Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Obecné nařízení o ochraně osobních údajů ve výrobním podniku

Lukáš Karásek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Lukáš Karásek

Informatika

Název práce

Obecné nařízení o ochraně osobních údajů ve výrobním podniku

Název anglicky

General Data Protection Regulation in a manufacturing company

---

Cíle práce

Cílem práce je zhodnotit a popsat požadavky obecného nařízení Evropské unie o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů zpracovávaných v konkrétním velkém výrobním podniku. Dále budou navrženy procesy pro zpracování osobních údajů a navržen způsob zabezpečení dat v souladu s tímto nařízením.

Metodika

Nejprve bude provedena deskripce a interpretace obecného nařízení Evropské unie o ochraně osobních údajů a jiné literatury zabývající se touto problematikou vzhledem k požadavkům zpracování osobních údajů ve velkém výrobním podniku. Dále budou zjištěny lokality, kde se zpracovávají osobních údaje ve firmě a nakonec na základě zjištěných informací zanalyzovány možnosti zpracování a zabezpečení těchto dat.

Doporučený rozsah práce

30-40 stran

Klíčová slova

GDPR, ochrana osobních údajů, zpracování dat, bezpečnost, nařízení Evropské unie

---

Doporučené zdroje informací

DOUCEK, P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

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). In: EUR-Lex [právní informační systém]. Evropská unie, © 1998-2016.

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

POŽÁR, J. *Manažerská informatika.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

Předběžný termín obhajoby

2017/18 LS – PEF

Vedoucí práce

doc. Ing. Vojtěch Merunka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 1. 12. 2017

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 12. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 07. 03. 2018

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Obecné nařízení o ochraně osobních údajů ve výrobním podniku" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. 3. 2018 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu bakalářské práce panu doc. Ing. Vojtěchu Merunkovi, Ph.D. za odborné rady a připomínky a také za vstřícný přístup. Dále bych chtěl poděkovat panu Ondřeji Samohýlovi a paní Mgr. Pavle Traspeové za zpřístupnění cenných informací a podporu při analýze. Závěrem bych rád poděkoval také jednatelům a celé společnosti PRAKAB PRAŽSKÁ KABELOVNA s.r.o. za možnost vypracovat a zveřejnit tuto bakalářskou práci.

Obecné nařízení o ochraně osobních údajů ve výrobním podniku

Abstrakt

Tato bakalářská práce se zabývá tématem obecného nařízení o ochraně osobních údajů, také známého pod zkratkou GDPR. Cílem práce je posoudit požadavky obecného nařízení, nastínit možnosti zabezpečení dat a navrhnout procesy zpracování osobních údajů. Teoretická část práce popisuje požadavky a pravidla GDPR a metody používané v praktické části. Praktická část je zaměřena na dotazníkovou analýzu souladu s požadavky obecného nařízení. Následně je provedena technická analýza rizik a jsou navrženy procesy pro zpracování osobních údajů fyzických osob. Výsledkem práce je návrh bezpečnostní politiky a procesů, které zajistí nejen soulad s nařízením, ale také zlepšení celkové bezpečnosti IT infrastruktury a dalších úseků společnosti, které zpracovávají osobní údaje.

Klíčová slova: GDPR, ochrana osobních údajů, zpracování dat, bezpečnost, nařízení Evropské unie, návrh procesů

General Data Protection Regulation in a manufacturing company

Abstract

This bachelor thesis deals with the topic of the General Data Protection Regulation, also known as GDPR. The aim of the thesis is to assess the requirements of the General Regulation, to outline the possibilities of data security, and to propose the processing of personal data. The theoretical part describes the GDPR requirements and the methods used in the practical part. The practical part focuses on a questionnaire analysis of the compliance with requirements of the General Regulation. Subsequently, a technical risk analysis is carried out and processes for the processing of personal data are proposed. The result of the thesis is a proposal for the security policy and processes that ensure compliance not only with the regulation but also improve the overall security of the IT infrastructure and other sections of the company, which process personal data.

Keywords: GDPR, protection of personal data, data processing, IT security, Regulation of the European Union, design of processes

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Ochrana osobních údajů je v současnosti velmi diskutovaným tématem a to zejména kvůli organizacím a jiným institucím, které zneužívají data fyzických osob, neoprávněně s nimi manipulují a prodávají je za nemalé finanční obnosy. Doposud však neexistoval přímo účinný zákon, který by takovéto chování společností reguloval. Od května roku 2018 by se však tato situace měla změnit. Vstoupí v platnost nové nařízení Evropské unie o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Nařízení přináší mnoho změn, které jsou popsány v teoretické části této bakalářské práce. Nacházejí se zde povinnosti firem, práva fyzických osob a popis důležitých pojmů které s GDPR souvisí.

Hlavním cílem práce je zjištění povinností a doporučení, které z obecného nařízení vyplívají. Rozdílovým porovnáním požadavků GDPR se současným stavem zabezpečení a činností organizace je možné zjistit, co je nutné zavést pro ustanovení souladu s nařízením. Každý systém je bezpečný přesně tak, jak je chráněný jeho nejslabší článek. Z tohoto důvodu je součástí bakalářské práce také technická analýza rizik, která podává ucelený přehled o zranitelnostech a jejich rizicích, které by mohly mít v případě incidentu nepříznivý dopad na osobní údaje fyzických osob. Nedílnou součástí práce je návrh procesů v návaznosti na okolnosti, za kterých může organizace zpracovávat osobní údaje. Procesy dále stanovují činnosti, které je nutné provést v případě, že subjekt údajů bude vymáhat svá práva.

Nové nařízení je pro organizace závažným problémem. Při ignoraci povinností mohou být firmám uloženy značné pokuty. Přitom splnění alespoň minimálních požadavků nemusí znamenat vynaložení nadměrného úsilí. Ve své bakalářské práci uvádím možný postup řešení, kterým se mohou inspirovat i jiné firmy při zavádění GDPR.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je zhodnotit a popsat požadavky obecného nařízení vzhledem ke zpracování osobních údajů ve velkém výrobním podniku, jehož výstupem je stanovení povinností a doporučení, která povedou k prokázání souladu s GDPR. Doplňkovým cílem je stanovení bezpečnostních opatření, které v případě implementace mohou vést ke zlepšení celkové ochrany IT infrastruktury. Dalším vedlejším cílem je návrh procesů legitimního zpracování osobních údajů fyzických osob, které jsou v souladu s obecným nařízením.

2.2 Metodika

Základním pramenem řešené problematiky bakalářské práce je studium Nařízení evropského parlamentu a rady (EU) 2016/679, jiné literatury a článků, které se touto problematikou zabývají. Primární záležitostí je pochopit požadavky a povinnosti plynoucí z obecného nařízení. Nejprve bude sestaven dotazník rozdělený na organizační a technickou část, kde za pomoci řízeného polostrukturovaného rozhovoru budou zjištěny veškeré potřebné informace o společnosti. Z výsledků dotazníku bude možné porovnat současný stav společnosti s požadavky GDPR a stanovit povinnosti a doporučení, která z obecného nařízení plynou.

Metodika pro stanovení bezpečnostních opatření je založena na studiu a porozumění analýze rizik a na průzkumu nástrojů IT bezpečnosti. Nejprve bude nutné za pomoci nestrukturovaného rozhovoru zjistit aktiva společnosti a prozkoumat jejich případné hrozby a zranitelnosti, které budou ohodnoceny na základě zvolené stupnice. Následným stanovením rozsahů pro jednotlivé úrovně rizika lze ohodnotit závažnost zranitelností a navrhnout opatření vedoucí ke snížení tohoto rizika.

