VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

OCHRANA OSOBNÍCH ÚDAJŮ VE FIRMĚ
PERSONAL DATA PROTECTION IN THE COMPANY

BAKALÁŘSKA PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Tomáš Vrbecký
AUTHOR

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

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Tomáš Vrbecký**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2017/18

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

Ochrana osobních údajů ve firmě

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Navrhnout systém ochrany osobních údajů.

Základní literární prameny:

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

DOSEDĚL, Tomáš. 21 základních pravidel počítačové bezpečnosti. Brno: CP Books, 2005. ISBN 80-2510-574-1.

KNAP, Karel. Ochrana osobnosti podle občanského práva. 4. dopl. vyd. Praha: Linde, 2004. ISBN 80-7201-484-6.

MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012. ISBN 978-80-87576-12-0.

MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana. 2. dopl. vyd. Praha: ASPI, 2008. ISBN 80-7357-322-9.

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

V Brně dne 28.2.2018

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato bakalářská práce je zaměřena na analýzu zacházení s osobními údaji ve firmě, která se řídí současnými platnými zákony o ochraně osobních údajů a návrh na implementaci nařízení GDPR a seznámení tohoto nařízení se zaměstnanci.

Abstract

This bachelor thesis focuses on the analysis of the treatment of personal data in the company, which is governed by the current laws on personal data protection and proposal for the implementation of the GDPR regulation and familiarization of this regulation with the employees.

Klíčová slova

Ochrana osobních údajů, osobní údaj, zákon č.101/2000 Sb., o ochraně osobních údajů, nařízení 2016/679 (GDPR), firma, subjekty

Keywords

Protection of personal data, personal data, Act No.101/2000 Sb., Personal Data Protection, Act 2016/679 (GDPR), company, subjects

Bibliografická citace

VRBECKÝ, T. *Ochrana osobních údajů ve firmě.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 58 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 20. května 2018

_____

podpis studenta

Poděkování

Rád bych zde poděkoval vedoucímu práce panu Ing. Viktoru Ondrákovi, Ph.D., za poskytnutí informací a cenných rad, které pomohly při tvorbě této bakalářské práce a rovněž i rodině za podporu při celém studiu.

OBSAH

ÚVOD

Žijeme v době, kdy se informační a komunikační technologie neustále rozvíjí a informace mají vysokou hodnotu, a proto se s nimi i v jisté míře obchoduje. Dnes se už bez těchto technologií neobejdeme, protože nám usnadňují práci a zároveň však přináší nové hrozby a nebezpečí, před kterými se z důvodu rychlosti vývoje nestačíme bránit či jim dostatečně a účinně předcházet.

Dá se říci, že osobní údaje tvoří jakousi ekonomickou hodnotu pro digitální trh, hlavně pro online platformy jako jsou vyhledávače nebo sociální sítě. Tyto údaje je pak možné považovat jako ekonomické aktivum složené z identit a chování osob, se kterým se obchoduje výměnou za vyšší kvalitu služeb a produktů.

Lidé, v tomto případě spotřebitelé, si většinou neuvědomují, jak se jejich osobní údaje mohou používat v online světě, zejména pokud nejsou dostatečně chráněny. Firmy pak mohou „těžit“ z těchto informací a přizpůsobovat přímo na míru své služby a produkty svým potencionálním zákazníkům. Čím více těchto informací společnost má, tím získává lepší místo na trhu, proto jsou také databáze s informacemi a osobními údaji velice drahé.

V českém právním prostředí platí zákon č. 101/2000 Sb., o ochraně osobních údajů, který se věnuje ochraně osobních údajů a zacházení s nimi. A jelikož tento zákon je téměř 20 let starý, bylo nutné zajistit nová aktuální pravidla, jak se k osobním údajům chovat. O to se postaralo nařízení GDPR, celým názvem nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, které představuje určitý právní rámec ochrany osobních údajů platný na celém území Evropské unie.

Toto nařízení přichází v platnost 25. května 2018 a dá se říci, dle informací od různých právních poraden nebo přímo GDPR online poraden, že velká část firem či organizací, kterých se nařízení týká, podcenily přípravu a začaly velmi pozdě s přípravnými akcemi. Pokud však firma dodržovala již český zákon č. 101/2000 Sb., o ochraně osobních údajů, nebude to pro ni extrémní změna a přechod na GDPR bude tedy snazší. Jestli se však nepodaří firmám implementovat Obecné nařízení do výše uvedeného data, čekají je vysoké sankce ve výši několika milionů EUR či 4 % z celosvětového obratu společnosti.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem této práce je navrhnout na základě analýzy zpracovávání osobních údajů ve firmě potřebné kroky k implementaci nařízení GDPR do chodu firmy, která se řídí současnými zákony o ochraně osobních údajů.

Jako první seznámení bude vývoj a grafické shrnutí vývoje ochrany osobních údajů, dále co to jsou osobní údaje, jak je dělíme, proč by se měly vůbec chránit a jak se zpracovávají. Pak nastane právní část, kde bude zmíněn zákon o ochraně osobních údajů, význam úřadu pro ochranu osobních údajů a nově také evropské nařízení o ochraně osobních údajů (GDPR).

2 TEORETICKÉ VÝCHODISKA PRÁCE

2.1 Vývoj

Za jeden z nejvýznamnějších a prvotních dokumentů mezinárodního významu, který zaručuje právo na soukromí, je považována Všeobecná deklarace lidských práv, jež byla přijata Valným shromážděním Organizace spojených národů v San Francisku roku 1948. Mimo jiné byl v čl. 12 této deklarace stanoven zákaz vystavovat kohokoliv svévolnému zasahování do soukromého života a korespondence (1, 13. s.).

Právo na respektování rodinného a soukromého života bylo taktéž deklarováno v čl. 8 Evropské úmluvy o ochraně lidských práv a základních svobod, podepsané roku 1950 v Římě. Jak Všeobecná deklarace lidských práv, tak Evropská úmluva o ochraně lidských práv a základních svobod, zaručovaly právo na ochranu soukromí v obecné rovině a právu na ochranu osobních údajů nevěnovaly větší pozornost, jelikož bylo považováno za jeden z komponentů práva na ochranu soukromí a v době vzniku těchto významných dokumentů nebyl důvod oblast ochrany osobních údajů speciálně oddělovat (1, 13, s.).

Jak v průběhu následujících let docházelo k rozvoji společnosti a rozvoji automatizovaných prostředků, které byly využívány ke zpracování osobních údajů, bylo nutné začít chápat ochranu osobních údajů při zpracování a věnovat jí zvláštní právní pozornost (1, 13. s.).

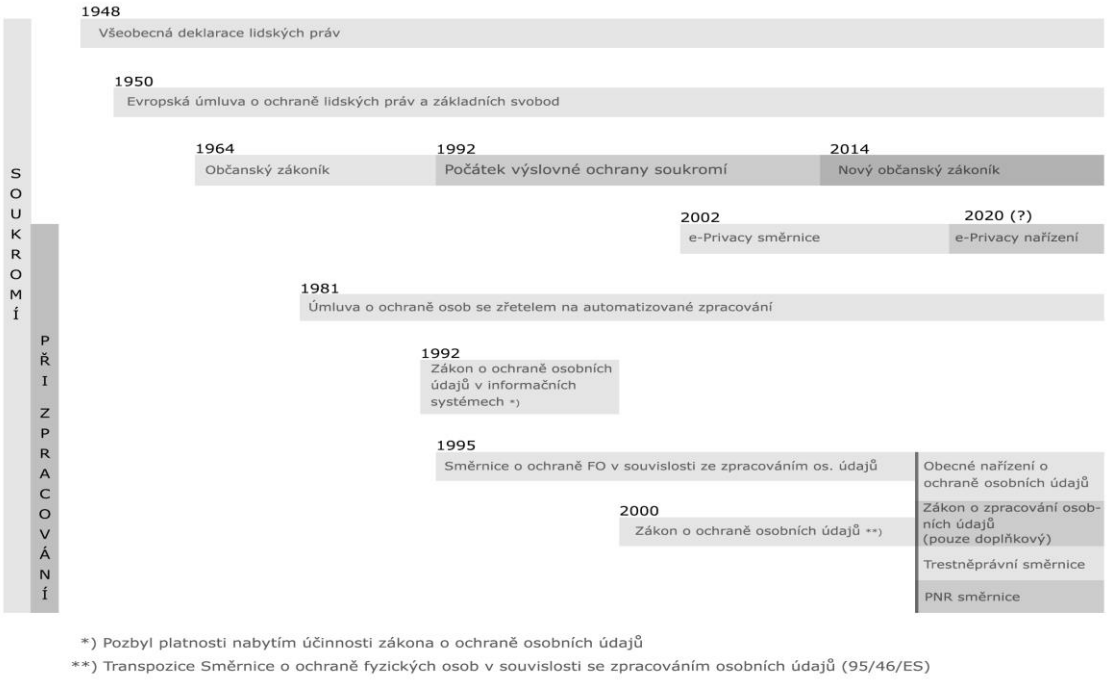
Úmluva č. 108, která se plným názvem označuje jako Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (č.115/2001 Sb., m. s.) lze neformálně přiřadit k 28. lednu roku 1981, kdy poprvé definovala pojmy jako osobní údaj, správce údajů, automatizované zpracování, definovala zvláštní skupiny údajů, určila zásady zpracování osobních údajů, nutnost zabezpečení osobních údajů a další aspekty týkající se automatizovaného zpracovávání (1, 14. s.).

Bylo tedy nutné vytvořit takový právní instrument, který by zpracování osobních údajů podrobně upravil jako celek a zároveň by právní úpravu v evropském prostoru částečně sjednotil. Tímto instrumentem se stala směrnice Evropského parlamentu a Rady 95/46/ES z 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Tato směrnice je inspirována Úmluvou č. 108 a současně

pojímala zpracování osobních údajů komplexně, protože se vztahovala jak na částečné nebo plně automatizované zpracování, tak nově i na neautomatizované zpracování osobních údajů, které byly obsaženy v rejstříku nebo do něj měly být zařazeny (1, 14. s.).

Státům Evropské unie, tak jednotlivě vznikla povinnost přijetí odpovídajících požadavků kladeným směrnicí 95/46/ES. Stanovuje sice čeho mají dosáhnout ve svých vnitrostátních řádech, ale nestanovuje práva a povinnosti subjektům vnitrostátního práva přímo (1, 15. s.).

2.1.1 Grafické shrnutí vývoje



Obr. 1 - Shrnutí vývoje základních dokumentů upravujících soukromí a ochranu osobních údajů při zpracování – *vlastní zpracování (1, 12. s.).*

2.2 Proč chránit osobní údaje?

Existuje několik argumentů, proč by se měly osobní údaje chránit. Já zde uvedu dvě odpovědi, filozofickou a pragmatickou.

