Univerzita Pardubice
Fakulta ekonomicko-správní

Analýza a implementace GDPR ve vybrané firmě

Markéta Vaňásková

Bakalářská práce
2019

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Markéta Vaňásková**
Osobní číslo:	**E16241**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Ekonomika a provoz podniku**
Název tématu:	**Analýza a implementace GDPR ve vybrané firmě**
Zadávající katedra:	**Ústav matematiky a kvantitativních metod**

Zásady pro vypracování:

Cílem práce je analýza a identifikace procesů zpracování osobních údajů a následná implementace opatření a vnitřních úprav k zabezbečení souladu s nařízením GDPR ve vybrané firmě.

Osnova:
- Rešerše odborné literatury a dalších pramenů.
- Stanovení cílů práce a hypotézy, volba metod.
- Obecné nařízení GDPR.
- Zpracování osobních údajů.
- Opatření a vnitřní úpravy k zabezpečení osobních údajů v rámci GDPR ve zvolené firmě.
- Formulace závěrů a doporučení.

Rozsah grafických prací: –

Rozsah pracovní zprávy: **cca 35 stran**

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

Seznam odborné literatury:

BIRD & BIRD, ÚZ č.1209 - Ochrana osobních údajů (GDPR)2017. Praha: Sagit, 2017. ISBN 978-80-7488-241-8.
JANEČKOVÁ, E. GDPR: Praktická příručka implementace. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.
NAVRÁTIL, J. a kol. GDPR pro praxi. Aleš Čeněk, s.r.o., 2018. ISBN 978-80-7380-689-7.
NEZMAR, L. GDPR: praktický průvodce implementací. Praha: GRADA Publishing,a.s., 2017. ISBN 978-80-271-0668-4.
NULÍČEK, M. a kol. GDPR-obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-765-3.
ŽÚREK, J. Praktický průvodce GDPR. Olomouc: Anag, 2017. ISBN 978-80-7554-097-3.

Vedoucí bakalářské práce: **Mgr. Jana Heckenbergerová, Ph.D.**
Ústav matematiky a kvantitativních metod

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**

L.S.

doc. Ing. Romana Provazníková, Ph.D.
děkanka

doc. Ing. Marcela Kořená, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 4. 2019 Markéta Vaňásková

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala svému vedoucímu práce Mgr. Janě Heckenbergerové Ph.D. za její odbornou pomoc, cenné rady, které mi pomohly při zpracování bakalářské práce. V neposlední řadě také děkuji své rodině a svým blízkým za podporu, kterou mi po celou dobu poskytovali.

ANOTACE

Analýza a implementace GDPR ve vybrané firmě. Fakulta ekonomicko-správní, Univerzita Pardubice. 2019. 63 s. Bakalářská práce
Cílem bakalářské práce je přiblížit analýzu a identifikaci procesů zpracování osobních údajů. Práce dále popisuje následnou implementaci opatření a vnitřních úprav k zabezpečení souladu s nařízením GDPR ve vybrané firmě. Důležitou částí předkládané práce je osvětlení obecných pojmů a vysvětlení nařízení GDPR.

KLÍČOVÁ SLOVA

osobní údaj, citlivý údaj, správce, zpracovatel, subjekt údajů, způsoby zpracování, bezpečnost osobních údajů, nařízení GDPR

TITLE

Analysis and implementation of GDPR in selected company.

ANNOTATION

Analysis and implementation of GDPR in selected company. Faculty of Economics and Administration, University of Pardubice. 2019. 63 pp. The aim of this thesis is to analyze and identify the processes of personal data processing. The thesis also describes the subsequent implementation of measures and internal adjustments to ensure compliance with the GDPR regulation in the selected company. An important part of this work is to explain general terms and explain the GDPR.

KEYWORDS

personal data, sensitive data, controller, processor, data subject, processing methods, personal data security, GDPR

OBSAH

.

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

GDPR	General Data Protection Regulation
EU	Evropská unie
ČR	Česká republika
Sb.	Sbírka zákonů
Sb. m.s.	Sbírka mezinárodních smluv
Odst.	Odstavec
č.	číslo
ZoOU	Zákon o ochraně osobních údajů
čl.	článek
ÚOOÚ	Úřad pro ochranu osobních údajů
USIS	Úřad pro státní informační systém
WP 29	Pracovní skupina pro ochranu osobních údajů zřízená dle směrnice 95/46/ES
DPIA	Data Protection Impact Assessment (posouzení vlivu na ochranu osobních údajů)
DPO	Data Protection Officer (pověřenec pro ochranu osobních údajů)
GAP	Rozdílová analýza
IT	Informační technologie
PC	Personal Computer (osobní počítač)
VPN	Virtual Private Network (virtuální soukromá síť)
IČO	Identifikační číslo organizace / osoby
DIČ	Daňové identifikační číslo
SW	**S**oftware
HW	Hardware
OÚ	osobní údaj

ÚVOD

Tato bakalářská práce se zabývá zpracováním a následnou ochranou osobních údajů. Osobní údaje doprovází každého člověka po celý život a přináší mu tak odlišnost a jedinečnost. Z tohoto důvodu má každá fyzická osoba právo na ochranu osobních údajů, které ji zaručuje Listina základních práv Evropské unie a ústavy jednotlivých členských zemí EU. V ČR má tuto funkci Listina základních práv a svobod, vyhlášená Usnesením předsednictva České národní rady č. 2/1993 Sb. ze dne 16. prosince 1992.
(Listina základních práv a svobod č. 2/1993 Sb.)

Moderní doba na jedné straně umožňuje rozvoj informačních technologií a technický pokrok s rychlou komunikací a efektivním obchodem přesahujícím hranice jednotlivých států, na druhé straně však dochází k pořizování a volnému přenášení velkého množství údajů o fyzických osobách. Počítačové databáze jsou v dnešní době doslova zahlcené obrovským množstvím dat s osobními údaji a ty mohou být zneužity. Ochranu osobních dat tedy nelze řešit výlučně na národní úrovni, ale pomocí mezinárodní koordinace. Z této potřeby vzešla nutnost vypracovat jednotnou právní úpravu na evropském poli ochrany osobních údajů. Evropský parlament a Rada EU stanovily Nařízení 2016/679 v podobě GDPR, díky kterému dochází ve firmách a organizacích k obezřetnějšímu přístupu k zabezpečení osobních dat.
(GDPR 2016/679)

Výrazně se zvyšuje jejich zodpovědnost a kontrola nad procesy, při kterých dochází ke zpracování osobních údajů. Na základě vyšších povinností kladených na organizace a instituce, jsou občanům poskytnuta větší práva na soukromý život a základní svobody.
(Navrátil a kol., 2018, s. 22)

Cílem předkládané bakalářské práce bude analýza a identifikace procesů, ve kterých ve vybrané firmě dochází ke zpracování osobních údajů. Zjištěné skutečnosti budou porovnány se zásadami, které jsou požadovány Nařízením GDPR a v případě nesouladů budou navržena případná opatření k jejich odstranění. Bakalářská práce je rozdělena do dvou logických částí. V první všeobecné části je provedena rešerše odborné literatury a ostatních pramenů. Dále jsou definovány základní pojmy a objasněny vybrané nové instituty v souvislosti s ochranou osobních údajů. Jsou popsány základní kroky, které budou použity při procesu implementace GDPR do organizace.

Druhá praktická část je věnována přípravné fázi, ve které je managementem firmy vypracován podrobný plán implementace včetně finančního rozpočtu. V další fázi autorka bakalářské práce na základě svých zkušeností vycházejících z odborných seminářů, školení, workshopů a přednášek zabývajících se problematikou ochrany dat vypracovala studii zabývající se zmapováním všech operací probíhajících ve firmě. Podrobně je popsán vztah

mezi zaměstnanci a zaměstnavatelem se zaměřením na ochranu osobních údajů v pracovně - právních vztazích. Dále se studie zaměřuje na oblast obchodu, vztahy zákazníka a obchodníka. V této části jsou zmíněny i oblasti marketingu či kamerového systému, který je ve firmě používán.V neposlední řadě se věnuje osobním údajům, které jsou používané v oblasti internetového obchodu.

Ve třetí fázi podrobí GAP analýze všechny procesy a dokumenty, které byly po předchozí fázi identifikovány a porovná je se zásadami uvedenými v GDPR. Výstupem tohoto kroku jsou neshody mezi skutečností a požadavky Nařízení. Na vyhodnocení GAP analýzy navaže další analýza, která určí dopady GDPR na jednotlivé oblasti činností ve firmě. V této fázi je také vyhodnoceno, zda bude organizace potřebovat pověřence pro ochranu osobních údajů.

V závěrečné fázi jsou popsány změny v jednotlivých procesech probíhajících v rámci implementace technických a organizačních opatření k zajištění ochrany osobních údajů ve zvolené firmě, jak v každodenní praxi, tak i v dlouhodobém výhledu.

1 REŠERŠE ODBORNÉ LITERATURY A DALŠÍCH PRAMENŮ

O každém člověku se během života nashromáždí mnoho informací přinášejících jednoznačnou identifikaci např.: jméno, příjmení, adresa bydliště, místo a datum narození, rodné číslo, rovněž i číslo občanského či cestovního průkazu. Ve zdravotní kartě jsou uložené informace o zdravotním stavu, DNA, sexuální orientaci a biometrické údaje. Dále se vedou záznamy o případném členství v politické straně nebo odborovém hnutí. Pokud je osoba odsouzena, tak i záznamy o trestných činech. (Kohútová, 2018, s. 6)

Pro svůj mimořádný význam soukromí je v zájmu člověka snaha nedovolit zneužití informací o své osobě. V dávných dobách se toto úsilí vztahovalo pouze na osoby postavené ve vysokých státních či armádních funkcích. Postupně se okruh lidí rozrůstal i do hospodářské sféry. Právě v historii je možné dohledat, jak docházelo k zneužívání osobních údajů a přispělo k mnoha nelidským činům v průběhu dějin, což postupem času vedlo ke vzniku principů, na základě niž se začala vyvíjet ochrana osobních údajů. V období náboženských válek a pronásledování lidí s odlišným náboženským vyznáním nastal první mezník vedoucí k ochraně svého soukromí. Dalším krokem bylo nesmyslné stíhání a zabíjení v období Velké francouzské revoluce. Druhá světová válka a především nacismus spojený s rasistickou genocidou umožnily pochopení snadného zneužití údajů i vlastním státem a položily základ k ochraně soukromí a dat osob. (Navrátil a kol., 2018, s. 26)

Vyústěním snah o zaručení práv na život a soukromí byla 10. prosince 1948 Valným shromážděním Organizace spojených národů schválena Všeobecná deklarace lidských práv (Všeobecná deklarace lidských práv DE01/48), která ve svých článcích zaručovala ochranu soukromí, jehož přirozenou součástí byla i ochrana osobních údajů. Rozvojem společnosti, obzvláště zavedením technických prostředků, které zpracovávaly osobní údaje, nastala potřeba vyčlenit z práv na ochranu soukromí samostatnou část věnující se ochraně osobních dat. Z tohoto důvodu došlo v lednu v roce 1981 k přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. (č. 115/2001 Sb. m.s.) Objevily se tak poprvé definice některých pojmů a zásady zpracování informací z oblasti ochrany osobních údajů. Z Úmluvy poté vycházely i další evropské dokumenty řešící otázky ochrany dat (viz. str. 17). (Žurek, 2017, s. 13)

Na základě narůstající globalizace a zásad fungování Evropské unie, které byly založené na volném pohybu osob, zboží a služeb nesoucích sebou i volný pohyb osobních informací, se stala nutností potřeba tvorby ucelených pravidel platných v celém evropském prostoru.

„*Směrnice Evropského parlamentu a Rady 95/46/ES měla za cíl zakotvení jednotné úpravy*

ochrany osobních údajů a jejich pohyb na území Evropského společenství, což umožnilo i svobodnější pohyb osob po zemích tzv. Schengenského prostoru". (Směrnice 95/46/ES)
(Navrátil a kol., 2018, s. 27)

Předpis určoval jednotlivým členským státům Evropské unie právní rámec, nestanovoval však přímo práva a povinnosti v jednotlivých zemích, která se tak mohla od sebe výrazně lišit. Bleskový nástup používání počítačů a internetu na začátku milénia způsobil tlak na vnitrostátní zákony a donutil zákonodárce ke změnám. Vzrůstající napětí z postupující globalizace se projevilo v revizi Směrnice a vytvoření Nařízení Evropské unie, které přesně stanovuje práva a povinnosti vnitrostátních subjektů platná ve všech státech EU. (Žurek, 2017, s. 15)

Právní ochrana osobních údajů na českém území má počátek v zákonech č. 87/1862 Sb. z. s., o ochraně svobody osobní a 88/1862 Sb. z. s. na ochranu svobody domovní. (Zákon č. 87/1862 Sb. z. s., Zákon č. 88/1862 Sb. z. s.) V První republice ochranu soukromí zajišťoval Ústavní zákon č. 293/1920 Sb. o ochraně svobody osobní, domovní a tajemství listovního. (Zákon č. 293/1920 Sb.) Až do roku 1992 nedošlo k samostatnému řešení otázky o ochraně osobních údajů v právním řádu, jednalo se pouze o sporadickou zmínku v oblasti vydávání a držení cestovních dokladů. Přijetím zákona č. 256/1992 Sb. o ochraně osobních údajů v informačních systémech došlo k její kodifikaci. (Zákon č. 256/1992 Sb.)

Velmi důležitým zákonem na území ČR v oblasti ochrany osobních dat se stal od 1. června 2000 zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, který zpracování údajů začal řešit komplexně. (Zákon č. 101/2000 Sb.) Po vstupu ČR do Evropské unie prošel zákon v roce 2004 novelizací, která umožnila převzít v zákonné podobě Směrnici 95/46/ES. Tak jako celé EU, ani České republice se nevyhnul rozvoj nových technologii přinášející rozsáhlý sběr a zpracování osobních údajů a proto musela zareagovat zavedením nových technických a organizačních opatřeních v oblasti ochrany osobních dat. Společně s ostatními státy Evropské unie naše země přijala Nařízení, které je závazné pro všechny členské státy. (Žurek, 2017, s. 18 - 19)

Vedle GDPR, které má unijní formu, má každý stát možnost používat adaptační zákon, který upravuje a doplňuje některé oblasti ochrany osobních údajů dle GDPR. V České republice je právním doplňkem Zákon o zpracování osobních údajů tzv. adaptační zákon č. 110/2019 Sb, který nahradil zákon č. 101/2000 Sb. (Zákon č.110/2019 Sb.)