Metodika návrhu procesů zpracování osobních údajů je založena na porozumění principu návrhu procesů a na volbě vhodného modelovacího nástroje. Základním předpokladem je také znalost problematiky GDPR. Nejprve bude nutné zjistit lokace zpracování osobních údajů, na jejichž základě bude možné provést asociaci při manipulaci s údaji. Na závěr bude možné navrhnout a popsat procesy zpracování osobních údajů.

3 Teoretická východiska

Cílem této kapitoly je seznámit čtenáře s obecným nařízením o ochraně osobních údajů a jeho vlivem na fyzické a právnické osoby. Nejprve budou představeny pojmy a požadavky, které z tohoto nařízení vychází a poté popsán postup vstupní analýzy a technické analýzy rizik. Závěrem budou popsány organizační a technické způsoby ochrany dat proti únikům, zneužití nebo ztrátě.

3.1 Zákon č. 101/2000 Sb.

Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů vstoupil v České republice v platnost 25. 4. 2000 s účinností od 01. 06. 2000 a reguluje ochranu osobních údajů a účinnost Úřadu pro ochranu osobních údajů. Smyslem tohoto zákona je Listina základních práv a svobod, která zaručuje právo na ochranu občana před neoprávněným zasahováním do jeho soukromí ve smyslu neoprávněného shromažďování, zveřejňování nebo jiného zneužívání osobních údajů. Tento zákon bude však novelován nebo zcela nahrazen novým nařízením 2016/679 vydaným Evropskou unií (dále jen EU) schválený dne 27. 4. 2016 s účinností od 25. 5. 2018. [1] [2]

3.2 Nařízení evropského parlamentu a rady (EU) 2016/679

General Data Protection Regulation (dále jen GDPR) je nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Toto nařízení je přímo účinné, což znamená, že je závazné pro všechny členské státy EU. Charakteristické pro GDPR je jeho univerzální použitelnost a tudíž také sjednocující účinek. Hlavním cílem nařízení je hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich osobními údaji. Obecné nařízení se týká všech institucí, firem a online služeb, které zpracovávají data fyzických osob. Zejména důrazné jsou pokuty za nedodržování nekompromisních pravidel. [2]

3.2.1 Subjekt osobních údajů

Nařízení definuje subjekt údajů jako „*identifikovanou nebo identifikovatelnou osobu*“. Neexistuje žádné omezení ohledně státní příslušnosti dané fyzické osoby nebo místa trvalého pobytu, takže subjekt údajů může být z libovolného místa na světě. Korporace a jiné právnické osoby nejsou subjektem údajů a informace o nich není nutné dle nařízení chránit. Subjektem údajů taktéž není osoba zesnulá. [5] [16, str. 26]

3.2.2 Zpracování osobních údajů

Zpracování je úkon nebo soubor úkonů, které provádí správce nebo zpracovatel, ať už automatizovaně neboli pomocí výpočetní techniky bez lidského zásahu nebo jiným způsobem. Součástí automatizovaného zpracování může být také profilování, což je zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě. Zpracováním se rozumí shromažďování, zpřístupňování, ukládání, zaznamenávání, uspořádávání, strukturování, pozměňování a úprava, vyhledávání, používání, nahlédnutí, předávání, šíření, zveřejňování, uchování, výměna, blokování, likvidace, třídění a kombinování. [14] [6, str. 33]

Osobní údaje lze zpracovávat pouze za předpokladu existence legitimního důvodu. Typy legitimních důvodů jsou vypsány v kapitole 3.2.7 Souhlas se zpracováním. Důležitým aspektem je minimalizace dat, což znamená uchovávat pouze takové množství dat a pouze po takovou dobu, která je bezprostředně nutná k danému účelu nebo je dána zákonným důvodem. Nelze uchovávat osobní data pro případ, že by se mohly hodit v budoucnu. Veškerá nadbytečná data je správce povinen bezodkladně smazat. [15]

3.2.3 Správce a zpracovatel

Správce je každý subjekt, který určuje účel a způsob zpracování osobních údajů a odpovídá za dodržování povinností kladených obecným nařízením. Základním předpokladem pro zpracování osobních údajů je existence řádného právního důvodu, který musí být správce schopný v případě potřeby doložit. Správce musí také zabezpečit, že údaje budou dostatečně chráněny proti úniku či zneužití. Správce může pověřit jiný subjekt, který bude osobní údaje za něj zpracovávat, tento subjekt se nazývá zpracovatel. Správce by však měl vybírat pouze takové zpracovatele, kteří dokážou poskytnout dostatečnou záruku ochrany osobních údajů

subjektů. Dále by měl správce přihlédnout k povaze a množství předávaných údajů a možnostem zpracovatele.[3]

3.2.4 Úřad pro ochranu osobních údajů

Role úřadu pro ochranu osobních údajů (dále jen ÚOOÚ) není adaptace právního prostředí pro ČR, ale podpora práce vlády a ministerstev. Jeho cílem je zejména dozor nad dodržováním právních předpisů. Je to připomínkovým místem v případě změn právních předpisů. Dále poskytuje odborné konzultace organizacím, zejména správcům a zpracovávatelům osobních údajů, ohledně dopadů a návrhů praktických řešení GDPR. ÚOOÚ průběžně zveřejňuje výkladové materiály k jednotlivým částem obecného nařízení, na jehož zpracování se podílí členské státy EU v rámci bruselské poradní skupiny WP29. Jeden z prvních výkladů se týká zřízení nové firemní role, která se dotkne celé řady státních i soukromých organizací. Jedná se o takzvaného pověřence pro ochranu osobních údajů neboli Data Protection Officer (dále jen DPO). Nastavení nezávislého dozorového úřadu v souladu s nařízením o ochraně osobních údajů je úkolem státu. S nově příchozími dozorovými agendami, technologickými a bezpečnostními otázkami stoupají také nároky na personální obsazení ÚOOÚ. [7]

3.2.5 Pověřenec pro ochranu osobních údajů

Povinnost jmenovat pověřence pro ochranu osobních údajů neboli DPO je v následujících případech:

- Zpracování osobních údajů provádí orgán veřejné moci nebo veřejný subjekt.
- Hlavní činnosti správce nebo zpracovatele spočívají v systematickém a dlouhodobém monitorování subjektů údajů.
- Hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštní kategorie údajů (zejména citlivých údajů) nebo údajů týkajících se rozsudku trestů a trestných činů.
- Na základě práva EU nebo členského státu. [8]

Z výše uvedeného vyplývá, že povinnost jmenovat pověřence pro ochranu osobních údajů není dáno vždy. Skupina WP29 však důrazně doporučuje v případě nejmenování DPO disponovat stanoviskem či odůvodněním nejmenování tohoto pověřence. Pokud se však

organizace dobrovolně rozhodne v rámci usnadnění plnění povinností a zmírnění své odpovědnosti poukazem na to, že vynaložili veškeré úsilí k dodržení doporučení v oblasti ochrany osobních údajů jmenovat pověřence pro ochranu osobních údajů. Tak se v tomto případě vztahuje na DPO stejné postavení a úkoly jako by se jednalo o zákoně jmenovaného pověřence. Pozici pověřence může zastávat jak zaměstnanec dané organizace, tak externě spolupracující konkrétní osoba, která bude úkoly plnit na základě smlouvy o poskytování služeb. [8]

Hlavním úkolem DPO je sledování a audit procesů v organizaci a posouzení jejich souladu s právní úpravou. V případě nedodržování pravidel je jeho zákonnou povinností ohlásit tuto skutečnost místnímu ÚOOÚ. Jeho dalším úkolem je poskytování informací, rad a doporučení správci nebo zpracovateli osobních údajů. Organizace však může DPO pověřit i jinými úkoly a povinnostmi. Je však nezbytné zajistit, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmu na straně pověřence. DPO by měl být přímo podřízený vrcholovému managementu firmy, což ve většině případů znamená jednatelům dané společnosti. [8]