Filozofická

„Jde o součást ochrany osobnosti člověka. Pokud se k sobě mají lidé chovat slušně, pak by součástí tohoto slušného chování mělo být i odpovědně nakládat s jejich osobními údaji. Povinnosti stanovené zákonem na ochranu osobních údajů představují pouze

uzákonění něčeho, co slušní lidé, kteří mají k dispozici osobní údaje jiných lidí, stejně dělají. Ochrana osobních údajů by tak měla být součástí lidské slušnosti"(3).

Osobní údaje se mohou stát bránou do soukromí všech. Je jen na každém z nás, koho necháme vstoupit, koho necháme projít a koho necháme před těmito pomyslnými branami stát (2, 17. s.).

Pragmatická

„Plnit povinnosti stanovené zákonem na ochranu osobních údajů je třeba, protože za jejich neplnění hrozí sankce. Je to obdobné jako placení daní. Platit daně a vyplňovat daňová přiznání je velká otrava, která nás připravuje o čas i peníze. Pokud bychom však daně neplatili, vystavujeme se buď finančnímu nebo jinému postihu (např. trest odnětí svobody). S ochranou osobních údajů je to v tomto smyslu stejné jako s daněmi. Sankce za nerespektování ochrany osobních údajů jsou přitom ve srovnání se sankcemi za neplacení daní mnohem přísnější" (2, 17. s.).

2.3 Co je to osobní údaj?

Osobní údaj je v zákoně o ochraně osobních údajů definován poměrně stručně a jednoduše jako „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*" (4, 18. s.).

Osobní údaje jsou všechny opatřené informace o fyzické osobě, kterou lze podle těchto údajů zjistit (21).

Nikdo nebude překvapen, že jméno a příjmení, datum narození, adresa nebo číslo bankovního účtu je osobním údajem. Nicméně, mezi tyto údaje se řadí i emailová adresa, telefonní číslo, konfekční velikost, IP adresa nebo chování uživatelů na webu (5).

Cookies

V momentě, kdy začnete využívat internetové stránky, začnou tyto stránky ukládat na vaše zařízení, ať už počítač, tablet či mobil, malé textové soubory tzv. cookies. Znamená

to, že si na určitý čas zapamatují vaše jednání a preference, které jste na těchto stránkách realizovali (například velikost písma, jazyk, přihlašovací údaje apod.) (6).

2.4 Zvláštní kategorie osobních údajů?

„Zvláštní kategorie osobních údajů jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby“ (7).

2.4.1 Subjekt údajů podle GDPR

„Subjekt údajů je osoba, ke které se údaje vztahují a která může být pomocí těchto údajů identifikována. Subjekt osobních údajů má právo přístupu k údajům a právo na jejich přenositelnost. Také má právo na opravu, výmaz, právo vznášet námitky a má právo na omezení zpracování dat.“ (8).

Obr. 2 - Základní práva subjektu údajů podle GDPR (8).

2.5 Zpracování

Zpracování osobních údajů lze označit jako jakoukoli činnost nebo soubor činností, které správce nebo zpracovatel běžně provádí s osobními údaji automatizovanými nebo jinými postupy, jako jsou shromažďování, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, použití, nahlédnutí, použití, šíření, uchovávání, třídění a likvidace (9).

Zpracování dle obecného nařízení nelze chápat jako jakékoli nakládání s osobním údajem, je nutné jej považovat již za sofistikovanější činnost, kterou správce provádí systematicky a za určitým účelem (9).

Zde jsou uvedeny příklady, u kterých dochází ke zpracování osobních údajů:

- vyplňování a zpracovávání objednávkového formuláře, při nákupu přes e-shop
- při realizaci zakázkové tvorby (kontakty, rozměry zákazníka)
- vystavování faktury zákazníkovi
- rozesílání marketingových akcí pomocí emailu

Z hlediska zaměstnavatele, kdy zpracovává údaje pro plnění zákonných povinností. Jde o rodinný stav zaměstnance, počet dětí, zdravotní pojišťovnu a další podobné údaje (5).

2.5.1 Právní důvody zpracování

Právní důvody znamenají oprávnění pro správce osobní údaje zpracovávat. Správce může osobní údaje zpracovávat pro různé účely, a přitom každý účel musí mít právní důvod zpracování osobních údajů. Je možné využívat tedy jedny osobní údaje pro různé účely, a přitom tyto účely mohou vznikat i zanikat, aniž by to představovalo osobní povinnost údaje likvidovat (18, 33. s.).

2.6 Správce osobních údajů

Správce obecně je odpovědný za plnění povinností určených Obecným nařízením. Naprosto důležitým je dodržování podstaty zpracování osobních údajů, toto dodržování musí být schopen správce kdykoliv doložit. Aby správce mohl osobní údaje zpracovávat, musí mít náležitý právní důvod a splňovat i další povinnosti určené Obecným nařízením. Je současně nutné tyto zpracovávané osobní údaje dobře zabezpečit (10).

2.6.1 Zaměstnavatel

Za správce osobních údajů můžeme nepochybně označit zaměstnavatele, ten může zpracovávat pouze takové osobní údaje, které jsou nutné pro plnění povinností zaměstnavatele. Mezi tyto povinnosti se řadí výpočet mzdy, oznámení na sociálním úřadě, odvod sociálního a zdravotního pojištění. K tomu jsou potřebné tyto údaje: Příjmení, Jméno, Dřívější příjmení, Datum a místo narození, Rodné číslo, Číslo občanského průkazu. V případě, že zaměstnanec pobírá slevu na daních na své děti, musí zaměstnavatel dodat, a tudíž zpracovávat, rodná čísla dětí zaměstnanců. Pokud zaměstnavatel zaměstnancům vyplňuje daňová přiznání, potřebuje také informace o manželovi, popř. manželce. Předchozí pracovní zkušenost (zaměstnání) jsou většinou potřebná pro výpočet mzdy (11).

Podle zákoníku práce zaměstnavatel uzavírá s budoucím zaměstnancem pracovní smlouvu, která obsahuje osobní údaje zaměstnance (jméno, příjmení, datum a místo narození a trvalé bydliště) (11).

Zaměstnavatel má právo zpracovávat tyto osobní údaje:

- *„Pro evidenční listy důchodového pojištění zasílaných na OSSZ (podle § 37 zákona o organizaci a provádění sociálního zabezpečení): datum a místo narození, všechna dřívější příjmení, rodné číslo, místo trvalého pobytu. Byl-li občan účasten důchodového pojištění v cizině a zaměstnavatel je jeho prvním zaměstnavatelem po ukončení důchodového pojištění v cizině, rovněž údaj o názvu a adrese cizozemského nositele pojištění a cizozemském čísle pojištění).*
- *Pro správný výpočet mzdy: vzdělání, předchozí praxe*
- *Pro správný výpočet měsíčních záloh na daně (podle zákona o správě daní a poplatků): druh pobíraného důchodu*
- *Pro zjištění přesného data nároku na odchod do starobního důchodu (podle zákona o organizaci a provádění sociálního zabezpečení): počet dětí (u žen)*
- *Pro plnění povinného podílu osob se zdravotním postižením na celkovém počtu zaměstnanců (podle § 83 zákona o zaměstnanosti): zdravotní znevýhodnění*
- *Pro placení zdravotního pojištění (podle § 10 zákona o veřejném zdravotním pojištění): zdravotní pojišťovna*
- *Za účelem hlášení zaměstnávání cizinců: státní občanství*

- *Prohlášení poplatníka daně z příjmu (podle zákona o správě daní poplatků):*
- *pokud zaměstnanec uplatňuje daňové zvýhodnění a manžel/ka je zaměstnán/a: příjmení a jméno manžela/ky, název a adresa zaměstnavatele*
- *pokud zaměstnanec uplatňuje zvýhodnění na vyživované dítě: jméno, příjmení a rodné číslo dítěte.“* (11).

Správce (zaměstnavatel) musí brát osobní údaje svých zaměstnanců jako jejich vlastnictví, které má pouze zapůjčené k určitým a zákonem stanoveným účelům (viz výše) a používat je jen pro tyto účely. Jde například o výpočet mzdy, komunikace se zaměstnancem apod. Správce musí učinit taková opatření, aby nebylo možné dojít k neoprávněnému přístupu k osobním údajům dle ustanovení § 13 zákona o ochraně osobních údajů. Kdokoli, kdo nemá ze zákona povinnost s osobními údaji pracovat je označován jako neoprávněná osoba. Možnost přistupovat k různým personálním spisům, ať už v papírového či elektronického zpracování, musí být omezeno na úzký počet zaměstnanců a dle § 13 zákona o ochraně osobních údajů je nutné všechna zpracování, což je i nahlížení do záznamů, logovat – vést záznam (11).

2.6.2 Zpracovatel

Ke zpracování osobních údajů může správce přidat i další subjekt, který bude tyto údaje pro něj zpracovávat. Tento subjekt by měl mít vyhovující technické a organizační opatření, aby při zpracování osobních údajů neporušoval požadavky obecného nařízení a byla zaručena ochrana práv subjektu údajů. Z tohoto důvodu musí být mezi dvěma stranami, správcem a zpracovatelem, uzavřena písemná smlouva, v níž je stanoven účel, povaha a doba trvání zpracování, typ a kategorie osobních údajů a povinnosti a práva správce (10).

2.7. Souhlas se zpracováním osobních údajů

Souhlas je jedním z právních důvodů, díky kterému může správce zpracovávat osobní údaje subjektu. Souhlas by měl být svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným jasným potvrzením své svolení ke zpracování svých osobních údajů. Subjekt údajů by měl vždy znát účel zpracování osobních údajů, k němuž dal souhlas (18, 34. s.).

Aby byly zachovány podmínky souhlasu, měl by být oddělený od smluv nebo obchodních podmínek (18, 34. s.).

2.8 Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“)

Zákon o ochraně osobních údajů upravuje práva fyzických osob, s jejichž osobními údaji nakládá někdo jiný a zároveň upravuje povinnosti těch, kdo osobní údaje jiných lidí používají způsobem, který zákon vymezuje jako zpracování osobních údajů. *„Tento zákon byl přijat proto, aby i v právním řádu České republiky byla rozšířena práva na ochranu soukromí fyzických osob o instituty zformované v řadě demokratických států světa a zakotvené v dokumentech významných mezinárodních organizací – zejména Evropské unie a Rady Evropy“.* V rámci Evropské unie bylo nutné vytvořit v České republice nezávislý orgán s kontrolní pravomocí vůči těm, kdo osobní údaje jednotlivců zpracovávají. Smysl takto institucionalizované ochrany osobních údajů je především v preventivním působení (12, 10. s.).