Soukromí člověka je dále chráněno zákonem č. 89/2012 Sb. Občanským zákoníkem. (Zákon č.. 89/2012 Sb.) Ten zaručuje každému člověku právo na život v příznivém prostředí, důstojnost, vážnost, čest, zdraví a soukromí. (Žurek, 2017, s. 20)

1.1 Obecné nařízení (GDPR)

Obecné nařízení EU o ochraně osobních údajů neboli GDPR, z anglického „*General Data Protection Regulation*“ (Nezmar, 2017, s. 27), vstoupilo v platnost 25. 5. 2018 a týká se všech firem, institucí, živnostníků a internetových služeb, které zpracovávají osobní data fyzických osob. Cílem GDPR je v první řadě sjednocení práv ochrany osobních údajů ve všech zemích EU s přizpůsobením právní regulace poměrům dnešní doby. Zaměřuje se na posílení práv v oblasti ochrany osobních dat všech osob, které jsou subjekty údajů.
(Nezmar, 2017, s. 27)

Samotná ochrana osobních dat byla v České republice prováděna již od roku 1992 a byla regulována zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů a dalšími právními předpisy. (Zákon č. 101/2000 Sb.) Výše uvedené Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů nahrazuje směrnici 95/46/ES . (Nezmar, 2017, s. 27-28)

V dubnu 2019 poslanecká sněmovna přijala adaptační zákon č.110/2019 Sb. o zpracování osobních údajů. (Zákon č. 110/2019 Sb.) Tento právní doplněk k GDPR zavádí přípustné výjimky z pravidel evropského nařízení, např. v oblasti snížení sankcí či úpravy věkové hranice pro udělování souhlasu se zpracováním osobních údajů z 16 na 15 let v souvislosti s nabídkou služeb informační společnosti. (Pattynová, Suchánková, 2019)

Na dodržování zákonů v oblasti ochrany osobních údajů v ČR podobně jako v ostatních zemích EU dozorují ústřední úřady. V roce 2000 se transformoval z dosavadního dohlížecího odboru ochrany osobních údajů (Úřadu pro státní informační systém - ÚSIS) Úřad pro ochranu osobních údajů (ÚOOÚ), který nyní jako ústřední správní úřad v ČR dohlíží na ochranu soukromí a osobních údajů. (Matoušová, Hejlík, 2003, s. 298-300)

Jeho činnost spočívá v oblasti dozorovací, kde kontroluje nevyžádaná obchodní sdělení a reguluje reklamu v rozhlasovém a televizního vysílání či jiných informačních společnostech. Dále úřad dohlíží na dodržování povinností při zpracování osobních údajů, které ukládá zákon a vyřizuje následné stížnosti při jejich porušení. (Žurek, 2017, s. 167)

Veřejný registr zpracování osobních údajů zřízený ÚOOÚ, vznikl na základě zápisů oznámení o zpracování osobních údajů nebo zápisů oznámení změny zpracování osobních údajů a byl veden až do prosince 2019. Z důvodu zavedení GDPR a zrušením směrnice 95/46/ES se tato povinnost stává neplatnou.
(Nezmar, 2017, s. 44)

Pro doplnění jsou uvedeny související právní předpisy platné v EU:

- Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat, pro Českou republiku nabyla účinnosti dne 1. listopadu 2001,
- Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat, v České republice platný od dne 1. července 2004,
- Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích),
- Směrnice Evropského parlamentu a rady 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (Směrnice o elektronickém obchodu),
- Smlouva o fungování Evropské unie, ve které je ochraně osobních údajů věnován čl. 16,
- Listina základních práv EU, ochrana osobních dat je zmiňována v č. 8,
- 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,
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu,
- Nařízení Evropského parlamentu a Rady 2001/45/ES ze dne 18. prosince 2001, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů,
- Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí,
- Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008, o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech,
- Doporučení Komise 2014/724/EU ze dne 10. října 2014, o šabloně pro posouzení dopadů inteligentních sítí a inteligentních měřicích systémů na ochranu údajů.

(Morávek, 2013, Doležílek, 2016, Nulíček, 2018)

Výše uvedený zákon č.101/2000 Sb. specifikuje osobní údaje (osobní data), dále rozlišuje osoby zpracovávající tyto data, tzv. správce nebo zpracovatele osobních údajů. Správcům a zpracovatelům jsou při ochraně osobních dat ukládány především povinnosti. Dále zákon vymezuje pojem subjekty údajů, tedy osoby, jimž jsou dávána práva na ochranu osobních dat. Další část práce se zaměří na bližší specifikaci obecných pojmů z oblasti ochrany osobních údajů. (Kohútová, 2018, s. 4-7)

1.2 Základní pojmy používané v oblasti ochrany osobních dat

ZoOU v § 4 vymezuje řadu základních pojmů, které jsou primární ve smyslu svého hmotného obsahu nebo jsou to pojmy, které popisují procesy. Uvedené ustanovení patří mezi nejdůležitější, protože rozhoduje, zda údaje, které jsou zpracovávány, patří do oblasti ochrany osobních údajů a vztahuje se na ně zákon. Tedy až po posouzení zařazení se přistupuje k dalším ustanovením ZoOU, upravují se práva a povinnosti těch, kteří splňují kritéria § 4. (Pattynová, Suchánková, Černý a kol., 2018)

1.2.1 Osobní údaj

Pojem osobní údaj je specifikován několika prvky. Mezi první faktory patří vymezení rozsahu. Osobní údaj je nejzásadnější a nejvyužívanější pojem, který obsahuje jakoukoliv informaci týkající se identifikované nebo identifikovatelné fyzické osoby nebo-li subjektu údajů. Za identifikovatelnou fyzickou osobu lze označit každou fyzickou osobu, kterou je možné přímo, tedy přímým vztahem mezi údajem a osobou nebo nepřímo, přes spojení s disponujícími daty, identifikovat zejména odkazem na určitý identifikátor. Tímto identifikačním prvkem podle čl. 4 odst.1 GDPR může být např. jméno a příjmení, rodné číslo, datum narození, lokační údaje, povolání, kód, síťový identifikátor nebo jeden či více specifických prvků pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. (Kohútová, 2018, s. 6)

GDPR rozšiřuje ve srovnání se Směrnicí 95/46/ES výčet identifikátorů ve snaze zvýšit právní jistotu správců dat. Příkladem může být síťový identifikátor (IP adresa) nebo údaj o platu či odměně konkrétního zaměstnance, které jsou nově podle GDPR považovány za identifikační prvky vedoucí k identifikaci osoby. Mezi osobní údaje naopak nespadají údaje o právnických osobách. (Kohútová, 2018, s. 6)

Rozdělení údajů podle vazby k fyzické osobě :

- ***identifikační osobní údaje*** - jméno, příjmení, adresa bydliště, e-mailová adresa,
- ***číselné osobní údaje*** - datum narození, rodné číslo, telefonní číslo, číslo platební

karty, číslo občanského průkazu, číslo cestovního dokladu, číslo pojištěnce, SPZ motorového vozidla, osobní číslo zaměstnance, (Nulíček, 2018, s. 78-80)

- ***citlivé údaje -*** zdravotní stav, DNA, náboženské, filozofické nebo politické smýšlení, sexuální orientace, členství v politické straně nebo odborovém hnutí, biometrické údaje, odsouzení za trestný čin, (Nonnemann, 2018, s. 21-23)
- ***audiovizuální osobní údaje -*** fotografie, snímky, obrazové nebo zvukové záznamy, (Navrátil, 2018, s. 73)
- ***biometrické osobní údaje -*** otisky prstů, scany částí těla, zachycení způsobu chůze, (Nulíček, 2018, s. 75)
- ***anonymní údaje -*** tyto údaje nemají vazbu ke konkrétní fyzické osobě, tudíž se na ně nevztahuje ZoOU, mohou být výsledkem způsobu zpracování dat, takzvané anonymizace, (Žurek, 2017, s. 41-42)
- ***psedonymizované údaje*** – údaje, které lze ke konkrétní osobě přiřadit pouze s použitím dodatečných informací, dodatečné informace jsou uchovávány odděleně, vztahují se na ně technické a organizační opatření, (Žurek, 2017, s. 42-43)
- ***zveřejněný osobní údaj*** – osobní údaj, který je součástí veřejných seznamů nebo je zpřístupněn hromadnými sdělovacími prostředky, dále může být zpracováván pouze po provedení testu zákonného zpracování

(*Businesscenter.podnikatel.cz*[online]. Businesscenter ©2019 [cit. 2019-11-20]. Dostupné z: https://www.*Businesscenter.podnikatel*.cz/)

Tabulka č. 1 znázorňuje rozdíly mezi údaji osobními, anonymními a pseudonymizovanými.

Tabulka 1: Osobní , anonymní, psedonymizované údaje

Jméno	Příjmení	Adresa	Věk	Vzdělání	Příjem	Odměny	Benefity	Služ.auto	Stav
Josef	Novotný	V háji 8, Praha	38	SŠ	30000	5000	1500	ANO	Ženatý
			38	SŠ	30000	5000	1500	ANO	Ženatý
Josef	Novotný	V háji 8, Praha	38	SŠ	30000	5000	1500	ANO	Ženatý

001			38	SŠ	30000	5000	1500	ANO	Ženatý

Zdroj: upraveno podle (Žurek, 2017, s. 42)

V prvním řádku tabulky jsou uvedeny identifikační osobní údaje, podle kterých lze jasně identifikovat fyzickou osobu. Druhá kolonka obsahuje údaje, které jsou v uvedené podobě anonymní a nemají vazbu ke konkrétní osobě. Třetí řádek je rozdělen na dvě částí, které by byly uchovávány odděleně. Vybarvené části bude posléze přiřazen číselný kód a pouze

spojením dodatečné informace je možné subjekt údajů určit. (Žurek, 2017, s. 42-43)

1.2.2 Správce

O subjektu správce nerozhoduje jeho právní forma. Správcem se stane jak fyzická tak i právnická osoba, orgán veřejné moci nebo jiný subjekt, pokud samostatně nebo společně s jinými zpracovává osobní údaje a primárně za ně nese zodpovědnost. Dále určuje účely a prostředky zpracování osobních údajů. (Žurek, 2017, s. 85 - 86)

Pro správce je nejdůležitější účel zpracování osobních údajů, na který se vážou zásady a povinnosti zpracování. Zavedení GDPR přineslo dva nové přístupy pro správce, které přesně vymezují jeho odpovědnost při zpracování osobních dat s přihlédnutím k tomu jaké osobní údaje budou shromažďovány a kdo je bude shromažďovat. Zda bude nutností souhlas subjektu údajů, informovanost subjektu, doba, po kterou budou údaje shromažďovány a účely zpracování. Správce má povinnost zavést vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracovává standardně pouze osobní údaje, které pro svůj účel nezbytně potřebuje. Činnosti s daty jsou posuzovány jak z pohledu množství shromažďovaných osobních údajů, tak i rozsahu jejich zpracování. Sledováno je jejich uložení i dostupnost. Zvolená opatření musí být podle potřeby revidována, zdokumentována, sledována a aktualizována. (Nezmar, 2017, s. 39 – 40)

1.2.3 Zpracovatel

Zpracovatel je subjekt, fyzická nebo právnická osoba, která na rozdíl od správce osobní údaje pouze zpracovává, a to způsobem určeným správcem. Vhodný zpracovatel by měl správci poskytovat náležité technické a organizační opatření zajišťující požadavky GDPR, jelikož předáním dat se správce nezbavuje své odpovědnosti za ochranu osobních dat, kterou mu zákon ukládá. Správce předává data na základě výslovného zákonného zmocnění, dále na základě smluvního vztahu nebo je zpracování určeno přímo zákonem.
(Nezmar, 2017, s. 32 - 33)

Ve vztahu mezi správcem a zpracovatelem se nejčastěji používá smlouva o zpracování osobních dat v písemné podobě, jejíž náležitosti stanovuje GDPR v čl. 28 odst. 3. Ve smlouvě se uvádí předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních dat, kategorie subjektů údajů, povinnosti a práva správce (Nulíček, 2018, s. 294)
Dále musí ze smlouvy přesně vyplývat povinnosti pro zpracovatele:

- zpracovává osobní údaje pouze na základě pokynů správce,
- osoby, které se účastní zpracování, jsou vázány mlčenlivostí,
- poskytne bezpečnostní opatření v souladu s čl. 32 GDPR,

- dodržuje podmínky pro řetězení zpracovatelů a řídí se v něm pokyny správce,
- podle rozhodnutí správce po ukončení zpracování osobní údaje vymaže, znehodnotí kopie nebo údaje vrátí správci, umožní správci provést audit zpracování. (Nulíček, 2018, s. 294)

1.2.4 Subjekt údajů

Mezi základní pojmy je zařazen pojem subjekt údajů. Podle Zákona o ochraně osobních údajů se jedná o fyzickou osobu, ke které se osobní údaje vztahují. GDPR se dotýká pouze žijících fyzických osob. Ze zákona jsou z ochrany vyjmuty osobní údaje zemřelých fyzických osob, ale i údaje o právnických osobách. V případě podnikající fyzické osoby zákon dělí údaje na ty, které se dotýkající soukromí této osoby a na údaje vztahující se k její podnikatelské činnosti. Záznamy z podnikatelské aktivity nepobírají ochranu zákona. (Nezmar, 2017, s. 32)

1.2.5 Práva subjektu údajů

V obecné rovině je pojem práva chápán jako minimum morálky, obsahuje základní právní normy, které musí být dodržovány. Přijetím GDPR došlo k výraznému posílení výkonu práv fyzických osob. Práva jako např. právo na informace či přístup k osobním údajům z oblasti pracovně-právní, která byla již dříve uvedena např. ve Směrnici 95/46/ES či v Zákoně 101/2000 Sb. prošla aktualizací a vedle již dříve uvedených práv se objevila práva nová, jako např. právo na přenositelnost údajů. GDPR sice stanovuje jednotlivé povinnosti pro správce týkajících se výkonu práv subjektů, ale v praxi probíhají často souběžně a vzájemně se nevylučují. V první řadě by tato práva měla zaručovat zásadu transparentnosti zpracování, subjekt by měl mít právo na informace a to zcela automaticky, aniž by musel o to správce požádat. K základnímu poskytovanému minimu informací patří znalost osoby správce případně jeho zástupce popř. pověřence, byl-li stanoven. (Janečková, 2018, s. 21)

Subjekt údajů by měl znát oprávněné zájmy správce nebo třetí strany, pokud je zpracování prováděné na základě právního důvodu. Dále by měl být obeznámen s případnými příjemci osobních údajů a úmyslem správce předávat data do třetích zemí. V neposlední řadě má správce povinnost subjektu údajů sdělit kategorie dotčených osobních údajů. Vedle tohoto informačního minima může správce v rámci zajištění spravedlivého a transparentního zpracování poskytnout i další informace a to např. dobu, po kterou hodlá data používat, skutečnost zda poskytnutí je na základě smluvního nebo právního důvodu, který ho opravňuje ke zpracování. Subjekt má právo vědět, z jakého zdroje správce získal informace o jeho osobě a o svoji možnosti případné kontroly, opravy nebo výmazu těchto dat. S transparentností zpracování souvisí i další právo subjektu údajů a to právo na přístup k osobním údajům, které spadá mezi práva aktivní, závislá pouze na vůli subjektu. Od správce

se požaduje takový přístupke zpracování, který kdykoli umožňuje poskytnout potvrzení o jeho činnostech v oblasti nakládání s osobními daty.

Shromážděné údaje podléhají aktualizaci a subjekt údajů při ní využívá další svoje právo na opravu a doplnění v případě zjištění neúplnosti informací. I samotný správce může také přispět k aktuálnosti dat prostřednictvím zaslané žádosti o kontrolu osobních údajů předanou subjektu při vzájemné komunikaci nebo při internetovém přihlášení na jeho stránky. Subjekt údajů může požádat o likvidaci údajů a využít tak svého práva na výmaz v případě, pokud již pominul důvod jejich shromažďování nebo je správce zpracoval protiprávně. Údaje budou správcem také povinně smazány po odebrání souhlasu, na základě kterého je směl zpracovávat.