3.2.6 Osobní údaje a citlivé osobní údaje

Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou osobou je každá fyzická osoba, kterou je možné přímo či nepřímo identifikovat pomocí dané informace. Osobním údajem tedy může být jméno, adresa, telefonní číslo, IP adresa, fotografie, ale také více zvláštních prvků fyzické, fyziologické, genetické, psychické, kulturní, ekonomické nebo společenské identity dané fyzické osoby. [3] Speciálním případem osobních údajů jsou takzvané citlivé osobní údaje, které mohou subjekt osobních údajů samy o sobě poškodit na veřejnosti a zapříčinit jeho diskriminaci. Jsou to údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci, trestních deliktech či pravomocném odsouzení osob a nově také genetické a biometrické údaje. Zpracování citlivých osobních údajů podléhá přísnějšímu režimu než zpracování obecných údajů. [4]

3.2.7 Souhlas se zpracováním

V případě, že organizace zpracovává osobní údaje z jiného než zákonného důvodu, je povinností správce doložit, že subjekt údajů podepsal souhlas se zpracováním osobních údajů a byl projevem jeho svobodné vůle. Souhlas se zpracováním osobních údajů se vztahuje vždy pouze ke konkrétnímu účelu. Z čehož vyplívá, že není možné mít univerzální souhlas.

Souhlas musí být psán prostým, jednoznačným a srozumitelným jazykem a musí být oddělen od smlouvy, aby nevznikl pocit, že smlouvu není možné bez udělení souhlasu uzavřít, tedy musí být nepodmíněný. Obecně platí, že souhlas se zpracováním osobních údajů by měl být využíván střídmě, protože ve většině případů ani není potřeba. Právem subjektu údajů je také možnost souhlas se zpracováním osobních údajů kdykoli odvolat. Pro zpracování údajů bez souhlasu subjektu údajů je možné aplikovat legitimní důvody, které jsou:

- Zpracování za účelem plnění smlouvy.
- Oprávněný zájem správce.
- Plnění zákonné povinnosti. [9] [10]

Spekulativním pojmem mohou být oprávněné zájmy správce. Údaje fyzické osoby je možné zpracovávat bez souhlasu za předpokladu, že nepřevyšují zájmy subjektu údajů před zájmy správce. Nezbytně nutné zájmy správce pro zpracování osobních údajů mohou být účely pro zamezení podvodů, zajištění veřejné bezpečnosti, ochranu majetku kamerovými systémy, předávání údajů ve skupině pro administrativní účely a dokonce i údaje pro účely přímého marketingu. [11]

Souhlas se zpracováním osobních údajů musí obsahovat kontaktní údaje správce, případně kontaktní údaje na DPO, kategorie údajů, účely zpracování, oprávněné zájmy správce nebo třetí strany, kategorie příjemců osobních údajů, případný úmysl správce předat údaje do třetí země, informace o právech subjektu údajů a pokud je to možné, tak doba po kterou budou osobní údaje uloženy. Bližší informace lze nalézt v Příloze 1 - Vybrané články obecného nařízení, článek 13 a 14. [12]

3.2.8 Práva subjektů údajů

Subjekt údajů má právo na přístup k osobním údajům, neboli na informace ohledně účelu zpracování údajů, totožnosti správce a o příjemcích osobních údajů. V tomto případě jde o pasivní právo, jelikož aktivitu musí projevit správce, jak již bylo zmíněno výše. [13]

Správce musí informovat subjekt údajů o existenci práva na přístup k osobním údajům, jejich opravu nebo výmaz, omezení zpracování, vznešení námitky proti zpracování a právo na přenositelnost údajů, případně má subjekt údajů právo podat stížnost u dozorového úřadu. Dále musí správce informovat subjekt údajů o tom, zda se jedná o zákonný či smluvní požadavek na osobní údaje a případně, zda budou údaje zpracovávány automatizovaně včetně

profilování či nikoli. V případě, že údaje nebyly získány od subjektu údajů, je také nutné informovat subjekt údajů o zdroji, ze kterého osobní údaje pocházejí. [12]

Mezi práva subjektů údajů patří:

- Právo na aktualizaci údajů – v případě, že se údaje změnily nebo jsou nepřesné.
- Právo být zapomenut – povinnost správce zlikvidovat veškeré osobní údaje subjektu údajů kromě údajů držených z legitimních důvodů zmíněných v kapitole 3.2.6 Souhlas se zpracováním.
- Právo na přenositelnost údajů – povinnost správce poskytnout subjektu údajů ve strukturovaném, běžně používaném a strojově čitelném formátu veškeré osobní údaje, které správce o daném subjektu eviduje.
- Právo vznést námitku proti zpracování osobních údajů – je právo subjektu údajů vznést námitku proti zpracování údajů na základě legitimního důvodu, správce musí prokázat zákonné oprávnění nebo převyšující zájmy a případně omezit nebo zcela zastavit zpracovávání.
- Právo nebýt předmětem rozhodnutí založeného na automatizovaném zpracování – je právo subjektu údajů nesouhlasit s výhradně automatizovaným zpracováním údajů včetně profilování bez přezkoumání člověka. [13]

Žádostem subjektu údajů musí být vyhověno bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Výjimečně lze důvodně prodloužit o dva měsíce, o čemž musí být subjekt údajů informován. Veškeré úkony se poskytují a činí bezúplatně. [13]

3.2.9 Pokuty

Ukládání pokut musí být účinné, přiměřené a zároveň odrazující. Obecně však platí, že pokuty by neměly být pro organizaci likvidační. Podstatné však je, že udělení pokuty není ve většině případů nutné. Správce může být nejprve upozorněn nebo mu může být uděleno upomenutí, že jedná v rozporu s GDPR, případně mu může být nařízeno, aby vyhověl žádosti subjektu údajů nebo aby uvedl zpracování údajů do souladu s obecným nařízením. [17] Výše pokuty je rozdělena do dvou skupin:

- Až 10 000 000 EUR (nebo až 2% z celkového celosvětového ročního obratu jde-li o podnik).

- Týká se nejčastěji porušení ustanovení týkajících se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů.

- Až 20 000 000 EUR (nebo až 4% z celkového celosvětového ročního obratu jde-li o podnik).
    - Týká se nejčastěji porušení povinností upravujících zásady a zákonnost zpracování, podmínky souhlasu se zpracováním osobních údajů, podmínky zpracování zvláštních kategorií osobních údajů a práva subjektu údajů. [6, str. 82 - 83]

Při ukládání pokut jsou brány v úvahu polehčující či přitěžující okolnosti, které jsou vypsány v článku 83, odstavec 2, obecného nařízení. Tento odstavec je k nahlédnutí v příloze 1 – Vybrané články obecného nařízení. [6, str. 82 - 83]

V případě, kdy vznikne subjektu údajů hmotná či nehmotná újma v důsledku porušení obecného nařízení ze strany správce nebo zpracovatele má subjekt údajů právo na úhradu újmy, kterou musí daný správce či zpracovatel plnit. [17]

3.2.10 Pseudonymizace, anonymizace a šifrování

Pseudonymizace je zpracování osobních údajů takovým způsobem, že osobní údaje již nemohou být přiřazeny ke konkrétnímu subjektu údajů bez použití dodatečných informací. Za předpokladu, že takové dodatečné informace jsou uchovávány odděleně a jsou předmětem technických a organizačních opatření k zajištění toho, aby nebyly volně přístupné. Dále nesmí být pseudonymizační značky a údaje takové, aby mohly vést k určité identifikované nebo identifikovatelné fyzické osobě. [16, str. 31]