2.9 Význam

Jednoduše lze říci, že důvodem, proč byl tento zákon přijat, je, aby zajistil ochranu práv jednotlivce. Hlavním významem je, že pokud jiný zákon nestanoví jinak, lze osobní údaje náležící k jednomu určitému člověku zpracovávat pouze s jeho souhlasem, nebo pokud byly oprávněně zveřejněny. Z toho vyplývá, že použití osobního údaje nemusí být podle zákona o ochraně osobních údajů jeho zpracováním (23).

Přímým významem tedy můžeme chápat tento zákon jako zajištění informovanosti o tom, že někdo zpracovává osobní údaje. Tento význam má i pro člověka, který se jako fyzická osoba angažuje při zpracovávání osobních údajů podléhajících zákonu o ochraně osobních údajů. Jsou zde také stanoveny povinnosti a při jejich porušení hrozí vymahatelnost sankcí (12, 33. s.).

2.10 Úřad pro ochranu osobních údajů

Jako nezávislý správní orgán můžeme chápat Úřad pro ochranu osobních údajů (ÚOOÚ), který:

- *„Provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů.*
- *Vede registr povolených zpracování osobních údajů.*
- *Přijímá podněty a stížnosti občanů na porušení zákona.*
- *Poskytuje konzultace v oblasti ochrany osobních údajů"(13).*

Činnost Úřadu je vymezena zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a některými dalšími zákony, a nově i obecným nařízením GDPR" (13).

2.11 GDPR

Vzhledem k rozvoji počítačové techniky, internetu či sociálních sítí již nestačily zastaralé vnitrostátní zákony. Bylo třeba je novelizovat, neboť tyto zákony vycházejí ze zastaralé Směrnice 95/46/ES. Když se tato směrnice tvořila, nikdo nepředpokládal tak obrovský vývoj, velice ovlivňující zpracování osobních údajů. Zároveň bylo třeba vzít v úvahu efektivní zajišťování osobních údajů při zahraničním zpracovávání. Ochrana osobních údajů v evropském prostoru, jež začala po roce 2010, odstartovala revizi celého právního rámce (1, 16. s.).

Nařízení Evropské unie přímo stanovuje povinnosti a práva vnitrostátním subjektům, nikoliv primárně státu k provedení vnitrostátních Legislativních opatření. Jednoduše řečeno, nařízení Evropské unie lze z pohledu jeho adresátů označit za obdobu zákona (1, 16. s.).

Nařízení EU tak má, oproti směrnici, větší sjednocující účinek,protože jeho pravidla jsou přímo aplikovatelná na adresáty ve všech státech Evropské unie. Použitím nařízení EU, jakožto právního předpisu, odpadá pro správce a zpracovatele velká část právní nejistoty ohledně možných důležitých odlišností v jednotlivých vnitrostátních právních úpravách v členských zemích, protože práva a povinnosti jsou upraveny napříč členskými státy Evropské unie jednotně, bez zásadní nutnosti přijímat vnitrostátní předpisy, které by tato

práva a povinnosti prováděly na vnitrostátní úrovni. Tím pro subjekty, které chtějí působit v jiné Evropské zemi, odpadá nutnost tyto vnitrostátní předpisy podrobně studovat (1, 16. s.).

„Další etapou, resp. reakcí na vývoj lidského společenství a související zpracování osobních údajů je Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 29. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů = GDPR) se stanovenou ***účinností od 25. května 2018****"* (1, 16. s.).

Dá se říci, že použití nařízení EU je v této souvislosti revoluční, jelikož nebylo nikdy nařízení Evropské unie použito pro úpravu tak širokého souboru vztahů, a to i takových, které vznikají při zpracování osobních údajů. Nejen z pohledu ochrany osobních údajů, ale i z pohledu občana ČR, vstupujeme do nové doby, kde budeme poprvé ve velké míře aplikovat evropský předpis namísto zákona (1, 16. s.).

2.11.1 Hlavní znaky GDPR (obecně):

- *„Je jednotně aplikovatelné v celé EU.*
- *Rozšiřuje pojem osobních údajů – nově také biometrické prvky (sken oční sítnice).*
- *Zpřesňuje souhlas se zpracováním osobních údajů – nově zákaz předvyplněných políček.*
- *Vyžaduje vyšší technickou a organizační bezpečnost správců a zpracovatelů.*
- *Při rozsáhlém a systematickém zpracování osobních údajů požaduje jmenování pověřence na ochranu osobních údajů.*
- *Při rizikových zpracování osobních údajů požaduje příchozí provedení posouzení vlivu na ochranu osobních údajů.*
- *Posiluje stávající práva fyzických osob a zakládá práva nová – právo být zapomenut či právo na přenositelnost údajů.*
- *Porušení ochrany dat musí být oznámeno do 72 hodin jak fyzické osobě, tak Úřadu pro ochranu osobních údajů.*

- *Zavádí nepoměrně vyšší sankce za porušení ochrany osobních údajů – oproti současnosti (maximálně 10 000 000 korun) bude možné uložit až 20 000 000 eur nebo 4 % celosvětového obratu podniku (podnikatel)“* (20).

Obr. 3 - Hlavní pilíře GDPR (26)

2.11.2 DPO

Pověřenec pro ochranu osobních údajů (DPO) má jako hlavní úkol, monitorování zpracování osobních údajů v dané organizaci s povinnostmi dané nařízením, školením a auditem. Jde o celkové řízení agendy pro interní ochranu dat. Může se jednat o externího

i interního pracovníka. U menších firem je pravděpodobnost, přirazení zodpovědnosti vhodné osobě. Nenese však osobní zodpovědnost za nedodržování GDPR (14).

Na pověřence nejsou kladeny žádné nároky, co se týče vzdělání nebo certifikace, měl by však ovládat dostatečně Obecné nařízení a pak už je na firmě, jestli jí bude vyhovovat pověřenec s právním nebo technickým vzděláním (18, 42. s.).

Obr. 4 - Vlastnosti pověřence pro ochranu osobních údajů (27)

2.11.3 Vedení záznamů

Mezi povinnostmi GDPR je, i vedení záznamů o činnostech zpracování (logování). Určuje tedy správci vést záznam o tom, jaké konkrétní údaje se zpracovávají, jejich účel a rozsah i plánované lhůty pro výmaz (16).

2.11.4 Posouzení vlivu

Posouzení vlivu (DPIA) je nová povinnost, kterou GDPR přináší. Měla by se provádět už při implementaci GDPR do chodu firmy. Obsahem by mělo být to, jak chce organizace nakládat se zpracovanými údaji a zda je nutné provádět určité operace, vzhledem k účelům zpracování. Mělo by být provedeno, pokud hrozí, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob (16).

Posouzení vlivu na ochranu osobních údajů podle odstavce 1 je nutné zejména v těchto případech:

- *„systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,*
- *rozsáhlé zpracování zvláštních kategorií údajů (např. údajů o rasovém či etnickém původu, politických názorech či zdravotním stavu anebo biometrických údajů atd.) nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů,*
- *rozsáhlé systematické monitorování veřejně přístupných prostorů"* (25).

Pokud si správce nebude jistý, zda jeho operace s daty podléhají DPIA, doporučuje se v pokynech pracovní skupiny WP29, aby správce DPIA vykonal (25).

2.12 Zabezpečení ve společnosti

Zde jsou popsány činnosti zálohování a archivace.

2.12.1 Zálohování

Důležitá činnost, co se týká bezpečnosti uložení dat. Pokud dojde ke ztrátě nebo poškození dat, existence záloh má pak nevyčíslitelnou hodnotu. Nejčastějším příčinám poškození dat je selhání hardwaru nebo softwaru (22).

Cílem zálohování je navrácení dat do stavu, v jakém byla v námi požadovaném okamžiku. Zálohy by neměly být fyzicky situované na jednom stejném místě, ale oddělené od zdrojových dat (17).

2.12.2 Archivace

Často se můžeme setkat se zaměněním výrazů archivace a zálohování. Zálohování je proces, který zajišťuje, že o data nepřijdeme. Oproti tomu archivace souvisí s přesouváním již neaktuálních dat na archivní média, ať z důvodů výkonových či daných legislativou (19).

2.13 Skupina WP29

Pracovní skupina WP29 je složena z vedoucích zástupců dozorových úřadů členských zemí Evropské unie. Mezi její činnosti patří mimo jiné posuzování otázek týkajících se uplatňování vnitrostátních předpisů přijatých k provedení směrnice 95/46/ES s cílem přispívat k jejich jednotnému uplatňování. WP29 vydává stanoviska a doporučení pro správné použití GDPR (18, 44. s.).

3 ANALÝZA SOUČASNÉHO STAVU

3.1 Základní údaje o společnosti

Po vzájemné dohodě obou stran, z důvodů ochrany bezpečnosti firmy, budu uvádět smyšlené jméno firmy a smyšlené důležité interní informace.

V této práci jsem prováděl analýzu systému ochrany osobních údajů ve firmě XY s.r.o. Firma je velmi úspěšnou a uznávanou součástí světového holdingu XY GROUP s hlavním sídlem v německém Stuttgartu. V České republice a na Slovensku působí 20 let a zachovává si čelní postavení v oblasti distribuce průmyslových kabelů a kabelového příslušenství na českém a slovenském trhu a v oblasti výroby kabelové konfekce v rámci evropských výrobních aktivit skupiny XY Group.

V roce 2007 byla zahájena výstavba nových administrativních, vývojových, výrobních a skladovacích prostor, které pomohly umožnit vytvořit ideální podmínky pro realizaci nových rozvojových plánů. Vzniklo tak nové Logistické a administrativní centrum firmy XY na Moravě, jehož provoz byl zahájen na jaře roku 2008.

V květnu roku 2016 investovala společnost do nové výrobní haly, zahrnující úpravy stávajících prostor pro 200 nových zaměstnanců. Tímto krokem rozšiřuje XY s.r.o. své stávající aktivity také o výrobu kabelové konfekce pro dceřiné společnosti XY Group.

Produkty jsou vyráběny ve vlastních výrobních závodech XY. Těchto závodů mají po celém světě téměř 20, dále více než sto obchodních zastoupení a 40 distribučních společností a celkem 3 450 zaměstnanců.

Všechny informace, které jsou v analýze uvedeny, byly diskutovány s odpovědnými zaměstnanci z oddělení IT, HR a ZC a použity určité části ze směrnic firmy.

3.2 Kategorie subjektů

Ve společnosti se zpracovávají a ukládají osobní údaje, které jsou různorodé a z tohoto důvodu jsou rozděleny do následujících kategorií:

Kategorie subjektů osobních údajů

- Uchazeči o zaměstnání
- Zaměstnanci
- Obchodní partneři – kontaktní osoby (lidé)
- Zákazníci webu

V následující části analýzy se budu věnovat popisu jednotlivých kategorií subjektů.