Dalším právem subjektu údajů je omezení zpracování, kterým jsou dané údaje označeny a jejich použití do budoucna je omezeno. Jak již bylo výše uvedeno GDPR zavádí nové právo a to právo na přenositelnost údajů. Toto právo připomíná právo na přístup k osobním údajům, podstatnou odlišností mezi těmito dvěma právy je ale strukturovaný, běžně používaný a strojově čitelný formát. Po splnění podmínek jako je souvztažnost údajů k subjektu, poskytnutí dat subjektem či uvedený formát, smí upravené údaje subjekt údajů předat jinému správci k dalšímu zpracování nebo si je ponechat. Předpokládá se postupný vývoj i výklad práva na přenositelnost údajů a jeho kodifikace. Zpracovává-li správce údaje, které byly shromážděny původně na základě právního důvodu, pro účely přímého marketingu, má subjekt údajů právo vznést proti tomuto konání námitku. Podle GDPR má subjekt údajů právo nebýt předmětem automatizovaného individuálního rozhodování, zahrnující i profilování, není-li nutností k uzavření nebo plnění smlouvy mezi správcem a subjektem.
(Janečková, 2018, s. 21-26)

1.2.6 Příjemce

Subjekt, který údaje nezpracovává, ale v rámci postupů a úkonů při jejich zpracování jsou mu zpřístupněny, se nazývá příjemce. I v případě jakékoliv činnosti příjemce v oblasti kontrolní, dozorové či dohledové, musí být zajištěna ochrana práv subjektu.
(Vodička, Drábková, 2019, s. 7)

Do skupiny příjemců se řadí:

- poskytovatelé informačních systémů,
- orgány státní správy a státního dozoru,
- zákazníci,
- dodavatelé služeb, kteří se podílejí na realizaci obchodních případů,

- potenciální zákazníci,
- externí dodavatelé služeb (např. služby ostrahy objektů či úklidu),
- ostatní subjekty (např. poškození při dopravních nehodách).
  (Pattynová, Suchánková, Černý a kol.,2018, s. 56)

1.2.7 Pověřenec pro ochranu osobních údajů (DPO)

S přijetím GDPR se zavádí také působnost nového institutu pověřence pro ochranu osobních údajů, který zajišťuje konzultace a další odbornou pomoc u právnických či fyzických osob v oblasti plnění povinností dle GDPR. Pověřenec nese za svou činnost odpovědnost, ale dojde-li k porušení předpisů v oblasti ochrany údajů, nese následky správce a až následně pověřenec.

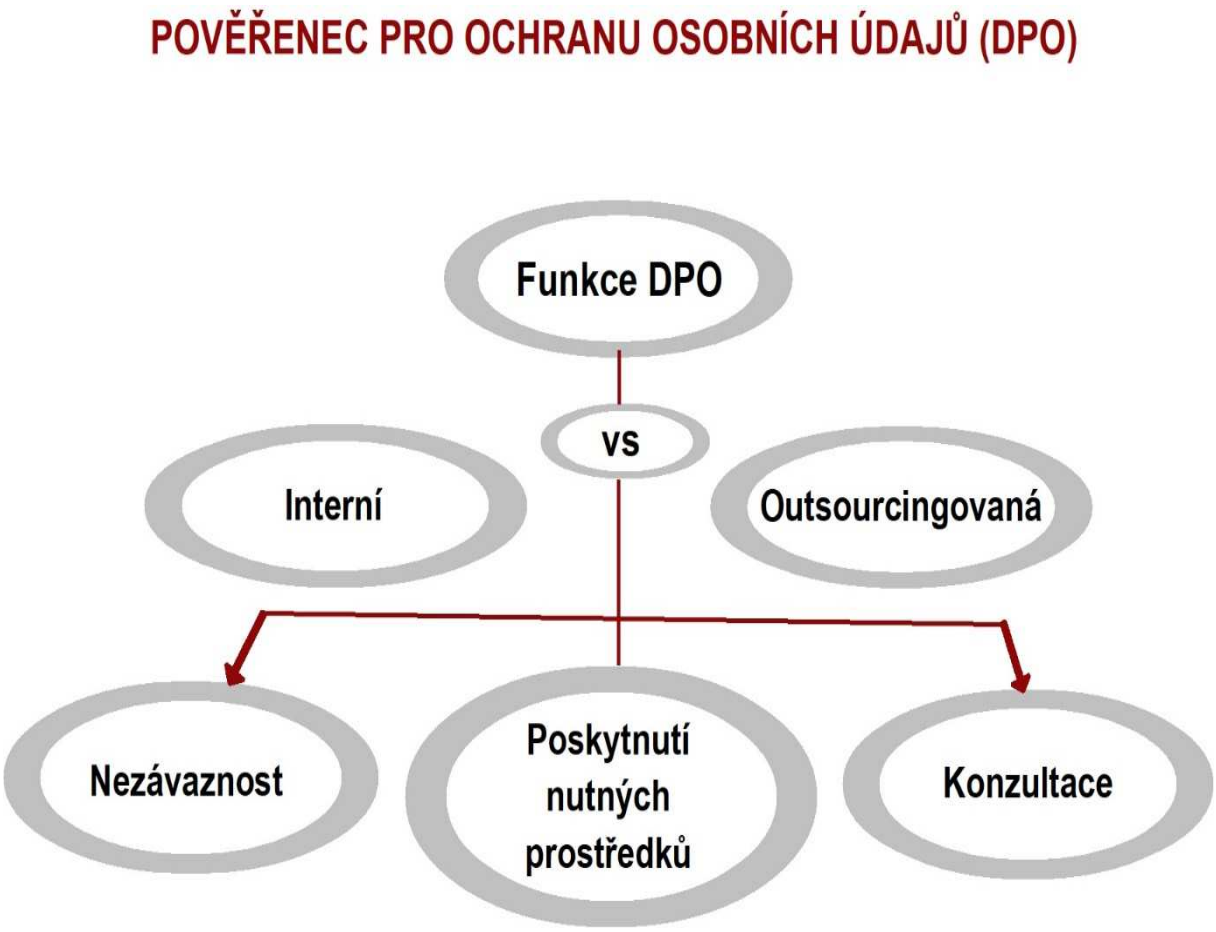
Funkci DPO může vykonávat osoba, která je zaměstnancem instituce nebo tuto funkci bude vykonávat na základě uzavření smlouvy o poskytování služeb externě viz. Obrázek č. 1. Interního pověřence budou pravděpodobně využívat velké organizace a to vzhledem k časové náročnosti a množství práce, které bude muset plnit. Důležitá je otázka, kdo musí mít povinně pověřence. (Navrátil a kol., 2018, s. 241)

Podle čl. 37 odst. 1 GDPR musí jmenovat pověřence:

- všechny orgány veřejné moci a veřejné subjekty, řadí se sem státní orgány, územní samosprávné celky, fyzické a právnické osoby, které mají působnost v oblasti veřejné správy. V této oblasti dochází v rámci GDPR k rozporu, protože jsou vyčleněny mikropodniky, které nemusí mít pověřence a současně jako orgány veřejné správy nebo veřejné subjekty ho mít musí, příkladem jsou notáři, advokáti, insolvenční správci či exekutoři; (Žurek, 2017, s. 106 - 107)
- osoby, které jako správce nebo zpracovatel, zpracovávají v hlavní činnosti data v takovém rozsahu a povaze či účelu, že vyžadují pravidelné a systematické monitorování subjektu údajů, tedy zdravotnická zařízení, vzdělávací instituce, bezpečnostní agentury, městská hromadná doprava, pojišťovny, banky, poskytovatelé telefonních a internetových služeb či příspěvkové organizace;
  (Nulíček, 2018, s. 367 - 368, Nonnemann, 2018, s. 17)
- osoby, které jako správce nebo zpracovatel, zpracovávají v hlavní činnosti zvláštní kategorie dat uvedených v čl. 9 GDPR a osobní údaje týkajících se trestních činů a rozsudků. (Pattynová, Suchánková, Černý a kol., 2018, s. 279)

Pokud si organizace není jistá, zda má mít pověřence, doporučuje se provedení interní analýzy, pomocí niž dospějí k závěru a určení potřeby institutu pověřence. Interní analýza je

poté součástí dokumentace ochrany osobních údajů v této organizaci. (Žurek, 2017, s. 105)



Obrázek 1: Funkce DPO

Zdroj: vlastní zpracování

2 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A JEHO DRUHY

„*Zpracováním osobních údajů se rozumí jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, použití, šíření, zpřístupnění přenosem, omezení, výmaz nebo zničení*“.

(Nulíček, 2018, s. 74, Pattynová, Suchánková, Černý a kol., 2018, s. 47)

Osobní údaje, jak vyplýva z definice, mohou být zpracovány jednou operací nebo se použije celý soubor činností. Z druhé její části je zřejmé, že správce či zpracovatel provádí systematickou činnost s určitým záměrem. Pojem „ *systematické zpracování* “ je pro zákon rozhodný, protože na pouhé nahodilé shromažďování se neaplikuje. Údaje se nejčastěji zpracovávají pomocí výpočetní techniky, ale také je možné manuální zpracování.

(Žurek, 2017, s. 54 – 55)

Při všech činnostech zpracování dat však musí být vždy dodrženy základní zásady pro zpracování osobních dat, které stanovuje GDPR v čl.5 odst. 1. V tabulce č. 2 je uveden výčet zásad zpracování jako je zákonnost, korektnost, transparentnost zpracování, účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita, důvěrnost a odpovědnost. Dále tabulka obsahuje stručný popis zásady, tedy v čem spočívá. Poslední sloupec odkazuje na článek v Nařízení, kde je uvedená zásada upravena. (Žurek, 2017, s. 58)

Jak již bylo uvedeno výše pojem zpracování v sobě zahrnuje více operací, které může správce nebo zpracovatel s osobními údaji provádět. Mezi nejčastěji používané druhy zpracování dat jsou zařazeny shromažďování, uchovávání, blokování a likvidace. (Nonnemann, 2018, s. 123 - 124)

Tabulka 2: Základní zásady při zpracování údajů

Základní zásada	Popis v čem spočívá	Upravena
Zákonnost	zpracování probíhá v souladu s právem, tedy podle zákona, na základě souhlasu dotčené osoby nebo na základě jiného důvodu : splnění smlouvy, splnění právní povinnosti, nezbytné z důvodu ochrany životně důležitých zájmů osoby, splnění veřejného zájmu a pro účely oprávněných zájmů příslušného správce	čl. 5/1/a
Korektnost	v poctivosti a ohleduplnosti správce při zpracování dat s přihlédnutím k zájmům a očekáváním subjektu dat	čl. 5/1/a
Transparentnost	realizována informační povinností při sběru dat k dotčené osobě, zajišťuje technika a správně nastavené prostředí, informace a sdělení o zpracování bude jednoduše přístupné a srozumitelné, informovanost o budoucím zpracování osobních údajů	čl. 5/1/a
Účelové omezení	doplňuje zásadu transparentnosti, v tom, že účel zpracování osobních dat musí být znám již při sběru dat, pozdější změna nebo rozšíření nesmí být v rozporu s původním účelem existuji tři výjimky v účelovém omezení: • souhlas dotčené osoby, • právní předpis dle čl.23/1 a 6 odst.4, • veřejný archivační zájem, statistický, historický a vědecký výzkum.	čl.5/1/b
Minimalizace údajů	data musí být pro daný účel podstatná, potřebná a přiměřeně omezená na vhodný stupeň odpovídající sledovanému účelu,	čl.5/1/c
Přesnost	zpracovaná data by měla být věcně správná a dle potřeby aktuální. Nepřesná data musí být opravena nebo vymazána	čl.5/1/d
Omezení uložení	údaje jsou uloženy pouze po dobu nutnosti identifikace osoby s účelem zpracování	čl.5/1/e
Integrita a důvěrnost	při zpracování musí být zajištěna přiměřená bezpečnost, zamezení před neoprávněným a nezákonným zpracováním, ochrana před ztracením, zničením nebo poškozením dat	čl.5/1/f

Základní zásada	Popis v čem spočívá	Upravena
Odpovědnost	zajištění dodržování zásad Nařízení a jejich prokázání pomocí technických a organizačních opatření v souladu s GDPR	čl.5/2

Zdroj: upraveno podle (NEZMAR, 2017)

2.1 Shromažďování osobních údajů

Shromažďováním dat je označována systematická činnost, jejíž cílem je získat osobní údaje pro okamžité použití popř. uložení a pozdější využití. Správce s určitým cílem vytváří pomocí technických prostředků uspořádané soubory, které ukládá na nosiče informací. Tyto nosiče zákon nijak nespecifikuje, určující je pro ně schopnost informace uchovávat. Následná využití shromážděných osobních údajů nejsou limitována, závisí na správci popř. zpracovateli, který určuje sled činností dalšího zpracování dat. (Nulíček, 2018, s. 85)

2.2 Uchovávání osobních dat

Uchovávání je další činnost, která následuje po shromáždění dat, pokud má správce nebo zpracovatel za cíl data dále využívat. Data by měla být uchována v takové podobě a na takovém nosiči, který umožňuje kdykoliv je následně zpracovávat bez omezení. Během uchovávání je možné údaje převádět z jedné formy do druhé. Například data uložená v písemné formě převést do elektronické podoby. Je na osobním rozhodnutí správce či zpracovatele zhodnotit kvalitu použitého nosiče vzhledem k cennosti získaných informací. Vždy by měli k zpracování dat přistupovat s vědomím a znalostí § 4 písm. e ZoOU. (Nulíček, 2018, s. 85)

2.3 Blokování osobních údajů

Blokování je proces dočasného znepřístupnění a ochranné opatření, nikoliv samostatný způsob zpracování dat. Blokováním osobních údajů nebo-li zamezením přístupu ke zpracování shromážděných dat může správce či zpracovatel reagovat v případě zjištění, že zpracovávaná osobní data nejsou aktuální nebo došlo-li k porušení ochrany osobních údajů. Aktuální stav údajů mohou zpracovatelé zjistit porovnáním informací z různých přístupných registrů nebo jim je sdělí sám subjekt údajů, který požádá o opravu, doplnění či likvidaci shromážděných dat. (Kohútová, 2018, s. 24)

2.4 Likvidace osobních údajů

K likvidaci osobních údajů může dojít ve dvou případech. Buď se jedná o plánovanou

operaci, kdy správce nebo zpracovatel v některých případech ukončí proces zpracování osobních údajů nebo dojde k neoprávněnému poškození a zničení při zneužití osobních dat. Vždy se jedná o již nevratný krok a ztracené informace nelze obnovit. Správce a zpracovatel musí přijmout vhodná opatření, aby riziko nepředvídatelného neoprávněného přístupu bylo co nejmenší. Při plánované likvidaci o způsobu zničení dat rozhoduje použitý nosič informací. Papírová podoba je zlikvidována skartací, elektronická smazáním. (Žurek, 2017, s. 133 – 134)

2.5 Souhlas se zpracováním osobních dat

Pro použití souhlasu jsou stanoveny přesná pravidla, která zaručují, aby se jednalo o svobodný a vědomý projev od subjektu údajů, který není v žádném případě podmíněný. Žádost o souhlas by měla být pro osobu viditelná a oddělená od ostatních smluvních podmínek. Subjekt údajů by měl v každém případě vědět pro koho, pro jaký účel zpracování údajů a k jakým osobním údajům poskytuje souhlas, aby byla splněna další z podmínek GDPR, tedy jeho informovanost. (Nulíček, 2018, s. 93-94)

Souhlas musí být také konkrétní, což znamená, že správce či zpracovatel při jeho získání konkrétně vyspecifikuje účel zpracování dat a jeho rozsah. Velmi důležitou podmínkou při udělování souhlasu je jeho jednoznačnost. V praxi existují tři způsoby získání souhlasu. V písemné podobě subjekt údajů uděluje souhlas podepsáním prohlášení s textem, v případě elektronického formuláře zatrhává příslušné políčko a provádí zjevné potvrzení. Ve třetím případě, kdy subjekt údajů dává souhlas ústně přes telefon nebo jeho ekvivalent, je nutné uložení záznamu pro možnou kontrolu. (Nonnemann, 2018, s. 128, Žurek, 2017, s. 69 - 74)

Novou povinností pro správce v souladu s GDPR je zastavení zpracování dat, pokud se subjekt údajů rozhodne využít své právo na odvolání souhlasu. Toto odnětí podle článku 7 je dáno na stejnou úroveň jako jeho udělení. (Žurek, 2017, s. 75)

„ *Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Odvolat souhlas musí být stejně snadné jako je poskytnout* “. (Žurek, 2017, s. 75)

Splnění nového požadavku je tedy nutné zakomponovat již do oblasti tvorby informačních systémů a návrhů webových stránek správce, aby mu probíhající procesy a postupy umožnily potvrzení nebo odebrání souhlasu pro jednotlivé účely zpracování a dále zajistily systematickou kontrolu těchto procesů.
(Navrátil, 2018, s.114, Nezmar, 2017, s. 148-149)

Správce či zpracovatel nemusí požadovat pro povolení zpracování osobních údajů vždy pouze udělený souhlas od subjektu údajů, může využít dalších ustanovení uvedených v Nařízení v článku 6 odst. 1.