Anonymizace je nevratný proces, při kterém dochází k výmazu veškerých osobních údajů daného subjektu údajů a v budoucnu již zmíněný subjekt není možné dohledat. Zde je rozdíl oproti pseudonymizaci, což je proces vratný, kde data jsou pouze nahrazena nebo oddělena a pomocí „klíče“ je možné je zpětně dohledat. [19]

Šifrování je metoda zabezpečení dat, při které dochází za pomoci kryptografického algoritmu k převodu dat z čitelné podoby na podobu nečitelnou. V případě, že bychom chtěli opět získat původní data, je třeba provést dešifrování, při kterém je potřeba znát takzvaný klíč vygenerovaný při procesu šifrování. Pokud představuje únik citlivých dat daného subjektu údajů nebezpečí, je nutné, aby v případě, že k takovému úniku dojde, byl subjekt organizací

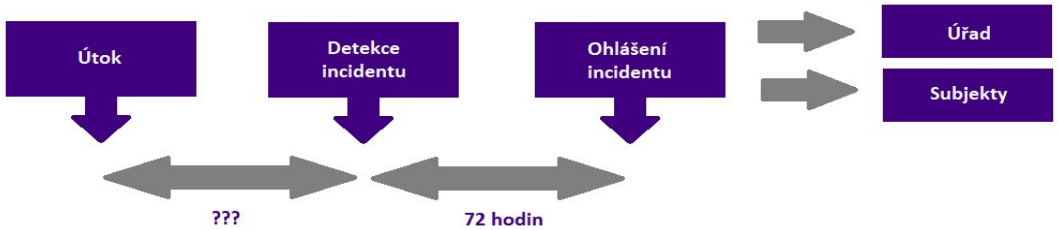
jednoduše a srozumitelně informován. Více informací ohledně hlášení úniků dat subjektů údajů lze nalézt v kapitole 3.2.12 Ohlašovací povinnost. Pokud jsou však uniklá data šifrována, a tudíž se k nim nemůže útočník dostat, tak ohlašovací povinnost odpadá. [20] [21]

3.2.11 Zabezpečení osobních údajů

Správce či zpracovatel by měl zajistit dostatečné zabezpečení osobních údajů *„s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob,“* aby nedošlo k jejich úniku, zneužití nebo jiné manipulaci. Toho lze dosáhnout již výše zmíněnou pseudonymizací či šifrováním osobních údajů nebo použitím jiných technických a organizačních opatření. Opatření, která pomohou správci či zpracovateli zabezpečit osobní údaje budou rozebrána v dalších kapitolách. Vhodně zvolené technické zabezpečení a organizační opatření může do určité míry zmírnit rizika manipulací s daty a z toho plynoucími postihy. Je třeba si však uvědomit, že nikdy není možné garantovat 100% zabezpečení. Bližší informace ohledně povinností správce či zpracovatele na zabezpečení osobních údajů lze nalézt v článku 32 obecného nařízení, tento článek je obsažen v příloze 1 - Vybrané články obecného nařízení. [6, str. 51-52]

3.2.12 Ohlašovací povinnost

Podle obecného nařízení se jakékoli porušení zabezpečení osobních údajů považuje za incident. Může jít o náhodné nebo protiprávní zničení, ztrátu, změnu nebo neoprávněné zpřístupnění osobních údajů. Řešení incidentů musí být provedeno v co možná nejkratším časovém horizontu, jelikož může dojít k fyzické, hmotné či nehmotné újmě u subjektů údajů. Jakmile se správce dozví o porušení zabezpečení osobních údajů, je jeho povinností bezodkladně, nejpozději do 72 hodin, ohlásit tuto skutečnost příslušnému dozorovému úřadu – ÚOOÚ viz obrázek 1. [18]



Obrázek 1 – Zpracování incidentu [18]

V případě, že hrozí vysoké riziko pro práva a svobodu subjektům údajů, je nutné tento incident ohlásit také jim, aby mohly případně učinit vhodná opatření. Správce musí vydat dokumentaci obsahující podrobnosti o rozsahu a dopadu incidentu a také musí být schopen obnovit dostupnost dat v případě jejich fyzických či technických ztrát. Důležitým faktem je, že pod pojmem incident se neskrývá pouze únik nebo krádež dat, ale také jejich neoprávněné pozměnění, například DDoS útokem (přehlcení cílové služby požadavky a tím způsobena její kolize) nebo vyděračským kryptovirem ransomwarem (způsobí zašifrování dat na cílové stanici a pro jejich obnovení požaduje výkupné). Účinná pomoc s řešením incidentů může být zavedení systému pro řízení kontinuity nebo incident management systém. [18]

Ohlášení musí obsahovat minimálně:

- Popis daného porušení zabezpečení, tedy jak a co bylo napadeno.
- Kontaktní údaje na DPO nebo jiné kontaktní místo.
- Popis důsledků porušení zabezpečení, tedy co se pravděpodobně stalo.
- Popis opatření k vyřešení porušení zabezpečení osobních údajů. [23, str. 11]

3.2.13 Poskytování údajů třetím stranám a do jiných zemí

V případě poskytování osobních údajů zpracovatelům mimo danou organizaci využije správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky obecného nařízení, a aby byla zajištěna ochrana práv subjektu údajů. Pověřený zpracovatel nesmí zapojit do zpracování údajů žádného dalšího zpracovatele bez povolení správce. Osoby zpracovávající údaje u zpracovatele musí být vázáni mlčenlivostí. Správce určuje zpracovateli, jak a jakým způsobem mají být data zpracovávána. [6, str 49]

Poskytování osobních údajů do třetích zemí, ať již v rámci EU nebo mimo ni, je možné pouze na základě právního důvodu viz 3.2.7 Souhlas se zpracováním. Pokud předáváme údaje v rámci EU je právní důvod jedinou podmínkou pro předání údajů. Pokud však předáváme osobní údaje do třetích zemí a mezinárodních organizací mimo EU je nutné zjistit, jestli komise EU rozhodla, že daný stát splňuje podmínky pro bezpečnost stanovené zejména dodržováním lidských práv a svobod, existencí příslušných právní, trestních a bezpečnostních předpisů a že jsou vymahatelná práva subjektů údajů. Předání do třetích zemí je však možné i bez tohoto nebo jiného povolení a to v případě, že se správce nebo zpracovatel zaručí za třetí

stranu a existuje pro subjekt možnost vymáhat svá práva. Další podmínkou je existence účinné právní ochrany subjektů údajů blíže specifikované v článku 46 obecného nařízení, který lze nalézt v příloze 1 – Vybrané články obecného nařízení. [6, str 60-62] Předat osobní údaje lze i za předpokladu existence takzvaných závazných podnikových pravidel, kdy jednorázově nebo souborově předáváme osobní údaje v jedné nebo ve více třetích zemích v rámci skupiny podniků nebo uskupení vykonávající společnou hospodářskou činnost. [22]

3.2.14 Povinnosti firem

Kromě již zmíněné ohlašovací povinnosti v kapitole 3.2.12 a případné povinnosti jmenovat pověřence pro ochranu osobních údajů neboli DPO zmíněné v kapitole 3.2.5 plynou z obecného nařízení povinnosti posouzení vlivu na ochranu osobních údajů a povinnost vést záznamy o činnostech zpracování. [23, str. 10-14]

3.2.14.1 Povinnost posouzení vlivu na ochranu osobních údajů

V případě vysoké rizikovosti zpracování osobních údajů jsou firmy povinné posoudit dopady zpracování těchto údajů, vypracovat takzvané DPIA (Data Protection Impact Assessment). Tato povinnost je v případě, že se jedná o automatické, systematické zpracování a hodnocení osobních údajů, velkokapacitní monitorování veřejného prostoru, velkokapacitní zpracování citlivých údajů, zpracování při využití „nových technologií“ a podobně. [23, str. 11] Podle skupiny WP29 bude muset takovéto posouzení vlivu obsahovat:

- Popis plánovaných operací zpracování a účel zpracování.
- Posouzení nezbytnosti a přiměřenosti zpracování.
- Posouzení rizika z hlediska práv a svobod subjektů údajů.
- Předpokládaná opatření:
    - Jak řešit případná rizika.
    - Prokázat soulad s obecným nařízením. [24, str. 16]

3.2.14.2 Povinnost vést záznamy o činnostech zpracování

Tato povinnost se nevztahuje na malé a střední podniky, které zaměstnávají méně než 250 zaměstnanců. Zároveň tyto podniky nesmějí zpracovávat údaje ohrožující práva a svobody

osob nebo nakládat s citlivými údaji. V opačném případě mají také povinnost vést záznamy o činnostech zpracování. Každý povinný správce a zpracovatel povede záznamy o činnostech zpracování, za něž odpovídá. Záznamy obsahují:

- Název a kontaktní údaje správce.
- Důvod zpracování údajů.
- Popis kategorie subjektů údajů a osobních údajů.
- Kategorie organizací, které údaje obdrží.
- Přenos údajů do jiné země či organizace.
- Lhůtu pro odstranění údajů.
- Popis bezpečnostních opatření uplatňovaných při zpracovávání. [23, str. 12]

3.3 Vstupní analýza

Před samotným nasazením GDPR a navržením potřebných technických a organizačních opatření je nutné zjistit, co je vlastně potřeba změnit a naimplementovat. Je třeba si uvědomit, že GDPR se netýká pouze HR a IT oddělení, ale celé firmy a tudíž by do této problematiky mělo být začleněno každé oddělení společnosti. [25]

3.3.1 Postup GDPR analýzy

První věcí, kterou by se měla organizace zabývat je, jestli daná firma potřebuje DPO a pokud ano, tak je před dalším postupem nejprve potřeba tohoto zaměstnance obstarat či jmenovat. Pověřenec pro ochranu osobních údajů by měl být rozhodně přítomen již od začátku řešení obecného nařízení. Poté může začít úvodní porada vedení firmy, kde se představí problematika GDPR a její rozsah. Následuje vytvoření GDPR týmu, který se bude skládat ze zástupců všech oddělení pracujícími s osobními údaji. Jednotliví účastníci týmu provedou audit ve svém oddělení a poskytnou informace o zpracovávaných osobních údajích. Tyto informace jsou poté uceleně zpracovány. Závěrem je třeba vytvořit výstupní zprávu pro vedení společnosti s upozorněním na rizika a návrhem praktických opatření. [23, str. 16]

3.3.2 Analýza jednotlivých oddělení

Při interním auditu každého oddělení je nutné stanovit druh osobních údajů, které jsou zpracovávány. Zdali se jedná o běžné osobní údaje nebo citlivé osobní údaje, případně zdali se zpracovávají údaje dětí. Dalším důležitým stanoviskem je, kdo tyto údaje zpracovává a kdo k nim má přístup. Případně, jestli data zpracovávají externí dodavatelé nebo jsou zpřístupňována zahraničním organizacím. V jakých systémech a v jakém formátu se data nacházejí. Zdali existují strukturovaná data v informačních systémech a jiných softwarech nebo zda existuje nějaká elektronická či papírová evidence. V neposlední řadě je třeba také stanovit, z jakého právního titulu se data zpracovávají (viz kapitola 3.2.7 Souhlas se zpracováním), za jakým účelem a po jak dlouhou dobu. [23, str. 15-16]

3.3.3 Technická analýza rizik

Cílem technické analýzy rizik je definování hrozeb, stanovení pravděpodobnosti jejich uskutečnění a dopadu na aktiva. Postup vychází z obecné analýzy rizik. V našem případě je třeba se zaměřit především na aktiva, která uchovávají, zpracovávají či jiným způsobem manipulují s osobními údaji. [27, str. 69-75] Postup analýzy je následující:

1. **Identifikace a stanovení hodnoty aktiv** – nalezení všeho (hmotného i nehmotného) co má pro organizaci hodnotu a stanovit odhad možné ztráty při modifikaci, poškození nebo odcizení daného aktiva.

2. **Stanovení hodnoty aktiv –** ohodnocením významu aktiva pro subjekt lze určit, jaký dopad by na subjekt měla ztráta, změna nebo poškození aktiva, hodnoty jsou nejčastěji v rozsahu 1 – 5.

3. **Identifikace hrozeb a slabin** – určení událostí a akcí, které mohou negativně ovlivnit hodnotu aktiv neboli nalezení takzvaných slabých míst subjektů.

4. **Stanovení závažnosti hrozeb a míry zranitelnosti** – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči této hrozbě.

5. **Stanovení dopadu** – stanovení dopadu určuje hodnota aktiva, dopad však může být nižší v případě, že dojde pouze k částečnému ohrožení aktiva.

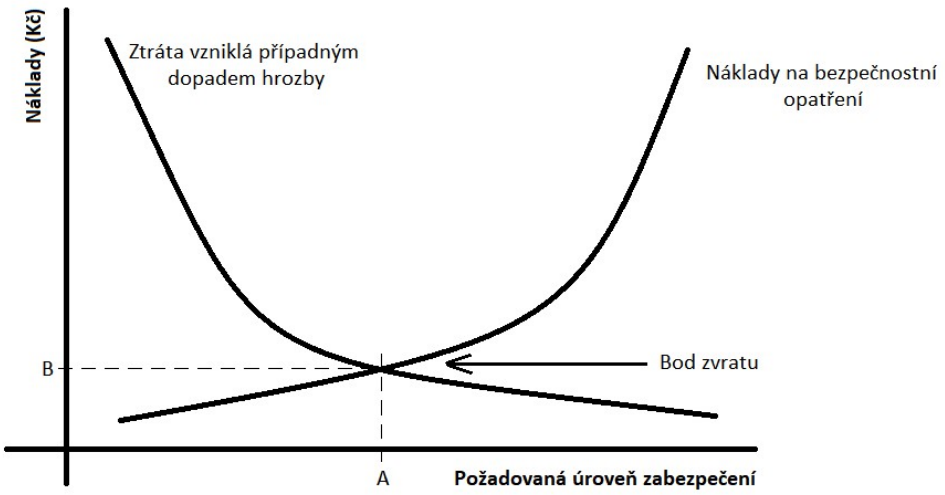
6. **Výpočet míry rizika** – výpočet míry rizika je proveden na základě hodnot pravděpodobnosti incidentu a dopadu na subjekt a to ve vztahu součinu těchto dvou parametrů.

7. **Existující opatření** – pravděpodobnost incidentu je snižována existujícím opatřením. [27, str. 69-75] [39]

Vyhodnocení analýzy rizik nám pomůže stanovit opatření, která jsou nutná provést pro vyšší bezpečnost informačních systémů. Je zřejmé, že nelze dokonale zabezpečit celou IT infrastrukturu, jelikož by to znamenalo vynaložení nadměrných finančních nákladů a také by to negativně ovlivnilo funkčnost daného subjektu. Vždy je třeba volit rozumné vyvážení s ohledem na následující tři aspekty:

- míra zabezpečení,
- použitelnost,
- finanční náročnost. [45, str. 346-350] [27, str. 69-75]

Se zvyšující se mírou zabezpečení se zároveň snižuje použitelnost. S rostoucí bezpečností také rostou nároky a požadavky, které je třeba splnit, aby byl umožněn přístup k daným informacím, což vede ke snížení efektivity práce. Dále se zvyšující mírou zabezpečení rostou také finanční nároky, které nejsou v oblasti IT rozhodně zanedbatelné. Z výše uvedeného vyplývá, že je potřeba najít optimální míru zabezpečení. Tuto míru nám může pomoci nalézt metoda přínosů a nákladů uvedená na obrázku 2 níže. [27, str. 69-75] [39]



Obrázek 2 – Nákladový model bezpečnostního opatření [26, str. 101]

V bodě B na obrázku můžeme vidět, jaké maximální náklady by měli být organizací vynaloženy na bezpečnostní opatření. Pokud bychom zvolili vyšší požadovanou úroveň zabezpečení, než je v bodě A, tak náklady na její realizaci by byly vyšší než náklady spojené s případným dopadem hrozby. Závěrem je nutné zvolit takovou optimální úroveň zabezpečení, aby náklady na implementaci tohoto zabezpečení nebyly vyšší než případný dopad hrozby. [26, str. 101]

3.3.4 Bezpečnostní správa organizace

Bezpečnostní správa neboli security management je nezbytná pro bezchybný provoz každé organizace. Můžeme jí dělit podle působení na tři oblasti, které je třeba analyzovat a zabezpečit a to:

- **Informační bezpečnost** – zde se jedná o zabezpečení informačních systémů a dat, která jsou v těchto systémech zpracovávána. Má nejvyšší prioritu, jelikož nejcennějším materiálem pro útočníka jsou cenné informace a know-how firmy.
- **Majetková bezpečnost** – někdy také nazývána jako fyzická bezpečnost, protože finance a majetek mohou pro útočníka znamenat jisté obohacení.
- **Personální bezpečnost** – zde se útočník zajímá o informace osob ve smyslu jejich charakteristik, jako jsou vlastnosti, znalosti a dovednosti, které je možné využívat nebo prodat, jelikož prodej osobních údajů je v dnešní době velmi výnosný. [28, str. 71-72]

3.4 Bezpečnostní opatření

Obsahem této kapitoly je analýza bezpečnostních opatření, systémů a technologií s jejichž pomocí je možné zmírnit rizika zneužití, odcizení, ztráty nebo nelegitimního zpracování dat. Základním předpokladem pro zajištění souladu s GDPR je vybudovat takové organizační a technické opatření, které bude přiměřeným prostředkem ochrany „*s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.*“ [6, str. 51]

3.4.1 Organizační opatření

Organizační bezpečnostní politika je často neprávem považována za doplňkovou. Přitom pokud budeme dbát na důsledné dodržování stanovených pravidel, tak lze dosáhnout poměrně značného zvýšení bezpečnosti s ohledem na relativně nízké náklady. [30, str. 268]

Organizační opatření určuje pravidla, směrnice a zvyklosti, které udávají způsob, jakým jsou v dané organizaci a jejích systémech řízena, chráněna a distribuována aktiva, včetně citlivých informací. Jedná se o soubor kritérií pro aplikaci bezpečnostních služeb. Stanovení pravidel však nestačí, je třeba také zajistit pravidelnou revizi a kontrolu dodržování těchto pravidel, kterou by měli být pověřeni pracovníci organizace. [26, str. 133]

3.4.1.1 Úprava dokumentů

Základním předpokladem implementace obecného nařízení je úprava interních dokumentů, směrnic a smluv. Vnitropodnikové směrnice je nutné upravit tak, aby splňovaly požadavky GDPR a ve většině organizací bude také potřeba přidat směrnice nové. Nové směrnice se budou týkat zejména procesů, které určují jakým způsobem pracovat s osobními údaji a jak zprostředkovat práva subjektů údajů. [25]

Další důležitá úprava se týká smluv a to nejen mezi běžnými dodavateli a odběrateli zboží, materiálů a výrobních prostředků, ale zejména mezi dodavateli služeb a produktů ve smyslu zpracovatelů, přičemž tito dodavatelé přijdou do styku s osobními údaji, které poskytují subjekty údajů správci. [25] [29]

Speciální dokumenty určené přímo obecným nařízením, které by měly být dále vytvořeny a vedeny za určitých podmínek specifikovaných v kapitole 3.2.14. Povinnosti firem, jsou DPIA (Data Protection Impact Assessment) neboli vypracování posouzení vlivu na ochranu osobních údajů pro veškeré používané programy, systémy a procesy. A vést záznamy o činnostech zpracování. Souhlas se zpracováním osobních údajů je další dokument, který je nutné doplnit o nové náležitosti. Podle GDPR je nutné vytvořit pro každý účel speciální souhlas a není možné mít souhlas univerzální. [25] [29]

3.4.1.2 Školení

Po úpravě směrnic a implementaci vhodných organizačních a technických opatření je zejména důležité provést také školení zaměstnanců a to nejen těch, kteří se podílí na zajištění souladu

s GDPR, ale všech zaměstnanců firmy, kteří pracují s osobními údaji. Největším rizikem zajištění bezpečnosti a ochrany dat je totiž lidský faktor. Odhaduje se, že až 80 % případů porušení ochrany informací je způsobeno právě jimi. Pokud vezmeme v úvahu také jejich případnou nespokojenost, pomstychtivost nebo zlobu, je riziko ještě větší. Riziko zároveň roste také s rostoucími pravomocemi. Pokud se firmě podaří eliminovat základní rizika bezpečnosti, je velká pravděpodobnost, že zvládne přechod na obecné nařízení o ochraně osobních údajů bez vynaložení nadměrného úsilí a finančních prostředků. Výsledkem procesu školení bude přiměřená vnitřní ochrana před úniky a zneužití dat. [23, str. 17] [30, str. 261]

3.4.1.3 ISO 27000

ISO 27000 je skupina norem, které vydala mezinárodní organizace pro standardizaci (ISO) ve spolupráci s mezinárodní elektrotechnickou komisí (IEC). Jedná se o mezinárodně uznávané standardy zabývající se zejména informační bezpečností. Vzhledem k GDPR je nejdůležitější normou tohoto standardu ISO 27001, která se věnuje systémům řízení bezpečnosti informací neboli ISMS, kde se požadavky na ISO a na obecné nařízení v mnoha bodech překrývají. ISMS je systém procesů a postupů k zajištění co nejlepší možné bezpečnosti informací a minimalizaci hrozeb. ISO 27001 je tedy dobrým výchozím bodem pro organizace, které chtějí dosáhnout souladu s GDPR. [31, str. 195-196] [32, str. 395]

V případě, že organizace uchovává data v cloudu (veřejném uložišti), je vhodné implementovat také normu ISO 27018, která je určena pro ochranu osobně identifikovatelných informací ve veřejných uložištích vystupujících jako zpracovatelé. [31, str. 213]

3.4.1.4 Audit

Audit je prověření a přezkoumání informací, dat a předepsaných činností s cílem ověřit jejich platnost a spolehlivost. Osoba, která provádí audit se nazývá auditor. Z hlediska bezpečnosti a ochrany osobních údajů je třeba se zaměřit na audit informačního systému neboli IT audit, který prověřuje hardware, software, informace, bezpečnost a provozní dokumentaci informačního systému. Dalším důležitým auditem je audit bezpečnostní, který ověřuje systém řízení bezpečnosti v organizaci. Z pohledu osoby vykonávající tuto činnost rozdělujeme audit na interní a externí. Interní audit provádí osoba nebo útvar uvnitř organizace, tedy zaměstnanci dané organizace. Externí audit je prováděn externím subjektem. Výstupem auditu by měla být zpráva, která popisuje cíle, kritéria, rozsah, nálezy a závěr auditu. Určitým

typem auditu může být také zkoumání a vyhodnocování logů nebo provádění penetračních testů. Audit zavedených pravidel a systémů by měl být nedílnou součástí bezpečnostní politiky. [33] [26, str. 200-204]

3.4.2 Technická opatření

Technické bezpečnostní opatření dokáže do jisté míry ochránit důležité informace a data společnosti a v některých případech také ulehčit administrativní a analogickou práci spojenou s bezpečností. Bezpečnost informací je odvětví, které nemá tendenci dlouhodoběji stagnovat, což má za následek vysoké finanční nároky na nové technologie. [26, str. 218]