3.2.1 Uchazeč o zaměstnání

Nový uchazeč o zaměstnání je osoba, která se uchází o zaměstnání a je zařazena do systému výběrového řízení. Veškeré evidované údaje jsou uvedeny v uchazečově osobním životopisu. Zpracovávané údaje tedy nejsou vedeny zvlášť (jméno, adresa, kontakt, …), ale jsou zpracovávány jako celek – životopis v papírové podobě.

Účel zpracování těchto údajů:

- Nutné podklady pro proces přijetí zaměstnance

Právní titul:

- Souhlas se zpracováním osobních údajů

Zdroj:

- Uchazeč o zaměstnání
- Personální agentura
- Úřad práce

Místo uložení:

Životopisy nejsou ukládány v elektronické formě, ale pouze jako papírový dokument v kanceláři HR.

Výmaz:

Tento dokument je uložen po dobu výběrového řízení, poté je zlikvidován viz „Skartace“.

Užití dat:

K těmto dokumentům mají přístup jen zaměstnanci z oddělení lidských zdrojů.

3.2.2 Zaměstnanci

Při nástupu nového zaměstnance je potřeba z důvodu plnění pracovní smlouvy evidovat osobní údaje. Nový zaměstnanec je tedy povinen vyplnit osobní dotazník, ve kterém vyplňuje následující údaje, které jsou povinné:

Tab. 1 - zpracovávané osobní údaje zaměstnanců *– (vlastní zpracování)*

Osobní údaje	Povinné	Nepovinné
Příjmení, jméno	●	
Rodné příjmení	●	
Titul	●	
Datum narození	●	
Rodné číslo	●	
Místo narození	●	
Státní příslušnost	●	
Zdravotní pojišťovna	●	
Číslo bankovního účtu	●	
Telefon	●	
Email	●	
Nejvyšší dosažené vzdělání	●	
Další vzdělání a odborné kurzy	●	
Adresa bydliště	●	

Kontaktní adresa	●	
Rodinný stav	●	
Rodinní příslušníci (manžel/ka, děti)	●	
Předchozí zaměstnavatel	●	
Zdravotní stav	●	
Kontakt pro případ nutnosti	●	
Fotografie	●	
Číslo OP	●	

Důvody zpracování těchto údajů:

- Zákonem dané povinnosti zaměstnavatele (viz Zaměstnavatel)

Právní titul:

- Plnění smlouvy nebo jednání o jejím uzavření
- Souhlas se zpracováním (fotografie a číslo OP)

Zdroj:

- Osobní dotazník

Na konci dotazníku je souhlas se zpracováním osobních údajů ve smyslu zákona č.101/2000 Sb., o ochraně osobních údajů. Další souhlas se týká zpracování osobní fotografie pro firemní účely.

Místo uložení:

Všechny získané informace jsou zapisovány do personálního systému TARGET 2100, jehož administrátorem je právě oddělení HR a (externí) mzdová účetní, nikdo jiný nemůže měnit nebo zadávat údaje.

Výmaz

Data jsou uložena po dobu trvání uzavřené pracovní smlouvy. Po zániku pracovního poměru zaměstnavatel neukládá již dále osobní údaje zaměstnance, pokud to nevyžaduje archivační zákon.

Užití dat:

K těmto údajům mají přístup zaměstnanci z oddělení lidských zdrojů, externí mzdová účetní, přímý nadřízený zaměstnance a také sám zaměstnanec. Osobní údaje potřebné pro tvorbu mezd a daňové úkony jsou zpracovávány externí účetní, která tyto údaje potřebuje.

3.2.3 Obchodní partneři – kontaktní osoby

Tato kategorie se skládá z kontaktních osob našich zákazníků a zpracovávají se následující údaje:

Tab. 2 - zpracovávané osobní údaje kontaktních osob zákazníků – (*vlastní zpracování)*

Osobní údaje	povinné	nepovinné
Oslovení	●	
Jméno	●	
Příjmení	●	
Oddělení		●
Funkce		●
E-mail	●	
Telefonní číslo	●	
Fax		●

Důvody zpracování těchto osobních údajů:

- Příprava a realizace smluv
- Plnění právních povinností obou stran
- Poskytování služeb

- Plnění přání a požadavků zákazníků

Právní titul:

- Plnění smlouvy nebo jednání o jejím uzavření

Zdroj:

- Obchodní partner

Místo uložení:

Veškeré údaje jsou zpracovávány a ukládány elektronicky na serverech uvnitř společnosti a na serverech, kde běží systém SAP, tedy v mateřské společnosti v Německu. Smlouvy, či jiné dokumenty v papírové podobě, obsahující osobní údaje jsou zakládány do kartotéky v obchodním oddělení.

Výmaz:

Data jsou uložena po dobu trvání uzavřené obchodní smlouvy. Po zániku obchodního vztahu již nejsou osobní údaje potřeba, ale z důvodu archivace je nutné tyto údaje mít stále po určitou dobu k dispozici (viz Archivace).

Odvolání souhlasu a vymazání údajů

Zákazník může kdykoli odvolat svůj souhlas se zpracováním svých osobních údajů nebo uplatnit své právo na přístup k údajům, které o něm jsou společností XY s.r.o. zpracovávány, právo na opravu těchto údajů jsou-li nepřesné. K tomu postačuje zaslání e-mailu. V případě odvolání souhlasu se zpracováním osobních údajů už nemůže zákazník využívat služeb internetového obchodu společnosti.

Vymazání osobních údajů

Osobní údaje budou vymazány:

- když zákazník odvolá svůj souhlas se zpracováním jeho osobních údajů,
- když zpracování osobních údajů zákazníka už dále není potřebné k účelu, pro který byly údaje poskytnuty,
- když zpracování osobních údajů není možné z jakýchkoli jiných právních důvodů.

Užití dat:

Přístup k datům o zákaznících má hlavně obchodní oddělení, zákaznické oddělení a některé přístupy jsou umožněny i marketingovému oddělení.

3.2.4 Zákazníci webu

Elektronické obchodování společnosti slouží k obchodování na úrovni B2B. Aby mohla společnost zajistit bezpečný nákup a zamezit zneužití nákupu jinou osobou, je potřeba vyplnit „*Autorizační formulář k elektronickému obchodování se společností XY s.r.o.“*

V tomto formuláři se vyplňují stejné údaje jako jsou uvedeny výše a určuje se stupeň oprávnění pro osobu, která bude e-shop využívat (viz Příloha č. 1)

Zpracovávané údaje jsou stejné jako u kontaktních osob zákazníků.

Důvody zpracování těchto osobních údajů:

- Příprava a realizace smluv
- Plnění právních povinností obou stran
- Poskytování služeb
- Plnění přání a požadavků zákazníků

Právní titul:

- Plnění smlouvy nebo jednání o jejím uzavření

Zdroj:

- Obchodní partner (webový formulář, emailový nebo telefonický kontakt)

Místo uložení:

Veškeré údaje jsou zpracovávány a ukládány elektronicky na serverech uvnitř společnosti a na serverech, kde běží systém SAP, tedy v mateřské společnosti v Německu. Smlouvy, či jiné dokumenty v papírové podobě, obsahující osobní údaje jsou zakládány do kartotéky v obchodním oddělení.

Výmaz:

Data jsou uložena po dobu trvání uzavřené obchodní smlouvy. Po zániku obchodního vztahu již nejsou osobní údaje potřeba, ale z důvodu archivace je nutné tyto údaje mít stále po určitou dobu k dispozici (viz Archivace).

Užití dat:

Přístup k datům o zákaznících má hlavně obchodní oddělení, zákaznické centrum a některé přístupy jsou umožněny i marketingovému oddělení.

Práce s daty na webu

Jakmile zákazníci navštíví webové stránky elektronického obchodu společnosti, webové servery společnosti standardně dočasně ukládají za účelem bezpečnosti systému následující údaje:

- spojovací data dotazujícího počítače (IP adresu),
- identifikační data použitého internetového prohlížeče a operačního systému,
- internetové stránky společnosti navštívené našimi zákazníky,
- datum a délku návštěvy.

Další údaje nad tento rámec, jako například jméno, adresa, telefonní číslo nebo e-mailová adresa, nejsou zpracovávány, pouze pokud by byly zákazníkem dobrovolně zadány, například v rámci registrace, průzkumu, veřejné soutěže, za účelem uzavření smlouvy nebo požadavku na informace. Jelikož automaticky zaznamenávané údaje, zmíněné výše, jsou anonymní, nemůže společnost XY s.r.o. přiřadit tyto hodnoty konkrétním osobám a údaje jsou navíc po statistickém vyhodnocení vymazány.

Osobní údaje získané od zákazníků jsou využity společností jen za účelem technické administrace internetových stránek a plnění přání a požadavků zákazníků, zpravidla pro přípravu a realizaci smluv, dodávku zboží a poskytování služeb, pro realizaci plateb a potřebné kontroly, případně pro usnadnění objednávání prostřednictvím vedení účtu zákazníka nebo pro zodpovídání dotazů.

Společnost využívá tyto údaje i pro komunikaci se zákazníkem o produktech, službách a objednávkách, ale i pro zlepšování elektronického obchodu a webu celkově, k zajištění technických a logistických služeb pro společnost třetími osobami. Je nutné tyto údaje

používat i k ukládání předloh objednávek, tak aby je zákazník mohl opět využít při dalším přihlášení.

Osobní údaje je společnost oprávněna zjišťovat a zpracovávat k uvedeným účelům. Zákazník k tomu uděluje v rámci Všeobecných obchodních podmínek výslovný souhlas a ten je společností protokolován. Rovněž je možno oprávněně vstupovat se zákazníky do kontaktu v souvislosti s registrací v elektronickém obchodu.

Pokud zákazník předem dal svůj souhlas, využije společnost tyto údaje i pro průzkumy orientované na produkty nebo marketingové účely. V případě nesouhlasu, samozřejmě nikoliv.

Sdělení nebo předání osobních údajů třetí osobě, pouze v těchto případech:

- pokud je to nutné pro dodržení smluvních závazků – zákazník je informován,
- pokud zákazník udělil výslovný souhlas.

Odvolání souhlasu se zpracováním osobních údajů

Vzhledem ke specifickým požadavkům zákazníků je zajištěn sběr a zpracování pseudonymizovaných údajů pomocí služeb společnosti Econda. Data se používají pro vytváření uživatelských účtů pod pseudonymy. Mohou být použity Cookies, které umožňují rozpoznání webového prohlížeče, bez výslovného souhlasu návštěvníka nedojde k propojení účtu s daty prostřednictvím nosiče pseudonymu. Jakmile návštěvník vstoupí na webové stránky, je znemožněno rozpoznání IP adresy, což brání přiřazování uživatelských účtů k těmto adresám. Na webu společnosti XY s.r.o. mohou návštěvníci, pomocí odkazu na web Econdy, kdykoliv odvolat souhlas se zaznamenáváním a ukládáním těchto dat.