Bez souhlasu může zpracovávat osobní data v těchto případech:

- jedná - li se o plnění smlouvy v případě dodání zboží nebo služby požadované fyzickou osobou, dále o splnění závazků vyplývajících z pracovní smlouvy,
- v případě, že jde o splnění právní povinnosti dle právních předpisů či zákonů (zákon o účetnictví, archivnictví),
- týká- li se zpracování údajů ochrany životně důležitých zájmů (záchrana života, léčba),
- plnění při výkonu veřejné moci nebo ve veřejném zájmu, pokud zpracovává data při plnění úředních povinností,v rámci oprávněného zájmu v oblasti podnikání. (Navrátil a kol., 2018, s. 113)

2.6 Souhlas dítěte a ochrana osobních údajů dětí

GDPR ve zvýšené míře dohlíží na ochranu osobních údajů dítěte, protože může být více vystaveno riziku ohrožení v oblasti marketingu nebo při tvorbě osobních profilů. Také obsahuje zvláštní ustanovení o službách informačních služeb poskytnutých přes internet v článku 8, odst. 1, které se vztahuje na souhlas dětí v souvislosti s nabídkou služeb informačních společností. Děti nemohou uzavírat obchodní smlouvy a pokud jsou služby nabízeny přímo dětem, podle nařízení tedy osobám mladším 16 let, je nutné ověření jejich věku a vyžadován souhlas zákonného zástupce dítěte. Veškeré informativní texty týkající se zpracování dat musí být podány srozumitelně a co nejjednodušším způsobem, doplněné i obrázky. Hranice 16 let se po schválení adaptačního zákona snížila na 15 let.
(Žurek, 2017, s. 76 - 77)

3 DOZOROVÉ ORGÁNY

V jednotlivých členských státech jsou stanoveny nezávislé orgány veřejné moci jako dozorové instituce, které mají za úkol monitorovat ochranu osobních údajů při jejich zpracování. Dozorové úřady jednotně chrání základní práva a svobody osob v celé EU a vzájemně mezi sebou spolupracují při uplatňování GDPR. Pro naplnění jednotnosti v oblasti ochrany osobních údajů při jejich zpracování byla zřízena pracovní skupina WP29, kterou tvoří vedoucí zástupci dozorových úřadů ze všech států Unie.
(Morávek, 2003, s.144, Janečková, 2018, s. 99)

3.1 Skupina WP29

Vzniku pracovní skupiny WP29 dohlížející na oblast ochrany osobních údajů v EU dala základ Směrnice 95/46/ES. Po přijetí GDPR 25. května 2018 se skupina transformovala na Evropský sbor pro ochranu osobních údajů. Sbor pokračuje v podávání doporučení a stanovisek z oblasti zpracování osobních údajů, které publikuje na svých stránkách. Dále sbor pomocí vydávávaných dokumentů objasňuje nové zaváděné prvky, které sebou přináší Obecné nařízení. Zveřejněním výkladových materiálů napomáhá k objasnění novinek a odstranění nejasností. (Žurek, 2017, s. 28 – 29)

3.2 Dozorový úřad v České republice

Funkci dozorového úřadu a ústředního správního úřadu v oblasti zpracování osobních údajů v rámci České republiky zastává Úřad pro ochranu osobních údajů (ÚOOÚ). Rozsah jeho činností je velmi široký (Janečková, 2018, s. 99).

Hlavním úkolem, stejně jako u ostatních dozorových úřadů v Evropské unii, je monitoring a kontrola dodržování Obecného nařízení. Vedle své dozorové činnosti, monitoringu a kontroly dále působí v oblasti osvěty a poradenství. Snaží se o rozšíření znalostí správců a zpracovatelů v oblasti ochrany osobních údajů. Působnost úřadu však není směřována jen na oblast správců a zpracovatelů či státních orgánů a institucí, je mnohem širší, protože zasahuje taktéž veřejnost. I tu seznamuje s právy, povinnostmi, podmínkami a riziky zpracování osobních údajů. Úřad přijímá a následně vede šetření předložených stížností a s výsledky seznamuje dotčené subjekty. Mapuje vývojové trendy v oblastech, kde dochází k přenosu a následnému zpracování dat, tedy v informačních oblastech, komunikačních technologiích a obchodu. Eviduje smluvní doložky, které upravují vzájemné vazby mezi správci a zpracovateli či doložky umožňující přenos údajů do třetích zemí. (Žurek, 2017, s. 166 - 168)

Dále úřad, jako člen Evropského sboru, seznamuje s překladem aktuálních výkladů, které se vztahují k aplikaci GDPR. Nastavuje mechanismy a zavádí kritéria pro výběr subjektů, kte-

ré vydávají osvědčení o ochraně osobních dat. Vydaná osvědčení poté pravidelně prochází jeho kontrolou. V neposlední řadě zaznamenává zjištěná popř. nahlášená porušení Obecného nařízení. Veškeré činnosti, které úřad poskytuje pro subjekty údajů a pověřence, jsou bezplatné. (Žurek, 2017, s. 170 – 171)

3.2.1 Kompetence dozorového úřadu

Ke splnění úkolů z oblasti ochrany osobních údajů dozorový úřad vhodně propojuje vyšetřovací, nápravné, povolovací a poradní kompetence. Vyšetřovací kompetence se řadí k základním pravomocem každého dozorového úřadu a umožňují mu např. nařízení spolupráce pro dotčené subjekty či neomezený přístup k osobním údajům a informacím v rámci šetření. Úřad má zásadní pravomoc v rámci vyšetřování provádět audit u kontrolované osoby na základě kontrolního řádu. Pokud při posouzení nejsou přestupky dle správního řádu tak závažného rázu, uplatní dozorový orgán další ze svých pravomocí, které mají preventivní či nápravný charakter. Umožňují mu upozorňovat subjekty zpracovávající data na případná porušení GDPR a následně předat doporučení k uvedení zpracování do souladu s GDPR vhodným způsobem a v dané lhůtě. (Žurek, 2017, s. 168 - 169)

Dozorový úřad může správci nebo zpracovateli z důvodu nápravy stavu zpracování údajů přikázat opravení nebo výmaz dat, které jsou chybně zpracované. Článek 36 Nařízení umožňuje úřadu poradenskou činnost, kterou lze poskytnout správci po proběhlé konzultaci. (Žurek, 2017, s. 170)

Do oblasti povolovacích kompetencí spadá možnost dozorového orgánu stanovit subjekty vydávající osvědčení či schvalování kodexu chování nebo povolení smluvních doložek, které upravují předávání informací mezi správci a zpracovateli. (Žurek, 2017, s. 171)

3.3 Sankce a pokuty

Každý zákon nebo nařízení obsahuje i sankce, které mají donutit a preventivně působit na subjekty svého určení. V Obecném nařízení jsou uvedené v čl. 83, který popisuje podmínky uložení a následně i výši pokuty za porušení ustanovení. Z nařízení vyplývá, že výše pokut se posuzuje podle jednotlivých případů, nikoliv plošně. Pokuta by měla být účinná, přiměřená a v neposlední řadě odrazující. V některých případech porušení nemusí být pokuta vůbec uložena, správce je napomenut za porušení nebo upozorněn na chybné zamýšlené operace v oblasti zpracování dat. (Žurek, 2017, s. 178 - 180)

Dozorový úřad posuzuje a zohledňuje tyto okolnosti při udělení a rozhodnutí o výši pokuty:

- úmyslné nebo nedbalostní porušení,
- povahu, závažnost a délku porušení, počet dotčených subjektů, míru způsobené škody,

- kroky vedoucí k zmírnění poškození,
- míru odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením,
- míru spolupráce s dozorovým úřadem,
- kategorie osobních dat, kterých se porušení dotklo,
- způsob a míru oznámení porušení správcem či zpracovatelem,
- splnění opatření v případě, že se jedná o stejný předmět, za který byla správci nebo zpracovateli již nařízena opatření dle čl.58 odst.2 Nařízení,
- jakoukoliv skutečnost, která je polehčující nebo přitěžující v případě porušení. (Žurek, 2017, s.179)

Obecné nařízení je tedy v oblasti ukládaní sankcí a pokut velmi variabilní, umožňuje je neudělit nebo současně s pokutou přikázat nápravná opatření dle čl.58 odst.2 písm. a) až h). Dozorový úřad může správce či zpracovatele upozornit na skutečnost, že operace, které zamýšlí provést, jsou v rozporu s Obecným nařízením. Při již vzniklém porušení jim udělit napomenutí. Dále nařídit správci nebo zpracovateli výkon práv subjektu dle Nařízení, uvedení operací zpracování do souladu s GDPR, dočasné nebo trvalé omezit zpracování, opravit, vymazat nebo omezit zpracování a ohlašování opatření příjemcům. Jako další nápravné opatření působí odebrání osvědčení nebo zákaz jeho vydání subjektem, který je oprávněný jej vydat. Úřad může nařídit správci přerušení předávání zpracovaných dat do třetích zemí. Jedním z možných opatřeních je i uložení správní pokuty dle čl. 83 GDPR a její výši stanovit na základě posouzení jednotlivého případu.
(Nezmar, 2017, s. 43 - 44, Žurek, 2017, s. 180)

Z výše uvedeného vyplývá, že pokuty jsou udělovány pouze v případech hrubého porušení a v ostatních, kdy dojde pouze k formálnímu porušení Obecného nařízení s minimální společenskou škodlivostí, postačí některé z nápravných opatření. Správce obdrží informativní dopis, kde bude informován o svých povinnostech uvedení zpracování osobních údajů do souladu s GDPR. Zákon o zpracování osobních údajů také upřesňuje pro udělování pokut materiálně – formální definici přestupku. Nestačí „pouhé“ porušení zpracování osobních údajů, z jednání musí být patrná i materiální neboli společenská škodlivost. Obsahuje ustanovení, které umožňuje upustit od uložení pokuty, pokud dojde k okamžité nápravě po zjištění porušení. (Žurek, 2017, s. 180)

3.3.1 Promlčecí doba

Přijetím zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich 1. července 2017 došlo k významnému posunu v úpravě přestupků a správních deliktů. Před přijetím

tohoto zákona byla úprava promlčecí doby rozmístěna do jednotlivých zákonů, které se v určení její délky značně lišily. Výše uvedeným zákonem č. 250/2016 Sb. došlo ke sjednocení promlčení přestupků. V případě menšího porušení se jedná o 1 rok, pokud se jedná o závažnější přestupek k promlčení dojde za 3 roky. Závažnost přestupku je posuzována podle horní hranice pokuty, která musí dosáhnout alespoň výše 100 000 Kč. Přestupky z oblasti porušení GDPR se řadí svou závažností, ale hlavně hranicí pokuty do 3 leté promlčecí doby. (Žurek, 2017, s. 181)

3.3.2 Výše pokut

Porušení se dle GDPR dělí do dvou kategorií možných sankcí, které se stanovují podle míry ohrožení ochrany práv a svobod subjektu údajů. Vyšší sankci následně dostane subjekt za nedodržení zásad zpracování, nižší v případě nevyhotovení záznamů o zpracování osobních dat. Rozdělení do kategorií je vázáno na porušení povinností vyplývajících z daných článků. (Navrátil a kol., 2018, s. 91, Žurek, 2017, s. 181)

I. Kategorie: porušení povinností správce a zpracovatele podle čl. 8, 11, 25 až 39, 42 a 43, pokuta až do 10.000.000 EUR, jde-li o podnik, 2 % celkového ročního obratu, viz. tabulka č. 3,
(Pattynová, Suchánková, Černý a kol., 2018, s. 453 – 454, Žurek, 2017, s. 182)

II. Kategorie: porušení souladu se zpracování podle čl. 5, 6, 7 a 9, dále za porušení práv subjektů údajů čl. 12 až 22 a za porušení při předání osobních údajů do třetích zemí nebo mezinárodní organizaci podle čl. 44 až 49 Nařízení, pokuta až do 20.000.000 EUR, jde-li o podnik, 4 % celkového ročního obratu viz. tabulka č. 4.
(Pattynová, Suchánková, Černý a kol., 2018, s.453 – 454, Žurek, 2017, s.183)

Na výběr sankcí dohlíží dozorový úřad, který vybranou částku předává do státního rozpočtu. Úřad v případě neuhrazení pravomocně uložené pokuty pověřuje vymáháním celní úřad. (Žurek, 2017, s. 181)

Jednotlivé státy EU mohou podle čl. 83 odst. 7 GDPR využít možnost omezit výši sankce úpravou platnou pouze v dané zemi. V České republice se stal národní úpravou adaptační zákon č. 110/2019 Sb., který v ustanovení č. 61 odst. 5 stanovil pro správce a zpracovatele uvedené v čl. 83 odst. 7 Nařízení pokutu do 10 000 000 Kč. Hlavní důvod pro snížení sankcí pro veřejnoprávní instituce vyplývá z faktu, že finanční zdroje daných entit pochází z veřejných rozpočtů. Protože není možné ani v případě institucí s malým rozpočtem vyloučit pokuty úplně, musí být uloženy tak, aby se pro subjekt nestaly likvidační.
(Pattynová, Suchánková, 2019, s. 18 -19, Janečková, 2018, s. 108)

Tabulka 3: Výčet nejčastějších porušení povinností v kategorii I

SPRAVCE A ZPRACOVATEL	**KATEGORIE I. 10000000 EUR nebo v případě podniku 2 % obratu**
	- při zabezpečení ochrany osobních dat
	- při výběru a spolupráci se zpracovatelem
	- vyhotovení záznamů o zpracování
	- spolupráce s dozorovým úřadem
	- ohlášení porušení zabezpečení osobních údajů subjektu údajů popř. dozor. úřadu
	- posouzení vlivu na ochranu osobních dat
	- v oblasti jmenování a podmínek pověřence
	- stanovení zástupce v případě usídlení správce či zpracovatele mimo EUv oblasti získávání osvědčení

Zdroj: upraveno podle ŽUREK, 2017, s. 182

Tabulka 4: Výčet nejčastějších porušení povinností v kategorii II

SPRÁVCE A ZPRACOVATEL	**KATEGORIE I I. 20000000 EUR nebo v případě podniku 4 % obratu**
	- zákonného zpracování
	- při získávání souhlasu
	- práv subjektu údajů
	- při předávání údajů do třetí země
	- zvláštní případy zpracování, které GDPR umožňuje upravit v rámci státu
	- splnění příkazu nebo omezení nebo přerušení zpracování podle čl. 58 odst. 2 GDPR
	- nesplnění příkazu dozorového úřadu podle čl.58 odst. 2 GDPR

Zdroj: upraveno podle ŽUREK, 2017, s.183

4 PROJEKT IMPLEMENTACE GDPR DO FIRMY

GDPR vstoupilo v platnost 25. května 2018 a dotklo se všech společností, které nějakým způsobem pracují s osobními daty fyzických osob. Implementace opatření k zajištění souladu s GDPR byla pro firmu časově i finančně náročným projektem, který se dotkl celého systému v organizaci. Firma Bazalka s.r.o. musela celý projekt časově zvládnout tak , aby jí nehrozily případné sankce z nesplnění povinností. Vedení firmy si uvědomovalo, že výše finančních postihů by pro společnost mohla být až likvidační, proto k celému procesu přistoupilo s velkou zodpovědností.

