ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Bakalářská práce

Projekt implementace GDPR ve vybrané společnosti

GDPR implementation project in selected company

Barbora Pokorná

Plzeň 2024

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma

„Projekt implementace GDPR ve vybrané společnosti“

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

Plzeň dne 22. 4. 2024 v. r. *Barbora Pokorná*

Zásady pro vypracování práce

1. Představte problematiku GDPR v kontextu řízení podniků.
2. Představte vybraný podnik.
3. Popište průběh implementace GDPR ve vybraném podniku.
4. Zhodnoťte implementaci GDPR ve vybraném podniku a případně navrhněte zlepšení v oblasti ochrany osobních údajů.

Studijní program

Projektové řízení

Poděkování

Tímto bych ráda poděkovala vedoucímu mé bakalářské práce Ing. Adamu Faifrovi, Ph.D., za odborné připomínky a cenné rady při vedení mé práce. Také bych chtěla poděkovat Soně Pelcové a Janě Žižkové z firmy Langmatz CZ s.r.o. za poskytnuté informace, ochotu a příjemnou spolupráci.

Obsah

Úvod

V dnešní době je zpracováváno obrovské množství dat, která mají čím dál tím větší hodnotu, a proto je velmi důležitá jejich ochrana. Základním cílem ochrany osobních údajů je zajistit, že jednotlivci mají kontrolu nad tím, jak jsou jejich osobní údaje shromažďovány, zpracovávány a využívány (Evropský parlament a Rada EU, n. d.).

Význam ochrany osobních údajů za poslední dobu enormně vzrostl s ohledem na rozvoj technologií a digitalizaci (PrivacySense, 2023). Evropská unie reagovala na tento rozvoj přijetím Obecného nařízení o ochraně osobních údajů (GDPR), které vstoupilo v platnost 25. května 2018. Toto nařízení vneslo komplexní rámec ochrany osobních údajů pro společnosti, které musí dodržovat přísná pravidla týkající se sběru, zpracování a uchovávání osobních údajů. Každá firma musela prostřednictvím projektu přizpůsobit interní postupy a systémy novým požadavkům, které z nařízení vyplývají (Mohanakrishnan, 2023).

Cílem této bakalářské práce je analyzovat projekt implementace GDPR ve firmě Langmatz CZ s.r.o., zhodnotit úspěšnost tohoto projektu a případně navrhnout možná zlepšení.

V teoretické části budou nejdříve vysvětleny základní pojmy, které se týkají řízení projektů, jako je cíl a účel projektu, projektový trojimperativ, rozsah projektu nebo zainteresované strany. Dále budou v teoretické části vysvětleny základní pojmy, které se týkají problematiky ochrany osobních údajů a důležité skutečnosti, které GDPR přináší, jako například zásady pro zpracování osobních údajů nebo práva subjektů údajů. Poslední téma, které bude v teoretické části popsáno, je, jak by projekt implementace tohoto nařízení mohl vypadat – od analýzy současného stavu po školení zaměstnanců.

V praktické části bude nejdříve představena společnost Langmatz CZ s.r.o. a její činnost. Následně bude popsán projekt včetně jeho základních parametrů a předprojektová fáze. V této fázi byla provedena analýza současných procesů ve firmě a na základě výsledků analýzy byl sestaven seznam nezbytných opatření, která byla nutná pro dosažení souladu s GDPR. Následně budou tato opatření detailně popsána. Jednalo se zejména o úpravu postupů při práci s osobními údaji, úpravu a tvorbu dokumentů a zabezpečení dokumentů obsahujících osobní údaje. Na závěr bude projekt implementace GDPR ve firmě zhodnocen a budou navrhnuta možná zlepšení.

1 Projekt

Podle International Project Management Association (IPMA) je **projektem** jedinečný proces, který je omezen časově, nákladově a zdrojově. Je realizován za účelem vytvoření předem specifikovaných výstupů v požadované kvalitě, při dodržení uznávaných standardů a odsouhlasených požadavků. Tato definice je jednou z mnoha definic, které se mohou v konkrétní formulaci lišit. Právě kvůli různým a také vcelku širokým definicím může být pro mnoho podniků nejasné, kdy řídit nějaký soubor činností jako projekt. Projekt lze chápat jako nástroj změny v dynamickém prostředí, zatímco obvyklé činnosti managementu často slouží pro optimalizaci a zvýšení efektivity v obvykle statickém prostředí (Doležal a kol., 2016).

S projektem úzce souvisí **projektové řízení** - soubor norem, doporučení a pracovních zkušeností, které detailně popisují, jak efektivně řídit projekt. Projektové řízení je oborem vcelku novým, pořádně se o něm začalo mluvit až po 2. světové válce. Není to však tím, že by v dřívější době neprobíhaly akce projektového charakteru. Dříve byla doba pomalejší a právě omezení projektů, jak časově, tak zdrojově, pomohlo k rozvoji oboru projektového řízení (Doležal a kol., 2016).

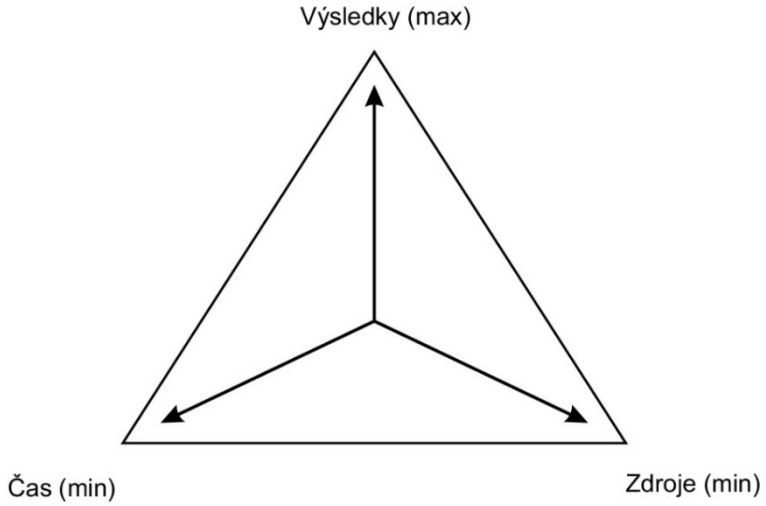
1.1 Cíl, účel a trojimperativ projektu

Cílem projektu je určitý unikátní výsledek - produkt, služba nebo jejich kombinace, která tak naplní požadavky zadavatele projektu. K tomuto výsledku se vztahuje jeho unikátnost (Svozilová, 2016). Každý projekt je unikátní z toho důvodu, že se nejedná o opakovatelný proces (Doležal a kol., 2016). Velmi podobný projekt u jiného zákazníka přináší jiné okolnosti – například jiný termín, rozpočet, lokalitu a personální obsazení. Výsledkem projektu může být zavedení změny už existujícího procesu nebo implementace nové technologie. Cíl musí být v každém případě SMART - konkrétní, měřitelný, dosažitelný, podstatný a časově ohraničený (Svozilová, 2016). **Účel projektu** je důvod, proč je projekt realizován. Bývá dlouhodobějšího charakteru, často může být abstraktní a pro jeho dosažení bývá potřeba kombinace několika projektů (Vacek & kol., 2017).

S projektem souvisí tři základní pojmy, které jsou navzájem provázány – rozsah, čas a zdroje (náklady). Tyto tři pojmy tvoří **trojimperativ** projektového řízení, neboli základní omezení projektu. V praxi to může znamenat například to, že pokud se

změní jedna z veličin a druhá zůstane nezměněna, třetí se určitým způsobem také změní – například, pokud má být něco provedeno rychleji, bude to na úkor nákladů nebo rozsahu (Doležal a kol., 2016).

Obr. 1 Trojimperativ projektu



Zdroj: Doležal (2016)

Pokročilejší úvaha přidává k těmto třem základním pojmům ještě čtvrtý pojem, kterým je kvalita výstupů (Doležal a kol., 2016).

1.2 Rozsah projektu, časový harmonogram a zainteresované strany

Při plánování projektu se nejdříve definuje jeho **rozsah**, který vyjadřuje, co všechno bude prostřednictvím projektu vyprodukováno - produkty, služby nebo jiné výsledky (Doležal & Krátký, 2017).

V rámci plánu projektu je velmi důležitý **časový harmonogram**. V něm jsou zaznamenány veškeré informace o termínech a časových sledech prací na projektu a jednotlivým segmentům časového harmonogramu jsou přiřazeny zdroje pro jejich realizaci. Mezi klíčové prvky časového harmonogramu projektu patří milníky a významné termíny, logické hierarchické struktury činností, které jsou převedeny do časových posloupností úkolů, informace o předpokládané délce trvání jednotlivých činností, vazby a souslednosti činností, které slouží k zachování logiky činností i při časových změnách a další údaje, které přispívají k údržbě harmonogramu. Časový harmonogram lze prezentovat za pomocí diagramů. Mezi tyto diagramy patří například metoda kritické cesty, metoda hodnocení a kontroly projektu a také Ganttovy diagramy,

které jsou dnes velmi často využívány hlavně díky jejich jednoduchosti a možnosti vytvoření i bez specializovaných softwarů (Svozilová, 2016).

„**Zainteresovanou stranou** v projektu je osoba/organizace, která je aktivně zapojená do projektu nebo jejíž zájmy mohou být pozitivně/negativně ovlivněny realizací projektu či jeho výsledkem. Často také může ovlivnit průběh projektu nebo jeho výsledky.“ (Doležal a kol., 2016, s. 65). Zainteresovaná strana může být jak jednotlivec, tak i skupina (organizace), kterou však většinou reprezentuje konkrétní osoba. Podle role, kterou zastávají, rozlišujeme tyto zainteresované strany projektu:

- zadavatel,
- zákazník,
- vlastník,
- realizátor,
- sponzor,
- dotčené strany (Doležal a kol., 2016).

Běžně dochází k splývání některých rolí do jedné – například u zadavatele a vlastníka projektu. Mezi dotčené strany lze řadit zájmy lidí, jež nepatří do žádné z výše uvedených skupin, ale jsou přímo nebo nepřímo projektem ovlivněni (Doležal a kol., 2016). V případě GDPR je dotčenou stranou například subjekt údajů.

Zainteresované strany jsou řízeny na základě čtyř kroků, jimiž jsou identifikace, analýza reálných očekávání, analýza vlivu a zájmu a v neposlední řadě vytvoření strategie pro jednání s jednotlivými zainteresovanými stranami (Doležal a kol., 2016).

Projektový manažer je odpovědný za dosažení projektového cíle projektu a dodržování předem stanovených pravidel. Má za úkol koordinovat projektový tým tak, aby došlo k vytvoření plánu projektu a úspěšné realizaci projektu. Dále také řídí změny, rizika, má za úkol podávat informace o průběhu projektu sponzorovi a také řeší problémy spojené s projektem (Doležal & Krátký, 2017).

1.3 Řízení rizik projektu

Každý projekt nese určitou úroveň rizika. Rizika lze chápat jako jevy nebo okolnosti, které však nejsou přímo ovlivnitelné projektem. Riziko může nastat s určitou pravděpodobností, která leží v intervalu od 0 do 1 a jeho působení pak může zapříčinit odchýlení projektu od jeho plánované trajektorie a oddálit ho mimo plánované náklady, harmonogram a produkt projektu (Svozilová, 2016). Řízení rizik je soubor aktivit, nimiž jsou dle PM BOK od Project Management Institute (PMI):

- plán řízení rizik,
- identifikace rizik,
- analýza rizik – kvalitativní a kvantitativní,
- plán odpovědi na rizika,
- sledování rizik (Doležal a kol., 2016).

Při plánování řízení rizik projektu je důležité správně identifikovat cíle a vnější a vnitřní kritéria, jako například v jakém prostředí bude projekt probíhat nebo v kterém ročním období. V rámci uvedení projektu do kontextu lze určit, která metoda pro identifikaci a analýzu rizik bude použita, jak se bude postupovat při její aplikaci a kdo za to bude zodpovědný. Výsledkem je plán řízení rizik (risk management plan), který by měl obsahovat informace o vybraných metodách a nástrojích, které budou v projektu použity, o rolích a zodpovědnostech, nákladech, časovém průběhu, kategoriích rizik a vymezeních úrovní pravděpodobností a dopadů, tedy co bude v projektu považováno za malou, střední a velkou pravděpodobnost (Doležal a kol., 2016).

Dalším krokem v úspěšném řízení rizik je identifikace potenciálních rizik spojených s projektem. To zahrnuje systematický průzkum a dokumentaci všech možných rizik. Do procesu identifikace rizik by měli být zapojeny všechny osoby, které se v budoucnosti budou podílet na tvorbě a implementaci opatření proti rizikům (Vacek & kol., 2017). Identifikace rizik je klíčová pro prevenci problémů a proaktivní přístup k jejich řešení (Doležal a kol., 2016).

Po identifikaci následuje analýza rizik, která přináší hlubší porozumění jejich významu a dopadu na projekt. Rizika lze kategorizovat podle pravděpodobnosti a dopadu, čímž vzniká hierarchie, která umožňuje identifikovat klíčová rizika, na která je třeba se zaměřit. Rizika lze analyzovat kvalitativně – nejsou používána konkrétní čísla pro vyčíslení rizika, ale slovní vyjádření, nebo kvantitativně – velikost dopadu

a pravděpodobnost nastání rizika jsou vyjádřeny konkrétními čísly. Často se však používá analýza semikvantitativní, která je kombinací kvalitativní a kvantitativní analýzy (Vacek & kol., 2017).

Plánování odpovědi na rizika zahrnuje implementaci strategií pro minimalizaci negativního dopadu a maximalizaci příležitostí. To může zahrnovat prevenci rizik, přijetí určitých rizik, jejich přesunutí nebo úplné omezování. Klíčovým aspektem je vytvoření plánu řízení rizik, který obsahuje opatření pro každé identifikované riziko. Sledování rizik umožňuje pružné reakce na změny a poskytuje týmu aktuální informace o stavu identifikovaných rizik (Doležal a kol., 2016).

2 Problematika GDPR

Tato kapitola má za cíl nastínit, jak se právně vyvíjela ochrana osob a osobních údajů v minulosti a vysvětlit důležité pojmy a samotné fungování nejaktuálnějšího právního dokumentu, který ochranu osobních údajů upravuje.