Cookies

Webové stránky elektronického obchodu využívají na více místech cookies. Ty jsou zde proto, aby bylo zajištěno příjemnější, efektivnější a spolehlivější prostředí pro uživatele webových stránek. Většina těchto používaných cookies jsou tzv. Session-Cookies", které se automaticky vymažou, pokud stránky uživatel opustí.

Dalším používaným typem je tzv. permanentní cookies, a to pro uchování informací o zákaznících, kteří opakovaně využívají web společnosti. Tímto lze poskytnout svým zákazníkům optimální průchod stránkami a přizpůsobit obsah individuálním potřebám.

Obsahem těchto cookies je jen identifikační číslo. Není zde ukládáno jméno ani IP adresa apod.

Návštěvníci mají možnost procházet web i bez ukládání cookies, a to tak, že mohou ve svém prohlížeči zakázat ukládání cookies, omezit jejich ukládání jen na určité webové stránky, nebo nastavit upozornění o zasílání cookies z prohlížených stránek. Cookies nepůsobí žádné škody a neobsahují viry.

3.3 Ochrana dat

Společnost XY s.r.o. dodržuje příslušné právní předpisy upravující ochranu osobních údajů, především zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Údaje zpracovávané společností nejsou nijak prodávané a není s nimi nakládáno v rozporu s právními předpisy.

Ve společnosti jsou servery, na kterých běží centrální disky a klient LOTUS, tento server obsahuje 12 disků o celkové kapacitě 9,6 TB a běží na typu RAID 1, disky jsou tedy zrcadleny tzv. mirroring. Záloha probíhá na pásky, které jsou každý 10. den vyjmuty a uloženy do trezoru.

Systém SAP běží na šifrované síti připojené na servery ve Stuttgartu a další zálohové servery umístěné cca 30 km od nich. Šifrování probíhá na dvou paralelně zapojených šifrovacích zařízeních.

V tomto systému jde o tok dat jak z hlediska obchodních styků, tak i osobní údaje zákazníků. Ve všech pobočkách po celém světě jde o stejný systém ukládání dat.

3.4 Přístupová práva k osobním údajům

Ředitel společnosti má možnost nahlédnout na záznamy svých podřízených. To platí i pro vedoucí jednotlivých oddělení (marketing, nákup, zákaznické oddělení atp.). Zaměstnanci mají možnost nahlížet do svých vlastních údajů v systému Target.

Nahlížení do osobních údajů zákazníků závisí na přiděleném oprávnění jednotlivých zaměstnanců. Tzn., že ne všichni mají právo na vytvoření, upravení, vymazání a nahlížení v informačním systému na osobní údaje zákazníků.

Údaje zákazníků webu je možné sledovat až po jejich registraci do e-shopu, kde závisí na výši oprávnění v daném oddělení, kdo může nahlížet. Tuto možnost má většinou celé zákaznické centrum (ZC), protože je potřebují k výkonu své činnosti.

Tab. 3 - přístupová práva k osobním údajům – *(vlastní zpracování)*

	Ředitel	**HR**	**Vedoucí jednotlivých oddělení**	**Ostatní zaměstnanci**	**Zaměstnanec** (*)
OÚ zaměstnanců	●	●	●		●
OÚ zákazníků			● (**)	●	
OÚ zákazníků e-shopu			● (**)		

Pozn.: *) konkrétní zaměstnanec jehož údaje jsou zpracovávány

**) záleží dle oprávnění (obchodní oddělení, marketing)

3.4.1 Human resources – HR

Hlavním zpracovatelem osobních údajů v této společnosti je Oddělení lidských zdrojů – HR. Toto oddělení zahrnuje celou řadu postupů a metod pro řízení lidských zdrojů a práci se zaměstnanci. Už od prvního kontaktu s novými zaměstnanci, kdy řeší osobní dotazníky, uzavírají pracovní smlouvy, evidují zaměstnance, přes povinnosti firmy vůči státu, plán rozvoje zaměstnanců, až po evidenci odpracované doby a zpracování mezd.

Řídí se zákonem č. 101/2000 Sb., o ochraně osobních údajů. S vybranými zaměstnanci, kteří přicházejí do styku s daty tohoto charakteru je sepsána Dohoda o zachování důvěrných informací.

Informace jsou zpracovávány buď elektronicky nebo v papírové formě. Elektronické formy jsou v personálním informačním systému, papírové zas v uzamčených skříních a v archívu.

3.5 Ukládání dokumentů

Prvním ukládacím místem pro vyřízené, ale stále ještě běžné provozně užívané dokumenty včetně vlastních kopií, jsou příruční registratury jednotlivých pracovníků nebo celého oddělení. Za řádné uložení dokumentů zodpovídá vedoucí oddělení.

V příruční registratuře jsou dokumenty uloženy po celou dobu provozní potřeby. Po jejím ukončení nebo z provozních důvodů jsou dokumenty ukládány ve spisovně původce. Pokud uplynula skartační lhůta dokumentu nebo dokument není nutné archivovat, může být přímo předán ke skartaci.

3.5.1 Archivace

Spisovna – slouží k ukládání dokumentů, které již nejsou zapotřebí pro běžnou provozní činnost oddělení (pracovníků). Dokumenty zde zůstávají uloženy do provedení skartačního řízení. Přístup do této místnosti je omezen jen na účtárnu, HR a administrativní referentku, pomocí přístupové karty. Do archivačních boxů v místnosti má přístup jen jedna osoba a to administrativní referentka.

V těchto boxech jsou uloženy například údaje o bývalých zaměstnancích po dobu maximálně dvou let – vše je řízeno dle archivačního a skartačního řádu. Každý dokument je veden v seznamu a má svůj skartační znak, podle kterého se eviduje a určuje, zda už uplynula doba archivace a je potřeba jej skartovat.

Ukládací jednotky (archivační boxy) se ve spisovně ukládají do regálů, uzamykatelných skříní a trezorů. Archivační boxy se ukládají tak, aby bylo využito prostoru, pokud možno co nejúčelněji při dodržení pravidel BOZP.

Základní evidenci spisovny tvoří soubory předávacích protokolů jednotlivých oddělení.

3.5.2 Skartace

Staré a nepotřebné osobní dokumenty je nutné skartovat/vyhodit. Za skartaci či likvidaci osobních dokumentů je zodpovědný každý zaměstnanec, řídí se dle interní směrnice Spisový a skartační řád.

Skartační znak – vyjadřuje hodnotu dokumentu podle obsahu a označuje způsob, jakým se s dokumentem naloží ve skartačním řízení.

Znak „A“ (archiv) – označuje dokument trvalé hodnoty, který bude ve skartačním řízení vybrán jako archiválie k trvalému uložení.

Znak „S“ (skartace) – označuje dokument bez trvalé hodnoty, který bude po uplynutí skartační lhůty navržen ve skartačním řízení ke skartaci.

Znak „V“ (výběr) – označuje dokument bez trvalé hodnoty, u kterého v době uložení nebylo možné určit, zda je z hlediska dokumentární hodnoty cenný či nikoliv, po uplynutí skartační doby bude tento dokument znovu posouzen a navržen buď k archivaci, nebo k vyřazení.

Skartační lhůta – je doba, po kterou dokument zůstává uložen ve spisovně původce. Počíná běžet dnem 1. ledna roku následujícího po vyřízení dokumentu nebo po jeho uzavření. Tato lhůta je závazná a nelze ji zkracovat. Pokud potřebuje původce dokument i nadále pro svou činnost, může být skartační lhůta výjimečně prodloužena. Tato lhůta se uvádí jako číslice za skartačním znakem a její jednotkou je rok.

Např. dokument, který vznikl v roce 2014 a je označen jako S10 je možné skartovat po uplynutí 10 let od jeho vzniku, tato lhůta začíná běžet od 1. ledna 2015, tzn., že skartace proběhne nejdříve v lednu 2025.

Skartační řízení – je postup, při kterém se vyřazují dokumenty nadále nepotřebné pro činnost původce.

Skartační plán – je přehled druhů dokumentů společnosti, doplněný o skartační znaky.

Průběh skartačního řízení

Skartační řízení je prováděno pověřeným pracovníkem jednou ročně komplexně za celou společnost a jeho předmětem jsou všechny dokumenty, u nichž uplynuly skartační lhůty. Pracovník spisovny tyto dokumenty označí, vedoucí oddělení, které bylo jejich původcem, je odsouhlasí a pracovník spisovny je fyzicky vyřadí ze spisovny.

3.6 Informační systémy

Informační systémy jsou neoddělitelnou součástí firmy, jsou na nich uloženy osobní údaje jak zaměstnanců, tak i zákazníků. Ve společnosti se využívá systému SAP. Tento systém využívá téměř každé oddělení, tj., od nákupu, zákaznické centrum, marketing, až po obchodní oddělení – obchodní styk, reklamace, nákup, sklad, fakturace.

3.6.1 TARGET 2100

Systém **„Target 2100“** je nástroj pro komplexní podporu práce nejen v organizačních, personálních a mzdových útvarech podniků, ale i pro vrcholový management společnosti.

V tomto systému jsou vedeny hlavně osobní údaje zaměstnanců společnosti. Zpracovávají se zde i pracovní smlouvy, úvazky vůči firmě a přehled vyplácení mzdy a benefitů. Tento systém běží na serveru uvnitř společnosti.

3.6.2 LOTUS NOTES

Elektronické zásilky přebírá každý pracovník na své e-mailové adrese v softwaru Lotus Notes. Mimo tyto pracovní adresy je zřízená centrální adresa info@XY.cz, kterou obsluhuje pověřený pracovník. Podle adresáta a podle obsahu rozesílá došlé zprávy příslušným adresátům na jejich adresu. Příchozí elektronické zásilky si eviduje a archivuje každý pracovník na své adrese. Je stanovená doba uložení na disku a po uplynutí této doby se dokumenty automaticky archivují. Nevyžádaná sdělení (spamy) příjemce el. pošty neeviduje a vymaže. Elektronický soubor, který je nutno zachovat v papírové podobě je nutno vytisknout a nakládat s ním jako s papírovým dokumentem.

Přijaté E-maily jsou na vstupu kontrolovány na přítomnost škodlivých programů, virů a spamů. Podezřelé emaily (ZIP přílohy v nich atd.) není možné doručit a jsou automaticky odstraněny SPAM filtrem. Pro doručování objemných příloh slouží služby jako například File-Share.

3.6.3 COMINFO

Záznamy o evidenci veškerých příchodů a odchodů z pracoviště jsou prováděny elektronicky. Zaměstnanci mají povinnost zaznamenat kromě příchodu a odchodu do nebo ze zaměstnání rovněž přestávky v práci (oběd v případě opuštění budovy, kuřácké přestávky apod.), překážky v práci na straně zaměstnance (vyšetření u lékaře apod.), dovolenou, služební cesty, školení, home office, příp. další období, kdy nevykonávají práci.

3.6.4 DMS (Document Management Systém)

EISOD – systém je složen ze samostatně pracujících programů - např. správa dokumentací, procesní modelování a měření procesů atd. => směrnice, nařízení, formuláře, obchodní smlouvy (dodavatel, zákazník), správa auditů a opatření.

Každý uživatel má přesně specifikován typ přístupu – roli, která mu přiděluje přístupová práva a rozsah činností, které může v jednotlivých modulech provádět.

3.6.5 CITRIX

Zabezpečená pošta Citrix – mobilní řešení pošty, poznámek a kontaktů. Lze jej využít na pracovních mobilních telefonech a tabletech. Tato aplikace vyžaduje speciální bezpečnostní certifikát.

3.7 Bezpečnostní opatření

3.7.1 Směrnice

Zde jsou uvedeny směrnice firmy, ve kterých je zmíněno zacházení s osobními daty.

Tab. 4 - Přehled směrnic *(vlastní zpracování)*

Popis dokumentu	**Obsah**
Směrnice IT	Způsob udělování práv
	Nakládání s osobními údaji
	Ukládání dokumentů
Směrnice HR	Popis zpracování osobních údajů
	Skartace
	Archivace

Pracovní řád společnosti	Zpracovávání osobních údajů
	Politika společnosti

3.7.2 Softwarová ochrana

Ochrana proti škodlivému software je zajištěna prostřednictvím antivirové ochrany a personálního Firewall. Toto zabezpečení nesmí být v žádném případě deaktivováno. Příslušný IT manažer (popř. smluvní partner) provádí min. jedenkrát za kalendářní rok programový audit všech pracovních stanic a přenosných počítačů. Na mobilní zařízení si provádí instalace uživatel sám. Používání pro soukromé účely je tolerováno, pokud nedojde k porušení firemních zájmů a nehrozí zneužití firemních dat.

Uživatel je povinen pracovat se svěřenými IT prostředky tak, aby minimalizoval riziko infekce počítačovým virem či jiným škodlivým kódem.

Zejména je nutné:

- Vyvarovat se stahování a spouštění software z neověřených zdrojů na internetu.
- Neotevírat přílohy elektronické pošty v nevyžádaných zprávách.
- Nespouštět aplikace uložené na externích mediích pocházejících z neověřených nebo nedůvěryhodných zdrojů.
- Zkontrolovat podezřelé soubory či aplikace antivirovým systémem.

Na všech firemních počítačích je instalován antivirový systém s centrální správou a pravidelnou automatickou aktualizací. Je zakázáno tento antivirový systém vyřazovat z činnosti nebo záměrně blokovat jeho pravidelnou aktualizaci. Antivirové systémy postupem času ztrácejí svou účinnost, neboť zohledňují pouze počítačové viry známé v době jejich vytvoření či v jejich poslední známé oficiální aktualizaci, a proto je nutné provádět jejich výše uvedenou pravidelnou aktualizaci.

Při jakémkoliv podezření na infekci počítače škodlivým kódem či nalezením konkrétního viru antivirovým systémem je nezbytné okamžitě informovat IT manažera nebo IT smluvního partnera.

3.7.3 Pravidla pro hesla

Základním bezpečnostním prvkem při používání jakéhokoliv IT systému je heslo. Pro správnou funkci musí heslo splňovat několik požadavků.

V případě podezření na prozrazení hesla je nutné ihned informovat IT manažera. Konkrétní IT systémy mohou klást specifické požadavky na tvorbu uživatelských hesel, jejich délku, složení a interval změny. Pokud je nutné v rámci údržby poskytnout heslo třetí osobě, musí se heslo na nezbytně nutnou dobu změnit. Nikdo se nesmí snažit jakýmkoliv způsobem získat přihlašovací údaje jiného uživatele nebo využívat jeho nepozornosti či neopatrnosti k používání jeho identity.

3.7.4 Hardware

Standardní HW definuje IT Manažer. Úpravy hardwaru a zásahy do konfigurace počítačů smí provádět pouze IT manažer (konzultant) nebo jím pověřená osoba.

Je zakázáno používání jakýchkoliv externích paměťových medií. USB porty jsou centrálně blokovány proti flash diskům a externím diskům (disketové jednotky, USB disky, externí pevné disky, externí vypalovací mechaniky, čtečky karet apod.). Používání těchto medií může být povoleno IT managerem nebo ředitelem společnosti v případě potřeby a doložením nutnosti pro pracovní činnost na základě písemné žádosti.

3.8 Mobilní systémy

3.8.1 Tablety a mobilní telefony

Tablety a mobilní telefony musí mít přístup výhradně prostřednictví centrální infrastruktury Mobile Device Management. Přístup a instalace musí být centrálně řízeny a monitorovány. E-maily uložené v tabletu musí být zakódovány a chráněny heslem (CITRIX). Přístup na lokální data nebo E-maily jen výjimečně a na základě důsledné autentifikace. V případě ztráty tabletu, nebo při odchodu zaměstnance musí mít IT Manažer (popř. smluvní partner) možnost okamžitě smazat („wipe“) data pomocí dálkového přístupu.

Při rozvázání pracovního poměru, je povinností zaměstnance odevzdat (na HR) mobilní zařízení (iPhone, iPad atd.) v továrním nastavení. Kontrola zařízení bude provedena IT pracovníkem (smluvním partnerem).

3.8.2 Home Office

Pro použití PC v případě Home Office platí pro zabezpečení dat a PC pravidla viz. softwarová ochrana. Na HO je zakázáno pracovat s účetními dokumenty a osobními daty zaměstnanců v papírové podobě.

3.8.3 VPN

Další využití je připojení k VPN například pro práci z domu. Přihlašování probíhá přes aplikaci Check Point. Opět vyžaduje bezpečnostní certifikát, který musí být umístěn v daném zařízení.

3.9 Požadavky investora

Investor – v tomto případě firma XY s.r.o., má požadavek na provedení analýzy zpracování osobních údajů a pomoc s implementací GDPR do chodu společnosti a nahrazení tak současného zákona 101/2000 Sb., o ochraně osobních údajů. Hlavní požadavek tedy je, aby firma byla schopna a připravena od prvního dne platnosti obecného nařízení, tj. 25.5.2018, plnit všechny náležitosti tohoto evropského nařízení.

3.10 Shrnutí analýzy

V analýze bylo zjištěno, že se pracuje s osobními údaji různých subjektů údajů. Osobní údaje jsou uloženy v několika interních informačních systémech, které pracují na serverech uvnitř firmy a na serverech v mateřské společnosti. Společnost se momentálně řídí podle současného platného zákona č.101/2000 Sb. o ochraně osobních údajů, a dle interních směrnic firmy. Dá se říci, že je velice dbáno na dodržování těchto pravidel a firma nemá žádné problémy s úniky dat, či pokusy o narušení serverů.

Byly nalezeny určité nedostatky, které je potřeba s přicházejícím nařízením GDPR řešit:

1) Uchazeč o zaměstnání není informován o zpracovávání jeho osobních údajů, jak je s nimi nakládáno a na jak dlouho

2) U zaměstnance není potřeba vyplňovat povinně a evidovat všechny údaje uvedeny v tabulce č. 1
    - Ověření nutnosti zpracovávání některých osobních údajů, např. údaje o rodinném stavu, dětech apod., které firma nemusí zpracovávat, když má externí účetní.
    - V pracovní smlouvě nejsou uvedeny potřeby užití konkrétních údajů.
    - Je potřeba rozšířit pracovní smlouvu o dodatek k GDPR.
    - Lékařské zprávy o způsobilosti k výkonu práce.
3) U zákazníků je potřeba ve smlouvě přesně uvést důvody zpracování os. údajů.
4) Zpracovávání cookies.
5) Přístupová práva jednotlivých pracovišť.
6) Ve firmě chybí dokument, který by definoval správné používání informačních systémů v souvislosti s výkonem své konkrétní pracovní činnosti.
7) Implementace GDPR.
8) Vytvoření politiky GDPR.

Návrhy řešení jsou uvedeny v další kapitole. Vytvoření politiky GDPR je uvedeno v příloze práce, jako příloha č. 2.

4 VLASTNÍ NÁVRHY ŘEŠENÍ

Společnost XY s.r.o. se řídí současným zákonem o ochraně osobních údajů (101/2000 Sb., o ochraně osobních údajů). Tento fakt je už poměrně dobrou zprávou z hlediska implementace GDPR, protože není potřeba velkých změn úplně od základu a implementace bude tedy jednodušší.

4.1 Přípravy na implementaci

Jako první při zavádění GDPR bych doporučil určit člověka nebo tým lidí, kteří budou mít na starost celý proces zavádění obecného nařízení do chodu firmy. Tento tým, by měl provést celkovou analýzu (audit) zacházení s osobními údaji ve firmě, tzn. jaké údaje jsou zpracovávány, kam jsou ukládány, na jak dlouho, archivace, skartace, k jakým účelům jsou používány a jestli je nutné všechny tyto údaje zpracovávat. Projít tyto kroky s vedoucími jednotlivých oddělení a na základě toho vytvořit rozdílovou analýzu.

Z výsledku tohoto auditu by nám mělo vyplynout, zda dělat posouzení vlivu na ochranu osobních údajů (DPIA). V našem případě toto posouzení je nutné provést, protože splňuje alespoň jeden bod z možných situací (viz 2.11.4 Posouzení vlivu).

4.2. Implementace

Při samotné implementaci by mělo dojít k úpravě externí dokumentace. Což jsou například Všeobecné obchodní podmínky (VOP) a zpracovatelské smlouvy. Mělo by zde být uvedeno nahrazení dosavadní právní úpravy a důvody zpracování osobních údajů. Dále by měl být vytvořen dokument popisující zásady, právní důvody a doby zpracování osobních údajů ve firmě.

4.2.1 Souhlas se zpracováním osobních údajů

Souhlas se zpracováním osobních údajů by měl mít hlavně dvě důležité vlastnosti, a to, aby byl svobodný a jednoznačný projev vůle, kterým dává subjekt svolení ke zpracováním svých osobních údajů.

Souhlas musí být samostatný, tedy odlišen od jiných skutečností, ke kterým se subjekt údajů vyjadřuje. Př. nesmí být součástí smlouvy nebo obchodních podmínek.

Příklad návrhu formy souhlasu:

Souhlas se zpracováním osobních údajů:

1. Udělujete tímto souhlas společnosti XY s.r.o., se sídlem ……., IČ ……., zapsané v obchodním rejstříku vedeném u ……. soudu v ……., oddíl ……., vložka ……. (dále jen „Správce“), aby ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (dále jen „GDPR“) zpracovávala tyto osobní údaje:

- Název a sídlo společnosti
- Jméno a příjmení zaměstnance
- Email
- Telefonní číslo
- Pracovní pozice

2. Tyto osobní údaje je nutné zpracovávat za účelem tvorby obchodních vztahů*. Tyto údaje budou správcem zpracovávány po dobu nezbytně nutnou k zajištění práv a povinností plynoucích jak ze závazkového vztahu, tak i z příslušných právních předpisů.

3. S výše uvedeným zpracováním udělujete svůj výslovný souhlas. Tento souhlas lze vzít kdykoliv zpět, a to například prostřednictvím emailu na adresu info@xy.cz s předmětem „Zrušení souhlasu se zpracováním osobních údajů“.

4. Zpracování osobních údajů je prováděno Správcem

Jméno společnosti/osoby, která uděluje tento souhlas

_____ _____

(Podpis obou stran)

_____

Pozn. * účel zpracování může být různý

4.2.2 Interní dokumentace

Zde by měly být vytvořeny a aktualizovány nové interní směrnice a nařízení. Doporučil bych vytvoření nové směrnice GDPR, kde by byly popsány základní znaky a postupy při práci s osobními údaji a dále rozšířené pro každý pracovní úsek firmy, kde by byly konkrétní postupy a místa uložení pro zpracovávání osobních údajů.

4.2.3 Pověřenec DPO

Dle požadavků GDPR by měl být jmenován pověřenec pro ochranu osobních údajů. Pro tuto společnost bych doporučil svěřit funkci již aktuálnímu zaměstnanci, který by měl mít povědomí o právní ochraně dat a zároveň neměl možnost stanovovat pravidla ukládání osobních údajů, aby nedocházelo ke konfliktu zájmů. Další možností je oslovení externího experta, který by v pravidelných intervalech prováděl funkci DPO.

4.3 Procesy zpracování osobních údajů

V tomto bodu by se měly upravit konkrétní procesy zpracování osobních údajů jednotlivých subjektů údajů.

4.3.1 Uchazeč o zaměstnání

Uchazeč o zaměstnání není dostatečně informován o zpracování jeho osobních údajů. Když tedy pošle svůj životopis emailem, měl by zpět obdržet nejen poděkování a oznámení o zařazení do výběrového řízení, ale například informaci o době uložení ve firmě. V případě nevybrání uchazeče do požadované pracovní pozice, mu bude oznámen výsledek a informace o likvidaci jeho životopisu nebo poskytnutí souhlasu o uchování pro další výběrové řízení na obdobnou pozici.

4.3.2 Zaměstnanec

Dle současného stavu je nový zaměstnanec povinen uvádět osobní údaje viz Tab.1.

Tuto tabulku bych upravil následovně:

Tab. 5 - upravené zpracování osobních údajů zaměstnanců *(vlastní zpracování)*

Povinné	Nepovinné
Příjmení, jméno	Zdravotní stav
Rodné příjmení	Další vzdělání a odborné kurzy
Datum narození	Kontakt pro případ nutnosti
Rodné číslo	Titul
Místo narození	
Státní příslušnost	
Číslo bankovního účtu	
Zdravotní pojišťovna	
Telefon	
Email	
Nejvyšší dosažené vzdělání	
Adresa bydliště	
Kontaktní adresa	
Rodinný stav	
Rodinní příslušníci	
Fotografie	
Číslo OP	
Předchozí zaměstnavatel	

Tab. 6 - vysvětlivky k předchozí tabulce (Tab. 4) *(vlastní zpracování)*

	Nutné pro vytvoření smlouvy	Zde se důvody prolínají
	Nutné pro účetní a daňové procesy	
	Interní firemní účely	

Zdravotní stav není nutné zpracovávat i kdyby tato informace měla vliv na vykonávání pracovní pozice. Tyto informace má k dispozici jen zaměstnanec a jeho lékař, pokud je nutné provést zdravotní prohlídku, ve zprávě pro zaměstnavatele by mělo být uvedeno jen „Je/Není způsobilý k vykonávání pracovní pozice…“. Ostatní konkrétní zdravotní údaje by měly zůstat u lékaře.

Další vzdělání a odborné kurzy není nutné taktéž zaznamenávat, pokud je to uvedeno v životopisu a ověřeno během výběrového řízení, na základě, kterého byl zaměstnanec vybrán.

Kontakt pro případ nutnosti není třeba uvádět, záleží na domluvě obou stran.

Číslo občanského průkazu a fotografie jsou poskytovány až se souhlasem o jejich zpracování a uvedení důvodů k čemu jsou potřeba.

Úprava pracovní smlouvy. V pracovní smlouvě není uvedeno, k jakým účelům jsou konkrétní osobní údaje zpracovávány. Proto by mělo dojít k aktualizaci smluv, popřípadě vytvoření dodatku GDPR, kde budou uvedeny důvody a způsoby zpracování jednotlivých údajů spolu se souhlasem zaměstnance k poskytnutí fotografie a čísla OP.

Přístupová práva jednotlivých pracovišť

Mělo by být jasně dáno a evidováno, kdo konkrétně zpracovává osobní údaje a kam je ukládá. Omezit jen na ty osoby, u kterých to vyžaduje pracovní náplň.

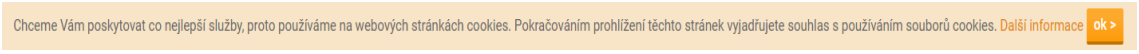
4.3.3 Zákazníci

Pro plnění smluvních podmínek je nutné zpracovávat osobní údaje zákazníků. Není možné specifikovat obecně o jaké údaje se konkrétně jedná, ale jsou to údaje, podle kterých je možno zákazníka identifikovat a např. zaslat toto zboží na požadované místo. Opět je nutné zákazníka uvědomit o tom, k čemu jsou údaje využívány. Není nutné

vyžadovat udělení souhlasu ke zpracování osobních údajů, pokud je zpracování nezbytné pro plnění smlouvy.

4.3.4 Zákazníci webu

Zde vyřešíme problematiku cookies. Z analýzy je evidentní, že web obsahuje dva druhy cookies, tzv. session-cookies a permanentní cookies. O používání cookies je uživatel seznámen a upozorněn hned při vstupu na web (upozorňovací lišta). Zabránit užívání cookies může uživatel sám v nastavení svého prohlížeče. Na rozdíl od ostatních cookies nemusí session-cookies navíc získávat předchozí souhlas návštěvníka.



Obr. 5 - upozorňovací lišta na webu *(web společnosti XY s.r.o.)*

K souladu ke GDPR by mělo být při vstupu na web uvedeno k čemu konkrétně je sběr cookies potřeba. Optimálně by měl web být připraven na možnost, kdy uživatel webu odmítne zpracování, a přesto chce využít služeb webu (zatím možné jen teoreticky). Tuto problematiku už řeší spíše nařízení ePrivacy.

4.4 Plán pro případ porušení zabezpečení osobních údajů

Měl by být vytvořen plán pro případ porušení zabezpečení osobních údajů. To znamená udělat postupy pro tyto varianty porušení. Jakékoliv porušení musí být nahlášeno bez zbytečného odkladu dozorovému úřadu – Úřad pro ochranu osobních údajů ve lhůtě 72 hodin po porušení.

Postupy by se měly obsahovat několik bodů:

- Předcházení incidentům
- Odhalení a vyhodnocení konfliktu
- Řešení incidentu
- Minimalizace následků
- Ohlášení na příslušná místa (dle závažnosti)

4.5 Poučení zaměstnanců

Pro správný a efektivní příchod GDPR je potřeba provést zaškolením všechny své zaměstnance, kteří se dostanou do styku s osobními údaji.

Dále by měla být vytvořena metodika se správným zacházením v informačním systému a ukládání jen těch údajů, které jsou potřeba.

4.6 Politika GDPR

Zde je uveden návrh dokumentu politiky GDPR ve společnosti.

Politika GDPR ve společnosti XY s.r.o.

Společnost XY s.r.o. zpracovává různé druhy osobních údajů svých zaměstnanců nebo obchodních partnerů a přistupuje k ochraně osobních údajů velice vážně a dodržuje příslušné právní předpisy. Od 25.května 2018 bude pro společnost platit **Nařízení EU č.2016/679 ze dne 27.4. 2016 - Obecné nařízení o ochraně osobních údajů (GDPR – General Data Protection Regulation).**

Osobní údaje, které jsou zde zpracovávány nejsou prodávány a není s nimi nakládáno ani jinak v rozporu s právními předpisy.

Následující informace poskytují přehled o tom jak společnosti XY s.r.o. přistupuje k ochraně osobních údajů svých zaměstnanců a obchodních partnerů. Cílem je poskytnout zaměstnancům a obchodním partnerům bezpečnost jejich osobních údajů a znemožnit tak jejich zneužití. Proto společnost přistupuje k GDPR nejen z povinnosti vůči evropskému parlamentu, ale hlavně z povinnosti vůči svých obchodních partnerů a zaměstnanců.

Aby společnost byla schopna plnit výše uvedené řádky, je potřeba plnit následující opatření:

1) **Systém managementu bezpečnosti osobních údajů**. Je třeba vést GDPR jako ucelený řád s odpovídající řídicí dokumentací, jako například směrnice, návody a školení.
2) **Zaměstnanci.** O zaměstnancích jsou vedeny jen záznamy nutné pro výkon personální a mzdové agendy. Zaměstnanci mají přehled o tom, jaká data jsou o nich zpracovávána a k potřebným údajům jsou uděleny souhlasy.
3) **Obchodní partneři.** O obchodních partnerech jsou vedeny záznamy nutné pro určitou činnost zpracování. Tyto údaje jsou nutné například pro plnění smluvních podmínek, zaslání objednaného zboží na správnou adresu, komunikaci a poradenskou činnost.

4) **Souhlas.** Použití osobních údajů zákazníků k marketingovým nebo jiným účelům je možno pouze, pokud je tato skutečnost odsouhlasena samotným subjektem údajů.
5) **Odvolání souhlasu.** Zákazník může kdykoli odvolat svůj souhlas se zpracováním svých osobních údajů nebo uplatnit své právo na přístup k údajům, které o něm jsou zpracovávány, právo na opravu těchto údajů jsou-li nepřesné, a právo na vysvětlení domnívá-li se, že správce nebo zpracovatel provádí zpracování jeho osobních údajů v rozporu s ochranou jeho soukromého a osobního života.
6) **Výmaz osobních údajů.** Pokud zákazník odvolá svůj souhlas se zpracováním osobních údajů, nebo pokud zpracování osobních údajů zákazníka již není dále potřeba k účelu, pro který byly údaje poskytnuty, jsou údaje vymazány.
7) **Zákazníci na webu.** Zákazníci jsou při vstupu na náš web informováni o ukládání cookies. Cookies jsou využívány dvojího typu, tzv. dočasné a permanentní. Cookies jsou ukládány na pevný disk prohlížejícího. Cookies společnost XY s.r.o. tedy nezpracovává. Upozorňovací okno na webu dává mimo jiné i informaci k čemu jsou cookies využívána.
8) **Bezpečnost osobních údajů.** Ve společnosti jsou prováděna veškerá technická a organizační opatření potřebná pro zajištění osobních údajů před ztrátou či zneužitím. Důvěrné informace, jako jsou osobní údaje, jsou kódovány prostřednictvím SSL a přenášeny protokolem HTTPS.

Důvěra je pro společnost XY s.r.o. velice důležitá. Proto je připravena kdykoli zodpovědět dotazy týkající se zpracování osobních údajů.

_____

Podpis odpovědného pracovníka

4.7 Ekonomické zhodnocení

V této části bude popsáno ekonomické zhodnocení implementace. Částky jsou pouze odhadované.

Tab. 7 - ekonomické zhodnocení – odhad *(vlastní zpracování)*

Popis	Částka
Školení odpovědných zaměstnanců	5 000 Kč
Audit interních procesů	35 000 Kč
Audit webových stránek	5 000 Kč
Právní audit	55 000 Kč
Školení zaměstnanců	10 000 Kč
Celkem:	**110 000 Kč**

ZÁVĚR

V této bakalářské práci bylo cílem provést analýzu zpracování osobních údajů ve firmě, na základě, které bylo potřeba navrhnout potřebné kroky k implementaci nařízení GDPR. V teoretické části byly popsány a vysvětleny důležité pojmy a úkony pro potřeby analýzy a návrhu. Samotná analýza současného stavu ve firmě už obsahuje popis subjektů údajů a jejich osobní údaje které jsou zpracovávány, důvody a právní tituly, kdo s nimi pracuje, kam jsou uloženy a na jak dlouho. Další částí analýzy byly uvedeny požadavky investora a v poslední části shrnutí a vytyčení problémů k řešení. Tyto problémy jsou postupně řešeny v části vlastních návrhů řešení, kde je i doporučený postup k implementaci GDPR do chodu firmy. Cíle práce, které byly na začátku stanoveny, jsou tedy úspěšně splněny, podařilo se mi nalézt i slabá místa při zpracovávání osobních údajů a podat návrhy na jejich zlepšení. Obsahem návrhu je i politika GDPR pro společnost, která je důležitá při implementaci a uvědomění si této problematiky. Při psaní práce jsem využíval nejrůznější dostupné materiály z webu, například Úřadu pro ochranu osobních údajů, prezentací poskytnutých při školení v samotné společnosti XY s.r.o. a knižních publikací zabývajících se ochranou dat nebo přímo obecným nařízením.

Při tvorbě této práce jsem byl seznámen s problematikou bezpečnosti ochrany dat nejen v korporátní sféře a získal tak mnoho poznatků v oblasti ochrany osobních údajů a nového nařízení GDPR.

SEZNAM POUŽITÝCH ZDROJŮ

[1] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: Nakladatelství ANAG, 2017. ISBN 978-80-7554-097-3.

[2] OPLETALOVÁ, Vendula. *OCHRANA OSOBNÍCH ÚDAJŮ V INFORMAČNÍM SYSTÉMU*. Brno, 2007. Bakalářská práce. Vysoké učení technické v Brně – Fakulta podnikatelská. Vedoucí práce JUDr. Tomáš Soukup.

[3] Proč chránit osobní údaje. *Ochrana osobních údajů* [online]. [cit. 2017-10-30] Dostupné z: http://www.oou.cz/zacinamesochranou/procchranitosobniudaje.

[4] MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 978-80-7357-322-5.

[5] KOŘÍNKOVÁ, Markéta. Ochrana osobních údajů se týká i módních návrhářů. *Právní prostor* [online]. [cit. 2017-10-26]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/ochrana-osobnich-udaju-se-tyka-i-modnich-navrharu.

[6] ÚOOÚ. Prohlášení Cookies: Úřad pro ochranu osobních údajů [online]. [cit. 2018-03-30]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=3099&n=prohlaseni-cookies

[7] ÚOOÚ. Zvláštní kategorie osobních údajů (citlivé údaje): Úřad pro ochranu osobních údajů [online]. 5.3.2018 [cit. 2018-03-30]. Dostupné z: https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaj-citlive-udaje/d-27274

[8] HelpGDPR. Subjekt údajů – Help GDPR.cz [online]. 05.09.2017 [cit. 2018-03-30]. Dostupné z: https://www.helpgdpr.cz/rstsp/clanky.nsf/i/subjekt_udaju_17080521_24045167

[9] GDPR.cz. Zpracování osobních údajů | GDPR.cz [online]. [cit. 2018-03-30]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/zpracovani-osobnich-udaju/

[10] Správce, zpracovatel: Základní příručka: Úřad pro ochranu osobních údajů [online]. 5.3.2018 [cit. 2018-03-30]. Dostupné z: https://www.uoou.cz/7-spravce-zpracovatel/d-27278/p1=4744

[11] Zaměstnavatel jako správce osobních údajů: Úřad pro ochranu osobních údajů [online]. 13.12.2013 [cit. 2018-03-30]. Dostupné z: https://www.uoou.cz/zamestnavatel-jako-spravce-osobnich-udaju/d-6171

[12] MATOUŠOVÁ, Miroslava. *Ochrana osobních údajů v otázkách a odpovědích*. Praha: ASPI, 2004. Otázky & odpovědi z praxe. ISBN 80-7357-037-8.

[13] Úřad: Úřad pro ochrnu osobních údajů [online]. ÚOOÚ [cit. 2018-03-30]. Dostupné z: https://www.uoou.cz/urad/ds-1059/cookiesAllowed=1

[14] GDPR | Platforma kybernetické bezpečnosti [online]. [cit. 2018-03-30]. Dostupné z: https://www.kybez.cz/bezpecnost/gdpr

[15] PravoIT. GDPR - 3. díl: Vedení záznamů o činnostech zpracování osobních údajů [online]. IT Systems č. 10/2017: CCB, 2017 [cit. 2018-03-30]. Dostupné z: http://www.pravoit.cz/novinka/gdpr-3-dil-vedeni-zaznamu-o-cinnostech-zpracovani-osobnich-udaju

[16] PLACHÁ, Lucie. Hospodářská komora ČR. Kdy musíte provést posouzení vlivu na ochranu osobních údajů? [online]. 2017 [cit. 2018-03-30]. Dostupné z: http://www.gdpr-ochrana-osobnich-udaju.cz/kdy-musite-provest-posouzeni-vlivu-na-ochranu-osobnich-udaju/

[17] KYSELA, František. SystemOnline. Zálohování a archivace jako součást bezpečnosti IT [online]. [cit. 2018-03-30]. Dostupné z: https://www.systemonline.cz/it-security/zalohovani-a-archivace-jako-soucast-bezpecnosti-it.htm

[18] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[19] František KYSELA, Dimension Data. Zálohování a archivace dat není totéž: Poznejte rozdíly [online]. 21. 10. 2013 [cit. 2018-03-30]. Dostupné z: http://onbusiness.cz/zalohovani-a-archivace-dat-neni-totez-poznejte-rozdily-134

[20] Ochrana osobních údajů se týká všech zaměstnavatelů - Podnikatel.cz. Podnikatel.cz - průvodce vaším podnikáním [online]. Copyright © 2007 [cit. 26.11.2017]. Dostupné z: https://www.podnikatel.cz/clanky/ochrana-osobnich-udaju-se-tyka-vsech-zamestnavatelu/.

[21] BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v životě podnikatele: 103 řešení modelových situací. Olomouc: ANAG, c2013. Právo (ANAG). ISBN 978-80-7263-811-6.

[22] DOSEDĚL, Tomáš. 21 základních pravidel počítačové bezpečnosti. Brno: CP Books, 2005. ISBN 80-2510-574-1.

[23] MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012. ISBN 978-80-87576-12-0.

[24] KNAP, Karel. Ochrana osobnosti podle občanského práva. 4. dopl. vyd. Praha: Linde, 2004. ISBN 80-7201-484-6.

[25] EU Datenschutz-Grundverordnung [online]. SecureDataService, 2017 [cit. 2018-04-28]. Dostupné z: http://www.privacy-regulation.eu/cs/index.htm

[26] GDPR směrnice a nařízení - Neofema s.r.o. [online]. [cit. 2018-05-07]. Dostupné z: http://blog.neofema.cz/novinky/gdpr-smernice-a-narizeni/

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

HO – Home Office

B2B – Business to business

DPIA – Data Protection Impact Assessment

GDPR – General Data Protection Regulation

DPO – Data Protection Officer

HR – Human Resources

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha č.1

Registrační formulář na webu (údaje o firmě jsou začerněny)

[redacted]

K rukám statutárního zástupce společnosti

Autorizace kontaktní osoby oprávněné k elektronickému obchodování se společností [redacted] s.r.o.

Elektronické obchodování společnosti [redacted] s.r.o. slouží k obchodování na úrovni B2B. Abychom Vám mohli zajistit bezpečný nákup a zabránit možnému zneužití nákupu našich materiálů neoprávněnou osobou jménem Vaší společnosti, žádáme Vás tímto o uvedení souhlasu s registrací kontaktní osoby. Tato osoba bude mít oprávnění nakupovat elektronicky jménem Vaší společnosti.

Níže můžete vybrat oprávnění, která bude mít daná osoba nastavena za Vaši firmu. Administrátor může pomocí Správy uživatelů nastavovat a měnit míru oprávnění za další osoby Vaší společnost a zároveň měnit jejich osobní údaje (jméno, telefon, e-mail apod.).

Společnost:

Název .....

IČO ..... Nejsme plátci DPH ☐

Adresa .....

Oprávněná osoba:

Jméno a příjmení .....

Funkce .....

Telefon .....

E-mail .....

Míra oprávnění (zaškrtněte požadované):

Administrátor ☐ Zadávání nových objednávek ☐

Sledování všech objednávek ☐ Zobrazení nákupních cen ☐

Výchozí měna (vyberte, kterou měnu si přejete nastavit jako výchozí):

CZK ☐ EUR ☐

Potvrzení statutárního zástupce společnosti:

Jméno statutárního zástupce .....

Podpis .....

Datum .....

V případě jakýchkoliv dotazů se prosím obracejte na zákaznické centrum:

[redacted]