4.1 Stanovení cílů , hypotéz a metod

Základem pro zvládnutí implementace GDPR ve firmě Bazalka bylo vytvoření plánu obsahujícího všechny fáze procesu a to včetně finančního rozpočtu a časového harmonogramu. Manažerka se domnívala, že nejvhodnější bude projekt rozdělit do pěti fází. Za hlavní cíl si stanovila zajištění souladu s GDPR ve všech oblastech činností probíhajících v organizaci do 25. května 2018.

V první fázi bylo nejdůležitější stanovit jakým způsobem bude implementace probíhat, zda celý projekt bude předán externí firmě nebo bude proveden interně zaměstnanci společnosti. Následující fáze plánu vycházely z přepokladu, že firma proces zvládne sama.

Druhá fáze zahrnovala možnosti nabídek odborných přednášek a školení z oblasti ochrany osobních dat. Poté nasledovala fáze, ve které by proběhlo zmapování všech procesů a datových toků probíhajících v organizaci. Měl být vytvořen katalog zpracování osobních údajů, který by evidoval operace zpracování, účely zpracování, nutnost souhlasu popř. délku uchování dat.

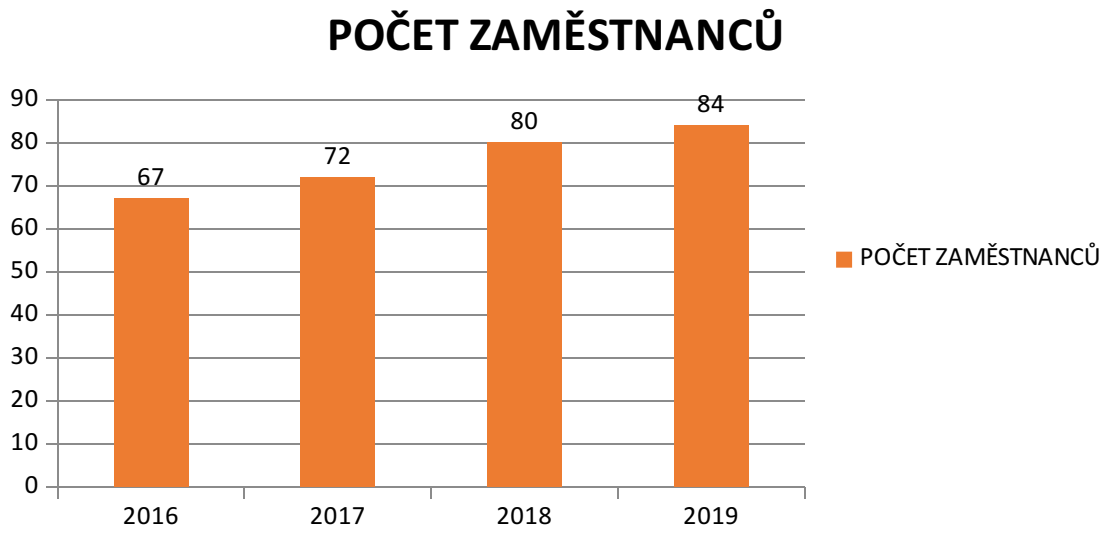
Ve čtvrté fázi budou všechny procesy včetně dokumentací podrobeny analýzám, které je porovnají se zásadami uvedenými v GDPR. Předpokládaným výstupem by měly být rozdíly mezi skutečným stavem a požadavky Nařízení. Mezi navrhované metody patří GAP analýza a následná dopadová analýza DPIA. V tomto kroku proběhne rozhodnutí, zda bude organizace potřebovat pověřence pro ochranu osobních údajů.

V závěrečné fázi proběhne samotná implementace, která bude zahrnovat změny v jednotlivých procesech, technická a organizační opatření k zajištění ochrany osobních údajů, tak aby odpovídaly platným zákonům a byly dokončeny ve stanoveném termínu.

4.2 Profil firmy

Firma Bazalka, s.r.o. má již dlouhou historii. Její základ položili v roce 1992 společně manželé Lukešovi. Nejprve podnikali jako fyzická osoba pod jménem Jany Lukešové, v roce 2010 firmu převedli na společnost s ručením omezeným a přejmenovali na Bazalku. Soukromý podnik podniká v oblasti zdravé výživy v Hradci Králové, kde tato společnost provozuje dva bio obchody, vegetariánskou a veganskou restauraci a v nedalekých Třebechovicích peče vlastní výrobky ve své pekárně. Se zvyšováním objemu výroby a ozšiřováním prodeje bylo nutné zvýšit také počet zaměstnanců. Obrázek č. 2 znázorňuje nárůst pracovní síly v období 2016 – 2019.

(*Bazalkahk.cz*[online]. Bazalka ©2019 [cit. 2019-11-23]. Dostupné z: https://www.*Bazalkahk*.cz/).



Obrázek 2: Počet zaměstnanců 2016-2019

Zdroj: vlastní zpracování

4.2.1 Předmět podnikání a provozovny

Společnost Bazalka, s.r.o. se řadí mezi významné výrobce a prodejce širokého sortimentu zdravé výživy. Specializuje se na potraviny pro bezlepkovou dietu, výrobky bez cukru a z celozrnné mouky. V jejím širokém sortimentu lze nalézt vegetariánské, veganské a makrobiotické produkty. Ve svých obchodech prodává bylinné a ovocné čaje, kofeinovou i bezkofeinovou kávu, přírodní, na zvířatech netestovanou kosmetiku a ekologicky šetrné hygienické prostředky.

Obyvatelé Hradce Králové již od roku 2000 navštěvují jídelnu, kde je možné si ve všední den pochutnat na zdravém obědě. Na počátku nového tisíciletí přebudovala Jana Lukešová bývalý fotoateliér na vegetariánskou jídelnu. Všechna jídla, která jsou zde nabízena, jsou

připravována podle vlastních receptur. Firma se snaží, aby pokrmy obsahovaly v maximální možné míře čerstvé suroviny, dále používá materiályv biokvalitě. Firma jídelnu nepoužívá jen pro pouhé stravování, ale i jako vhodnou inspiraci pro své strávníky. Jídla jsou totiž připravována ze surovin, které zákazníci běžně koupív prodejně, takže podobě mohou vařit i doma. Jsou-li méně šikovní, nebo zaneprázdnění, můžou si chutné jídlo odnést s sebou nebo si přes internet objednat rozvoz jídla domu nebodo zaměstnání.

V dubnu 2009 Bazalka v Hradci Králové otevřela novou prodejnu biopotravin, která je zařízena jako bezbariérová samoobsluha. Firma tak vyhověla přání mnoha svých zákazníků, kteří častokrát zdůrazňovali potřebu mít dostatek času na nákup zboží a větší nabídku sortimentu.

V roce 2012 došlo k rozšíření výrobních a skladovacích prostor v objektu v Třebechovicích. Výrobní prostory v jídelně Bazalce Ve Dvorku byly využity na maximum a nebylo možné zde rozvíjet firmu dál. V nových prostorách se proto začalo s rozšířením stávajícího sortimentu. Skladovací prostory umožnily také nakupovat najednou od regionálních ekologických zemědělců větší objem surovin. Podařilo se dobře rozjet výrobu a firma začala dodávat i do bioprodejen a zdravých výživ nejen v Hradci Králové, ale i Pardubic, Holic, Rychnova nad Kněžnou nebo Českých Budějovic.

V návaznosti na omezenou kapacitu jídelny Ve Dvorku a stále rostoucí zájem zákazníků Bazalka začala nabízet od listopadu roku 2013 také rozvoz jídel po Hradci Králové a nejbližším okolí. Na webových stránkách byl vybudován objednávkový systém, který umožňuje strávníkům objednat si dovoz obědů, pizz, koláčů, salátů a pečiva přímo domů nebo do zaměstnání. Každý všední den pak vyráží auto na předem připravenou trasu podle došlých objednávek.

Začátkem roku 2014 byl na firemních webových stránkách spuštěn také e-shop, který umožňuje výběr a zaslání zboží z téměř celého nabízeného sortimentu. Nabídka je neustále aktualizována a doplňována o nové produkty. Zákazníci si mohou v klidu svého domova prohlédnout, vybrat a objednat výrobky, o které mají zájem. Každý den tak přepravní služba odváží balíky s potravinami či kosmetikou, které míří za zákazníky po celé republice. Web také nabízí zákazníkům službu, kde si mohou objednat připravení celého nákupu v prodejně Bazalka BIO ještě před jejich příchodem. Přijdou si ho do obchodu pouze vyzvednout a zaplatit. Bazalka začala také na svých stránkách upozorňovat zákazníky na různé prezentace a ochutnávky zboží a zasílat jim obchodní sdělení přes e-maily.

(*Bazalkahk.cz*[online]. Bazalka ©2019 [cit. 2019-11-23]. Dostupné z: https://www.*Bazalkahk*.cz/).

4.3 Volba metody projektu

Vedení firmy Bazalka s.r.o. si uvědomovalo, že proces implementace GDPR bude velmi složitým úkolem, protože se dotkne velkého okruhu činností probíhajících v podniku. Firma měla několik možností jak přistoupit k přípravě a zvládnout vlastní zavedení GDPR. V době před zavedením Nařízení se na trhu objevilo mnoho společností, které nabízely provedení auditu a následného zavedení opatření. Výhodami tohoto řešení byla jednoduchost pro samotnou firmu a záruka odborných znalostí poradců. Ale vzhledem k velmi krátké době, v které nebylo možno ověřit kvalitu nabízených služeb a vysokým cenám pohybujícím se v řádu desetitisíců u tohoto způsobu řešení, majitelka a manažerka tuto možnost zamítly.

Další možnost spatřoval management v pořízení speciálního softwaru, který pomocí dokumentů a videí seznámí uživatele s úkony vedoucí k řešení implementace GDPR ve firmě. Tyto autorizované programy dokáží vytvářet formuláře, směrnice a potřebná hlášení vztahující se k ochraně osobních údajů. Pro firmu Bazalka se jevila jako vhodná např. aplikace eDPO – Průvodce GDPR od A do Z od firmy DATALITE, která je schopná analyzovat případná rizika a zajistit shodu zpracování dat s GDPR. Tento software lze pořídit za cenu 2200 Kč za měsíc v provedení Single. Dále firma mohla využít program xGDPR Express od společnosti ECOCRM, který je možné koupit do 15tis. Kč. Hlavní výhodou této možnosti přípravy na GDPR je rychlost provedení a nižší náklady na pořízení než v předchozím způsobu. Použitím tohoto typu zajištění ochrany osobních dat se však firma vystavuje značnému riziku, že zaměstnanec, který bude zodpovědný za její provedení, nemusí podle návodu provést implementaci správně.

Poslední možnost spatřovalo vedení firmy v provedení implementace svépomocí proškolením vybraného zaměstnance společnosti. Hlavní výhodou se jevila příznivá cena za nabízená školení a dostupné publikace. Ceny za školení se pohybovaly do desetitisíce Kč. Autorka práce, pracující ve firmě na pozici manažerky, absolvovala 6-hodinový seminář „GDPR bez obav pro malé a střední podniky“ pořádaný firmou FLYEYE s.r.o. v ceně 4500,- Kč. Protože povaha tohoto semináře byla spíše informativní, bylo žádoucí, aby pracovnice své znalosti dále rozšířila samostudiem odborné literatury a hledáním zkušeností, dotazů a rad u svépomocných skupin z řad podnikatelů na sociálních sítích. Podařilo se ji spojit s Asociací hotelů a restaurací, která zařadila přípravu na GDPR do svých stanov a pro své členy uspořádala školení vedené odborníky.

4.4 Přípravná část projektu

Vlastnímu procesu implementace předcházela přípravná fáze trvající více než půl roku, v které bylo nutné se seznámit s GDPR a dalšími souvisejícími zákony a vyhláškami platnými pro Českou republiku i EU. Majitelka a manažerka byly odborně proškoleny odborníky v oblasti GDPR a seznámeny s právními aspekty týkajících se samotného procesu implementace do procesů probíhajících ve společnosti.

Základem pro správné zavedení opatření byla nutnost znalosti všech procesů, kterých se projekt implementace ve firmě bude týkat. Manažerka firmy vytvořila podrobný plán celého projektu, jehož cílem bylo zvládnutí všech kroků do 25. května 2018. Podle plánu bylo žádoucí zanalyzovat stávající stav toku dat, definovat typy osobních údajů, stupeň současného fyzického i technického zabezpečení a následně určit pravděpodobnost hrozeb a rizik, které mohou data ohrozit. Dále bylo nutné zhodnotit rozdíly mezi zjištěnými výsledky a požadavky GDPR . Samotnou implementaci bylo nutné rozdělit na dvě části a to na proces, který zasáhne již probíhající operace a dále zavést nová opatření splňující Nařízení.

4.5 Analýza GAP

Analýza GAP je vstupní analýzou a lze ji nejpřesněji popsat jako „analýza mezery“, pomocí níž management firmy zjišťuje rozdíly mezi stavem probíhajících procesů a požadavky kladenými GDPR. Proběhlý rozbor stanovuje, kde se firma v oblasti ochrany osobních dat v současnosti nachází a kam by, pokud chce splňovat pravidla nařízení, měla směřovat. Pomocí GAP analýzy manažerka určila místa, kde ve firmě dochází ke sběru dat a jaké se k tomu využívají nástroje či používají systémy a aplikace. Podrobně popsala strukturu a formáty, které slouží pro sběr informací. Identifikovala osoby, které mají přístup k údajům a jaké k tomu používají oprávnění. Zhodnotila průběh zpracování dat, způsoby jejich uchovávání a případné ochrany. Analýze byly dále podrobeny smluvní závazky se zpracovateli.

Výstupní zpráva z GAP analýzy obsahovala zhodnocení všech procesů a posouzení souladu s nařízením GDPR, identifikovala rozdíly (viz. tabulka č.5) a na jejím základě vznikly návrhy k jejich odstranění. Výsledky analýzy se staly základním vodítkem pro vrcholový management firmy při volbě následné implementace opatření do jednotlivých oblastí činností. Pomocí ní měli přesně zmapovaná místa, kde se ve firmě zpracovávají data a kdo za sběr a zpracování dat zodpovídá (viz. Příloha A – Katalog zpracování osobních údajů).

Souhrnnou GAP analýzu tvoří analýzy jednotlivých klíčových oblastí:

- analýza osobní bezpečnosti,
- analýza personální oblasti,
- analýza IT systémů,
- analýza dokumentace,
- analýza e-shopů,
- analýza webů,
- analýza kamerových systémů,
- analýza marketingu,
- analýza přístupových práv a odpovědnosti,
- analýza souhlasů se zpracováním,
- analýza smluvního předávání dat,
- analýza interních předpisů a směrnic.