3.4.2.1 Firewall

Firewall někdy také nazýván „brána“ je zařízení, které může mít softwarovou nebo hardwarovou formu a je základem pro IT bezpečnost. Jeho funkcí je oddělit interní firemní síť od sítě jiné (nejčastěji internetu) a propouštět mezi sítěmi pouze taková data, která jsou předem definována podle určitých pravidel. Jeho úkolem je zamezit neoprávněnému průniku do sítě a tím zamezit případné manipulaci s daty. [34]

3.4.2.2 Šifrování

Šifrování je proces, při kterém dochází za pomoci šifrovacího algoritmu k přeměně otevřeného textu na text šifrovaný, který brání neoprávněným osobám tyto informace získat. Data lze zpětně dešifrovat (převést šifrovaný text na text otevřený) za pomoci klíče, který byl použit při šifrování. Popsaný způsob se nazývá symetrické šifrování. Pro komunikaci mezi dvěma a více subjekty je vhodnější použít asymetrické šifrování, kde se využívá páru klíčů. První z páru je klíč veřejný, který vygeneroval adresát a je možné za jeho pomoci zašifrovat zprávu. Druhý z klíčů je klíč soukromý, který vlastní pouze adresát a slouží pro dešifrování zprávy, která byla zašifrována veřejným klíčem. Základním principem je tedy poskytnutí veřejného klíče všem odesílatelům zprávy a pečlivé uschování klíče soukromého. [28, str. 191-203]

3.4.2.3 Zálohování

Zálohování je průběžné pořizování záložních kopií všech důležitých dat a programového vybavení používaných v organizaci s cílem zajistit dostupnost a případnou obnovu datových zdrojů a programového vybavení. Proces zálohování je následující:

- Vytvoření zálohovacího plánu.
- Dodržování stanoveného plánu.
- Testování čitelnosti zálohovaných dat.
- Bezpečné uložení záložních médií. [26, str. 143]

3.4.2.4 Bezpečnost osobních počítačů

Základem bezpečného počítače je aktualizovaný a legální operační systém. Z programového vybavení je nezbytné mít nainstalovaný dobrý antivirový program s aktualizovanou databází hrozeb. Dále je nezbytné mít zapnutý počítačový firewall, který hlídá korektní komunikaci mezi počítači. Je také dobré mít nainstalovaný antispyware, který kontroluje všechna data přicházející do počítače a v případě detekce škodlivého softwaru nebo jiné hrozby zamezí těmto spywarům přístup do počítače. [35]

3.4.2.5 Logy a síťová analýza

Již od počátku vývoje sítě vznikaly různé analytické síťové nástroje a zařízení sbírající logy, které měli pomoci administrátorům v jejich práci a vytvářet bezpečnostní analýzy. Mezi tyto nástroje patří:

- **Vulnerability assessment scanner** – je software pro hodnocení zranitelnosti, který se využívá pro audit počítačové a síťové bezpečnosti, dokáže identifikovat případné bezpečnostní problémy a nalézt chyby v konfiguraci různých zařízení nebo případné potřeby updatu.
- **Packet sniffers** – někdy také nazývaný jako paketový analyzátor je zařízení, které dokáže odchytávat provoz na síti. Tyto záznamy ukládá a případně třídí podle definovaných pravidel.
- **File integrity checker** – neboli kontrolor integrity souborů je software, který generuje a sleduje kontrolní součty adresářů a souborů a tím zajišťuje, že žádná neoprávněná osoba nezměnila daný soubor nebo adresář. Případně existují podobné nástroje, které sbírají logy ze souborového serveru a monitorují veškeré změny souborů nebo adresářů.

- **Password auditing** – je nástroj na audit hesel uživatelů. Jsou využívány různé metody za účelem zjistit heslo daného uživatele. Využívá se slovníkových útoků, brute force attack (testování kombinací množiny znaků na prolomení hesla) a podobných technik. V případě prolomení hesla je upozorněn IT administrátor, který by měl zažádat uživatele, aby heslo změnil na bezpečnější.

- **Network reconnaissance tool –** jsou nástroje na prozkoumání a shromáždění veškerých informací o síti. Využívají různých protokolů a možností k zjištění kompletní topologie sítě. [32, str. 32-35]

3.4.2.6 IDS a IPS

IDS (Instruction Detection System) je bezpečnostní systém, který monitoruje síťový provoz za účelem odhalit podezřelé chování na síti. V případě zjištění podezřelého chování systém tuto skutečnost okamžitě ohlásí IT administrátorovi. Problémem však je, že prodleva mezi detekcí problému a reakcí na něj může být v určitých případech tak velká, že již není možné škodlivé činnosti zabránit. V takových případech je vhodné využívat IPS (Instruction Prevention System), který dokáže reagovat na událost a případně odpojit od sítě podezřelá zařízení. Tím zamezí šíření hrozby, dokud tuto hrozbu administrátor neprověří.
[32, str. 53-55]

3.4.2.7 DLP

DLP (Data Loss Prevention) je nástroj, který minimalizuje rizika ztráty či úniku dat způsobených lidskou chybou. Pomocí tohoto nástroje je možné získat kontrolu nad pohybem dokumentů klasifikovaných jako důvěrné uvnitř organizace i mimo ni. Zároveň lze sledovat aktivity uživatelů, kteří pracovali s těmito soubory. Nástroj zabezpečuje dokumenty tak, že znemožňuje jejich kopírování a to jak celých souborů, tak i částí textu. Také zabraňuje vytváření kopií obrazovky při práci s těmito soubory a umožňuje nastavit spoustu dalších bezpečnostních opatření. [36] [37]

3.4.2.8 IAM

IAM (Identity and Access Management) je nástroj, který dokáže IT administrátorům výrazně usnadnit práci se správou oprávnění a přístupových údajů. Pomocí tohoto nástroje lze definovat kategorie podle organizační struktury nebo pracovních skupin, kde jsou poté jednotlivým uživatelům přidělována a odebírána oprávnění podle jejich pravomocí. Dále

umožňuje schvalování práv nadřízenými pracovníky, shromažďování logů z auditu, vedení evidence oprávnění, integrace jednotlivých systémů organizace, správa a dohled nad přístupovými údaji a hesly a spoustu dalších zajímavých funkcí, které mohou pomoci podnikům s implementací GDPR. [36]

3.4.2.9 IEEE 802.1X

IEEE 802.1X je bezpečnostní protokol, který umožní přístup do sítě pouze autorizovaným zařízením. Zařízení se většinou autorizují na základě uživatelského účtu vytvořeného organizací. Dalším způsobem autorizace je na základě shody MAC adresy, kdy administrátor prohlásí danou MAC adresu za důvěryhodnou a mechanismus jí poté umožní vstup do sítě. Výhodu, kterou protokol přináší, je automatizované třídění klientských zařízení do nastavených VLAN a tím může být omezen přístup klientům k jednotlivým částem sítě. IEEE 802.1X je tedy standard, který by měl zajistit, že se v organizaci nedostane do sítě žádné zařízení, o kterém administrátor neví. [38]

3.4.2.10 MDM

MDM (Mobile Device Management) je jednou z nejdůležitějších technologií pro zabezpečení firemních dat z pohledu mobilních zařízení. Technologie nabízí firmám možnost spravovat veškerá mobilní zařízení na pracovišti a to přes bezdrátovou síť bez narušování práce uživatelů. V případě ztráty nebo odcizení zařízení je možné vzdáleně vymazat firemní data. Administrátoři mohou distribuovat firemní mobilní aplikace, předpisy pro zabezpečení, nastavení a sbírat softwarová a hardwarová data ze zařízení. [41]

3.4.2.11 Penetrační testy

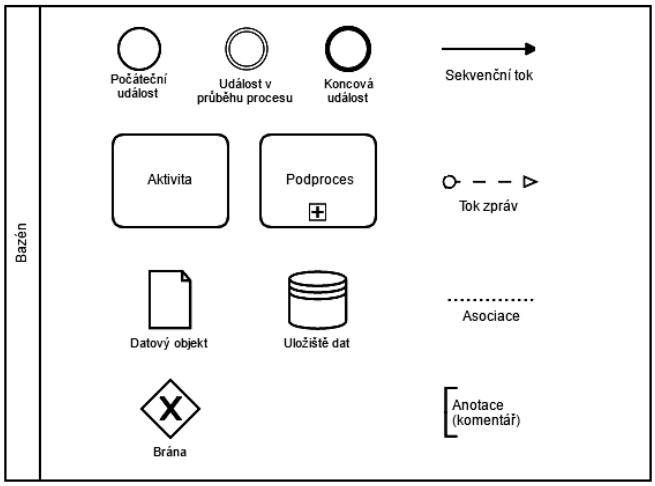
Penetrační testování je technika etického hackingu při které se ověřuje všestranná bezpečnost IT infrastruktury. Může jít o pokus vnějšího průniku do sítě, průniku na decentralizované servery (DMZ), vnitřního průniku do sítě nebo také zneužití důvěry zaměstnanců. Při tomto testování se snaží hacker pomocí speciálních technik najít co možná nejvíce bezpečnostních chyb a tím simulovat případné reálně napadení. Na nápravu těchto chyb by se poté měla organizace zaměřit a tím zvýšit celkovou informační bezpečnost. [42]

3.5 Procesní modelování BPMN

BPMN (Business Process Model and Notation) je nástroj pro návrh a grafické znázornění firemních procesů, který umožní firmám pochopit své interní postupy. Organizace mají možnost projednávat a předávat své postupy standardizovaným způsobem. Grafická notace usnadní pochopení spolupráce jednotlivých částí organizace a zpracování událostí. Tím se zajistí, že zaměstnanci firmy budou chápat podmínky podnikání a umožní organizaci rychle se přizpůsobit novým vnitřním a B2B podmínkám. [43]

3.5.1 Základní prvky

Základní prvky používané v modelovacím nástroji BPMN jsou znázorněny na Obrázku 3 níže. Bližší možnosti použití událostí a bran lze nalézt v Příloze 6 – Základní prvky procesního modelování BPMN.



Obrázek 3 – Základní prvky modelovacího nástroje BPMN [44]

4 Vlastní práce

Praktická část bakalářské práce je zaměřena na organizační a technickou analýzu stavu organizace doplněnou o analýzu rizik. Pomocí těchto dvou metodik lze zjistit důležité informace o podniku, jeho procesech a lokacích zpracování osobních údajů. S ohledem na zjištěné informace lze navrhnout organizační a technické opatření k zajištění souladu s obecným nařízením o ochraně osobních údajů a navrhnout procesy zpracování osobních údajů.

4.1 Základní informace o společnosti PRAKAB

V roce 1891 zakládá rodina Tremmelů společnost SKW. V roce 1921 většinový podíl přebírá pan Dr. Emil Kolben a tímto krokem vzniká společnost PRAKAB PRAŽSKÁ KABELOVNA, s.r.o., která se za dobu své existence stala tradičním českým výrobcem kabelů. PRAKAB je členem skupiny podniků SKB GROUP, kam patří Rakouské SKW a SKG, Ukrajinské IKK, Slovenské ICS a FCS. [40]

Profil společnosti 2017:

- **Adresa:** Ke Kablu 278, Praha 10 – Hostivař, 102 00
- **Počet zaměstnanců:** 350
- **Obrat:** 130 mil. EUR
- **Podíl exportu:** 75%
- **Objem produkce:** 146 000 km kabelů / rok
- **Výrobní plocha:** 35 000 m^2
- **Celková rozloha areálu:** 135 000 m^2 [40]

4.2 Vstupní analýza GDPR

Základním předpokladem pro úspěšné navržení a implementaci opatření, která zajistí soulad s obecným nařízením, je provedení dobré vstupní analýzy. Analýza se provádí formou řízeného polostrukturovaného rozhovoru a je rozdělena do dvou částí, a to do části

organizační a technické. Dotazy jsou vypracovány na základě znalostí získaných z teoretické části práce. Při dotazování je přítomna osoba, která má dobrou povědomost o daných postupech a skutečnostech v konkrétní části dotazů. Na organizační dotazy odpovídal zástupce HR oddělení a na technické zástupce IT oddělení. Obě tyto skupiny jsou stejně významné a často se v některých svých bodech prolínají. Vyhodnocením analýzy na základě znalostí získaných v teoretické části dostaneme dobrý přehled o povinnostech, kterými by se měla organizace zabývat.

4.2.1 Organizační část

Obsahem této části analýzy je prozkoumání organizační struktury společnosti, a to jak z pohledu GDPR, tak z pohledu běžných činností a postupů, které jsou již prováděny. Průběh celé analýzy je obsahem přílohy 2 – Vstupní analýza GDPR v sekci organizační dotazy. Zde budou probrány pouze takové pasáže, kterými je nutné se zabývat v souvislosti s povinnostmi a doporučeními obecného nařízení.

Je organizace správce nebo zpracovatel?

Organizace je správce. Správce určuje účel zpracování osobních údajů a zodpovídá za svěřené osobní údaje subjektů údajů. V souvislosti s tímto dotazem je důležité zhodnotit, zda údaje, které organizace zpracovává opravdu potřebuje nebo s údaji nakládá pouze za účelem, že by je mohla v budoucnu využít. Pokud organizace zpracovává osobní údaje za účelem, že by je mohla v budoucnu využít, bez souhlasu subjektu údajů podle kapitoly 3.2.7 Souhlas se zpracováním, tak jedná v rozporu s obecným nařízením. V takovémto případě existuje možnost smazání veškerých takovýchto údajů a v jejich zpracovávání nadále nepokračovat nebo si opatřit ve všech konkrétních případech souhlas se zpracováním. V případě zvolení druhé možnosti a zpracovávat údaje se souhlasem je však také nezbytné, aby existoval důvod zpracování za konkrétním účelem, který bude subjektu údajů sdělen v souhlasu. Další náležitosti, které musí souhlas se zpracováním obsahovat, lze nalézt v již zmíněné kapitole 3.2.7.

Má organizace předpisy a směrnice pro ochranu osobních údajů?

Organizace sice zmiňuje některé podmínky pro práci s osobními údaji, avšak tyto podmínky nejsou ucelené a dostatečné a to zejména vzhledem k legislativním změnám chystajícího se GDPR.

Provádí firma školení zaměstnanců?

Ano, školení provádí zaměstnanci i externí firmy, ale součástí školení není poučení o nakládání s osobními údaji. Vzhledem k citlivé povaze údajů a hrozících postihů z obecného nařízení, je významně doporučeno zahrnout do každoročního školení také školení o nakládání s osobními údaji. Také vzhledem ke skutečnosti, že uživatelé představují největší bezpečnostní riziko.

Poskytuje organizace osobní údaje externím firmám - zpracovatelům?

Organizace poskytuje osobní údaje externím společnostem. Zároveň neproběhla úprava smluv s externími firmami a nebyl stanoven plán informování o změnách nebo smazání údajů pro tyto externí zpracovatele. Povinností správce je vybrat pouze takové zpracovatele, kteří poskytují dostatečnou záruku pro ochranu údajů. Vhodné je tedy do smlouvy s těmito externími společnostmi zahrnout částečné přenesení zodpovědnosti za zpracovávané údaje a zahrnout smlouvu o mlčenlivosti. