDPR, které uděluje jednotlivým článkům různé výše sankcí. Druhým faktorem je hodnocení dopadu přímo na subjekty osobních údajů, kterým v případě úniku, může hrozit narušení jejich práv a svobod.

Nízká priorita Nízká

Je přidělena nálezům, které sice je nutné napravit, nicméně není nutné se jimi zabývat prioritně, jelikož nepředstavují v současné době vysoké riziko pro práva subjektů údajů. V některých případech reprezentují nálezy, které budou napraveny automaticky po napravení závažnějších nálezů, které z nich vyplývají.

Střední priorita Střední

Je přidělena nálezům, které je nutné napravit nicméně až po nápravě nálezů označených jako vysoká priorita. Těmto nálezům ve většině případů hrozí nižší pokuta dle nařízení GDPR, nebo nepředstavuje v současné době vysoké riziko pro práva subjektů údajů.

Vysoká priorita Vysoká

Je přidělena nálezům, které je nutné napravit prioritně. Za tato porušení hrozí správci vysoké pokuty či představují vysoké riziko pro práva a svobody subjektů údajů.

Tabulka č. 8: GAP analýza organizace Dentalife s.r.o.

Č.	Popis nedostatku	Priorita	Vazba na GDPR	Návrh řešení
1	Není zajištěno udržování souladu s nařízením GDPR (do budoucna) ve společnosti	Nízká	Všechny články	Zvolení pracovníka, který bude mít odpovědnost za monitorování souladu s nařízením GDPR. **Návrh implementačního detailu:** Odpovědná osoba – například asistentka prodeje bude monitorovat, zda nejsou dokumenty uchovávány déle či v širším rozsahu, než je nezbytně nutné k jejich účelu. Bude upozorňovat vedení na neoprávněné přístupy k osobním údajům a jejich neoprávněné zpracování.
2	Zaměstnanci společnosti nejsou dostatečně seznámeni s legislativou, pravidly a postupy v oblasti ochrany osobních údajů.	Nízká	Všechny články	Je třeba provést školení v oblasti ochrany osobních údajů a taková školení pravidelně opakovat. **Návrh implementačního detailu:** Odpovědná osoba – například asistentka prodeje bude vyslána na školení zaměřující se na zpracování osobních údajů dle nařízení GDPR. Následně předá tyto znalosti v rámci interního školení ostatním zaměstnancům. Tato školení se budou periodicky opakovat v časovém horizontu jednoho roku.
3	Společnost nemá zavedená pravidla a procesy pro vyhovění žádostem subjektů údajů, konkrétně práva subjektu údajů na opravu či výmaz osobních údajů, přístup ke svým osobním údajům a právo vznést námitky proti zpracování.	Vysoká	12, 15,-22, 34	Nastavení konkrétních pravidel a procesů pro vyhovění žádostem subjektů údajů. Je třeba připravit postupy, jakými bude žádostem vyhověno. S ohledem na systémy, které společnost využívá lze případně po výrobci požadovat i dodatečné funkcionality, které zjednoduší (ulehčí pracovníkům) vyřizování takových žádostí, nicméně nemalá část dokumentace je také v papírové podobě a s ohledem na ní bude třeba připravit i manuální část zpracování.

				Návrh implementačního detailu: Odpovědná osoba – například asistent prodeje získá od pracovníků komunikujících přímo se subjekty (např. obchodní zástupce) žádosti (ti musí být vyškoleni – znát pravidla pro přijímání těchto žádostí). Odpovědná osoba zpracuje žádosti subjektů osobních údajů (musí být jednoznačně připraven proces řešení jednotlivých žádostí). Znamená to připravit (**popsat například ve směrnici**) proces řešení požadavků od příjmu žádosti po přípravu a odeslání odpovědi s ohledem na základní práva: na přístup, opravu, výmaz, námitky, přenositelnost.
4	Společnost nemá zavedené procesy, na jejichž základě by byla připravena reagovat na případná narušení bezpečnosti osobních údajů, dle požadavků nařízení GDPR.	Střední	33,34	Je třeba připravit základní postup (proces) nejlépe dokumentovaný (nebude probíhat příliš často) např. ve **formě směrnice** nebo čistě postupu co dělat když nastane narušení ochrany osobních údajů. Dokument musí být snadno přístupný všem pracovníkům organizace.
5	Jednotlivé dokumenty nemají stanovenou dobu, po kterou jsou zpracovány, dokumenty se tak mohou hromadit na PC, v e-mailových schránkách či v tištěné podobě po neomezenou dobu.	Střední	5/1/e	Vypracovat skartační řád dle účelu jednotlivých dokumentů a platné legislativy. Nastavit automatickou likvidaci osobních údajů v systémech organizace. Připravit procesy pravidla (směrnici) po jaké době, kým a jakým způsobem mají být data zlikvidovány. Dokument musí být snadno přístupný všem pracovníkům organizace. **Návrh implementačního detailu:** Kontaktovat dodavatele jednotlivých softwaru (konkrétně softwaru PEDRO a účetního programu), aby dodali verzi programu, která umožňuje nastavit pravidla pro automatizovaný výmaz jednotlivých dokumentů. Pokud dodavatel nebude ochoten takovou verzi dodat, doporučuji změnit dodavatele.

6	Organizace pro zpracovávání osobních údajů pro účely náboru, zpracovává osobní údaje po dobu delší než je nezbytně nutná k jejich účelu. Pro takové zpracování nedisponuje uděleným souhlasem.	Vysoká	6/1/a	Opatřit si souhlas se zpracováním osobních údaje, v podobě životopisů pro ty, které si organizace bude chtít držet pro oslovení uchazeče v budoucnu. **Možnosti:** Opatřit si souhlas ke zpracování Životopisy smazat **Návrh implementačního detailu:** Implementace odkazu, po jehož rozkliknuti, se zobrazí kompletní informace o udělení souhlasu. Implementovat pod vypsaný inzerát na novou pozici. Odkaz bude doplněn zaškrtávacím oknem s funkcionalitou opt-in. V případě, že kandidát nebude zasílat osobní údaje prostřednictvím daného inzerátu, je možné mu na pohovoru předložit dokument k podpisu, prostřednictvím kterého, bude možné souhlas udělit. Je možné zvolit i elektronickou formu prostřednictvím emailové komunikace.
7	Subjekty osobních údajů v rámci náboru nejsou řádně informování dle nařízení GDPR.	Vysoká	13,14	Informovat uchazeče o zpracování osobních údajů. **Návrh implementačního detailu:** Implementace odkazu, po jehož rozkliknuti, se zobrazí kompletní informace o zpracování osobních údajů dle článku 13. Implementovat pod vypsaný inzerát na novou pozici. Odkaz bude doplněn zaškrtávacím oknem s funkcionalitou opt-in. V případě, že kandidát nebude zasílat osobní údaje prostřednictvím daného inzerátu, ale přímo emailem, pak je možné takové informace zaslat taktéž emailem.
8	Organizace zpracovává kopie občanských průkazů.	Vysoká	6	Skartovat kopie občanských průkazů a dále takové zpracování neprovádět.
9	Organizace zpracovává životopisy svých zaměstnanců.	Střední	6	Předat životopisy zaměstnancům, jimž náleží, v opačném případě, je nutné jej skartovat, smazat z emailu či serveru a dále takové zpracování neprovádět.

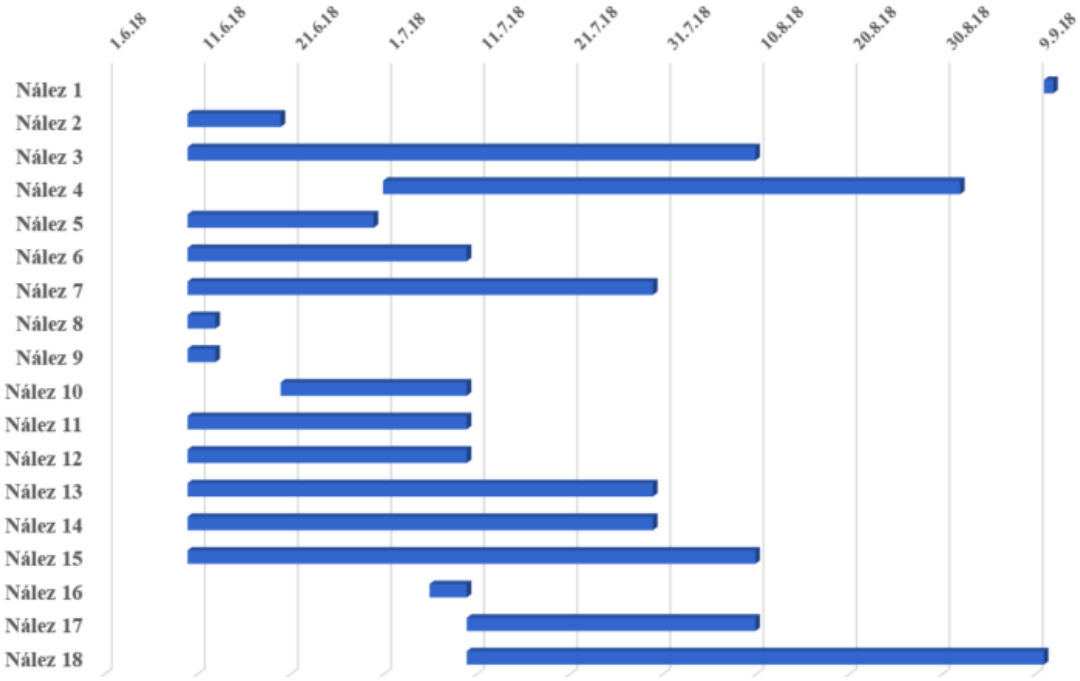
10	Organizace zpracovává osobní spisy zaměstnanců po dobu delší, než nutná k jejich účelu.	Střední	5/1/e	Nastavit dobu skartace osobního spisu zaměstnance, jenž v podniku již nepracuje dle skartačního řádu.
11	Webové stránky neumožňují zrušení sledovaní za pomocí cookie, které slouží pro marketingové účely.	Vysoká	6/1/a	Pro takové zpracování je nutné opatřit si souhlas subjektů osobních údajů se zpracováním. **Možnosti:** Doplnit stránky o požadavek na souhlas a až po získání souhlasu tyto cookies aktivovat. Odstranit cookies, pro které je vyžadován souhlas. **Návrh implementačního detailu:** Implementace odkazu, po jehož rozkliknuti, se zobrazí kompletní informace o udělení souhlasu. Implementovat do registračního a objednávkového formuláře. Odkaz bude doplněn zaškrtávacím oknem s funkcionalitou opt-in. Informace o udělení souhlasu umístit navíc na webové stránky. Zvolit místo, kde bude pro návštěvníky webu snadno k nalezení.
12	Potenciální zákazníci a zákazníci, kteří vytvářejí registraci nebo objednávku na webovém portálu organizace nejsou řádně informování o zpracování osobních údajů.	Vysoká	13	Subjekty osobních údajů je nutné informovat o zpracování osobních údajů. **Návrh implementačního detailu:** Implementace odkazu, po jehož rozkliknuti, se zobrazí kompletní informace o zpracování osobních údajů. Implementovat do registračního a objednávkového formuláře. Informace o zpracování osobních údajů umístit navíc na webové stránky. Zvolit místo, kde bude pro návštěvníky webu snadno k nalezení.
13	Zaměstnanci organizace nejsou řádně informování o prováděném monitoringu osobních počítačů.	Vysoká	13	Vypracovat směrnici, která ponese informaci o provádění monitoringu firemních počítačů dle požadavků uvedených v článku 13, nařízení GDPR. Směrnici umístit na server organizace, tak aby k ní měli přístup všichni pracovníci organizace.

14	Zaměstnanci a návštěvníci prodejny nejsou řádně informování o používání kamerových systémů.	Vysoká	13	Vypracovat směrnici, která ponese informaci o používání kamerových systémů v prostorách prodejny, dle požadavků uvedených v článku 13, nařízení GDPR. Směrnici umístit na server organizace, tak aby k ní měli přístup všichni pracovníci organizace. Umístit u vchodu do budovy ceduli s informací o natáčení prostor kamerovým systémem.
15	Organizace provádí monitoring služebních počítačů, který není v přiměřeném rozsahu k jeho účelu.	Vysoká	5/1/c	Omezit rozsah sledovaných informací o prohlížených webových stránkách na název domény a v rámci tisku nezobrazovat jméno uživatele ale využívat osobních čísel zaměstnanců.
16	Databáze zákazníků, kteří si nepřejí být již oslovování je zpracovávána v rozsahu širším, než je nezbytně nutné k jeho účelu.	Střední	5/1/c	Omezit rozsah zpracovávaných osobních údajů na jméno, příjmení, název organizace, IČO.
17	Pracovníci organizace disponují širšími právy na přístup k osobním údajům než je nezbytně nutné k výkonu jejich pracovní náplně.	Střední	5/1/f	Je nezbytné vytvořit směrnici, jenž bude obsahovat pravidla pro přístup pracovníků organizace k osobním údajům. Tyto pravidla je nezbytně nutné aplikovat v softwaru PEDRO. Konkrétně je nezbytné zrušit přístup k bankovnímu účtu zákazníka, všem pracovníkům, vyjímaje účetní.
18	Společnost využívá jako zpracovatele: • Obchodní zástupce (OSVČ) • Personální agenturu S takovými zpracovateli však nemá uzavřenou písemnou smlouvu o zpracování osobních údajů s náležitostmi stanovenými v nařízení GDPR.	Střední	28	Uzavřít/upravit smlouvy o zpracování, nebo dodatky ke stávajícím smlouvám tak, aby byly naplněny požadavky vyžadované nařízením GDPR na tento druh smluv.

(Zdroj: vlastní zpracování)

4.7 Časový návrh implementace nařízení GDPR

Vzhledem k faktu, že během analýzy současného stavu byly zjištěny především nedostatky, u kterých je nutné zajištění organizačními opatřeními, bude implementační doba záviset na časové dispozici pracovníků organizace, kteří budou jednotlivá doporučení implementovat. Přesto, že se doposud neví, kteří pracovníci budou implementací pověřeni, a jaké budou jejich časové možnosti, vznikl časový návrh (Graf 1), který zohledňuje pracovní vytíženost zaměstnanců organizace.



Graf č. 1: Časový návrh implementace

(Zdroj: vlastní zpracování)

Dle tohoto návrhu, by implementace uvedených doporučení měla trvat 90 dní. Datum, které bylo stanoveno, jako den, kdy organizace bude v souladu s nařízením GDPR, je 10. 9. 2018, což je necelé čtyři měsíce po uvedení nařízení GDPR v účinnost.

4.8 Finanční náročnost implementace nařízení GDPR

Organizace v současné době investovala finanční prostředky do provedení analýzy současného stavu externím dodavatelem. Dodavatelem byla tato analýza naceněna na 82 250 Kč bez DPH. Organizace bude muset investovat další finanční prostředky do proškolení svých zaměstnanců, kdy vzhledem k počtu zaměstnanců, se organizace rozhodla využít stejného dodavatele, jako v případě provedení analýzy současného stavu, který zaměstnance proškolí. Cena byla stanovena na 23 500 Kč bez DPH. Jedná se o cenu nižší, než by musela organizace investovat v případě veřejného školení, která se pohybují okolo 4 000 Kč bez DPH na jednu osobu. Dalším nákladem bude nákup nové verze softwaru, či úplně nového, v případě, že by dodavatel nebyl schopný novou verzi dodat, nebo by její cena byla příliš vysoká. Cenu není možné v tomto okamžiku vyčíslit.

4.9 Zhodnocení návrhů řešení

Během analýzy současného stavu bylo nalezeno celkem 18 porušení nařízení GDPR. V mnoha případech se jednalo o závažná porušení, jejichž nedodržení může být postihnuto správní pokutou až do výše 20 000 000 EUR. Bylo také zjištěno, že se organizace neřídila, ani současnou platnou českou legislativou, v oblasti ochrany osobních údajů. Tento fakt výrazně podpořil celkový počet nálezů.

Následně byla navržena jednotlivá opatření, která po jejich implementaci povedou k naplnění požadavků nařízení GDPR v organizaci. Na těchto základech byla sestavena GAP analýza, která jednotlivé nálezy a doporučení na jejich nápravu třídí dle priorit. Současně s GAP analýzou vznikl také časový návrh celé implementace.

Prioritní se pro organizaci stalo získání souhlasů se zpracováním osobních údajů, zavedení opatření, která budou řádně informovat subjekty o prováděném zpracování a zavedení procesů, na základě kterých bude možné uplatňovat jednotlivé práva subjektů údajů. Implementace bude náročná především po administrativní stránce, jelikož bude nutné vytvořit či přepracovat směrnice, zpracovatelské smlouvy, pracovní smlouvy, souhlasy se zpracováním osobních údajů na různé činnosti a dokument nesoucí informační povinnost správce.

Časová náročnost celé implementace byla stanovena na 90 dní a již nyní je zcela jisté, že organizace nebude v souladu s nařízením do počínajícího dne jeho účinnosti. Nicméně vzhledem k faktu, že se již nyní o soulad s nařízením GDPR aktivně zajímá, by měl kontrolní úřad v případě inspekce výrazně přihlédnout k těmto okolnostem. Organizace je sice malá, proto se nepředpokládá, že by měla patřit k prvním terčům úřadu, nicméně vždy hrozí udání ze stran bývalých zaměstnanců či zákazníků, které úřady nesmí ignorovat.

Ekonomickou náročnost nebylo možné přesněji stanovit, vzhledem k faktu, že organizace doposud nezná vyjádření svých dodavatelů softwaru. Nicméně již nyní se ví, že celá analýza a implementace nařízení GDPR bude organizaci stát minimálně 105 750 Kč bez DPH.

Závěr

Závěrem bych chtěla v prvé řadě říci, že v práci bylo dosaženo všech stanovených cílů. Byl vypracován návrh doporučení jednotlivých opatření, která po jejich implementaci uvedou organizaci Dentalife s.r.o. do souladu s nařízení GDPR a byl popsán i průběh celé analýzy současného stavu zpracování osobních údajů, prováděné ve společnosti Dentalife s.r.o., včetně kroků, které analýze předcházejí.

V průběhu analýzy současného stavu bylo zjištěno, že organizace, v rámci svých procesů zpracování osobních údajů, nesplňuje jak ustanovení obsažení v nařízení GDPR, které vstoupí v účinnost, již 25. května 2018, tak ani legislativu, která je v současné době platným právním předpisem a organizace by se podle ní měla řídit. Tento fakt způsobil vysoký nárůst jednotlivých nálezů, který by se v opačném případě zredukoval na polovinu.

V rámci nálezů byla doporučena taková realizace opatření, aby organizace po jejich implementaci byla v souladu s nařízením GDPR a zároveň, aby udržení kontroly nad těmito opatřeními bylo co nejefektivnější a organizaci usnadnil a ušetřil čas při jejich výkonu.

Byl také navržen časový plán implementace doporučených opatření, ze kterého vyplynulo, že organizace nestihne uvést současný stav zpracování osobních údajů do souladu s nařízením GDPR do data jeho účinnosti. Polehčující okolností v případě možné kontroly ze strany dozorového úřadu ovšem je skutečnost, že organizace již nyní podstoupila kroky, aby takového stavu dosáhla v nejbližší možné době.

Finanční náročnost celého projektu se nepodařilo zcela přesně vyčíslit. Stalo se tak z toho důvodu, že organizace doposud neví, zda dodavatelé informačních systémů, které organizace využívá, budou schopni dodat takové verze svých systémů, které odpovídají požadavkům nařízení GDPR. Již nyní je ovšem jisté, že cena celého projektu, včetně jeho implementace bude vyšší jak 105 750 Kč bez DPH.

Seznam literatury a informačních zdrojů

1. Příručka k nový pravidlům ochrany osobních údajů od Hospodářské komory ČR. Praha: *Hospodářská komora České republiky*, 2018. Dostupné také z: https://www.komora.cz/files/uploads/2017/06/GDPR_p%C5%99%C3%ADru%C4%8Dka_aktualizace_fin%C3%A1l.pdf

2. ZIMEK, Josef. *Ústavnost a český ústavní vývoj.* 3.,nezměněné vyd. Brno: Masarykova Univerzita, 2006. 179 s. ISBN 80-210-4094-7. S 172.

3. Listina základních práv a svobod ze dne 16. prosince 1992

4. Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech ze dne 01.06.1992

5. Právní předpisy: Aplikace Úmluvy Rady Evropy č. 108 ve vztahu k povinnosti žádat Úřad o povolení k předání osobních údajů do zahraničí: *Úřad pro ochranu osobních údajů*. [online]. Copyright © 2013. [cit. 17.03.2018]. Dostupné z: https://www.uoou.cz/pravni-predpisy/ds-1257/archiv=0&p1=1657

6. 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

7. ŠRÁMKOVÁ, Jana. *Ochrana osobních údajů v České republice*. Praha, 2009. 60 s. Bakalářská práce. Bankovní institut vysoká škola Praha. Mgr. Zdeněk Milík.

8. Zákon č. 101/2000 Sb., o ochraně osobních údajů ze dne 4. dubna 2000

9. NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5. S 110.

10. NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5. S 250.

11. Proč potřebuje Evropa lepší ochranu osobních dat | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. [cit. 17.03.2018]. Dostupné z: https://www.gdpr.cz/gdpr/proc/

12. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 13.

13. Všeobecné nařízení o ochraně osobních údajů (GDPR) | MPO. *Ministerstvo průmyslu a obchodu* [online]. Copyright © Copyright 2005 [cit. 17.05.2018]. Dostupné z: https://www.mpo.cz/cz/podnikani/ochrana-osobnich-udaju-gdpr/gdpr-dokumenty/narizeni-eu-2016-679-gdpr-a-trestnepravni-smernice--233003/

14. Vláda schválila návrh zákona o zpracování osobních údajů. *Ministerstvo vnitra České republiky*. [online]. Copyright © 2018 Ministerstvo vnitra České republiky, všechna práva vyhrazena
[cit. 17.05.2018]. Dostupné z: http://www.mvcr.cz/clanek/vlada-schvalila-navrh-zakona-o-zpracovani-osobnich-udaju.aspx

15. GDPR ve vztahu k ISO 27001. *Quality Austria - školení, certifikace a posudková společnost* [online]. [cit. 17.04.2018]. Dostupné z: http://www.qualityaustria.cz/gdpr-ve-vztahu-k-iso-27001

16. ČSN ISO 27 001, *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky.* Praha: Český normalizační institut, 2014.

17. Zákon č. 89/2012 Sb., občanský zákoník ze dne 3. února 2012

18. DOLEJŠOVÁ, Petra. *Bublina jménem GDPR* [přednáška]. Praha. Hospodářská komora České republiky, 23.11.2017

19. Pracovní skupina 29 | GDPR.cz. GDPR | *Obecné nařízení o ochraně osobních údajů* — prakticky [online]. [cit. 17.04.2018]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pracovni-skupina-29/

20. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016

21. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 64.

22. Pracovní skupina podle článku 29. *Vodítka k souhlasu podle Nařízení 2016/679*. WP 259. 2017

23. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 110.

24. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 89.

25. Cílený marketing - Ekonomika. *Ekonomika - Vše co student potřebuje vědět* [online]. Copyright © 2018. Všechna práva vyhrazena. [cit. 17.05.2018]. Dostupné z: http://ekonomika-otazky.studentske.cz/2009/02/cileny-marketing.html

26. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 224.

27. Pracovní skupina podle článku 29. *Vodítka k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679.* WP 251. 2017.

28. Pracovní skupina podle článku 29. *Pokyny týkající se práva na přenositelnost údajů.* WP 242 rev.01. 2017. S 16.

29. Direct marketing | MediaGuru. *MediaGuru* [online]. Copyright © 2018 [cit. 17.05.2018]. Dostupné z: https://www.mediaguru.cz/slovnik-a-mediatypy/slovnik/klicova-slova/direct-marketing/

30. Pracovní skupina podle článku 29. *Pokyny týkající se pověřenců pro ochranu osobních údajů.* WP 243 rev.01. 2017. S 5.

31. Pracovní skupina podle článku 29. *Pokyny týkající se pověřenců pro ochranu osobních údajů.* WP 243 rev.01. 2017. S 9-10.

32. Zákon č. 262/2006 Sb., zákoník práce ze dne 21. dubna 2006

33. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 230.

34. Safetica Auditor, nejen bezpečnostní audit | Safetica. *Safetica | Ochrana citlivých firemních dat před únikem* [online]. [cit. 17.04.2018]. Dostupné z: https://www.safetica.cz/produkty/safetica-auditor

35. Infocar a.s. - Satelitné GPS systémy, Monitorovanie vozidiel. *Infocar a.s. - Satelitné GPS systémy*, Monitorovanie vozidiel [online]. Copyright © Infocar, a. s. [cit. 17.05.2018]. Dostupné z: http://www.infocar.sk/

36 Co jsou Cookies | Adaptic . *Tvorba webu | Adaptic* [online]. Copyright © 2001 [cit. 17.05.2018]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/cookies/

37. Slovníček nejdůležitějších pojmů: Cookies: přechod z principu opt-out na opt-in: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů*. [online]. [cit. 18.03.2018]. Dostupné z: https://www.uoou.cz/slovnicek-nejdulezitejsich-pojmu/ds-2617/archiv=0&p1=1853

38. Zákon č. 328/1999 Sb., o občanských průkazech ze dne 30. listopadu 1999

39. Zákon č. 89/2012 Sb. občanský zákoník ze dne 3. února 2012

40. Zákon č. 563/1991 Sb., o účetnictví ze dne 12. prosince 1991

41. Zákon č. 235/2004 Sb., zákon o dani z přidané hodnoty ze dne 1. dubna 2004

42. Zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení ze dne 20. listopadu 1992

43. Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení ze dne 17. prosince 1991

44. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 81.

45. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 160-163.

46. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. S 173-175.

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam příloh

Přílohy

Příloha č. 1

Vzorový souhlas se zpracováním osobních údajů

1. Udělujete tímto souhlas společnosti Dentalife s.r.o., se sídlem Ulice 24, Brno 123 00 IČO: 12345678, zapsané ve veřejném rejstříku vedeném u Krajského soudu v Brně, oddíl A vložka 1234 (dále jen „Správce“), aby ve smyslu zákona č.101/2000 Sb., o ochraně osobních údajů (dále jen „zákon o ochraně osobních údajů“) zpracovávala tyto osobní údaje:
   - jméno a příjmení
   - datum narození
   - e-mail
   - telefonní číslo
   - trvalou adresu

2. Jméno, příjmení, datum narození, e-mail, telefonní číslo a trvalou adresu je nutné zpracovat za účelem případného budoucího náboru subjektu osobních údajů. Tyto údaje budou Správcem zpracovány po dobu dvou let.
3. S výše uvedeným zpracováním udělujete svůj výslovný souhlas. Souhlas lze vzít kdykoliv zpět, a to například zasláním emailu nebo dopisu na kontaktní údaje společnosti Dentalife s.r.o..
4. Zpracování osobních údajů je prováděno Správcem, osobní údaje však pro Správce mohou zpracovávat i tito zpracovatelé:
   a. Personální agentura PERSONELA s.r.o., se sídlem Ulice 32, Brno, 123 00 IČO: 12345678, zapsané ve veřejném rejstříku vedeném u Krajského soudu v Brně, oddíl A vložka 1244.
6. Vezměte, prosíme, na vědomí, že podle zákona o ochraně osobních údajů máte právo:
   - vzít souhlas kdykoliv zpět,
   - požadovat po nás informaci, jaké vaše osobní údaje zpracováváme,
   - požadovat po nás vysvětlení ohledně zpracování osobních údajů,
   - vyžádat si u nás přístup k těmto údajům a tyto nechat aktualizovat nebo opravit,
   - požadovat po nás výmaz těchto osobních údajů,
   - v případě pochybností o dodržování povinností souvisejících se zpracováním osobních údajů obrátit se na nás nebo na Úřad pro ochranu osobních údajů.

Příloha 2

Vzor informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů

1. Společnost Dentalife s.r.o., se sídlem Ulice 24, Brno 123 00 IČ: 12345678, zapsané ve veřejném rejstříku vedeném u Krajského soudu v Brně, oddíl A vložka 1234 (dále jen „Správce“), ve smyslu zákona č.101/2000 Sb., o ochraně osobních údajů (dále jen „zákon o ochraně osobních údajů“) bude zpracovávat tyto osobní údaje:

- jméno a příjmení
- datum narození
- e-mail
- telefonní číslo
- trvalou adresu

2. Jméno, příjmení, datum narození, e-mail, telefonní číslo a trvalou adresu je nutné zpracovat za účelem náboru subjektu osobních údajů. Tyto údaje budou Správcem zpracovány po dobu šesti měsíců.
3. Zpracovávat tyto osobní údaje pro účely náboru subjektu je organizace oprávněna na základě zákona o ochraně osobních údajů.
4. Zpracování osobních údajů je prováděno Správcem, osobní údaje však pro Správce mohou zpracovávat i tito zpracovatelé:
   b. Personální agentura PERSONELA s.r.o., se sídlem Ulice 32, Brno, 123 00 IČO: 12345678, zapsané ve veřejném rejstříku vedeném u Krajského soudu v Brně, oddíl A vložka 1244.
7. Vezměte, prosíme, na vědomí, že podle zákona o ochraně osobních údajů máte právo:
   - požadovat po nás informaci, jaké vaše osobní údaje zpracováváme,
   - požadovat po nás vysvětlení ohledně zpracování osobních údajů,
   - vyžádat si u nás přístup k těmto údajům a tyto nechat aktualizovat nebo opravit,
   - požadovat po nás výmaz těchto osobních údajů,
   - vznést námitku proti takovému zpracování,
   - v případě pochybností o dodržování povinností souvisejících se zpracováním osobních údajů obrátit se na nás nebo na Úřad pro ochranu osobních údajů.

Příloha č. 3

Mapa osobních údajů organizace Dentalife s.r.o.

Účel zpracování	Zákonnost zpracování / právní titul	Související legislativa	Dataset	Oddělení	Subjekty zpracování	Forma zpracování	Digitální prostředky zpracování	Fyzické prostředky zpracování	Další osoby s přístupem k osobním údajům	Třetí strany seznamující se s údaji	Role ve zpracování	Plánovaná doba zpracování
Nábor zaměstnanců	Smlouva		Jméno, příjmení, trvalá adresa, datum narození, email, telefon, vzdělání, pracovní zkušenosti	Personální oddělení	Uchazeč o zaměstnání	Fyzická i digitální	Email, složka na serveru	Vytištěné CV pro účely pohovoru	Ředitel organizace	Personální agentura v omezené míře	Správce	Neomezená
Vedení personální agendy	Smlouva	**Zákon č. 262/2006 Sb.**, Zákoník práce	Jméno, příjmení, trvalá adresa, datum narození, email, telefon, vzdělání, pracovní zkušenosti, místo narození, rodné číslo, číslo účtu,	Personální oddělení	Zaměstnanec	Fyzická		Spis zaměstnance v kanceláři na účetním oddělení Kancelář uzamčena v době nepřítomnosti Uzamčená plechová skříň	Účetní oddělení		Správce	Neomezená
Provedení školení	Zákon	**Zákona č. 258/2000 Sb.**, O ochraně veřejného zdraví a o změně některých souvisejících zákonů, **Zákon č. 262/2006 Sb.**, Zákoník práce **Zákon č. 133/1985 Sb.** o požární ochraně	Jméno, příjmení, společnost	Personální oddělení	Zaměstnanec	Digitální i fyzická	e-mail (avízo o školení)	Formulář založen do složky zaměstnance	Účetní oddělení	Oblastní inspektorát práce (OIP), externí společnost zajišťující školení přes webovou aplikaci	Správce	Neomezená
Poskytnutí benefitu zaměstnanci	Smlouva		Jméno, příjmení, datum narození, trvalá adresa, telefonní číslo	Personální oddělení	Zaměstnanec	Digitální i fyzická	Elektronické vyúčtování hovorů	Dokumenty založeny v personální složce	Účetní oddělení	Poskytovatel tarifu	Správce	Neomezená
Zpracování mezd, výplata mezd	Zákon Oprávněný zájem	**Zákon č. 235/2004 Sb.**, o dani z přidané hodnoty **Zákon č. 563/1991 Sb.**, o účetnictví **Zákon č. 582/1991 Sb.**, o organizaci a provádění sociálního zabezpečení **Zákon č. 48/1997 Sb.**, o veřejném zdravotním pojištění	Jméno, příjmení, adresa trvalého bydliště, rodné číslo, variabilní symbol od sociálního úřadu, datum narození, pohlaví, občanství, zdravotní pojišťovna, počet dětí a jejich rodné číslo, bankovní spojení	Účetní oddělení	Zaměstnanec	Digitální	PEDRO, e-mail, docházkový systém			Finanční úřad, OSSZ, soud - trestně právní řízení, pojišťovna	Správce	Neomezená

Účel zpracování	Zákonnost zpracování / právní titul	Související legislativa	Dataset	Oddělení	Subjekty zpracování	Forma zpracování	Digitální prostředky zpracování	Fyzické prostředky zpracování	Další osoby s přístupem k osobním údajům	Třetí strany seznamující se s údaji	Role ve zpracování	Plánovaná doba zpracování
Srážky ze mzdy za zdravotní a sociální	Zákon	**Zákon č. 235/2004 Sb.**, o dani z přidané hodnoty **Zákon č. 563/1991 Sb.**, o účetnictví **Zákon č. 582/1991 Sb.**, o organizaci a provádění sociálního zabezpečení **Zákon č. 48/1997 Sb**., o veřejném zdravotním pojištění	Jméno, příjmení, adresa trvalého bydliště, rodné číslo, variabilní symbol od sociálního úřadu, datum narození, pohlaví, občanství, zdravotní pojišťovna, počet dětí a jejich rodné číslo, bankovní spojení	Účetní oddělení	Zaměstnanec	Digitální i fyzická	Portál pojišťovny	Dokumenty založeny v pořadači v kanceláři Kancelář uzamčena v době nepřítomnosti Uzamčená plechová skříň		Finanční úřad, OSSZ, pojišťovna	Správce	Neomezená
Zpracování cestovních příkazů	Zákon	**Zákon č. 262/2006 Sb.**, Zákoník práce	Jméno, příjmení	Účetní oddělení	Zaměstnanec	Digitální	Excel, e-mail, monitorovací program			Finanční úřad	Správce	Neomezená
Zpracování účetních dokladů, zpracování podkladů pro fakturaci	Zákon	**Zákon č. 563/1991 Sb**., o účetnictví **Zákon č. 235/2004 Sb.**, o dani z přidané hodnoty	Jméno, příjmení, trvalá adresa, IČO, DIČ, rodné číslo	Účetní oddělení	Zaměstnanec Zákazník Dodavatel	Fyzická i digitální	Email, PEDRO, účetní software	Dokumenty založeny v pořadači v kanceláři Kancelář uzamčena v době nepřítomnosti Uzamčená plechová skříň	Všichni zaměstnanci v případě potřeby	Finanční úřad	Správce	Neomezená
Archivace účetních dokladů	Zákon	**Zákon č. 563/1991 Sb**., o účetnictví **Zákon č. 235/2004 Sb.**, o dani z přidané hodnoty	Jméno, příjmení, trvalá adresa, IČO, DIČ, rodné číslo, datum narození	Účetní oddělení	Zaměstnanec Zákazník Dodavatel	Fyzická i digitální	Email	Dokumenty založeny v pořadači v kanceláři Kancelář uzamčena v době nepřítomnosti Uzamčená plechová skříň	Všichni zaměstnanci v případě potřeby	Finanční úřad	Správce	Neomezená
Objednávka	Smlouva Oprávněný zájem		Jméno, příjmení, společnost, trvalá adresa, telefonní kontakt, email	Obchodní oddělení	Zákazník Oslovený potenciální zákazník Dodavatel	Digitální	Email, PEDRO	Dokumenty založeny v pořadači v kanceláři Kancelář uzamčena v době nepřítomnosti Uzamčená plechová skříň	Všichni zaměstnanci v případě potřeby		Správce	Neomezená
Marketing	x		Jméno, příjmení, společnost, email	Marketingové oddělení	Zákazník Potenciální zákazník	Digitální	Email, excel				Správce	Neomezená
Registrace	Oprávněný zájem		Jméno, příjmení, email, společnost, trvalá adresa, telefonní kontakt	Marketingové oddělení	Zákazník Potenciální zákazník	Digitální	Web				Správce	Neomezená
Monitoring	x		Jméno, příjmení	Nezařazeno	Zaměstnanec	Digitální	Aplikace, excel		Ředitel		Správce	Neomezená