4.6 Posouzení vlivu na ochranu osobních údajů (DPIA)

Data Protection Impact Assessment neboli posouzení vlivu na ochranu osobních údajů je dopadová analýza navazující na předchozí analýzu GAP. Cílem zvolené metody DPIA byla přesná identifikace a popis zpracování dat ve firmě, případná eliminace zbytečných dat nepotřebných pro zpracování. Manažerka si uvědomila, že každé zpracování osobních údajů sebou přináší jistou míru rizika a je nutností přijmout opatření, aby data nebyla zneužita.

Ve firmě Bazalka, která je v pozici správce, který zpracovává osobní údaje, byly systematicky popsány operace zpracování osobních údajů v jednotlivých procesech probíhajících v organizaci (viz. Příloha A Katalog zpracování osobních údajů). U každé operace byl posouzen účel a nezbytnost zpracování osobních údajů. V následující části analýzy DPIA byla stanovena pravděpodobnost vzniku rizika, které by mohlo mít vliv na práva a svobody dotčených subjektů údajů. Po zhodnocení míry ohrožení dat byly navrženy vhodné bezpečnostní mechanismy, aby dostatečně a v souladu s GDPR zajišťovaly ochranu osobních údajů. Protože byl již v minulosti ve firmě Bazalka s.r.o. kladen důraz na ochranu osobních údajů vycházející ze znalosti požadavků směrnice 95/46/ES a zákona č. 101/2001 Sb., nebyly zjištěné rozdíly a požadavky GDPR velké.

5 OBLASTI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Na základě GAP analýzy manažerka určila oblasti, ve kterých dochází ke zpracování osobních dat v organizaci. Pomocí ní byly identifikovány probíhající procesy a stanoveny účely zpracování. Analýza umožnila managementu operace rozložit na jednotlivé kroky a následně si uvědomit každý okamžik získávání osobních údajů a práci s nimi.

Toky dat lze ve firmě rozdělit do těchto oblastí:

- personální oblast,
- mzdová oblast,
- dodavatelská oblast,
- odběratelská oblast,
- finanční (prodejní) oblast,
- bezpečnostní oblast,
- oblast marketingu,
- IT oblast.

5.1 Zjištěné neshody

Po zhodnocení současného stavu, který GAP analýza přesně zmapovala, následoval důležitý krok určení nesouladů v nakládání s osobními daty. Do tabulky č. 5 byly zaznamenány všechny zjištěné neshody. Analýza odhalila, že ve společnosti chybí v jednotlivých oblastech činností přesně stanovený účel a rozsah zpracování dat. Dále není stanovená doba využívání dat. Firma nevede žádný záznam evidující zpracování osobních údajů. Zákazníci nejsou informaváni o svých právech. V oblasti marketingu společnost postradá formulář pro souhlas se zasíláním obchodních sdělení. Nedostatky byly nalezeny také v kontrolní činnosti a oblasti zabezpečení přístupu k osobním údajům. Za hlavní nesoulad manažerka označila chybějící interní předpis, který by obsahoval zásady pro zpracování osobních dat .

V třetím sloupci tabulky jsou uvedeny opatření, které firma musela následně provést, aby zpracovávání dat probíhalo v souladu s GDPR.

Tabulka 5: Zjištěné nesoulady a opatření

POŘADÍ	NESOULAD	OPATŘENÍ
1.	V jednotlivých oblastech činností chybí přesně stanovený účel zpracování osobních údajů.	Při implementací Nařízení je nutné doplnit přesné účely.
2.	Chybí rozsah zpracovávaných osobních údajů v jednotlivých oblastech.	GDPR požaduje minimalizaci zpracovávaných dat. Nutnost vyspecifikovat, v jakém rozsahu budou informace zpracovány.
3.	Není stanovena přesná doba využívání dat v jednotlivých oblastech.	Je nutné stanovit dobu použití informací.
4.	Společnost nevede evidenci zpracování dat.	Zpracování katalogu zpracování dat
5.	Není vytvořena metodika pro přístupová práva a oprávněnost jednotlivých osob zodpovědných za zpracování dat.	Vytvoření interního předpisu se stanovením přesných pravidel pro přístup k datům.
6.	Chybí informace pro zákazníky o jejich právech v oblasti zpracování osobních dat.	Nařízení požaduje sdělit kupujícím, která data firma zpracovává, za jakým účelem, zda k tomu potřebuje jejich souhlas a informovat ho o jeho právech či možnosti odvolání souhlasu.
7.	Firma nemá formulován souhlas se zpracováním osobních údajů pro zasílání obchodních sdělení.	Dle GDPR potřebuje firma výslovný souhlas zákazníka pro tento účel.
8.	Chybí informovanost zákazníka o ukládání cookies.	Doplnit informaci o ukládání cookies na web stránky firmy.
9.	Firma nemá stanoven kontrolní mechanismus.	V interním předpisu stanovit metodiku pro kontrolu v oblasti zpracování dat.
10.	Společnost nemá vypracovaný interní předpis obsahující zásady pro zpracování osobních dat	Vytvoření interního předpisu pro zpracování osobních dat.

11.	Chybí metodika pro vyhodnocení rizik ohrožující data subjektů.	Vytvoření metodiky pro vyhodnocení rizik

Zdroj: vlastní zpracování

6 OPATŘENÍ A VNITŘNÍ ÚPRAVY K ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ V RÁMCI GDPR

Vlastní projekt implementace je založen na nutnosti provedení změn v souvislosti s dosažením shody s Obecným nařízením. V rámci tohoto procesu dojde k odstranění všech neshod , které byly zjištěny v průběhu analýzy současného stavu zpracování osobních údajů v dané společnosti.

Nejdůležitějším krokem v projektu je stanovení účelu zpracování osobních dat, který bude přehledně zaznamenán do Katalogu zpracování osobních údajů (viz. Příloha A). Dále je nutné určení rozsahu zpracování údajů a vytvoření formulářů pro udělení výslovného souhlasu se zpracováním (viz. Příloha D). Všechny zásady týkající se zpracování osobních dat pro firmu musí být přehledně zpracovány do interního předpisu, jehož součástí jsou bezpečnostní opatření organizačně – technického charakteru, frekvence školení zaměstnanců, stanovení odpovědnosti pověřených osob či procesy kontroly.

6.1 Interní předpis a směrnice

Manažerka zpracovala interní předpis pro ochranu osobních údajů, který upravuje sběr, zpracování, nakládání a uchovávání dat ve firmě. V interním předpisu jsou uvedeny výklady základních pojmů, co jsou osobní data, jaké operace lze zařadit ke zpracování údajů, kdo je správce a kdo je zpracovatel. Je v něm stanovena odpovědnost každého zaměstnance, který v rámci své práce ve firmě zaměstnavatele získává, využívá a zpracovává data a jeho povinnost provádět tyto úkony v souladu s právními předpisy, interním předpisem a dalšími dokumenty společnosti. Odpovědné osoby v podobě vedoucích provozoven jsou pověřeny pravidelnými kontrolami plnění povinností a to v rozsahu daným předpisem. Další část interního předpisu je věnována obecným zásadám zpracování osobních dat. V nich je uveden přesný popis, jakým způsobem společnost získává jednotlivé informace, jak je třídí a dále ukládá. Dále je zde také článek o archivaci a likvidaci osobních údajů. Jako nedílné součásti interního dokumentu jsou uvedeny různé bezpečnostní postupy k zajištění ochrany osobních údajů. Součástí interního předpisu je také formulář, který slouží pro potvrzení, že byl zaměstnanec s dokumentem seznámen (viz. Příloha B).

6.2 Bezpečnostní opatření

Bezpečnostní rizika jsou ve firmě vyhodnocována pravidelně 1 x ročně. V případě výrazných změn ve společnosti, které by mohly mít dopad na ochranu osobních dat nebo v případě narušení zabezpečení ochrany, je revize rizik provedena okamžitě.

Ve společnosti byla vytvořena metodika vyhodnocení bezpečnostních rizik a sestaven formulář pro jejich zápis (viz. tabulka č.6 Vyhodnocení bezpečnostních rizik):

A) riziko vztahující se na práva a svobody subjektů údajů,
B) možný dopad, pokud dojde k realizaci rizik z písmene A,
C) hodnocení závažnosti dopadu a stanovení kategorii,
D) pravděpodobnost výskytu událostí ohrožující subjekty údajů,
E) zvolená a plánovaná bezpečnostní a nápravná opatření

Tabulka 6:Vyhodnocení bezpečnostních rizik

Typ rizika	Možný dopad	Hodnocení dopadu	Pravděpodobnost	Ochranná opatření
Porušení přiměř. a nezbyt. zpracování				
Porušení práv subjektu				
Neoprávněný přístup k OÚ				
Neoprávněná změna OÚ				
Nedostupnost nebo výmaz OÚ				

Zdroj: vlastní zpracování

Do kategorie rizik vztahujících se na práva a svobody jsou zařazena rizika týkající se porušení principů přiměřenosti a nezbytnosti zpracování. Dále sem patří porušení práv subjektů údajů či neoprávněný přístup k osobním údajům nebo jejich neoprávněná změna.

Do druhého sloupce tabulky se zapisují možné dopady např. zasílání nevyžádaných obchodních sdělení nebo způsobení hmotné a nehmotné ztráty v případě nezajištění výkonu práva subjektu. Třetí sloupec obsahuje hodnocení dopadu dle kategorie závažnosti od 1. stupně minimálního dopadu až po vysoký 4. stupeň, kdy jsou důsledky nezvratné a v některých případech neodstranitelné (velké dluhy, pracovní neschopnost, smrt) .

Pravěpodobnost výskytu události, která se zapisuje do páteho sloupce, může být zanedbatelná, pokud se ještě nikdy nevyskytla v dané společnosti popř. v rámci odvětví nebo omezená v případě výskytu v odvětví. Významná pravědpodobnost bude zvolena, jestliže se ve firmě v minulosti podobná událost stala. Pokud byl výskyt opakovaný, jedná se o vysokou pravěpodobnost. V další části práce jsou popsána bezpečnostní opatření zvolená firmou pro ochranu osobních dat.

6.3 Fyzická bezpečnost

Fyzická bezpečnost, pomocí které se firma snaží ochránit svoje prostory před neoprávněnými osobami, je přirozeným základem ochrany osobních údajů a její přiměřenost a dostatečnost vychází z analýzy rizik.

Společnost si v rámci ní stanovila pevná pravidla, která jsou zanesena do interního předpisu:

- Vstup do prostor obsahujících osobní data jako jsou kanceláře nebo archiv, je umožněn pouze oprávněným zaměstnancům společnosti, kteří vlastní fyzický klíč.
- Na všech pracovištích firmy jevyžadována zásada prázdného stolu, zamčené a vypnuté obrazovky.
- Do serverovny mají přístup pouze pracovníci IT.
- Vnější dveře a okna jsou chráněny vhodným detekčním systémem.
- Není dovoleno nechávat osobní údaje volně bez dohledu, Písemnosti a nosiče informací musí být uchovávány v uzamykatelných skříních a místnostech.

6.4 IT bezpečnost

IT bezpečnost je řízena interním předpisem společnosti a stanovuje pravidla pro běžné a pověřené uživatele systémů firmy. Společnost používá pouze legální a evidované SW a HW, které jsou předem schválené IT oddělením. Veškeré informace, které firma získává a zpracovává, jsou chráněny před počítačovými viry, spamy a spywary vhodnými bezpečnostními mechanismy a aplikacemi nainstalovanými na servery, firewally či jednotlivé počítačové stanice. Oprávněným zaměstnancům a IT administrátorům je umožněn přístup k osobním údajům pomocí přiděleného hesla a pouze v rozsahu, který potřebují nutně pro výkon svojí funkce. Přístupová hesla jsou automaticky po 30 dnech obměňována.

Zálohování dat probíhá v souladu s interním předpisem, který mimo jiné přikazuje zaměstnancům uchovávání záloh v trezoru společnosti umístěného v jiném prostoru než je serverová místnost. Zaměstnanci firmy nesmí při své práci používat veřejná úložiště např. uloz.to, uschovna.cz, leteckaposta.cz a další. V interní předpisu je dále stanoveno, že data, která byla uložena nebo zálohována, a již nebudou dále potřebná, pověřený pracovník zlikviduje a o jejich likvidaci provede záznam. Na případný vývoj a změny v informačních systémech jsou stanovena pravidla, která by umožňovala firmě rychle reagovat a případně upravit některé oblasti IT bezpečnosti.

6.5 Narušení zabezpečení osobních dat

V souladu s GDPR si firma stanovila v interním předpisu metodiku pro případ zjištění, že došlo k porušení zabezpečení osobních údajů. Dle této metodiky musí být jakékoli vzniklé změny v bezpečnosti dat neprodleně posouzeny, zdokumentovány (co se stalo, jaké a čí osobní údaje unikly, možné následky, popis přijatých opatření s cílem vyřešit daný případ, identifikace rizika) a následně oznámeny odpovědné osobě. Odpovědná osoba ohlásí okamžitě pomocí speciálního dokumentu , nejpozději do 72 hodin od zjištění incidentu, porušení zabezpečení dozorovému úřadu. Výjimku tvoří pouze případy, kdy nedošlo k žádnému riziku vzniku ohrožení pro práva a svobody fyzických osob. Pokud jsou zjištěná rizika významná, musí firma bez zbytečného odkladu oznámit porušení zabezpečení a ohrožení osobních údajů dotčenému subjektu údajů.

6.6 Evidence zpracování dat

Po zjištěné identifikaci jsou pomocí softwarových programů graficky zakresleny jednotlivé toky dat do Katalogu zpracování osobních údajů (viz Příloha A). K osobním údajům v jednotlivých oblastech je doplněn právní titul, na jehož základě jsou data pořizována. V některých oblastech je nutný souhlas (viz. Příloha D), v jiných stačí, že zpracování je prováděno na základě plnění nebo uzavření smlouvy, oprávněného zájmu či právní povinnosti. Pokud by firma zpracovávala citlivé údaje, musela by od subjektů údajů získat výslovný souhlas nebo obhájit právní nároky na zpracování takových údajů.

6.6.1 Personální a mzdová oblast

Firma v oblasti personalistiky používá v první řadě informace o uchazečích v rámci zpracování životopisů pro nábor nových zaměstnanců. Výsledkem výběrového řízení je uzavření pracovní smlouvy, tudíž firma nepotřebuje od uchazečů výslovný souhlas ke zpracování jejich osobních údajů. Uchazeči jsou již přečtením inzerátu na pracovní pozici obeznámeni s firmou, které poskytují svá data a souhlas udělují zasláním žádosti o pracovní místo. Pokud se firma rozhodne pro uchování osobních údajů zájemců i po skončení výběrového řízení, předkládá uchazeči formulář, ve kterém ji zájemce uděluje souhlas v písemné formě. Získaná data ve výběrových řízeních se uchovávají pouze na dobu nutnou, nejdéle do jeho ukončení a poté jsou předána ke skartaci a likvidaci.

V další části personalistiky firma získává, eviduje a používá také osobní údaje zaměstnanců v rámci pracovního poměru. Jedná se o tyto osobní údaje: jméno, příjmení, datum narození, rodné číslo, místo narození, bydliště, číslo zdravotní pojišťovny, stav, jména dětí a jejich rodná čísla, telefonní kontakt, číslo účtu, vzdělání a zdravotní způsobilost pro

výkon pracovní pozice. Firma osobní údaje zaměstnanců zpracovává jednak automatizovaně pomocí elektronického personálního systému PAMICA a dále neautomatizovaně v osobních spisech v papírové podobě.

Ke zpracování informací potřebných pro pracovněprávní agendu nepotřebuje souhlas pracovníka, protože podle GDPR se jedná o plnění smlouvy a některé údaje spadají do zákonné povinnosti. Společnost se rozhodla nevyužívat na svých webových stránkách portrétní fotografie zaměstnanců spojených s jejich jménem, pracovní pozicí a pracovním kontaktem. Manažerka určila osoby, které smějí pracovat s osobními údaji zaměstnanců pouze na základě seznámení se zásadami GDPR. Dále stanovila přístupová hesla do personálního informačního systému a zakoupila uzamykatelnou sekcí pro šanony s osobními spisy zaměstnanců. Vedoucí personálního oddělení pravidelně provádí revizi záznamů zaměstnanců a vymazává data, která jsou neplatná nebo zastaralá.

Pracovní vztah mezi zaměstnavatelem a zaměstnancem vzniká uzavřením pracovní smlouvy, dohody o provedení práce nebo dohody o pracovní činnosti. Firma má v důsledku toho zákonnou povinnost ke zpracování osobních údajů zaměstnanců. Získané osobní údaje využívá pro mzdovou, daňovou, sociální oblast či pro nemocenské nebo zdravotní pojištění. Důležitou zákonnou povinností každého zaměstnavatele, firmy Bazalka nevyjímaje, je vedení a uchovávání mzdových listů po dobu 30 let. Firma si mimo svou zákonnou povinnost uchovává některá data o mzdách zaměstnanců pro účely statistiky, ale tyto údaje nespadají do kategorie osobních dat, protože nemají žádnou vazbu na konkrétního zaměstnance.

Při zpracování osobních dat v rámci mzdové a personální oblasti firma informuje svoje zaměstnance o podmínkách zpracování a uchovávání případné skartaci a likvidaci údajů. Pracovníci, kteří přicházejí do styku s osobními daty a mohli by představovat riziko, jsou proškoleni a seznámeni s interním předpisem pro ochranu osobních údajů.

6.6.2 Dodavatelsko – odběratelská oblast

Pro naplnění obchodních účelů v odběratelsko-dodavatelských vztazích firma Bazalka s.r.o. zpracovává z důvodů plnění smluvních povinností tyto osobní údaje: jméno, příjmení, titul, datum narození, trvalé bydliště, kontaktní adresu, email, telefon, bankovní spojení, IČO/DIČ. O zásadách ochrany osobních údajů informuje dodavatele i zákazníky na svých webových stránkách v sekci „Sdělení ke splnění informační povinnosti“(viz. Příloha B).

Poskytuje jim informace, že výše uvedené osobní údaje získává a zpracovává manuálně nebo automatizovaně pomocí elektronického ekonomického systému POHODA prostřednictvím svých pověřených zaměstnanců v souvislosti s objednávkami a dodávkami zboží, při reklamacích a uzavírání ostatních dodavatelsko-odběratelských vztahů. Firma jako správce zpracovává jejich osobní údaje po dobu nezbytně nutnou k dosažení účelu. Pro splnění svojí

zákonné povinnosti eviduje a uchovává účetní dokumenty 5 let, daňové dokumenty následně 10 let po jejich uskutečnění. Manažerka při ukládání dokumentů provádí roztřídění a označení spisů. Vyřazené podle archivačního a skartačního řádu předává ke skartaci.
Společnost nezaměstnává více jak 250 zaměstnanců, podle ze zákona ji tudíž nevyplývá povinnost jmenovat Pověřence pro ochranu osobních údajů.

6.6.3 Prodejní a marketingová oblast

Bazalka provozuje v Hradci Králové tři kamenné obchody. Dále si zákazníci mohou většinu nabízeného zboží objednat přes objednávkový formulář e-shopu na webových stránkách firmy. V objednávce vyplňují své jméno, příjmení, fakturační adresu, popř. dodací adresu, pokud se liší od fakturační. Poskytují svůj e-mail a číslo telefonu. Nakupující má svobodnou volbu zaškrtnout při výběru zboží i políčka a udělit tak firmě svůj souhlas k zasílání obchodních sdělení. Teprve po získání jeho souhlasu má společnost právo obeslat ho newsletterem nebo jinými marketingovými nabídkami.

Po zavedení GDPR firma obeslala všechny své stávající zákazníky e-mailem, kde je požádala o udělení souhlasu. Výsledek byl managementem hodnocen negativně, protože z databáze obsahující cca. 8000 klientů dalo souhlas pouze 300 osob. Pro společnost to znamenalo, že musela změnit strategii ve svém marketingu a využít jiné cesty propagace svých výrobků. Firma informuje na své webové stránce kupující o jejich právu zrušit kdykoli tento souhlas zasláním zprávy pomocí elektronické cesty (viz. Příloha D)

Společnost využívá také remarketing v systému Google Adwords, kde dochází k ukládání tzv. cookies. Tato mezidata, která obsahují pouze informace týkající se vkládání zboží do košíku a počty návštěv webu, neprofilují zákazníka a nezasahují do jeho soukromí a tudíž není nutné získávat k jejich pořízení souhlas.

6.6.4 IT oblast

Vedení společnosti Bazalka si dobře uvědomilo, že hlavním důvodem pro přijetí GDPR byl rychlý rozvoj informačních technologii v PC, notebooků, tabletů či inteligentních telefonů.

Ochranná opatření a postupy v oblasti IT, které firma používá, lze rozdělit na technologická a organizační. K technologickým opatřením přijala nástroje, které ji umožnily zvýšit ochranu osobních dat v digitální podobě. Na všech PC je bezpodmínečně používán aktualizovaný antivirový a antispamový program, firewall. Všechny PC jsou dále zabezpečeny proti riziku neoprávněného vniknutí pomocí přístupových hesel uzamknutím obrazovky a přístupu do sítě prostřednictvím VPN. Dále využívá šifrované připojení k internetu (htpps) a firemní certifikáty. Přístup do elektronické pošty je také chráněn heslem.

Používaná přístupová hesla jsou kontrolována a pravidelně obměňována.

Technická opatření by samostatně byla nedostatečná a tak firma současně přijala i organizační opatření, aby snížila případná rizika. Veškeré přístupy do IT systémů se řídí Interním předpisem pro ochranu osobních údajů, který stanovuje přesná pravidla a nastavení přístupových práv pro určené a běžné uživatele systémů společnosti.

O IT oblast se společnosti stará autorizovaná IT firma. Provádí správu, servis, hosting a ukládá data v digitální podobě do cloudových úložišť. S touto firmou má společnost Bazalka podepsanou zpracovatelskou smlouvu s doložkou mlčenlivosti a záruky zabezpečení osobních údajů dle GDPR. V Interním předpisu je stanovena odpovědnost určených osob za provádění a kontrolování zálohování dat. Tyto osoby také zodpovídají za zamezení přístupu do IT systémů firmy nepovolaným osobám.

6.6.5 Bezpečnostní oblast – kamerový systém

Po zavedení GDPR v květnu 2018 došlo k zpřísnění podmínek ochrany soukromí v pořizování záznamů z bezpečnostních kamer. Pro majitele prodejen to znamená, že musí svoje návštěvníky plně informovat o použití kamerového systému, protože pořizování videozáznamů patří do kategorie shromažďování osobních dat. Společnost Bazalka používala kamerový systém z bezpečnostních důvodů k prevenci kriminality a odhalování krádeží ve své provozovně se samoobslužným prodejem. Střežený prostor byl již před účinností GDPR označen cedulkou „Prostor je střežen kamerovým systémem se záznamem“ (viz. Obrázek č. 5).

Správce zpracování : BAZALKA s.r.o.

Bližší informace lze získat na tel……. nebo www …….

Obrázek 3:Označení pro prostor střežený kamerovým systémem se záznamem

Zdroj: upraveno podle(ŽUREK, 2017)

Po nabití platnosti GDPR firma zveřejnila pro zákazníky prodejny na své webové stránce informace o účelu zpracování z důvodu bezpečnosti a 14 denní lhůtě uchování záznamu. Dále byli na tomto monitorovaném prostoru odborně proškoleni všichni zaměstnanci, aby byli schopni kvalifikovaně reagovat na dotazy týkajících se použití kamer. Zákazníci jsou také informováni o možnosti využití práva vznést námitku proti zpracování jejich osobních údajů a následným vyřízením ze strany společnosti, které bude v souladu s nařízením EU.

6.7 Proškolení zaměstnanců

Po vytvoření Interního předpisu a zavedení všech kroků k zabezpečení osobních dat ve firmě dle GDPR bylo nutné proškolit všechny zaměstnance o interních pravidlech podle GDPR a o správě jejich osobních údajů. Pracovníci jsou proškolováni majitelkou nebo manažerkou formou osobního školení zaměřeného na bezpečnost a ochranu osobních dat při nástupu do zaměstnání a pak pravidelně 1x ročně. Na všech provozovnách jsou zaměstnanci seznámeni s novým systémem zacházení a uchování veškerých osobních údajů stanovených metodikou firmy. Dále jsou jim vysvětleny přístupy k jednotlivým datům a přidělena přístupová hesla. Evidence o absolvování školení je zpracována vedoucí personálního oddělení společnosti do Záznamu o proškolení zaměstnance (viz. Příloha B).

6.8 Kontrolní činnost

Velmi důležitou součástí implementace GDPR bylo navržení a zavedení kontrolní činnosti uvnitř společnosti, která je zaměřena na systém zpracování osobních údajů a slouží k tomu, aby zde nedocházelo k chybným krokům. V interním předpisu jsou stanoveny osoby odpovědné za jednotlivé oblasti dle Katalogu zpracování osobních údajů, které zajistí kontrolu plnění povinností, které jim byly svěřeny.

Kontroly jsou prováděny v následujícím rozsahu:

a) 1 x ročně je provedena kontrola celé společnosti,
b) 1 x měsíčně odpovědná osoba vykoná namátkovou kontrolu vybrané oblasti,
c) probíhá každodenní kontrola fyzické ochrany rizikových úseků,
d) následná kontrola po změně zákonů nebo Interního předpisu,
e) mimořádná kontrola po řešení incidentu v zabezpečení osobních dat.

Společnost si vede o pravidelných kontrolách záznam a tento záznam je uložen u vedoucí kanceláře firmy.

7 ZHODNOCENÍ PROCESU

Cílem procesu byla implementace GDPR ve vybrané firmě Bazalka s.r.o.. Projekt byl postaven tak, aby realizace proběhla do 25. května 2018 a nenastal důvod k udělení případných sankcí ze strany dozorového úřadu. Vedle významných přínosů, které proces společnosti přinesl, způsobily příprava a samotná implementace firmě nemalé časové i finanční zatížení. Mezi negativní stránky projektu bych zařadila snížení počtu zákazníků v databázi po neudělení souhlasu se zasíláním obchodních sdělení v oblasti marketingu.

Hlavní přínos implementace spočívá v bezproblémovém fungování společnosti v oblasti zpracování dat a regulace jejich množství. Provedené analýzy současného stavu zpracování a uchovávání dat odhalily nesoulady s GDPR. Zjištěné neshody byly zaznamenány a dále byl stanoven časový harmonogram k zavedení opatření k jejich odstranění. Byl vytvořen Interní předpis, který popisuje veškeré operace zpracování osobních dat probíhající ve firmě. K dalším přínosům patří celkové povědomí o firmě jak mezi zaměstnanci tak zákazníky, kteří jsou všichni obeznámeni, že s jejich údaji je nakládáno pouze v souladu s GDPR, nemusí se obávat úniku svých dat a mohou se dožadovat svých práv.

V neposlední řadě implementace GDPR přinesla vedení společnosti kompletní přehled o tom, kde se zpracovávají a ukládají veškerá data a kdo k nim má jaký přístup. Díky zmapování toku informací by v případě pochybení měla firma jasný obraz, kdo měl k datům a dokumentům přístup a kdo způsobil chybu. Společnost může také tento přehled využít jako podklad pro případnou kontrolu ze strany Úřadu na ochranu osobních údajů.

ZÁVĚR

Hlavním cílem bakalářské práce bylo popsání projektu implementace GDPR ve vybrané společnosti Bazalka s.r.o. Po zhodnocení současného stavu společnosti a techniky lze konstatovat, že GDPR nepřineslo pro firmu Bazalka s.r.o. žádnou převratnou revoluci, protože společnost již před nabitím platnosti GDPR dodržovala pravidla uvedená v zákoně o ochraně osobních údajů a pouze evolučně zareagovala na změny, které pro ni tak GDPR přineslo.

V úvodní fázi praktické části proběhla vstupní analýza, která zhodnotila současný stav všech toků dat ve společnosti. Pomocí analýzy bylo možné vytvořit přesnou mapu oblastí zpracování a uchovávání veškerých dat ve firmě. Porovnáním výsledků současného stavu zpracování osobních údajů a požadavků GDPR byl stanoven přehled nesouladů doplněný o popis opatření, které je nutné provést k odstranění těchto neshod. Poté byl vytvořen Katalog zpracování osobních dat, kde došlo k rozdělení na jednotlivé oblasti, byl stanoven účel a rozsah zpracovaných dat, právní titul, způsob uchováni, bezpečnostní opatření a určena doba použití údajů. Dále byly vytvořeny potřebné formuláře a dokumenty, které umožňovaly např. získat souhlas se zpracováním osobních dat, pověřovaly odpovědné osoby, stanovovaly pravidla zacházení s osobními údaji, obsahovaly systém vyhodnocení rizik a kontrolní mechanizmy. Firma musela proškolit veškeré zaměstnance a stanovit metodiku následného proškolování s vytvořením záznamního dokumentu.

Celý proces implementace byl spojen s vytvořením nejdůležitějšího vnitřního dokumentu v podobě Interního předpisu pro zpracování osobních údajů. Závěrem je možné konstatovat, že nejdůležitější pro firmu bylo zvládnutí přípravné fáze i samotné aplikace projektu v časovém horizontu tak, že úspěšně předešla případným sankcím ze strany dozorového orgánu. Došlo také k posílení povědomí o společnosti u spolupracujících firem, protože svoje zkušenosti s procesem implementace dokázala Bazalka předat i jim.

POUŽITÉ ZDROJE: LITERATURA

[1] DOLEŽÍLEK, Jiří ; *Přehled judikatury ve věcech ochrany osobnosti,* 3.vydání, Praha: Wolters Kluwer ČR, a.s., 2016 , 328 s., ISBN 978-80-7552-074-6

[2] JANEČKOVÁ, Eva ; *GDPR. Praktická příručka implementace,* Praha: Wolters Kluwer ČR, a.s., 2018 , 136 s., ISBN 978-80-7552-248-1

[3] KOHÚTOVÁ, Zuzana; *GDPR pro účetní a mzdové účetní* , *Metodické aktuality 4/2018*, *Registrované periodikum svazu účetních České republiky*, Praha: Svaz účetních České republiky. 2018 , 64 s., ISBN 978-80-87367-86-5.

[4] MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav; *Osobní údaje a jejich ochrana. Knižka pro praxi.* 1.vydání, Praha: ASPI Publishing, s.r.o., 2003 , 416 s., ISBN 80-86395-50-2.

[5] MORÁVEK, Jakub, *Ochrana osobních údajův pracovněprávních vztazích*, 1.vydání, Praha: Wolteker Kluwer ČŘ a.s., 2013 , 436 s., ISBN 978-80-7478-139-1.

[6] NAVRÁTIL, Jiří, a kol.; *GDPR pro praxi*, Plzeň: Aleš Čeněk s.r.o.. 2018 , 339 s., ISBN 978-80-7380-689-7.

[7] NEZMAR, Luděk; *GDPR: Praktický průvodce implementací*, 1. vydání. Praha : GRADA Publishing a.s., 2017 , 302 s., ISBN 978-80-271-0921-0.

[8] NONNEMANN, František; *Praktická příručka GDPR* , 1.vydání, Praha: Klika. 2018 , 144 s., ISBN 978-80-88298-10-6.

[9] NULÍČEK, Michal, a kol.; *GDPR – obecné nařízení o ochraně osobních údajů. Praktický komentář* , 2.vydání, Praha: Wolteker Kluwer ČŘ. 2018 , 580 s., ISBN 978-80-7598-068-7.

[10] PATTYNOVÁ, Jana, SUCHÁNKOVÁ, Lenka; *Úplné znění č.1319, Zpracování osobních údajů nový zákon o zpracování osobních údajů další předpisy, GDPR obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů*, Ostrava: Sagit, 2019 , 96 s., ISBN 978-80-7488-353-8.

[11] PATTYNOVÁ, Jana, SUCHÁNKOVÁ, Lenka, ČERNÝ, Jiří a kol.; *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář.* 1.vydání, Praha: Leges, 2018 , 488 s., ISBN 978-80-7502-288-2.

[12] VODIČKA, Milan, DRÁBKOVÁ, Tereza; *GDPR praktický průvodce pro účetní . Metodické aktuality 7/2019*, *Registrované periodikum svazu účetních České republiky* Praha: Svaz účetních České republiky. 2018 , 64 s., ISBN 978-80-87367-99-5.

[13] ŽUREK, Jiří; *GDPR v personalistice* , 1. vydání. Olomouc: Anag. 2019 , 176 s., ISBN 978-80-7554-210-6.

[14] ŽUREK, Jiří; *Praktický průvodce GDPR* , 1.vydání. Olomouc: Anag. 2017 , 224 s., ISBN 978-80-7554-097-3.

POUŽITÉ ZDROJE: WEB

[15] *Bazalkahk.cz*[online].Bazalka ©2019 [cit. 2019-11-23]. Dostupné z: https://www.*Bazalkahk*.cz/)

[16] *Businesscenter.podnikatel.cz*[online].Businesscenter ©2019 [cit. 2019-11-20]. Dostupné z: https://www.*Businesscenter.podnikatel*.cz/)

POUŽITÉ ZDROJE: ZÁKONY

[17] ČESKO. Listina základních práv a svobod, vyhlášená usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku ČR. In: *NOVE ASP1* [právní informační systém]. Wolters Kluwer ČR ©2018[cit.2019-11-25].Dostupnéz: http://ftp .noveaspi.cz/products/lawText/1/40453/1/2vtextu=listina%20základních%20práv%20a %20svobod#lema0

[18] Všeobecná deklarace lidských práv, Usnesení Valného shromáždění OSN, Zdroj: Vybraných Deklarací Valného shromáždění OSN, 10.12.1948, In: *NOVE ASP1* [právní informační systém]. Wolters Kluwer ČR ©2018 [cit. 2019-11-25]. Dostupné z: http://ftp.noveaspi.cz/products/search

[19] ČESKO. 115/2001 Sb. m. s., Sdělení Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob In: *NOVE ASP1* [právní informační systém]. Wolters Kluwer ČR ©2018[cit.2019-11-25]. Dostupné z: http://ftp.noveaspi.cz/products/lawText/1/51231/1/2? vtextu=Úmluva%20o%20ochraně%20osob%20se%20zřetelem%20na%20automatizované %20zpracování%20osobních%20dat#lema0

[20] 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 , In: *NOVE ASP1* [právní informační systém]. Wolters Kluwer ČR ©2018

[cit. 2019-11-25]. Dostupné z: http://ftp.noveaspi.cz/products/search

[21] ČESKO. Zákon č. 87/1862 Sb.z.s., o ochraně svobody osobní , In: *ASP1* [právní informační systém]. Wolters Kluwer ČR ©2018 [cit. 2019-11-25]. Dostupné z :http://ftp.aspi.cz/opispdf/1962/052-1962.pdf

[22] ČESKO. Zákon č. 88/1862 Sb.z.s., o ochraně svobody domovní , In: *ASP1* [právní informační systém]. Wolters Kluwer ČR ©2018 [cit. 2019-11-25]. Dostupné z :http://ftp.aspi.cz/opispdf/1962/052-1962.pdf

[23] ČESKO. Ústavní zákon č. 293/1920 Sb. o ochraně svobody osobní, domovní a tajemství listovního, In: *ASP1* [právní informační systém]. Wolters Kluwer ČR ©2018 [cit. 2019-11-25]. Dostupné z : http://ftp.aspi.cz/aspi/opispdf/1920.html

[24] ČESKO. Zákon č. 256/1992 Sb. o ochraně osobních údajů v informačních systémech, In: *AION CS. s.r.o.,* © AION CS, s.r.o. 2010-2019 [cit. 2019-11-25]. Dostupné z : https://www.zakonyprolidi.cz/cs/1992-256

[25] ČESKO. Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, In: *AION CS. s.r.o.,* © AION CS, s.r.o. 2010-2019 [cit. 2019-11-25]. Dostupné z : https://www.zakonyprolidi.cz/cs/2000-101

[26] ČESKO. Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů, In: *AION CS. s.r.o.,* © AION CS, s.r.o. 2010-2019 [cit. 2019-11-25]. Dostupné z : https://www.zakonyprolidi.cz/cs/2019-110

[27] ČESKO. Zákon č. 89/2012 Sb. Občanský zákoník, In: *AION CS. s.r.o.,* © AION CS, s.r.o. 2010-2019 [cit. 2019-11-25]. Dostupné z : https://www.zakonyprolidi.cz/cs/2012-89

SEZNAM PŘÍLOH

BAZALKA s.r.o.

KATALOG ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ

Oblast	Účel zpracování	Právní titul	Subjekt údajů	Osobní údaje	Zpracovatel	Způsob zpracování	Příjemce	Bezpečnostní opatření	Doba uchovávání
Personální oblast	Nábor zaměstnanců	Plnění smlouvy (resp.opatření před uzavřením smlouvy)	Uchazeči o zaměstnání	Rozsah dle cíle výběru	NE	Šanony a lokální disk	Personální a mzdové oddělení	Fyzické zabezpečení, administrátorské login,	Do ukončení výběrového řízení
Personální oblast	Pracovněprávní agenda	Zákonná povinnost / Plnění smlouvy	Zaměstnanci	Rozsah dle pracovní smlouvy	NE	Šanony, program PAMICA, lokální disk	pojišťovny,OSSZ,personální a mzdové oddělení	Fyzické zabezpečení, administrátorské login,	Do konce pracovního poměru/30 let doklad o délce zaměstnání
Mzdová oblast	Mzdová agenda	Zákonná povinnost	Zaměstnanci	Rozsah dle mzdové agendy	NE	Šanony, program PAMICA, lokální disk	FÚ, pojišťovny,OSSZ,personální a mzdové oddělení	Fyzické zabezpečení, administrátorské login,	30 let (mzdový list, evidenční listy důch.pojištění)
Mzdová oblast	Docházka	Zákonná povinnost	Zaměstnanci	Rozsah dle systému docházky	NE	Docházkový list,šanony	Úřad inspekce práce, personální a mzdové oddělení	Fyzické zabezpečení, administrátorské login,	Trvání pracovně právního vztahu 10 let po ukončení
Dodavatelská oblast	Nákup zboží a služeb	Plnění smlouvy	Dodavatelé	Jméno, příjmení, adresa, telefon, email	NE	Šanony, účetní program POHODA, lokální disk	obchodní oddělení, účetní	Fyzické zabezpečení, administrátorské login,	10 let dle č.235/2004 Sb. O dani z přidané hodnoty
Odběratelská oblast	Prodej zboží a služeb	Plnění smlouvy	Zákazníci	Jméno, příjmení, adresa, telefon, email	NE	Sanony, účetní program POHODA, lokální disk	obchodní oddělení, účetní	Fyzické zabezpečení, administrátorské login,	10 let dle č.235/2004 Sb. O dani z přidané hodnoty

BAZALKA s.r.o.

KATALOG ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ

Oblast	Účel zpracování	Právní titul	Subjekt údajů	Osobní údaje	Zpracovatel	Způsob zpracování	Příjemce	Bezpečnostní opatření	Doba uchovávání
Prodej finanční oblast	E-shop a rozvoz obědů	Plnění smlouvy	Zákazníci	Jméno, příjmení, adresa, telefon, email	NE	Sanony, účetní program POHODA, objednávkový systém ADMIN, lokální disk	obchodní oddělení, účetní	Fyzické zabezpečení, administrátorské login,	Do 3 let po posledním objednání
Prodej finanční oblast	Prodej zboží a obědů	Plnění smlouvy	Zákazníci	Jméno, příjmení, adresa, telefon, email	NE	Sanony, účetní program POHODA, lokální disk	obchodní oddělení, účetní	Fyzické zabezpečení, administrátorské login,	Do 3 let po posledním objednání
IT oblast	Provoz IT a řízení přístupů	Oprávněný zájem	Zaměstnanci a zákazníci	Dle agendy IT	ANO	Dle agendy	outcoursing IT firmy	administrátorské login, Zpracovatelská smlouva	Doba nezbytně nutná k dosažení účelu
Bezpečnost	Ochrana majetku kamerovým systémem	Oprávněný zájem	Osoby v zorném poli kamer	Digitální videozáznam, dochází ke snímání tváře a postavy osob.	NE	Kamerový systém		administrátorské login	14 dní
Marketing	Newsletter	Souhlas se zpracováním osobních údajů	Zákazníci	Jméno, příjmení, adresa, telefon, email	NE	Email	Marketing	administrátorské login	Nezbytně nutná ke splnění účelu /nejdéle 3 roky
Marketing	Soutěže	Souhlas se zpracováním osobních údajů	Zákazníci	Jméno, příjmení, adresa, telefon, email	NE	Email	Marketing	administrátorské login	Nezbytně nutná ke splnění účelu /nejdéle 3 roky
Marketing	Propagace novinek	Souhlas se zpracováním osobních údajů	Zákazníci	Jméno, příjmení, adresa, telefon, email	NE	Email	Marketing	administrátorské login	Nezbytně nutná ke splnění účelu /nejdéle 3 roky

PŘÍLOHA B: Potvrzení zaměstnance o seznámení s interním předpisem

BAZALKA®
VÍC NEŽ BIO

POTVRZENÍ ZAMĚSTNANCE, ŽE BYL SE ZNÁMEN/PROŠKOLEN S INTERNÍM PŘEDPISEM PRO OCHRANU OSOBNÍCH ÚDAJŮ

Potvrzuji svým podpisem, že jsem se seznámil (a) s Interním předpisem zaměstnavatele pro ochranu osobních údajů ze dne .....

JMÉNO A PŘÍJMENÍ	PRACOVNÍ ZAŘAZENÍ	DATUM PROŠKOLENÍ A SEZNÁMENÍ SE S PŘEDPISEM	PODPIS

PŘÍLOHA C: Sdělení ke splnění informační povinnosti

SDĚLENÍ KE SPLNĚNÍ INFORMAČNÍ POVINNOSTI

Společnost BAZALKA s.r.o.
IČO: 28810902
se sídlem : Gočárova třída 516/18, 500 02 Hradec Králové

(„Správce")

zpracovává osobní údaje v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, obecné nařízení o ochraně osobních údajů („GDPR") a dalšími právními předpisy.

Za účelem ***náboru zaměstnanců, pracovněprávní agendy,mzdové agendy, docházky, provozování e-shopu ,objednávek rozvozů obědů, ochraně majetku kamerovým systémem, zasílání obchodních sdělení, pořádání akci a soutěží v rámci firmy Bazalka, upozornění na novinky*** ,jsou zpracovávány tyto osobní údaje/kategorie osobních údajů: ***jméno, příjmení, rodné číslo, adresa, telefonní číslo, e-mail***, a to na základě ***zákonné povinnosti, plnění smlouvy (resp.opatření před uzavřením smlouvy), provozem IT, ochranou majetku kamerovým systémem, souhlasem se zpracováním osobních údajů.***

Osobní údaje bude Správce zpracovávat manuálně i automatizovaně přímo prostřednictvím svých k tomu pověřených zaměstnanců.
Osobní údaje bude Správce zpracovávat po dobu nezbytně nutnou k dosažení účelu.
Subjekt údajů má právo přístupu ke svým osobním údajům zpracovávaných Správcem, jejich opravu nebo výmaz, popřípadě omezení zpracování, a právo vznést námitku proti zpracování.

Subjekt údajů má dále právo získat od Správce osobní údaje, které se subjektu údajů týkají a jež subjekt údajů Správci poskytl. Správce na základě žádosti subjektu údajů poskytne subjektu údajů údaje bez zbytečného odkladu ve strukturovaném, běžně používaném a strojově čitelném formátu nebo je na žádost subjektu údajů poskytne jinému jednoznačně určenému správci. Toto právo se nevztahuje na osobní údaje, které nejsou zpracovávány automatizovaně.

Správce ***nemá*** úmysl poskytovat osobní údaje do třetích zemí.
Domnívá-li se subjekt údajů, že dochází k neoprávněnému zpracování jeho osobních údajů, může se obrátit se stížností na dozorový orgán, kterým je pro území České republiky Úřad pro ochranu osobních údajů (www.uoou.cz).

Kontaktní údaje Správce
Bazalka s.r.o.
Gočárova třída 516/18
500 02 Hradec Králové
tel. 723 360 721
e-mail : info@bazalkahk.cz

PŘÍLOHA D: Souhlas se zpracováním osobních údajů

BAZALKA®
VÍC NEŽ BIO

SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Tímto uděluji svůj souhlas se zpracováním těchto osobních údajů: jméno, příjmení, adresu, číslo telefonu a e-mailovou adresu společností BAZALKA s.r.o., IČO: 28810902, se sídlem Gočárova třída 516/18, 500 02 Hradec Králové („Správce"), za účelem zasílání obchodních sdělení, pořádání akci a soutěží v rámci firmy Bazalka, upozornění na novinky, a to na dobu nezbytně nutnou k dosažení účelů, nejdéle 3 roky.

Osobní údaje bude Správce zpracovávat manuálně i automatizovaně přímo prostřednictvím svých k tomu pověřených zaměstnanců.

Poučení o právech Subjektu údajů vztahujících se k výše uvedenému souhlasu se zpracováním osobních údajů

Udělení souhlasu je dobrovolné. Tento souhlas můžete kdykoli odvolat, a to pro kterýkoli z výše uvedených účelů zpracování. Odvolání souhlasu je možné provést zasláním e-mailu na adresu Správce: info@bazalkahk.cz, anebo zasláním písemné žádosti na adresu sídla Správce: Bazalka s.r.o., Gočárova třída 516/18, 500 02 Hradec Králové.

Máte právo přístupu ke svým osobním údajům zpracovávaných Správcem, jejich opravu nebo výmaz, popřípadě omezení zpracování, a právo vznést námitku proti zpracování.

Dále máte právo získat od Správce osobní údaje, které se Vás týkají a jež jste Správci poskytnul/poskytla na základě tohoto souhlasu. Správce Vám na základě Vaší žádosti poskytne údaje bez zbytečného odkladu ve strukturovaném, běžně používaném a strojově čitelném formátu nebo je na Vaši žádost poskytne jinému jednoznačně určenému správci. Toto právo se nevztahuje na osobní údaje, které nejsou zpracovávány automatizovaně.

Domníváte-li se, že dochází k neoprávněnému zpracování Vašich osobních údajů, můžete se obrátit se stížností na dozorový orgán, kterým je pro území České republiky Úřad pro ochranu osobních údajů (www.uoou.cz).