2.1 Vývoj

Prvním klíčovým mezinárodním dokumentem v oblasti lidských práv, který upravoval právo na soukromí, byla Všeobecná deklarace lidských práv, která byla přijata v roce 1948 v San Francisku. Ta v článku 12 vymezila zákaz vystavit kohokoliv svévolnému zásahu do soukromí a korespondence. Dalším významným dokumentem byla Evropská úmluva o ochraně lidských práv a základních svobod, která byla sjednána v Římě v roce 1950 a zaručovala, podobně jako Všeobecná deklarace lidských práv, právo na respektování osobního života. Oba dokumenty byly důležité z důvodu ochrany soukromí osob, nevěnovaly se však podrobněji ochraně osobních údajů při jejich zpracování. Ochrana osobních údajů byla z důvodu nepotřeby zvláštního členění zahrnuta v právu na ochranu soukromí (Žůrek, 2018).

Postupem času však díky rozvoji společnosti a vývoji v oblasti technologií, konkrétně informačních technologií, které zpracovávaly osobní údaje, vzešla v platnost dne 28. ledna 1981 Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (č. 115/2001 Sb. m. s.). Od tohoto dne se právo na ochranu osobních údajů při jejich zpracovávání vymezilo jako zvláštní část práva (Žůrek, 2018).

Dalším důležitým stupněm v ochraně osobních údajů byla Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Evropský parlament a Rada EU, 1995). Tato směrnice platila až do května 2018, kdy ji nahradilo nařízení o GDPR (Navrátil a kol., 2018).

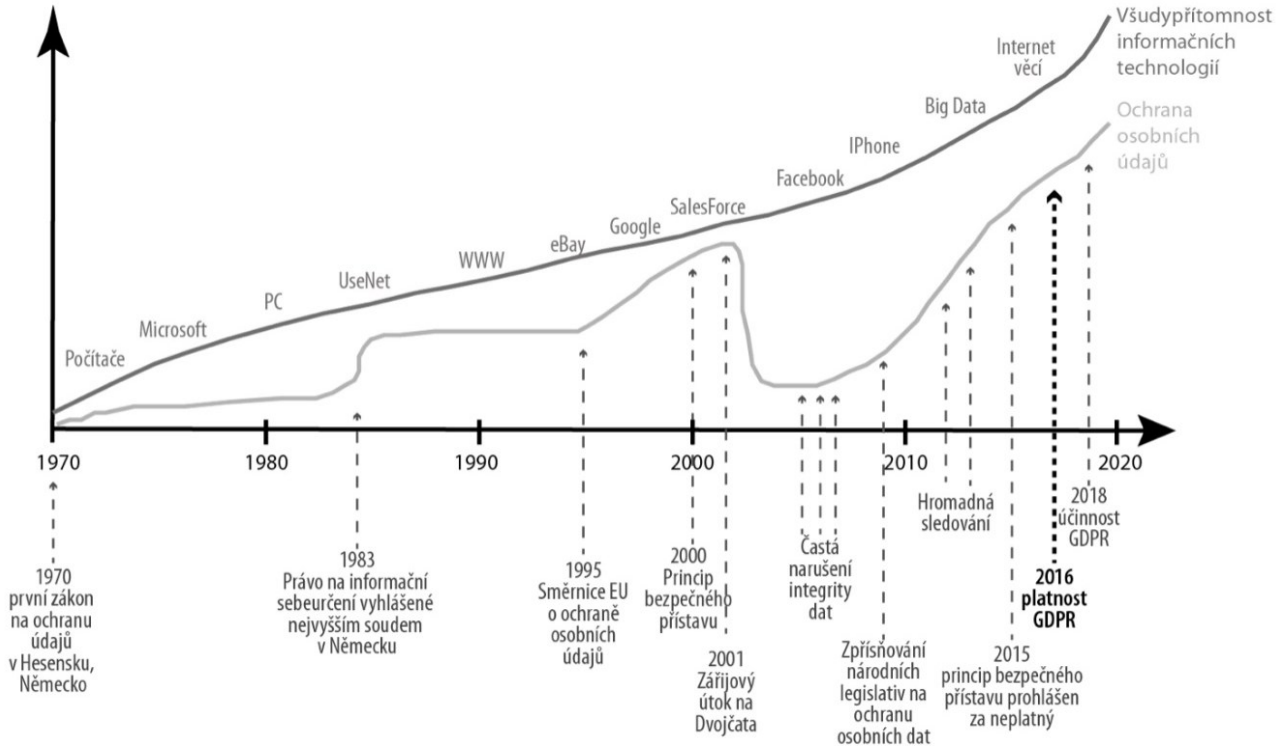
Obecné nařízení o ochraně osobních údajů, v angličtině General Data Protection Regulation a plným názvem NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které vzešlo v platnost 25. května

2018, je zatím posledním právním předpisem, který ochranu osobních údajů upravuje (Nezmar, 2017).

Obecné nařízení o ochraně osobních údajů má za cíl „dotvořit prostor svobody, bezpečnosti a práva a hospodářské unie, k hospodářskému a sociálnímu pokroku, k posílení a sblížení ekonomik v rámci vnitřního trhu a k dobrým životním podmínkám fyzických osob.“ (Evropský parlament a Rada EU, 2016, str. 1, odst. 2).

Jelikož je GDPR nařízení a ne směrnice, tak přímo určuje pravidla pro zpracování osobních údajů v celé Evropské unii. GDPR však dovoluje modifikaci některých témat, jako je například snížení výše pokut za porušení předpisů o ochraně osobních údajů apod. (Navrátil a kol., 2018). V České republice platí zákon č. 110/2019 Sb., o ochraně osobních údajů, který upravuje tato témata, například snižuje věkovou hranici pro souhlas se zpracováním osobních údajů dětí, která je Evropskou unií stanovena na 16 let, ale zákonem č. 110/2019 Sb. je stanovena na 15 let (Chlebus & Dostál, 2019).

Obr. 2 Porovnání vývoje legislativy s rozvojem technologií



Zdroj: Nezmar (2017)

2.2 Základní terminologie GDPR

Pro správné pochopení problematiky GDPR je nutné porozumět základním pojmům, které se jí týkají. V této kapitole budou vysvětleny pojmy, které jsou potřeba pro správné pochopení dalších částí této práce.

Osobní údaje jsou „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*.“ (Evropský parlament a Rada EU, 2016, čl. 4, odst. 1). Pro osobní údaje není klíčové to, jestli je údaj naprosto pravdivý, objektivně měřitelný nebo pouze odhadnutý na základě charakteristiky subjektu údajů, ale to, jaký vztah má údaj k subjektu údajů (Nulíček a kol, 2017).

Zpracování osobních údajů je „jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“ (Evropský parlament a Rada EU, 2016, čl. 4, odst. 2).

Profilování je „jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.“ (Evropský parlament a Rada EU, 2016, čl. 4, odst. 4).

Správcem se rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.“ (Evropský parlament a Rada EU, 2016, čl. 4, odst. 7).

Zpracovatel je „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.“ (Evropský parlament a Rada EU, 2016, čl. 4, odst. 8). Zpracovatelem osobních údajů může být také **třetí strana**, neboli „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.“ (Evropský parlament a Rada EU, 2016, čl. 4, odst. 10).

Příjemce je „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.“ (Evropský parlament a Rada EU, 2016, čl. 4, odst. 9).

Souhlasem rozumíme „subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.“ (Evropský parlament a Rada EU, 2016, čl. 4, odst. 11).

2.3 Zásady zpracování osobních údajů

Zásady zpracování osobních údajů se dají považovat za úplný základ, na kterém je GDPR postaveno. Nejedná se však o žádné nové vyjádření, ve Směrnici 95/46/ES byly tyto zásady popsány jako dílčí povinnosti, novinkou je tedy pouze jejich přesné vyjmenování a popsání jako zásady pro zpracování osobních údajů (Žůrek, 2018).

Zásada zákonnosti spočívá v nutnosti zpracování osobních údajů v souladu s právními předpisy (Navrátil a kol., 2018). Tuto zásadu lze považovat za nejpodstatnější, především kvůli tomu, že správce může údaje zpracovávat, jen pokud má ke zpracování alespoň jeden právní důvod (Žůrek, 2018). Podle článku 6 GDPR rozlišujeme tyto právní důvody zpracování osobních údajů:

- souhlas subjektu údajů,
- plnění smlouvy,
- právní povinnost,

- ochrana životně důležitých zájmů,
- splnění úkolu prováděného ve veřejném zájmu,
- oprávněné zájmy (Evropský parlament a Rada EU, 2016).

V podnikové oblasti se člověk může nejčastěji setkat s třemi výše uvedenými právními důvody zpracování, kterými jsou souhlas subjektu údajů, plnění smlouvy a oprávněný zájem. Souhlas subjektu údajů je poskytnutý projev vůle, kterým dává subjekt údajů zjevně najevo, že souhlasí se zpracováváním svých osobních údajů a to v souvislosti s konkrétním zpracováním. Souhlas může být udělen nejen písemně, ale i slovně, ať už telefonicky nebo přes internet, důležité je, aby byla zachována jeho dobrovolnost. Souhlas může také subjekt údajů kdykoliv odvolat. V praxi se souhlas se zpracováním osobních údajů vyskytuje spíše jako právní důvod, který doplňuje nějaký jiný právní důvod, například při uzavírání smlouvy.(Žůrek, 2018).

Plnění smlouvy je právním důvodem, který má dost jasně vymezen účel, při němž může být použitý, zároveň do něj může patřit spousta činností, z důvodu, že plnění smlouvy může být různé. Plnění smlouvy obsahuje i zpracování, které je nutno podniknout před samotným uzavřením smlouvy. Jde tak například o přijetí dotazníku uchazeče o zaměstnání, kdy podnik musí zpracovat osobní údaje, aby pak mohl smlouvu s daným člověkem uzavřít (Žůrek, 2018).

Oprávněný zájem je v podnikovém prostředí často spojován s přímým marketingem a kamerovými systémy. V případě přímého marketingu musí provozovatel prokázat, že jeho zájem je v rovnováze s dotčenou osobou. V případě, že by dotčená osoba měla námitku ohledně zpracování jejích osobních údajů, musí provozovatel zpracování zastavit a údaje vymazat. U kamerových systémů musí být prokazatelné, že oprávněný zájem existuje – například, pokud majitel chrání svůj majetek prostřednictvím kamer. Pokud v tomto případě dojde k námitce, zpracování je omezeno a provozovatel má prostor k prokázání splnění podmínek zpracování (Kuchař, 2018).

Pokud právní důvod pro zpracování těchto údajů zanikne, je třeba osobní údaje zlikvidovat. Pokud ale právní důvod k zpracování neexistoval, jedná se o nelegální zpracování (Janečková, 2018).

Zásada korektnosti a transparentnosti zaručuje, že správce nesmí zatajovat subjektu údajů účel, pro který jsou osobní údaje zpracovávány a zároveň má správce povinnost informovat subjekt údajů o tom, jak a v jakém rozsahu jsou jeho osobní údaje

zpracovávány a komu jsou následně předány. Zásada transparentnosti také po správci požaduje, aby informace, které subjektu údajů předává nebo by mohl případně předávat, byly pro subjekt údajů snadno přístupné – např. přes internet, a srozumitelné za využití zřetelných jazykových prostředků (Žůrek, 2018).

Zásada omezení účelu vyjadřuje nutnost mít určité a výslovně vyjádřené legitimní účely pro shromažďování osobních údajů, které nesmí být zpracovávány způsobem, který by byl s těmito účely neslučitelný (Žůrek, 2018). Není tedy možné, aby správce shromažďoval osobní údaje k určitému účelu a ty by pak byly zpracovány pro jiný účel, ať už samotným správcem nebo zpracovatelem. To by totiž znamenalo, že se o novém účelu subjekt údajů nedozví (Janečková, 2018). Zásada omezení účelu ale není absolutní a existuje výjimka, další zpracování. Další zpracování vyjadřuje skutečnost, kdy jsou údaje zpracovávány za jiným účelem, než za kterým byly shromážděny. GDPR dovoluje další zpracování ve čtyřech případech. Prvním případem je archivace v zájmu veřejnosti pro historické výzkumy, či statistické účely. Druhým případem může být zpracování, pokud k němu dal subjekt údajů souhlas. Třetím případem je zpracování založené na právu některého členského státu EU, které je nutným opatřením pro demokratickou společnost. Posledním případem je provedení posouzení slučitelnosti původního a nového účelu správcem, pokud vyhodnotí, že jsou účely slučitelné (Nulíček a kol., 2017).

Zásada minimalizace údajů zabezpečuje to, že budou shromažďovány a zpracovávány pouze osobní údajů, které jsou relevantní s ohledem na účel jejich zpracování a jen v rozsahu, který je pro naplnění účelu nutný (Nulíček a kol., 2017). V praxi to znamená, že je třeba, aby se o každém osobním údaji rozhodlo, zda je pro daný účel opravdu nutný a správce by měl být schopný u jednotlivých osobních údajů určit důvod, proč je daný údaj pro tento konkrétní účel potřeba (Janečková, 2018).

Zásada přesnosti představuje nutnost, aby zpracovávané osobní údaje byly přesné a odpovídaly realitě a pokud je to nutné, měly by být aktualizovány. V případě, že tyto údaje jsou nepřesné, nese správce odpovědnost, aby tyto údaje opravil nebo zlikvidoval (Nulíček a kol., 2017).

Vzhledem k tomu, že zpracování osobních údajů vyjadřuje určitý zásah do soukromí osoby a představuje bezpečnostní riziko kvůli samotnému zpracování, je důležitá **zásada**

omezení uložení. Ta zaručuje, že pokud pomine účel zpracování osobních údajů, je správce povinen údaje vymazat (Žůrek, 2018).

Poslední ze zásad je **zásada integrity a důvěrnosti**. Údaje, které jsou zpracovávány, je třeba dostatečně zabezpečit prostřednictvím vhodných opatření, které je budou chránit před neoprávněným nebo protiprávním zpracováním a také před zničením, ztrátou či poškozením (Žůrek, 2018). Osobní údaje je třeba zabezpečit před hrozbami uvnitř podniku i mimo podnik (Janečková, 2018).

2.4 Práva subjektu údajů

GDPR formalizuje již několik dříve existujících práv a vytváří nová práva (Sharma, 2020). Práva subjektu údajů podle GDPR jsou:

- právo na informace, což je základ pro naplnění zásady transparentnosti, zaručuje informovanost o zpracování osobních údajů subjektu údajů a pro subjekt údajů se jedná o pasivní právo, protože se jedná o aktivní povinnost správce,
- právo na přístup, je aktivním právem, které subjekt údajů uplatňuje podle sebe a správce má tím pádem povinnost tehdy, kdy subjekt údajů bude chtít zpřístupnit své osobní údaje,
- právo na opravu a doplnění, dává subjektu údajů právo na to, aby, pokud je to potřebné, byly správcem osobní údaje opraveny nebo nekompletní osobní údaje doplněny,
- právo na výmaz, nebo také právo být zapomenut, dává subjektu údajů právo na to, aby jeho osobní údaje byly bezprostředně vymazány správcem, pokud nastane důvod pro jejich výmaz,
- právo na omezení zpracování, které v určitých případech, jako je například popření správnosti osobních údajů subjektem údajů, nařizuje správci omezení zpracování,
- právo na přenositelnost údajů je úplně novým právem, které zajišťuje získání osobních údajů subjektu údajů, které poskytnul a týkají se ho a to ve formátu, který je normálně používaný, současně tyto údaje poskytnout jinému správci, lze i prostřednictvím prvotního správce, pokud je zpracování podloženo souhlasem subjektu či smlouvou a je prováděno automatizovaně,

- právo vznést námitku, dává subjektu údajů možnost se kdykoliv odvolat proti zpracovávání jeho osobních údajů,
- právo nebýt předmětem automatizovaného individuálního rozhodování, znamená, že, subjekt údajů má právo, aby vůči němu nebylo uskutečněno automatizované rozhodnutí s právním účinkem (Žůrek, 2018).

Je velmi důležité dodržovat všechna práva subjektu údajů, protože subjekty mají právo podat stížnost u dozorového úřadu (IT Governance Privacy Team, 2017).

2.5 Předávání osobních údajů do třetích zemí a mezinárodních organizací

Přestože je GDPR nařízení Evropského parlamentu a Rady, není omezeno pouze na hranice Evropské Unie (Sharma, 2020). V případě, kdy by předávání osobních údajů do ciziny bylo neuskutečnitelné, spousta služeb by nemohla vůbec fungovat, což by se promítlo na jejich přístupnosti a ceně, stejně tak jako na komfortu z jejich užívání. GDPR však přenos osobních údajů do ciziny umožňuje, pro legální předání však musí být splněno několik podmínek (Nulíček a kol., 2017). Předání bylo definováno Evropským sborem pro ochranu osobních údajů v pokynech č. 5/2021, která musí být splněna proto, aby se jednalo o předávání:

- pokud je vývozcem osobních údajů správce nebo zpracovatel podléhající GDPR, podle čl. 3,
- pokud vývozce v průběhu zpracování přesune nebo umožní přístup k osobním údajům jinému správci či zpracovateli, který je označován jako dovozce osobních údajů,
- pokud se dovozce osobních údajů vyskytuje ve třetí zemi, nebo je mezinárodní organizací, kdy nezáleží, jestli spadá pod čl. 3 GDPR (Benešová a kol., 2023).

Pokud jsou osobní údaje zveřejněny na internetu, nejedná se tak o předání, jelikož má k těmto osobním údajům přístup kdokoliv z celého světa (Nulíček a kol., 2017).

Pro předání osobních údajů do třetí země musí platit podmínka zákonnosti, která však musí platit vždy bez ohledu na to, kam jsou osobní údaje předávány. Dále však také musí platit dodatečné podmínky, které GDPR stanovuje a jsou potřebné z důvodu jiné právní ochrany osobních údajů v zemích mimo Evropskou unii, která nemusí být na stejné úrovni jako GDPR (Nulíček a kol., 2017).

Správce či zpracovatel, který předává osobní údaje do mimo unijních zemí, musí využít jeden z režimu předávání. Prvním režimem je **předání na základě rozhodnutí o odpovídající ochraně osobních údajů**. Vydání tohoto rozhodnutí má na starost Evropská komise. V případě, že země, její část nebo i určité oblasti poskytují dostatečnou ochranu osobních údajů, lze ji považovat za bezpečnou třetí zemi. V praxi to znamená, že se předávání usnadní, protože není třeba udělat tolik administrativních úkonů. Tato rozhodnutí jsou volně dostupná například na stránkách Úřadu pro ochranu osobních údajů (Benešová a kol., 2023).

Dalším režimem je **předání na základě přijatých záruk**, nejčastěji jde o standardní smluvní doložky nebo závazné podnikové pravidla. Předání osobních údajů bez rozhodnutí lze pouze při splnění tří kritérií. U standardních doložek a závazných podnikových pravidel není třeba povolení od Úřadu pro ochranu osobních údajů, pokud by však zpracovatel nebo správce chtěl použít ad hoc smluvní položky, musí úřad povolení vydat. U závazných podnikových pravidel může být považována za nevýhodu jejich malá flexibilita, protože pro taková pravidla je složitý proces přijímání (Benešová a kol., 2023).

Třetím režimem je **předání osobních údajů do amerických organizací podle Data Privacy Framework**, který tak od 10. července 2023, kdy ho Evropská komise přijala, opět zjednodušuje předání osobních údajů do USA, poté co byl Soudním dvorem EU zrušen Privacy Shield. Předání osobních údajů do USA je možno na základě certifikace. Pokud je organizace zapsána v rejstříku certifikovaných organizací, můžeme ji považovat za bezpečnou (Benešová a kol., 2023).

Čtvrtým a posledním režimem je **předání na základě takzvaných výjimek**. Mezi tyto výjimky patří například výslovný souhlas, v případě založení uživatelského účtu na sociální síti, kdy uživatel musí odkliknout políčko o souhlasu. Dále sem můžeme zařadit uzavření nebo splnění smlouvy a veřejný zájem (Nulíček a kol., 2017).

2.6 GDPR ve vztahu zaměstnanec a zaměstnavatel

Personalistika je jednou z oblastí, která je GDPR výrazně zasažena, co se týče počtu správců, zpracovatelů a subjektů údajů. Zpracovávané údaje v této oblasti bývají různé na základě právních důvodů a rozsah zpracovávaných informací bývá obrovský (Janečková, 2018). Nejčastěji však jde o mzdovou agendu nebo rejstříky, například rejstřík uchazečů o zaměstnání (Jouza, 2018).

V praxi se od začátku účinnosti GDPR vyskytují případy, kdy zaměstnavatel při podpisu pracovní smlouvy přidá dodatek o tom, že zaměstnanec souhlasí se zpracováním osobních údajů. Tento dodatek je však zbytečný a může v zaměstnanci, který ho podepíše, vyvolat dojem, že má kdykoliv možnost souhlas odvolat, tak tomu ale není. Zaměstnavatel má právní důvod pro zpracování osobních údajů zaměstnance, v tomto případě plnění smlouvy, a proto je tento dodatek nadbytečný (Jouza, 2018).

Důležitým tématem je rovněž občanský průkaz. V praxi podniků je běžné, že si zaměstnavatel okopíruje občanský průkaz zaměstnance. Pokud zaměstnanec udělil souhlas, tak je podle nařízení vše v pořádku, problém může nastat při kopírování občanského průkazu potencionálního zaměstnance, který souhlas udělí s pocitem, že při odmítnutí by se snížila jeho šance získat dané pracovní místo (Jouza, 2018).

2.7 Dozorový úřad a pokuty

Dozorový úřad představuje nezávislý orgán zřízený členským státem, jehož hlavním úkolem je dohlížet na dodržování GDPR. Mezi úkoly dozorového úřadu patří mimo jiné:

- šetření uplatňování GDPR,
- řešení stížností v případě podezření na nezákonné zpracování osobních údajů,
- vedení interních záznamů o porušování GDPR,
- spolupráce s ostatními dozorovými úřady za účelem sjednocení uplatňování GDPR,
- poskytování poradenství ohledně správných postupů při zpracování osobních údajů (Žůrek, 2018).

Dozorový úřad k plnění těchto úkolů využívá pravomoci, které se dají rozdělit do tří skupin – povolovací a poradní, nápravná a vyšetřovací. V případě potřeby funguje mezi

dozorovými úřady vzájemná pomoc, kdy se kterýkoliv dozorový úřad může obrátit na jiný dozorový úřad členského státu s žádostí různého charakteru (Žůrek, 2018).

Dozorový úřad České republiky je Úřad pro ochranu osobních údajů (ÚOOÚ). Pokud je zjištěno porušení některé ze zásad GDPR, dozorový úřad nejdříve informuje příslušný podnik o tomto zjištění a vyzve ho, aby chybu napravil. Pokud k nápravě nedojde, úřad podniku uloží správní pokutu. Výše pokut dělíme podle závažnosti porušení do dvou skupin. Méně závažné případy porušení GDPR se pohybují do výše 10 000 000 eur, nebo až do 2 % celkového celosvětového obratu, pokud jde o podnik. To, která z variant bude využita, záleží na tom, která částka je vyšší. V případě závažnějšího porušení jsou pokuty až 20 000 000 eur, nebo až do 4 % celkového světového obratu, opět pokud jde o podnik (Odrobinová, 2020). Mezi polehčující a naopak přitěžující okolnosti, které ovlivňují výši sankce, patří například povaha, závažnost a doba trvání porušení, kdy se přihlíží i k povaze, rozsahu, účelu dotčeného zpracování a počtu dotčených subjektů údajů a rozsah škody, kterou utrpěli. Pak se též kouká na způsob, jakým se o porušení dozorový úřad dozvěděl a zda správce spolupracoval s úřadem na možnostech nápravy (Ilavská, 2019).

V České republice bylo za rok 2023 uloženo 23 pravomocných trestů za porušení předpisů na ochranu osobních údajů. Součet těchto pokut činil 3 653 000 Kč (Úřad pro ochranu osobních údajů, 2024).

Zatím vůbec nejvyšší pokuta byla vyměřena v květnu 2023 společnosti META, mateřské společnosti Facebooku, a to ve výši 1,2 miliardy eur. Společnost měla neoprávněně posílat data o evropských uživatelích do Spojených států amerických. Pro firmu je to již několikátá pokuta, kterou v Evropě za poslední dobu dostala a považuje ji za neoprávněnou, a proto ji chce nechat pozastavit soudem (Sedláček, 2023). Další rekordní pokuta za porušení GDPR byla udělena v červenci 2021 firmě Amazon a to ve výši 746 milionů eur pro předávání osobních údajů, které se neslučovalo s pravidly GDPR. Firma se proti pokutě odvolala. Třetí nejvyšší pokutou je opět pokuta firmě META ze září 2022 na částku 405 milionů eur, kterou dostala za činnost sociální sítě Instagram, která měla údajně shromažďovat osobní údaje nezletilých uživatelů platformy (Fišer, 2023). Jednu z posledních pokut za porušení GDPR dostala firma ByteDance, která spravuje aplikaci Tiktok, v září 2023 ve výši 345 milionů eur. Pokuta byla udělena za nedostatečnou ochranu osobních údajů nezletilých, kteří aplikaci Tiktok používaly, podobně jako tomu bylo u aplikace Instagram (Drábek, 2023).

3 Přístupy k implementaci GDPR ve společnosti

Správná implementace GDPR v podniku je nezbytným krokem k zajištění úplného dodržování předpisů týkajících se ochrany osobních údajů (Nezmar, 2017). Každý projekt implementace GDPR probíhá v kontextu dané organizace. Proto rozsah, časový rámec a náklady závisí na konkrétní charakteristice podniku a okolnostech samotné implementace (Faifr & Januška, 2021). V této části budou představeny praktické postupy a opatření, které podniky musely přijmout pro zajištění souladu s GDPR.

Prvním krokem je, že firma musí posoudit, zda se na ni GDPR vztahuje. V tomto případě je odpověď vždy ano. Dále musí rozhodnout o tom, zda bude GDPR implementovat samostatně, nebo si na to najme externí firmu. Nelze však s určitostí říct, které řešení je lepší. Rozhodnutí závisí na potřebách a možnostech podniku a jeho velikosti (Křížová, 2018).

Pro firmy by mohlo být lákavé postupovat podle určitého schématu jiného podniku. To je však chybný přístup, který může vést k tomu, že zpracování osobních dat nebude v souladu s GDPR. I kdyby si firma jako vzor vybrala podnik, který se věnuje stejné činnosti a je podobně velký, s největší pravděpodobností oba podniky zacházejí s osobními daty jinak a jejich způsob zpracování osobních údajů je jiný. Obecně tyto zjednodušené návody jak GDPR zavést moc nefungují (Svaz průmyslu a dopravy České republiky, 2018).

Zásadním krokem pro implementaci ve větším podniku, který se rozhodne implementovat GDPR interně, je správně sestavit projektový tým. Ten by se měl skládat z několika klíčových členů z celé organizace, nejdůležitější je však právník, IT specialista, personální specialista, finanční specialista a člen nejvyššího zastoupení podniku. Pro správné fungování je vhodné zvolit si jednoho vedoucího týmu, který bude zajišťovat, aby všichni členové měli všechny informace. Cílem projektového týmu je zdařilá implementace GDPR do podniku, ta se však skládá z několika dílčích cílů, které budou popsány dále v textu. V případě menšího podniku stačí pro implementaci méně osob, firma tedy nemusí sestavovat projektový tým, který se skládá ze specialistů (Navrátil a kol., 2018).

3.1 Vstupní analýza

První krok, který je před samotnou implementací třeba udělat, je analyzovat to, jak jsou momentálně osobní údaje v podniku zpracovávány a vyhodnotit, jak moc je momentální způsob zpracování v souladu s GDPR a jaké má firma v tomto ohledu mezery. Tato analýza se nazývá GAP analýza a měla by mít několik kroků (Nezmar, 2017).

Nejdříve je potřebné zjistit a popsat základní parametry zpracování osobních údajů. Je například třeba zjistit a popsat jaké osobní údaje jako firma zpracováváme, v jakém rozsahu, pro jaké účely, jaký je zákonný důvod jejich zpracování, dále také jaké máme kategorie subjektů údajů a příjemců, jak předáváme osobní údaje do třetích zemí či mezinárodních organizací, po jakou dobu osobní údaje uchováváme, odkud osobní údaje pochází a v neposlední řadě je třeba zkoumat prostředky, kterými jsou osobní údaje zpracovávány. Následně námi získané informace porovnáme s GDPR (Janečková, 2018).

Je třeba rozhodnout o postavení firmy při kterémkoliv účelu zpracování, tedy jestli se nachází v pozici správce, či zpracovatele. Pokud správce osobní údaje zpracovává, tak za ně i odpovídá a určuje účel zpracování osobních údajů a prostředky pro toto zpracování. Dále se posuzuje obsah souhlasu s novými požadavky GDPR a rozsah plnění informační povinnosti, která byla zavedením GDPR rozšířena (Janečková, 2018).

Kromě toho je třeba posoudit obsah souhlasu, musí být zhodnocen rozdíl mezi dosavadní verzí a novými potřebami. Podobně tomu tak je i u informační povinnosti. Každý správce musí posoudit, jestli jsou subjekty údajů informovány dostatečně. Informační povinnost je obzvlášť důležitá z toho důvodu, že GDPR klade velký důraz na posílení postavení subjektu údajů. V neposlední řadě je potřeba analyzovat způsob zabezpečení osobních údajů. To znamená, že jsou třeba posoudit opatření, které se týkají počítačové a fyzické bezpečnosti, rozsah strategie v oblasti uchování a likvidace dat a rozsah kontrolní činnosti (Janečková, 2018).

Podnik si také musí uvědomovat rizika, která jsou spojená se zpracováváním osobních údajů a zavést opatření, která tyto rizika zmírní. V GDPR je několikrát zmíněna úvaha o tom, že by správce a zpracovatel měl brát ohled na rizika v mnoha fázích životního cyklu osobních údajů. Některé menší podniky mohou rizika řídit relativně neformálně, ale většina podniků bude mít k tomuto tématu více formální přístup, který bude zahrnovat například registr rizik (IT Governance Privacy Team, 2017).

Výstupem GAP analýzy by měl být souhrn zjištění a návrhů pro zlepšení. Management firmy by měl přijít se zprávou, která umožní firmě identifikovat možná rizika a problémy, stejně tak jako oblasti, které je třeba upravit pro dosažení souladu s GDPR. Zpráva by měla obsahovat také doporučení pro zabezpečení IT systémů, protože je spousta dat v elektronické podobě. Na základě této zprávy můžeme také vytvořit harmonogram projektu a kompletní plán pro implementaci s konkrétními kroky, termíny a osobami, za ně zodpovědnými (Nezmar, 2017).

3.2 Nové povinnosti pro podnik

Tato kapitola je zaměřena na nové povinnosti, které pro podniky přineslo GDPR. Těmito novými povinnostmi jsou záznamy o činnostech, zabezpečení osobních údajů, posouzení vlivu a jmenování pověřence pro ochranu osobních údajů. Některé z těchto nových povinností neplatí stejně pro každý podnik, přesto je důležité tyto prvky znát, protože představují kritickou součást ochrany osobních údajů a vyžadují pečlivou pozornost podniků k dosažení a udržení souladu s právními normami GDPR.

3.2.1 Záznamy o činnostech

Správce a zpracovatel mají povinnost uchovávat záznamy o činnostech zpracování. Z důvodu, aby údaje a následné důkazy nebyly zničeny nebo ztraceny v průběhu let. Zároveň by měly záznamy zvýšit transparentnost procesů zpracování osobních dat pro subjekty údajů, ale i dozorové úřady. Tyto záznamy je třeba uchovávat písemně, lze i v elektronické formě (Sharma, 2020).

Obsahem záznamů správce budou následující informace:

1. Jméno a kontaktní údaje
   a) Správce
   b) Společného správce
   c) Zástupce správce
   d) Pověřence pro ochranu osobních údajů
2. Účely zpracování
3. Popis kategorií subjektů údajů a shromážděných údajů
4. Kategorie příjemců
5. Informace o případném předávání osobních údajů do třetí země nebo mezinárodní organizace

6. Předpokládaná lhůta pro výmaz jednotlivých kategorií údajů
7. Obecný popis technických a organizačních opatření pro ochranu osobních údajů (Sharma, 2020).

Poslední dva body nejsou zcela povinné, je specifikováno, že tyto informace se udávají jen, pokud je to možné (Janečková, 2018).

Obsahem záznamů zpracovatele budou následující informace:

1. Jméno a kontaktní údaje
   a) Zpracovatele
   b) Dalšího zpracovatele
   c) Každého správce, pro kterého zpracovatel jedná
   d) Případného zástupce správce nebo zpracovatele
   e) Pověřence pro ochranu osobních údajů
2. Kategorie zpracování provedeného pro každého ze správců
3. Informace o případném předávání osobních údajů do třetí země nebo mezinárodní organizace
4. Obecný popis technických a organizačních opatření pro ochranu osobních údajů (Shaarma, 2020).

Pokud podnik zaměstnává méně než 250 lidí, není tato povinnost vyžadována. Vyžadována je pouze v případě, že zpracování není příležitostné, zabývá se speciálními údaji nebo se týká trestních rozsudků (Sharma, 2020).

3.2.2 DPIA

Data protection impact assesment (DPIA), v češtině posouzení vlivu zpracování na ochranu osobních údajů, je jedním ze specifických procesů nařízených GDPR. DPIA je používáno k identifikaci konkrétních rizik pro osobní údaje v důsledku jejich zpracování. Pro zachování bezpečnosti a zabránění zpracování osobních dat v rozporu s GDPR, je na správci, či zpracovateli, aby vyhodnotil rizika, která jsou se zpracováním spojená, a zavedl určitá opatření, která tyto rizika zmírní, jde například o šifrování (IT Governance Privacy Team, 2017).

DPIA je uplatněno v případě, kdy je značné riziko pro práva a svobody fyzických osob při určitém druhu zpracování, zvláště pak, pokud je pro zpracování využíváno nových technologií. Je ale potřeba přihlédnout i k povaze, rozsahu, kontextu a záměru zpracování

(Žůrek, 2018). DPIA je nezbytné především ve třech případech. Prvním případem je systematické a rozsáhlé vyhodnocování osobních aspektů tykajících se fyzických osob na základě automatizovaného zpracování, včetně profilování, a na kterém jsou založena rozhodnutí, která produkují právní účinky týkající se fyzických osob nebo mohou fyzickou osobu významně ovlivnit. Druhým případem je zpracování velkého rozsahu údajů zvláštních kategorií uvedených v článku 9 odst. 1 nebo osobních údajů týkajících se odsouzení za trestné činy a trestných činů uvedených v článku 10. Třetím případem, kdy je DPIA nezbytné, je při systematickém monitorování veřejně přístupného prostoru ve velkém měřítku (IT Governance Privacy Team, 2017).

Tři výše uvedené případy však nejsou jedinými, kdy je DPIA potřeba. Správce musí při posouzení rizikovosti rozhodnout, zda operace neobsahuje určité rysy, které jsou vysoce rizikové. Mezi tyto rysy patří profilování a ohodnocení subjektů údajů, automatizované rozhodování s právními či jiným způsobem podstatnými účinky, zpracování citlivých údajů nebo údajů ve velkém rozsahu, systematické monitorování osob, kombinování osobních údajů z odlišných datových sad apod. Pokud správce dojde k závěru, že plánovaná operace zpracování zahrnuje nejméně dva z těchto rysů, měl by provést DPIA (Nulíček a kol., 2017).

3.2.3 Zabezpečení osobních údajů

Pro soulad zpracování s GDPR je potřeba dostatečně zabezpečit osobní údaje v podniku. Je třeba posoudit, jaká je vhodná úroveň bezpečnosti především s ohledem na rizika, jako je náhodné či protiprávní zničení osobních údajů, jejich ztráta, pozměnění, neoprávněné povolení přístupu k předávaným, uloženým nebo jiným způsobem zpracovávaným osobním údajům, či neoprávněný přístup k nim (Janečková, 2018).

Mezi bezpečností a organizační opatření, kterými můžeme osobní údaje zabezpečit, řadíme jejich pseudonymizaci a zašifrování, dále také schopnost zabezpečit stálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb pro zpracování, schopnost obnovení dostupnosti osobních údajů a přístupu k nim, pokud dojde k nějakému technickému nebo fyzickému incidentu a v neposlední řadě sem řadíme pravidelné testování a hodnocení efektivnosti zavedených opatření pro zajištění bezpečnosti osobních údajů (Žůrek, 2018). Pseudonymizace je proces, kdy jsou osobní údaje zpracovány tak, že nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací (Sharma, 2020). Na rozdíl od pseudonymizace, šifrování osobní

údaje úplně skryje za pomocí technologie. K těmto osobním údajům se pak člověk může dostat s šifrovacím klíčem (Kramer, 2018). Pseudonymizace i šifrování slouží jako bezpečnostní opatření, nejsou povinná a je na každém správci či zpracovateli, aby se rozhodl, jaký ochranný prostředek využije. Pseudonymizace se uplatňuje v případech, kde je nutné udržet určitou míru identifikace subjektu údajů, naopak šifrování se využívá v situacích, kde je klíčové dosáhnout úplného zabezpečení dat (Žůrek, 2018).

Mnohem větší riziko zneužití osobních údajů nastává při použití internetu, proto je velmi důležité data dostatečně zabezpečit, k tomu nám může pomoci výše zmíněná pseudonymizace a šifrování, ale i bezpečná wi-fi, nebo bezpečný cloudový systém. Jedním z nejvíce nebezpečných způsobů online komunikace jsou otevřené wi-fi sítě (Nezmar, 2017).

V případě, že má podnik zakoupený informační systém od externího dodavatele, je velmi důležité, aby s ním od začátku implementace spolupracoval na potřebných úpravách s ohledem na GDPR. Tito dodavatelé by však také měli své produkty, v tomto případě software, těmto potřebám uzpůsobovat (Svaz měst a obcí České republiky, 2020).

3.2.4 Jmenování pověřence

V Směrnici 95/46/ES byla vyjádřena možnost pro členské státy stanovit si jako zjednodušení či výjimku z oznamovací povinnosti, v případě, že správce správně určil, osobu pověřenou ochranou údajů, anglicky data protection officer (DPO). Česká republika však tuto možnost do zákona o ochraně osobních údajů nezakotvila, a proto je pro české správce a zpracovatele novinou (Žůrek, 2018).

Pověřenec má za úkol jmenovat část správců a zpracovatelů, dohlížet na soulad zpracování, v případě potřeby radit správci, být kontaktním bodem pro subjekty údajů a dozorové úřady v případech, které se týkají zpracování osobních údajů (Nulíček a kol., 2017).

Ne každá organizace potřebuje pověřence pro ochranu osobních údajů. Správce a zpracovatel určí pověřence pokud:

- zpracování provádí orgán veřejné moci nebo veřejný subjekt, s výjimkou soudů jednajících v rámci své soudní pravomoci,

- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které na základě své povahy, rozsahu nebo účelu vyžadují pravidelné a systematické monitorování subjektů údajů,
- hlavní činnost správce nebo zpracovatele spočívají ve zpracování velkého rozsahu zvláštních kategorií údajů z čl. 9 a osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů podle čl. 10 (IT Governance Privacy Team, 2017).

Je důležité, že výše uvedené podmínky musí platit všechny tři kumulativně, aby vznikla povinnost pro subjekt jmenovat pověřence pro ochranu osobních údajů (Žůrek, 2018).

3.3 Implementace mechanismů

Rozsah potřeby implementace je různý na základě povahy organizace. Například u lékařských středisek byl už před zavedením GDPR stav ochrany osobních údajů dobrý s ohledem na tradiční dodržování lékařské mlčenlivosti. U podnikatelských subjektů je však situace jiná, protože před zavedením GDPR byla mnohdy problematika přehlížena, proto se bude následující text zabývat implementací mechanismů GDPR v podnikatelských subjektech (Navrátil a kol., 2018).

Podnik by se měl zaměřit na problémy zjištěné analýzou. Těmi hlavními jsou úprava externí dokumentace, jako jsou například obchodní podmínky tak, aby odpovídaly GDPR, a odstranění osobních údajů, které již nepotřebuje, a jsou nadbytečné. Důležité je také upravit a vytvořit příslušné interní dokumenty určené zaměstnancům, které jim budou k pochopení GDPR nápomocné, a upravit způsob zpracování osobních údajů dle GDPR jak uvnitř podniku, tak vně (Byznys, 2018). Podnik musí revidovat smlouvy a souhlasy a následně je aktualizovat tak, aby byly v souladu s GDPR. Nevyhnutelná je i úprava informačních systémů a vytvoření plánu pro případ porušení zabezpečení osobních dat, tudíž je třeba zajistit způsob interního reportování a následné mírnění důsledků tohoto porušení. Samotný správce pak musí dbát na zavedení všech potřebných organizačních a technických opatření pro zabezpečení práv subjektů údajů a musí zavést do podniku mechanismus, který zabezpečí to, že se budou automaticky generovat dokumenty pro uchování, které prokazují soulad s GDPR, který je v případě kontroly nutný prokázat (Byznys, 2018).

Samotná implementace může u každého podniku vypadat jinak, výše jsou uvedeny činnosti, kterými by se podnik měl zabývat, avšak seznam může být mnohem širší, ale naopak i užší. Co je však důležité, je, aby úroveň ochrany osobních údajů byla v daný moment dostatečná. Přestože podnik vyhodnotí, že je ochrana dostatečná, za rok tomu tak být nemusí. Implementace je nekončící proces, hlavně kvůli tomu, že neexistuje žádný všeobecný návod, jak GDPR implementovat, odpověď na jednu otázku může být různá v závislosti na kontextu. Dalším důvodem pro neustálou aktualizaci procesů v rámci GDPR je vývoj technologií a techniky, odhalení pochybení v oblasti zabezpečení osobních údajů a také změna právních předpisů, protože implementace GDPR nevychází pouze ze samotného nařízení, ale i z jiných právních předpisů, jako je například zákoník práce (TaylorWessing, 2019).

3.4 On-line zpracování osobních údajů

V on-line prostředí můžou vznikat osobní údaje i bez vědomí subjektu údajů, kvůli cookies a IP adrese, tyto identifikátory se však stahují na zařízení, takže v případě používání jednoho zařízení větším počtem lidí (např. rodina), to do určité míry znemožňuje získání informací o tom, zda jsou údaje jednoho uživatele nebo několika uživatelů (Nezmar, 2017).

Soubory cookies jsou důležitým nástrojem, který může firmám poskytnout velký přehled o on-line aktivitě jejich uživatelů. Inzerenti cookies používají ke sledování on-line aktivity, aby na uživatele mohli cílit vysoce specifické reklamy. Předpisy, které upravují soubory cookies jsou GDPR a Nařízení o soukromí a elektronických komunikacích. Cookies jsou zpracovávány a ukládány webovým prohlížečem a samy o sobě jsou neškodné, plní pro webové stránky zásadní funkce. Lze je také obecně snadno prohlížet a mazat. Mohou však ukládat velké množství dat, která jsou dostatečná k tomu, aby člověka potenciálně identifikovala bez jeho souhlasu (Koch, n. d.). Do roku 2022 v České republice mohli weby využít lišty pro povolení sběru cookies, nebo mohli uživatele pouze informovat o tom, že jejich zpracování na webu probíhá, třeba prostřednictvím obchodních podmínek. Od 1. 1. 2022 je lišta pro souhlas se sbíráním cookies povinná, musí se však řídit určitými pravidly. Jedním z těchto pravidel je, že souhlas se sběrem cookies nesmí být podmínkou pro vstup na webovou stránku, to by znamenalo, že je souhlas vynucený a nebyla by splněna zásada zákonnosti. Mezi další pravidla patří to, že souhlas nemůže být vymáhán agresivně a lišta by neměla vyskakovat moc často, stejně

tak jako pokud webová stránka nabízí možnost „Přijmout všechny cookies“, měla by nabízet i možnost „Odmítnout všechny cookies“. Dále by uživatelé měli mít možnost lištu snadno a shodit a to i bez udělení souhlasu. Stránka potřebuje mít vypracovaný dokument s informacemi o zpracování cookies, ve kterém je uvedeno, kdo je daná stránka, jaké cookies zpracovává, proč je zpracovává a na jak dlouho, jaké nástroje k tomu využívá, jaká práva má uživatel a jak popřípadě může souhlas odvolat (Černovský, 2021).

3.5 Příručky a školení zaměstnanců

Správce má na starost vytvořit a zavést do interní dokumentace příručky, které se zabývají ochranou osobních údajů. V příručkách by měly být popsány činnosti, způsob zpracování a také postupy k nim se vztahující. Příručky by měly být detailní a snadno pochopitelné a také aktuální. Zároveň je potřeba, aby bylo možné posoudit, zda se postupy shodují s fungováním firmy a také, aby postupy nebyly psány obecně, ale pro potřeby společnosti (Mrázová, 2019).

Na konci implementace je potřebné zaměstnance podniku zaškolit, protože narušení dat bývá zpravidla způsobené lidskou chybou, ať už se jedná o ztracení mobilního telefonu, nebo posílání emailů bez šifrování. Předtím, než GDPR vešlo v platnost, byla školení pouze doplňková, ale od května 2018 jsou nutnou povinností správce a zpracovatele, jako součást opatření, které směřují k ochraně osobních údajů. O školení musí být dokument, aby podnik mohl prokázat, že všechny procesy provádí v souladu s GDPR (Nezmar, 2017).

Aby se školení dalo považovat za zdařilé, mělo by splnit několik klíčových předpokladů. Prvním a nejdůležitějším z nich je, že zaměstnanci pochopí problematiku GDPR a s ním související rizika, která pro společnost vznikají, stejně tak jako důsledky, které to pro společnost ale i samotného jedince může mít. Důležité také je, aby školení bylo osobité pro danou společnost, kvůli tomu, že v každé společnosti je jiná hierarchie, metody a procesy. Pro zaměstnance je důležité pochopit, že ochrana osobních údajů je spojená s každodenními činnostmi, které vykonávají. Na školení se mohou probírat různá témata, od problematiky hesel až po způsob likvidace osobních údajů. Dalším předpokladem je to, že školení bude osobní, protože školení prostřednictvím e-learningu nemusí být efektivní, kvůli tomu, že to zaměstnanci často pouze naklikají, ale textu nevěnují velkou pozornost. V neposlední řadě je třeba, aby zaměstnanci byli schopni rozeznat porušení GDPR pro případy jeho nahlášení. To znamená, že musí mít dostatečný

rozhled v této oblasti, aby porušení poznali a věděli jak a komu ho nahlásit (Nezmar, 2017).

4 Představení vybrané společnosti

Praktická část této bakalářské práce byla zpracovávána ve firmě Langmatz CZ s.r.o., která sídlí v Klatovech. Firma působí na českém trhu již od roku 1998, tam tehdy vstoupila pod názvem LIC technika. Specializuje se na dodávku produktů, jako jsou polykarbonátové kabelové šachty, podzemní rozvaděče pro městskou zástavbu, přístroje pro dopravní signalizaci a další (Langmatz CZ, 2023a). Firma stojí za realizací několika projektů - instalace prvního chytrého chodeckého tlačítka v Plzni, dodávky kabelové šachty pro novou stáčecí linku v Plzeňském Prazdroji nebo dodávky podzemních rozvaděčů do zahrad Pražského hradu nebo na depo závodního okruhu v Mostě (Langmatz CZ, 2023b). Firma zaměstnává přibližně 32 zaměstnanců, z toho dva zaměstnanci jsou řídícími pracovníky (Justice.cz, 2023). Jednatelem firmy je od 1. 1. 2024 Sebastian Antoni a prokuristkou firmy je již několik let Soňa Pelcová.

Obr. 3 Logo firmy Langmatz CZ s.r.o.

Zdroj: solidline.de (2024)

Langmatz CZ s.r.o. je dceřinou společností firmy Langmatz GmbH, která sídlí v Německu. Od roku 2004 má její 100 % obchodní podíl se splaceným vkladem 6 000 000 Kč. Langmatz GmbH i Langmatz CZ s.r.o. jsou partneři, kteří společně spolupracují na implementaci systémových řešení pro zákazníky. Materiály pro vývoj a výrobu produktů jsou zpracovávány ekologicky a velmi šetrně (Langmatz CZ, 2023a). Firma získala pro svá inovativní řešení několik cen, například se v roce 2016 umístila na 2. místě v kategorii Zdravý management, ocenění jí udělila německá zdravotní pojišťovna AOK Bayern a v roce 2015 se umístila mezi prvními třemi v kategorii Recyklace a náhradní zdroje v GreenTec Award (Langmatz CZ, 2023a).

5 Projekt implementace GDPR ve firmě

Jak vychází z teoretické části této práce, přijetí GDPR přineslo pro v zásadě všechny podniky nové povinnosti, které musely zařadit do svého běžného provozu. Problematika, jíž se podniky zabývaly, byla představena v teoretické části práce. Praktická část bude věnována tomu, jak projekt implementace GDPR probíhal ve společnosti Langmatz CZ s.r.o.

Informace nezbytné k zpracování bakalářské práce byly získány prostřednictvím rozhovoru s prokuristkou a personální vedoucí firmy. Dále byly využity interní firemní dokumenty jako interní předpis pro ochranu osobních údajů k podpoře a doplnění dat získaných z rozhovorů.

Cílem projektu byla implementace GDPR do firmy Langmatz CZ s.r.o. tak, aby byl zajištěn soulad zpracování osobních údajů probíhající ve firmě s tímto nařízením. Implementace GDPR znamená zavedení procesů a opatření, které zajistí dodržování požadavků GDPR (Nezmar, 2017). Implementace probíhala nezávisle na mateřské společnosti Langmatz GmbH, které však byly poskytovány všechny relevantní informace o jejím průběhu. Projekt byl zahájen v dubnu roku 2017 s dokončením v květnu 2018 tak, aby do 25. května 2018 byly splněny všechny požadavky GDPR, a nedošlo tak k případným sankcím. Zahájení proběhlo jmenováním projektového týmu. Za projekt odpovídalo vedení firmy, konkrétně prokuristka firmy a personální vedoucí. Ty zároveň tvořily lidské zdroje pro tento projekt. Finanční zdroje byly po určení rozsahu projektu vymezeny částkou 120 tis. Kč. Rozpočet byl sestaven na základě odhadu a průzkumu trhu. Projektový tým nejprve vytvořil seznam předpokládaných nákladových položek a na základě tohoto seznamu prostřednictvím internetových stránek získal přibližné ceny jednotlivých položek – školení, nákup uzamykatelných skříní, apod. Odhadem byly stanoveny mzdové náklady, přičemž bylo předpokládáno, že analýza a implementace potrvají 20 dní a hodinová mzda pro jednoho člena projektového týmu je 250 Kč.

Jako hlavní riziko projektu firma vyhodnotila možný nesoulad s GDPR, kdy by i přes zavedení nových procesů a úpravu stávajících procesů týkajících se osobních údajů, mohlo dojít k pochybení, což by mohlo vést k narušení práv subjektů údajů a vysokým pokutám a sankcím ze strany dozorových orgánů. Toto riziko by mělo vážné finanční důsledky pro podnik.

5.1 Předprojektová fáze

Projektový tým nejdříve posuzoval možnosti implementace – interní implementaci a implementaci prostřednictvím externí firmy. I přesto, že se na trhu po publikování GDPR objevila spousta firem, která nabízela analýzu současného stavu a zavedení GDPR na míru, vedení podniku se vzhledem k velikosti firmy a menšímu rozsahu povinností rozhodlo, že implementace bude probíhat samostatně.

Začátkem roku 2018 se prokuristka firmy zúčastnila školení zaměřeného na GDPR. Vedení firmy se rozhodlo pro školení poskytované externí školitelkou, s níž mělo již v minulosti pozitivní zkušenosti. Školení poskytlo prokuristce komplexní pohled na problematiku GDPR z teoretického i praktického hlediska. Kromě toho firma investovala do informačních materiálů, které přispěly k lepšímu pochopení této problematiky, zejména z praktické perspektivy. Projektový tým se následně detailně seznámil s GDPR a dalšími relevantními právními předpisy a vyhláškami.

Na základě předchozího kroku, tedy seznámení se s požadavky GDPR, proběhla GAP analýza, při níž bylo projektovým týmem jasně definováno, jaké osobní údaje firma zpracovává, za použití jakých nástrojů nebo technologií, jaké osoby k nim mají přístup a jak jsou osobní údaje uchovávány a chráněny. Analyzovány byly oblasti IT bezpečnosti, osobní bezpečnosti, webů, dokumentů, personalistiky, vnitřních předpisů, předávání dat a přístupových práv a odpovědností. Následně byly výsledky této analýzy porovnány s požadavky GDPR, což umožnilo identifikovat nedostatky v dosavadních procesech práce s osobními údaji ve srovnání s požadavky GDPR.

Firma také musela posoudit, zda musí provádět i některou z nových povinností, které GDPR přinesla. Tyto povinnosti byly detailně popsány v kapitole Nové povinnosti pro podnik. Jde o povinnost vedení záznamů o činnostech, zabezpečení osobních údajů, provádění posouzení vlivu na ochranu osobních údajů a jmenování pověřence pro ochranu osobních údajů. Z výkladu teoretické části týkající se záznamů o činnostech, vyplývá, že firma není povinna je vést, protože nemá více než 250 zaměstnanců. Firma nemusela provádět posouzení vlivu, protože nespadá ani pod jeden z případů uvedených v kapitole DPIA a nemusela jmenovat pověřence pro ochranu osobních údajů, protože opět nesplňuje podmínky pro jeho jmenování, které jsou konkrétně jmenovány v kapitole Jmenování pověřence. Jedinou dodatečnou aktivitou, kterou firma musela při implementaci zvážit, bylo zajištění dostatečné ochrany osobních údajů, která je

klíčovým prvkem v každé společnosti. Výsledkem vstupní analýzy byla tabulka obsahující nedostatky v oblasti ochrany osobních údajů, která je uvedena níže. Prostřednictvím analýzy bylo například zjištěno, že pro kategorie osobních údajů chybí určit účel a rozsah, osobní údaje je třeba minimalizovat, je potřeba informovat zaměstnance a obchodní kontakty o jejich právech a to prostřednictvím vnitřního předpisu o ochraně osobních údajů pro zaměstnance a obecného informačního dokumentu pro ostatní osoby.

Tab. 1 Seznam neshod, zjištěných při GAP analýze a jejich nápravná opatření

Neshoda	**Nápravné opatření**
Není uveden účel a rozsah pro zpracování osobních údajů pro jednotlivé kategorie subjektů údajů	Doplnění účelů a rozsahů pro zpracování osobních údajů všech kategorií subjektů údajů
Nadbytečné shromažďování osobních údajů	Minimalizace osobních údajů, výmaz/skartace, vytvoření informačního dokumentu ohledně doby uchovávání dokumentů s osobními údaji
Přístup do některých počítačů není na základě individuálního přihlašovacího jména a hesla	Každý zaměstnanec, který ke své práci potřebuje počítač, získá jedinečné přihlašovací jméno a heslo
Nejsou určena možná rizika, která mohou ohrozit osobní údaje	Vytvoření seznamu rizik a naleznutí způsobu jak je eliminovat
Dokumenty obsahující osobní údaje nejsou dostatečně zabezpečeny	Nákup zamykatelných skříní, zavedení bezpečnostních opatřeních pro práci s dokumenty v elektronické podobě
Návštěvníci webových stránek nejsou informování o ukládání souborů cookies	Požádání externí firmy, která spravuje webové stránky o doplnění informací o ukládání souborů cookies
Chybí informace pro subjekty údajů o jejich právech	Zařízení školení pro zaměstnance a zahrnutí těchto informací do vnitřního předpisu o ochraně osobních údajů

Chybí souhlas pro zaznamenávání otisku prstů pro potřeby docházky	Vytvoření souhlasu s identifikací otisku prstu kvůli evidenci docházky a podepsání souhlasu již stávajícími zaměstnanci
Chybí souhlasy se zpracováním osobních údajů pro marketingové účely, dotazníky, kopie občanských průkazů a kartiček pojišťovny	Vytvoření souhlasu se zpracováním osobních údajů
Chybí kontrolní mechanismus	Stanovení postupů pro kontrolu zacházení s osobními údaji
Chybí vnitřní předpis o ochraně osobních údajů	Vytvoření vnitřního předpisu o ochraně osobních údajů, ve kterém budou shrnuty všechny postupy firmy a důležité informace pro zaměstnance

Zdroj: (Langmatz CZ, 2018), zpracováno autorkou

5.2 Rozsah projektu

Pro dosažení souladu s GDPR firma musela odstranit zjištěné nedostatky. Na základě tabulky shrnující nedostatky při zacházení s osobními údaji, vznikl plán činností, které pro soulad s GDPR byly nutné splnit. Tento plán určoval rozsah projektu. Mezi tyto činnosti, uvedené v logickém pořadí, patří:

- určení účelu a rozsahu pro jednotlivé kategorie subjektů údajů,
- minimalizace osobních údajů,
- vytvoření pravidel zpracování osobních údajů a vypracování nových interních směrnic a dokumentů,
- vytvoření souhlasu se zpracováním osobních údajů,
- úprava listin,
- zabezpečení osobních údajů na základě zjištěných rizik,
- kontrola,
- školení.

Firma se již před rokem 2016 řídila podle předpisu ISO 27001, který upravuje informační bezpečnost, a dodržovala zákon 101/2000 Sb., který v té době platil. Díky tomu byla

pro firmu implementace GDPR snazší, protože některé požadavky byly splněny ještě před samotnou implementací.

V rámci implementace byla provedena také úprava webových stránek, za kterou byla zodpovědná externí firma, která webové stránky firmy spravuje. Firma Langmatz CZ pouze na web doplnila dokument o ochraně osobních údajů, který je široké veřejnosti na stránkách dostupný.

5.3 Určení účelu osobních údajů

U všech kategorií subjektů údajů, musel být určen účel a právní důvod pro zpracování jejich osobních údajů. Tyto kategorie měla firma zavedeny již před GDPR, kvůli přehlednosti. Firma Langmatz CZ s.r.o. zpracovává osobní údaje zaměstnanců, žadatelů, obchodních kontaktů a také online uživatelů. Firma ve všech případech zpracování vystupuje jako správce i zpracovatel osobních údajů a ani u jedné kategorie subjektů údajů nepředává žádné osobní údaje do třetích zemí.

Zaměstnanci

Firma určila, že osobní údaje zaměstnanců, budou zpracovávány pouze v případě, že souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních pracovníků, se sociálním a zdravotním pojištěním a dále také osobní údaje, které jsou nezbytné pro plnění právní povinnosti a ochranu oprávněných zájmů firmy. Firma tedy uchovává pouze nezbytně nutné osobní údaje, mezi které patří například jméno a příjmení, datum narození, rodné číslo, trvalé bydliště a kontaktní osoba, rodinný stav, e-mailová adresa a telefonní číslo, v případě sociálního a zdravotního pojištění jsou to údaje jako dosažení vzdělání, délka praxe, funkční zařazení a v případě mzdové agendy jsou potřebné informace o pobíraném důchodu (zaměstnanec má nárok na slevu na dani) nebo o nařízené exekuci (zaměstnavatel musí částku ze mzdy posílat za zaměstnance). Pro potřeby docházky firma identifikuje zaměstnance pomocí otisku prstu, ke kterému potřebuje od každého zaměstnance souhlas.

V případě uchazečů o zaměstnání firma postupuje tak, že již v inzerátu uvede, že pro potřeby výběrového řízení zpracovává osobní údaje uchazečů a posláním životopisu uchazeč souhlasí se zpracováním osobních údajů. Výjimkou je uchazeč, který přichází přímo do firmy, aniž by předtím zaslal životopis on-line. V takovém případě musí uchazeč podepsat souhlas se zpracováním osobních údajů. V případě, že je uchazeč

vybrán na danou pozici, podepíše pracovní smlouvu a tím pádem zaniká nutnost souhlasu pro zpracování osobních údajů, protože má firma k zpracování právní důvod. Poskytnuté osobní údaje uchazečů firma uchovává pouze na dobu skutečně nutnou, takže pouze do skončení výběrového řízení, poté jsou dokumenty zlikvidovány, v případě, že uchazeč nebyl na danou pracovní pozici vybrán.

Žadatelé

Žadateli jsou myšleny osoby, či společnosti, které od firmy Langmatz CZ s.r.o. poptávají informace na základě vyplnění kontaktního formuláře skrze webové stránky firmy nebo přímým kontaktováním firmy e-mailem.

Firma určila, že účelem pro shromáždění a zpracování osobních údajů žadatelů je zpracování žádosti, zkouška vhodnosti a kontaktování. Právním základem pro zpracování je pak provedení předsmluvních opatření, která jsou provedena na žádost dotčené osoby, nebo dobrovolný souhlas dotčené osoby, to je případ odpovídajícího prohlášení o záměru. Příjemcem osobních údajů žadatelů může být zaměstnanec s účelovým oprávněním, úvěrová instituce, v případě platební transakce, nebo externí dodavatel, při zpracování objednávek.

Obchodní kontakty

Obchodními kontakty jsou myšleny kontaktní osoby zákazníků, dodavatelů, poskytovatelů služeb a partnerů. Obvyklé osobní údaje, které jsou pro tuto kategorii zpracovávány: jméno, příjmení, firemní příslušnost, případně oddělení, telefonní číslo a e-mailová adresa.

Účelem pro shromažďování a zpracovávání osobních údajů obchodních kontaktů je udržování obchodních kontaktů a zpracování transakcí. Právní základ pro zpracování se liší v závislosti na fázi daného kontaktu. Lze předpokládat tyto právní základy: provedení (i) předsmluvních opatření, která jsou prováděna na žádost dotčené osoby; dotčená osoba dobrovolně souhlasí – to je případ odpovídajícího prohlášení o záměru; zpracování je nezbytné k plnění smluvních povinností (jako jsou služby); pokud je to nutné, tak ochrana oprávněných zájmů.

Příjemcem osobních údajů obchodních kontaktů může být stejně jako u žadatelů zaměstnanec s účelovým oprávněním, úvěrová instituce nebo externí dodavatel.

On-line uživatelé

Při návštěvě webových stránek firmy uživatel přenáší z technických důvodů data přes internetový prohlížeč. Tyto data jsou během probíhajícího spojení zaznamenávána mezi daným internetovým prohlížečem a poskytovatelem. Jde o datum a čas žádosti, název požadovaného souboru, použitý webový prohlížeč a URL adresa a úplná IP adresa počítače. Tyto data firma uchovává z důvodu případné spolupráce s Policií ČR jeden rok.

V případě, že návštěvník prostřednictvím webu požádá o kontakt nebo kontaktuje firmu e-mailem, firma shromažďuje a zpracovává tyto osobní údaje pro účely žádosti.

5.4 Minimalizace osobních údajů

Po určení účelu zpracování osobních údajů, proběhla minimalizace osobních údajů. Firma byla povinna zdůvodnit, proč potřebuje konkrétní osobní údaje pro své fungování a v případě zjištění, že některé údaje nejsou nezbytné, byla povinna je zlikvidovat. Firma zlikvidovala dokumenty s osobními údaji, které již dále neměla potřebu uchovávat – jednalo se například o vstupní dotazníky bývalých zaměstnanců, jejich životopisy, kopie jejich občanských průkazů a průkazů zdravotních pojišťoven, které buď, v případě listinných dokumentů, byly skartovány, nebo v případě elektronických dokumentů, smazány.

Firma není oprávněna ihned po skončení pracovního poměru odstranit všechny dokumenty související s bývalým zaměstnancem, neboť podléhají různým právním předpisům, jako je například zákon o organizaci a provádění sociálního zabezpečení. Pro zlepšení transparentnosti a organizace má firma vypracovanou tabulku, která stanovuje lhůty pro smazání dokumentů obsahujících osobní údaje. Z důvodu obsáhlosti tabulky, je níže uvedena pouze její část.

Tab. 2 Archivační lhůta pro některé dokumenty

Dokument	**Archivační lhůta**
Dokumenty, týkající se vzniku a zániku pracovněprávního vztahu	30 let
Informace o docházce	3 roky
Dokumenty, které se týkají provedených srážek ze mzdy	30 let po roce, kterého se týkají

Prohlášení k dani, žádost o roční zúčtování	10 let po roce, kterého se týkají
Evidenční listy důchodového pojištění	3 roky po roce, kterého se týkají
Doklady, týkající se nemocenského pojištění	10 let po roce, kterého se týkají
Vnitřní předpis	10 let po ukončení jeho platnosti

Zdroj: (Langmatz CZ, 2021), zpracováno autorkou

Firma ve výrobním oddělení využívá kamerový systém pro zajištění bezpečnosti zaměstnanců. Zaměstnanci podepsali souhlas s tímto nahráváním prostřednictvím prohlášení o bezpečnosti práce, který byl s ohledem na GDPR aktualizován. Tyto kamerové záznamy se ukládají. Dříve byla doba ukládání těchto kamerových záznamů jeden měsíc. Při analýze stávajícího stavu vedení firmy došlo k závěru, že záznamy není nutné uchovávat celý měsíc a dobu zkrátilo na 20 dní.

5.5 Tvorba a úprava dokumentů

Tvorba a úprava dokumentů je pro firmu klíčová hlavně z toho důvodu, že se prostřednictvím těchto dokumentů projevují změny, které byly během implementace přijaty.

5.5.1 Tvorba souhlasu se zpracováním osobních údajů

Ve většině případů firma zpracovává osobní údaje na základě právního důvodu uzavření smlouvy. Nicméně, při analýze bylo zjištěno, že některá zpracování nemají daný právní důvod a bude pro ně potřeba vytvořit souhlas se zpracováním osobních údajů.

Firma vytvářela pět nových souhlasů se zpracováním osobních údajů. První dva souhlasy byly vytvořeny pro zaměstnance firmy. První se týkal souhlasu s identifikací pomocí otisku prstu pro evidenci docházky. Otisk prstu patří mezi biometrický údaj a řadí se mezi zvláštní kategorii osobních údajů. Pro zvláštní kategorii osobních údajů platí, že podnik musí mít vždy výslovný souhlas subjektu údajů pro jejich zpracování (Nezmar, 2017). Druhý souhlas se týkal vytvoření kopie občanského průkazu a kartičky zdravotní pojišťovny. V případě zákazníků byly vytvářeny dva souhlasy se zpracováním osobních údajů – první se týkal zasílání marketingových nabídek a druhý se týkal zasílání dotazníků

pro získání zpětné vazby. Poslední souhlas se vytvářel pro potencionální zaměstnance, kteří podpisem dávají souhlas k použití osobních údajů za účelem výběrového řízení. Uchazeč podepíše souhlas a vyplní dotazník, aby ho mohla firma v případě zájmu kontaktovat.

Každý souhlas obsahuje informaci o tom, jak dlouho bude uchováván, jaké práva subjekt údajů má a také je na něm uvedeno, že subjekt údajů, může svůj souhlas se zpracováním osobních údajů kdykoliv odvolat.

5.5.2 Vnitřní předpis o ochraně osobních údajů

Pro potřeby firmy byl vytvořen vnitřní předpis o ochraně osobních údajů, který shrnuje základní informace pro zaměstnance. V tomto předpise jsou vyjádřena:

- obecná ustanovení – úvod, název firmy a adresa, kontakt na osoby, které jsou odpovědné za zpracování osobních údajů a v jaké situaci je vhodné se na ně obrátit,
- působnost – informace o tom, že předpis upravuje postupy firmy při zpracování osobních údajů a pravidla pro zachování všech právních zásad za účelem zajištění souladu s požadavky GDPR,
- zásady nakládání s osobními údaji – vysvětlení zásad pro zpracování osobních údajů
- postupy firmy – konkrétní činnosti, které zaměstnanci musí v rámci souladu zpracování osobních údajů s GDPR vykonávat,
- organizační opatření k ochraně osobních údajů – jak se s osobními údaji ve firmě má zacházet,
- pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů,
- některé povinnosti firmy při zpracování osobních údajů.

Předpis je průběžně aktualizován na základě výsledků kontrol, nebo v případě, že firma přijde na efektivnější postup při zpracování a ochraně osobních údajů.

5.5.3 Ostatní dokumenty

V případě pracovních smluv byl přidán dodatek o zpracování osobních údajů, který je k vidění na

Obr. 4 . Tento dodatek je v pracovní smlouvě nadbytečný kvůli tomu, že firma má pro zpracování osobních údajů zaměstnance právní důvod – plnění smlouvy.

Obr. 4 Dodatek v pracovní smlouvě

9. Ostatní práva a povinnosti smluvních stran vyplývající z této pracovní smlouvy se řídí ustanoveními zákoníku
práce a dalšími předpisy upravujícími pracovněprávní vztahy.
Další ujednání:
- zaměstnanec souhlasí, že jím uvedené osobní údaje budou shromažďovány a dále zpracovávány pro potřeby personálního a mzdového výkaznictví
- zaměstnanec může být zaměstnavatelem vyslán na pracovní cestu
- zaměstnanec byl seznámen s BOZP, PO a vnitřními předpisy

V Klatovech dne .....

podpis zaměstnance/zák.zástupce razítko zaměstnavatele a podpis

....

Zdroj: Langmatz CZ (2024)

Vstupní dotazníky byly rozšířeny o výše zmíněný souhlas se zpracováním osobních údajů pro zaznamenávání otisku prstu a o souhlas s vytvořením kopie občanského průkazu a kartičky zdravotní pojišťovny. V případě kodexu chování společnosti Langmatz CZ s.r.o. byla přidána kapitola o ochraně osobních údajů.

Kromě vnitřního předpisu, který je určen pro zaměstnance, vytvořila firma také obecný dokument o ochraně osobních údajů, který je určen pro externí subjekty, ve kterém jsou uvedeny všechny důležité informace o tom, pro jaké účely jsou jejich osobní údaje zpracovávány, jaký je právní důvod pro jejich zpracování, kdo může být příjemcem těchto osobních údajů a jak dlouho jsou jejich osobní údaje uloženy, nebo jaká jsou pravidla pro jejich mazání na základě kategorie, do které patří.

5.6 Zabezpečení osobních údajů

Zabezpečení osobních údajů je ve firmě Langmatz CZ klíčovým prvkem pro ochranu důvěrnosti a integrity informací. Firma osobní údaje, které zpracovává, chrání vhodnými a dostupnými prostředky před jejich zneužitím a osoba, která je za zpracování odpovědná, dbá na uchování osobních údajů v předem určených prostorách nebo v systému. Z důvodu zpracovávání osobních údajů zaměstnanců firmy, musela personalistka podepsat upravenou dohodu o mlčenlivosti, ochraně důvěrných informací a zákazu jejich zneužití, která byla na základě nařízení GDPR rozšířena. Podpisem dohody se personalistka zavázala k dodržování technických a organizačních opatření přijatých zaměstnavatelem pro zajištění dostatečné úrovně zabezpečení informací, které odpovídají danému riziku.

5.6.1 Bezpečnostní rizika

Aby byly osobní údaje zpracovávané ve firmě dostatečně chráněny, bylo potřeba snížit pravděpodobnost vzniku incidentů nebo porušení zásad ochrany údajů. Firma nejdříve sestavila seznam rizik, do kterého zařadila rizika jako je náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněný přístup k předávaným, uloženým nebo jinak zpracovávaným osobním údajům, nebo přístupu k nim. V seznamu jsou také rizika spojená s třetí stranou, která by mohla být rizikem pro osobní údaje. Jde hlavně o kybernetické útoky, jako je například phishing nebo ransomware, útok na webové stránky, který by mohl mít za důsledek neoprávněné získání nebo poškození osobních údajů.

5.6.2 Zabezpečení tištěných dokumentů

Většina zpracovávaných osobních údajů ve firmě je vedena manuálně a je trvale uzamčena ve skříních v kancelářích k tomuto účelu určeným. Přístup k nim má pouze osoba odpovědná za zpracování osobních údajů - prokuristka a personalistka firmy. Osoba odpovědná za zpracování osobních údajů nesmí nechat dokumenty obsahující osobní údaje na libovolném místě a musí se postarat o to, že v případě odchodu z pracovního místa, budou dostatečně zabezpečeny.

5.6.3 Zabezpečení dokumentů v elektronické podobě

Před implementací se ve firmě využívalo přihlašování do většiny počítačů prostřednictvím jednotného přihlašovacího jména a hesla. Přestože šlo většinou o počítače ve výrobě, firma během implementace přidělila každému zaměstnanci, který pro svou práci počítač využívá, jedinečné přihlašovací jméno a heslo.

Osoba, která je zodpovědná za zpracování osobních údajů, nesmí odejít ze svého pracoviště bez toho, aby svůj počítač uzamkla nebo odhlásila. Do jejího počítače také nesmí nahlížet jiné osoby a v případě podezření na odhalení hesla, ho musí ihned změnit.

Firma se také v rámci ochrany osobních údajů rozhodla, že nebude elektronické dokumenty obsahující osobní údaje ukládat na cloud, a zakoupila externí datové úložiště pro zálohování těchto dokumentů. Kromě toho zavedla další technická opatření pro ochranu elektronických dokumentů firmy, jako je šifrování, antivirus a firewall, pravidelná aktualizace operačního systému, pravidla pro e-maily (mazání spamu a neotevírání nevyžádané pošty) a servis zabezpečení wi-fi.

5.6.4 Postup při podezření o porušení GDPR

Uplatněnou žádost subjektu údajů, která se týká jeho práva, řeší osoba odpovědná za zpracování osobních údajů. Každý bezpečnostní incident musí osoba odpovědná za zpracování osobních údajů řešit bezodkladně do 72 hodin od jeho zjištění. V případě, že je nepravděpodobné, že by porušení mělo za následek riziko pro práva subjektů údajů, porušení neohlašuje dozorovému orgánu. V případě, že by porušení mohlo nést riziko pro práva fyzických osob, dítěte, zaměstnance, zákonného zástupce či jiné osoby, informuje danou osobu a sdělí, jaká opatření byla přijata pro nápravu. O každém incidentu musí být sepsán záznam a o každém závažném incidentu firma informuje Úřad pro ochranu osobních údajů.

5.7 Kontrola

Jedním z velmi důležitých aspektů implementace GDPR je také následná kontrola. Přestože projekt, jako takový, skončil již v roce 2018, je potřeba pravidelně ověřovat, zda firma dodržuje zavedené postupy a zpracování osobních údajů je opravdu v souladu GDPR. První kontrola proběhla bezprostředně po skončení implementace, nejprve firmou Langmatz CZ a následně kontrolu provedla i mateřská firma Langmatz GmbH prostřednictvím bezpečnostního auditu.

Bezpečnostní audit prováděný mateřskou firmou je součástí pravidelných ročních kontrol. Kromě toho jsou v průběhu roku prováděny i namátkové kontroly obvykle jednou nebo dvakrát měsíčně, s cílem ověřit, zda jsou dodržovány stanovené postupy uvedené ve vnitřním předpisu o ochraně osobních údajů. Jednou za dva roky probíhá také audit na ISO, při kterém je kontrolována míra ochrany osobních údajů.

Osoba, která je za zpracování osobních údajů odpovědná, jednou ročně provádí zhodnocení všech procesů při nakládání a zpracování osobních údajů. Pokud zjistí, že jsou některé firemní postupy zastaralé, zbytečné, nebo se neosvědčily, učiní bezodkladně nápravu.

5.8 Školení zaměstnanců

Po implementaci GDPR a následné kontrole, bylo nutné provést školení pro zaměstnance, kteří se na implementaci nepodíleli. Školení bylo uspořádáno interně a vedly ho prokuristka firmy a personální vedoucí. Pro účely školení byl využit vnitřní předpis o ochraně osobních údajů, který obdržel každý zaměstnanec. Nejdůležitější body byly shrnuty v prezentaci, která byla rozdělena na dvě části. První část se zaměřovala na teorii, zaměstnancům bylo například vysvětleno, co jsou osobní údaje a jaké jsou zásady pro jejich ochranu, jaká jsou jejich práva v oblasti zpracování osobních údajů a jaké jsou právní důvody zpracování, včetně vysvětlené problematiky souhlasu se zpracováním osobních údajů. Druhá část se zaměřovala na GDPR z praktického hlediska. Zaměstnancům bylo detailně vysvětleno, jaká opatření firma přijala, jaké změny GDPR přineslo a jak mohou zaměstnanci sami nejlépe chránit své osobní údaje.

V prvních třech letech po přijetí GDPR, se díky každoročnímu bezpečnostnímu auditu, odhalilo několik nedostatků, které byly odstraněny prostřednictvím úpravy vnitřního předpisu o ochraně osobních údajů. V této době se školení konalo každý rok. Momentálně

se zaměstnanci školí každé dva roky, s ohledem na to, že v nedávné době nebyly zjištěny žádné nesrovnalosti. V případě, že by se nějaká nesrovnalost odhalila, školení by opět probíhalo každoročně. V případě, že do firmy nastupuje nový zaměstnanec, je poučen o problematice zpracování osobních údajů při podpisu smlouvy.

5.9 Zhodnocení a doporučení

Zhodnocení projektu

Projekt implementace GDPR ve firmě Langmatz CZ s.r.o. proběhl bez větších komplikací. Byl ukončen na začátku května 2018 a následně byla provedena kontrola procesů spojených s osobními údaji, která ukázala, že firma nakládá s osobními údaji v souladu s GDPR a tím pádem byl naplněn stanovený cíl. Projekt stál firmu necelých sto tisíc korun, takže byl dodržen předem stanovený rozpočet.

Tab. 3 Porovnání předpokládaných nákladů a reálných nákladů

Položka nákladů	**Předpokládané náklady [Kč]**	**Reálné náklady [Kč]**
Mzdové náklady	75 000	60 000
Školení	4 000	3 300
Nákup informačních materiálů	2 000	1 200
Nákup uzamykatelných skříní	32 000	28 500
Nákup externího datového úložiště	6 000	4 700
Úprava webových stránek	1 500	1 500
Celkem	**120 500**	**99 200**

Zdroj: Vlastní zpracování

Skutečné náklady projektu byly oproti plánu výrazně nižší, zejména díky mzdovým nákladům. Bylo to z důvodu, že projektový tým dokončil analýzu a implementaci za 16 dní, místo původně plánovaných 20 dnů. Projektový tým zároveň každé položce

přiřadil alespoň nějakou rezervu, kromě úpravy webových stránek, která byla domluvena již před samotným projektem implementace.

Zhodnocení věcné stránky implementace

Přestože byl projekt zhodnocen jako zdařilý, během analýzy bylo identifikováno několik oblastí, ve kterých je třeba provést dodatečné úpravy. Na základě zjištěných informací lze konstatovat, že jsou některé činnosti prováděny nadbytečně a nemusí být považovány v souladu s GDPR. Dodatek o souhlasu se zpracováním osobních údajů v pracovní smlouvě by měl být vymazán z důvodu existence právního důvodu pro zpracování osobních údajů. Dalším případem je uchovávání kopií občanského průkazu a kartičky zdravotní pojišťovny, které GDPR není výslovně zakázáno, ale při analýze nebyl zjištěn důvod, proč by firma tyto kopie měla uchovávat, z důvodu jejich evidence v elektronické podobě, v mzdovém účetnictví.

Při analýze bylo také zjištěno, že firma nemá vypracovaný konkrétní plán, jak postupovat v případě, kdy by došlo k porušení zabezpečení osobních údajů. Firma od roku 2018 neřešila zatím ani jeden případ porušení zabezpečení osobních údajů, takže konkrétní postup nebyl potřebný. Kvůli tomu, že se v případě porušení musí jednat co nejrychleji, by mohl plán v tomto případě usnadnit firmě práci.

Postup při porušení závisí na závažnosti daného porušení. V případě, kdy je pravděpodobné, že porušení ohrožuje práva a svobody fyzických osob, musí podnik informovat do 72 hodin dozorový úřad (Evropský parlament a Rada EU, 2016). Před ohlášením je Úřadem pro ochranu osobních údajů doporučeno seznámit se s Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení 2016/679 pracovní skupiny WP29, která je současně Evropským sborem pro ochranu osobních údajů a s Pokyny č. 01/2021 k příkladům týkajícím se ohlašování porušení zabezpečení osobních údajů (Úřad pro ochranu osobních údajů, n. d.).

Stejně tak je potřeba tuto skutečnost co nejdříve nahlásit subjektu údajů. Informace pro dozorový úřad a subjekt údajů by měla obsahovat popis povahy porušení, jméno a kontaktní údaje na místo, které může poskytnout více informací, popis možných následků porušení a popis opatření, která podnik přijal k nápravě daného porušení. V některých případech však subjekt údajů nemusí být o porušení informován. Jedná se například o případ, kdy osobní údaje, které byly dotčeny porušením, byly dostatečně ochráněny technickými a organizačními opatřeními, jako je například šifrování, které osobní údaje

pro ostatní dělá nesrozumitelnými. Dalším případem může být situace, kdy správce přijal určitá opatření, která sníží riziko pro fyzické osoby. V neposlední řadě jde o případ, kdy by informování subjektu údajů bylo až moc obtížné (Evropský parlament a Rada EU, 2016).

V případě, kdy dojde k porušení, které nenese vysoké riziko, správce pouze zavede nápravná opatření a zaznamená tento incident do dokumentace všech porušení, která obsahuje informace o příčinách porušení, popis – jaké osobní údaje byly dotčeny, jaké byly důsledky tohoto porušení a na závěr musí být evidováno, jaká nápravná opatření byla přijata. Případně je potřeba napsat i zdůvodnění, proč nedošlo k nahlášení (GDPR Solutions, n. d.).

Závěr

Cílem této bakalářské práce bylo analyzovat projekt implementace GDPR ve společnosti Langmatz CZ, zhodnotit ho a na základně zhodnocení navrhnout možná zlepšení, která by společnosti pomohla v efektivnějším dodržování GDPR.

Přestože projekt proběhl již před několika lety, je pro firmu velmi důležité věnovat pozornost problematice i nadále. V teoretické části byl zmíněn koncept Data Privacy Framework, který upravuje předávání osobních údajů mezi Evropskou Unií a Spojenými státy americkými. Ten vzešel v platnost v červenci roku 2023 jako náhrada za dříve zrušený Privacy Shield. Tento fakt poukazuje na důležitost sledovat i nadále vývoj ochrany osobních údajů a nedůvěřovat pouze dříve nabytým znalostem v této oblasti.

Teoretická část byla věnována problematice projektového řízení a GDPR, dále byl také představen možný přístup k projektu implementace GDPR do společnosti. Praktická část představila firmu Langmatz CZ a následně byl popsán průběh projektu implementace GDPR v této firmě. Na závěr byl projekt zhodnocen a byla navrhnuta možná zlepšení.

Prostřednictvím praktické části bylo zjištěno, že projekt implementace GDPR ve společnosti Langmatz CZ proběhl úspěšně, protože splnil požadovaný cíl, kterým bylo zajištění souladu zpracování osobních údajů ve firmě s GDPR. Zároveň byl dodržen stanovený rozpočet a termín dokončení. Přestože projekt splnil stanovený cíl, byly nalezeny oblasti, ve kterých firma má jisté nedostatky a mohly by být problematické v případě kontroly. Těmito oblastmi byla nadbytečnost souhlasu se zpracováním osobních údajů, který by měl být vymazán a uchovávání kopií občanských průkazů a kartiček zdravotní pojišťovny, které by z důvodu minimalizace uchovávaných osobních údajů měly být zlikvidovány. Doporučením, které by mohlo zefektivnit postup při porušení ochrany osobních údajů, je vypracování konkrétního plánu postupu.

Na základě této analýzy může podnik provést úpravy ve svém postupu dodržování GDPR.

Seznam použitých zdrojů

Benešová, T., Málek, J., & Šulc, R. (2023). *Předávání osobních údajů do třetích zemí*. Právní prostor. https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/predavani-osobnich-udaju-do-tretich-zemi

Byznys (2018). *Implementace GDPR*. https://www.byznys.eu/cs-cz/podpora/implementace-gdpr

Černovský, T. (2021). *GDPR cookie lišta na webu: je nutná v roce 2023?* https://www.cernovsky.cz/weby-e-shopy/gdpr-cookie-lista-na-webu/

Drábek, L. (2023). *TikTok dostal od EU rekordní pokutu: Porušil prý ochranu osobních údajů dětí.* CDR. https://cdr.cz/clanek/tiktok-dostal-od-eu-rekordni-pokutu-porusil-pry-ochranu-osobnich-udaju-deti

Doležal, J., Lacko, B., Hájek, M., Cingl, O., Krátký, J., & Hrazdilová Bočková, K (2016). *Projektový management: komplexně, prakticky a podle světových standardů*. Grada Publishing.

Doležal, J., & Krátký, J. (2017). *Projektový management v praxi: Naučte se řídit projekty!* Grada Publishing.

Evropská rada & Rada Evropské unie (n. d.). *Ochrana údajů v EU*. Dostupné 1. 4. 2024 z https://www.consilium.europa.eu/cs/policies/data-protection/

Faifr, A., Januška, M. (2021). Factors determining the extent of GDPR implementation within organizations: empirical evidence from Czech Republic. *Journal of Business Economics and Management*. *22*(5), 1124-1141. https://otik.uk.zcu.cz/handle/11025/45518

Fišer, M. (2023). *Meta není jediná. Za porušení GDPR platily obří pokuty Google i Amazon.* Novinky.cz. https://www.novinky.cz/clanek/internet-a-pc-meta-neni-jedina-za-poruseni-gdpr-platily-obri-pokuty-google-i-amazon-40432435

GDPR Solutions (n. d.). Jak postupovat při porušení zabezpečení osobních údajů. Dostupné 9. 4. 2024 z https://www.gdprsolutions.cz/poruseni-zabezpeceni/

Chlebus, T., & Dostál, J. (2019). *Nový zákon o zpracování osobních údajů*. Epravo. https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html

Ilavská, M, (2019). *Najčastejšie porušenia GDPR v praxi a pokuty*. i-Secure. https://www.isecure.sk/sk/aktuality/za-ake-porusenie-gdpr-mozu-firmy-dostat-pokuty.html

IT Governance Privacy Team. (2017). EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide (2. vyd.). IT Governance Publishing.

Janečková, E. (2018). *GDPR: praktická příručka implementace*. Wolters Kluwer.

Jouza, L. (2018). *Nařízení o ochraně osobních údajů (GDPR) v pracovněprávní praxi*. Bulletin-advokacie. http://www.bulletin-advokacie.cz/narizeni-o-ochrane-osobnich-udaju-gdpr-v-pracovnepravni-praxi

Justice.cz (2023). *Účetní závěrka firmy Langmatz CZ za rok 2022*. Dostupné 26. 2. 2024 z https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=75474829&subjektId=666947&spis=481781

Koch, R. (n. d.). *Cookies, the GDPR, and the ePrivacy Directive*. GDPR. Dostupné 8. 1. 2024 z https://gdpr.eu/cookies/

Kramer, J. (2018). *Začernit rodné číslo nestačí. Vhodnější je osobní údaje šifrovat*. Ekonom. https://pravniradce.ekonom.cz/c1-66071330-zacernit-rodne-cislo-nestaci-vhodnejsi-je-osobni-udaje-sifrovat

Křížová, V. (2018). *GDPR – základní postup v praxi*. Epravo. https://www.epravo.cz/top/clanky/gdpr-zakladni-postup-v-praxi-107200.html

Kuchař, R. (2018). *Využití oprávněného zájmu na zpracování osobních údajů podle GDPR*. Epravo. https://www.epravo.cz/top/clanky/vyuziti-opravneneho-zajmu-na-zpracovani-osobnich-udaju-podle-gdpr-107490.html

Langmatz CZ (2021). *Archivační doba dokumentů*. Interní dokument podniku Langmatz CZ se sídlem v Klatovech.

Langmatz CZ (2022). *Interní předpis o ochraně osobních údajů*. Interní dokument podniku Langmatz CZ se sídlem v Klatovech.

Langmatz CZ (2023b). *Naše projekty.* Dostupné 10. 12. 2023 z https://www.langmatz.cz/home/

Langmatz CZ (2023a). *O společnosti Langmatz CZ s. r. o.* Dostupné 10. 12. 2023 z https://www.langmatz.cz/o-spolecnosti/

Langmatz CZ (2024). *Pracovní smlouva*. Interní dokument podniku Langmatz CZ se sídlem v Klatovech.

Langmatz CZ (2018). *Seznam zjištěných neshod*. Interní dokument podniku Langmatz CZ se sídlem v Klatovech.

Mohanakrishnan, R. (2023). *What Is GDPR and Why Is It Important*? Spiceworks. https://www.spiceworks.com/it-security/security-general/articles/what-is-gdpr/

Mrázová, P. (2019). *Implementace principů GDPR ve společnosti AF Consult s.r.o*. [Diplomová práce, České vysoké učení technické v Praze]. Digitální knihovna ČVUT. https://dspace.cvut.cz/handle/10467/80402

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (2016). https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679

Navrátil, J., Dobrovolná, E., Mazálek, V., Svatošová, H., Bulánek, M., Umlauf, V., Popardowski, I., Ferencová, L., & Navrátilová, S. (2018). *GDPR pro praxi*. Wolters Kluwer.

Nezmar, L. (2017). *GDPR: praktický průvodce implementací*. Grada Publishing as.

Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., & Tomíšek, J. (2017). *GDPR / Obecné nařízení o ochraně osobních údajů*. Wolters Kluwer.

Odrobinová, V. (2020). *GDPR – Sankce a pokuty.* GT News. https://www.gtnews.cz/publikace/gdpr-sankce-a-pokuty/

PrivacySense (2023). *General Data Protection Regulation*. https://www.privacysense.net/terms/gdpr/

Sedláček, V. (2023). *Rekordní nepříjemnost pro Metu. Za porušení GDPR musí v Evropě zaplatit pokutu 1,2 miliardy eur.* Czechcrunch. https://cc.cz/rekordni-neprijemnost-pro-metu-za-poruseni-gdpr-musi-v-evrope-zaplatit-pokutu-12-miliardy-eur/

Sharma, S. (2020). *Data privacy and GDPR handbook*. John Wiley & Sons.

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu

těchto údajů (1995). https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31995L0046

Solidline (2024). *Referenzen: Langmatz GmbH*. Dostupné 5. 4. 2024 z https://www.solidline.de/referenz/langmatz-gmbh/

Svaz měst a obcí České republiky (2020). *Informační systém dodaný externím dodavatelem nezbavuje správce odpovědnosti za správné zpracování osobních údajů*. https://www.smocr.cz/cs/cinnost/gdpr/a/informacni-system-dodany-externim-dodavatelem-nezbavuje-spravce-odpovednosti-za-spravne-zpracovani-osobnich-udaju

Svaz průmyslu a dopravy České republiky (2018). *Jak správně implementovat GDPR ve firmách*. https://www.spcr.cz/muze-vas-zajimat/pravni-infoservis/12396-jak-spravne-implementovat-gdpr-ve-firmach

Svozilová, A. (2016). *Projektový management: Systémový přístup k řízení projektů* (3. vyd.). Grada Publishing.

TaylorWessing (2019). *GDPR rok poté: Mezi nejčastější stále se vyskytující chyby patří vynucování souhlasu se zpracováním osobních údajů*. Epravo. https://www.epravo.cz/top/aktualne/gdpr-rok-pote-mezi-nejcastejsi-stale-se-vyskytujici-chyby-patri-vynucovani-souhlasu-se-zpracovanim-osobnich-udaju-109765.html

Úřad pro ochranu osobních údajů (n. d.). *Porušení zabezpečení osobních údajů*. Dostupné 9. 4. 2024 z https://uoou.gov.cz/profesional/poruseni-zabezpeceni-osobnich-udaju

Úřad pro ochranu osobních údajů (2024). *Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2023*. Dostupné 5. 4. 2024 z https://uoou.gov.cz/novinky/vse/vyrocni-zprava-uoou-za-rok-2023

Vacek, J., Špicar, R., Sova Martinovský, V. (2017). *Projektový management: Cvičebnice* (1. vyd.). Katedra podnikové ekonomiky a managementu, Fakulta ekonomická, Západočeská univerzita v Plzni. Dostupné 1. 4. 2024 z https://dspace5.zcu.cz/handle/11025/29168

Žůrek, J. (2018). *Praktický průvodce GDPR* (2. vyd.). Nakladatelství ANAG.

Seznam tabulek

Seznam obrázků

Seznam příloh

Příloha A: Dohoda o mlčenlivosti, ochraně důvěrných informací a zákazu jejich zneužití

DOHODA O MLČENLIVOSTI, OCHRANĚ DUVĚRNÝCH INFORMACÍ A ZÁKAZU JEJICH ZNEUŽITÍ

Zaměstnavatel: **Langmatz Cz s.r.o.**
Dr. Sedláka 763, Klatovy III, 339 01 IČO: 25217526

a Jana [redacted] narozena [redacted] místo: [redacted]
trvale bytem: [redacted]
uzavírají tuto DOHODU O MLČENLIVOSTI, OCHRANĚ DUVĚRNÝCH INFORMACÍ A ZÁKAZU JEJICH ZNEUŽITÍ

1. Zaměstnanec při výkonu své práce ve mzdové účtárně zaměstnavatele spravuje důvěrné informace zaměstnavatele a zpracovává osobní údaje jeho zaměstnanců.

2. Zaměstnavatel poskytuje zaměstnanci pro výkon jeho práce důvěrné informace představující zejména část jeho obchodního tajemství (know-how), informace o personální a mzdové politice zaměstnavatele, informace o zaměstnancích zaměstnavatele a systému jejich odměňování v souhrnu i na jednotlivých pracovních pozicích, strategii zaměstnavatele na trhu práce, kalkulace a plány zajištění finančních zdrojů odměňování zaměstnanců, finanční ukazatele o vyplaceném objemu mezd, záloh na daň z příjmů, odvodů na sociální a veřejné zdravotní pojištění a jejich vyúčtování a dále veškeré osobní údaje fyzických osob spravovaných nebo zpracovávaných u zaměstnavatele, a to v ústní, písemné i elektronické formě, případně prostřednictvím softwaru nebo i jiným způsobem (dále společně jen „**důvěrné informace**").

3. Účelem těchto ujednání o mlčenlivosti je úprava podmínek, za kterých budou zaměstnanci zpřístupněny důvěrné informace, které jsou nutné pro výkon jeho práce ve mzdové účtárně zaměstnavatele, a stanovení povinností zaměstnance ve vztahu k ochraně těchto důvěrných informací. Tato ujednání o mlčenlivosti se vztahují rovněž na důvěrné informace, které zaměstnavatel poskytl zaměstnanci před sjednáním této dohody.

4. Zaměstnavatel neposkytuje zaměstnanci žádnou licenci ani žádná jiná obdobná práva k poskytnutým důvěrným informacím. Taková licence nebo jiné obdobné právo nemůže být odvozeno ani z předání jakýchkoliv informací, dokumentů (včetně strojově čitelných informací a dokumentů), software, předmětů a ostatních materiálů zaměstnanci.

5. Zaměstnanec je povinen zachovávat mlčenlivost o všech důvěrných informacích a zavazuje se, že bude zachovávat jejich důvěrný charakter v souladu s touto dohodou a platnými právními předpisy.

6. Zaměstnanec se zavazuje zachovávat technická a organizační opatření přijatá zaměstnavatelem, aby zajistil dostatečnou úroveň zabezpečení důvěrných informací odpovídající danému riziku, zejména náhodnému nebo protiprávnímu zničení, ztrátě, pozměňování, neoprávněnému zpřístupnění předávaných, uložených nebo jinak zpracovávaných důvěrných informací, nebo neoprávněnému přístupu k nim. Pro technické zabezpečení důvěrných informací zaměstnanec dodrží postupy zaměstnavatele pro jejich bezpečné skladování, uložení, přesun nebo přepravu jak v manuální, tak v elektronické podobě (zejména používáním aktualizovaného software, řádnou antivirovou kontrolu zaměřenou minimálně na nejznámější počítačové viry, logováním dostatečně silným heslem k zařízením, na nichž dochází ke zpracování důvěrných informací, zajištěním těchto zařízení v uzamčené schránce nebo místnosti, zamezením přístupu neoprávněných osob k těmto zařízením atp.).

7. Zaměstnanec se zavazuje, že důvěrné informace využije výhradně v rámci výkonu své práce ve mzdové účtárně zaměstnavatele a v žádném případě je nevyužije pro sebe anebo někoho jiného

anebo neposkytne důvěrné informace neoprávněným osobám v rámci zaměstnavatele ani vně zaměstnavatele. Zaměstnanec nebude reprodukovat, rozšiřovat ani zpřístupňovat třetím stranám, ať už vcelku, nebo po částech, žádné důvěrné informace zaměstnavatele, s výjimkou případů, kdy k tomu od zaměstnavatele dostane předchozí písemný souhlas, nebo ukládá-li mu to příslušný právní předpis.

8. Veškeré záznamy obsahující důvěrné informace, ať už v listinné, nebo elektronické podobě (včetně originálu i kopií, elektronické pošty, elektronického obsahu zaznamenaného na jiném trvanlivém nosiči dat, jako CD, DVD, USB klíč, paměťová karta atd.), budou na požádání neprodleně vráceny zaměstnavateli anebo zaměstnanec po předchozí písemné dohodě se zaměstnavatelem zajistí zničení příslušných záznamů obsahujících důvěrné informace a zaměstnanec vydá zaměstnavateli písemné potvrzení o jejich zničení (zejména pokud by se důvěrné informace nacházely na zařízení ve vlastnictví zaměstnance užívané např. v rámci práce z domova).

9. Zaměstnanec bere na vědomí, že porušení povinnosti o mlčenlivosti může ohrozit nebo poškodit činnost zaměstnavatele, porušit práva a oprávněné zájmy zaměstnavatele a jeho zaměstnanců, způsobit zaměstnavateli, respektive jeho zaměstnancům, újmu. V případě porušení ujednání o mlčenlivosti je zaměstnavatel oprávněn, vedle jakýchkoliv dalších nároků vyplývajících z těchto ujednání o mlčenlivosti anebo příslušných právních předpisů, zakázat zaměstnanci další použití důvěrných informací, vyzvat zaměstnance ke zdržení se protiprávního jednání a odstranění tohoto nežádoucího stavu, a také má právo provést veškerá opatření k zabránění dalšího porušování těchto ujednání o mlčenlivosti, respektive vzniku újmy a zaměstnanec je povinen neprodleně učinit potřebné kroky k zamezení dalšího porušování ujednání o mlčenlivosti a provést okamžitou nápravu.

10. Porušení ujednání o mlčenlivosti může založit porušení pracovních povinností vedoucích podle jejich intenzity k výtce, výpovědi nebo okamžitému zrušení pracovního poměru zaměstnance u zaměstnavatele a současně ke vzniku odpovědnosti zaměstnance nahradit způsobenou újmu.

11. Tato ujednání o mlčenlivosti se vztahují na období trvání pracovněprávního vztahu zaměstnance u zaměstnavatele a zůstávají v platnosti i po jeho skončení a tato ujednání o mlčenlivosti nezanikají ani zánikem práv a povinností smluvních stran vyplývajících z jakýchkoliv současných nebo budoucích smluv mezi zaměstnancem a zaměstnavatelem.

V Klatovech dne 1.5.2019

podpis zaměstnance

razítko zaměstnavatele a podpis

Seznam použitých zkratek a značek

DPIA	Data Protection Impact Assesment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
IPMA	International Project Management Association
ISO	International Organization for Standardization
PMI	Project Management Institute
SMART	Specific, Measurable, Achievable, Relevant, Time-bound
ÚOOÚ	Úřad pro ochranu osobních údajů

Abstrakt

Pokorná, B. (2024). *Projekt implementace GDPR ve vybrané společnosti* [Bakalářská práce, Západočeská univerzita v Plzni].

Klíčová slova: GDPR, implementace, ochrana osobních údajů, osobní údaje, projekt

Cílem této bakalářské práce je analyzovat projekt implementace GDPR ve firmě Langmatz CZ s.r.o., zhodnotit jeho úspěšnost a navrhnout možná zlepšení. Teoretická část představuje základní pojmy, které se týkají řízení projektů a problematiky GDPR, včetně nových povinností, které toto nařízení přináší. Dále představuje možný postup implementace GDPR v podnikovém prostředí. Praktická část práce pak představuje společnost Langmatz CZ s.r.o., podrobně popisuje průběh a specifikace projektu implementace GDPR v této společnosti a provádí jeho důkladnou analýzu. Na základě této analýzy je projekt zhodnocen a v závěru práce jsou formulována doporučení pro zlepšení způsobu, jakým společnost nakládá s osobními údaji.

Abstract

Pokorná, B. (2024). *GDPR implementation project in selected company* [Bachelor Thesis, University of West Bohemia].

Key words: GDPR, implementation, personal data, personal data protection, project

The aim of this bachelor thesis is to analyze the GDPR implementation project in the company Langmatz CZ s.r.o., evaluate its success, and propose possible improvements. The theoretical part introduces fundamental concepts related to project management and GDPR issues, including new obligations introduced by this regulation. It also presents a possible approach to GDPR implementation in a corporate environment. The practical part of the thesis introduces the company Langmatz CZ s.r.o., provides a detailed description of the process and specifications of the GDPR implementation project in this company, and conducts a thorough analysis thereof. Based on this analysis, the project is assessed, and recommendations are formulated in the conclusion of the thesis for improving the company's handling of personal data.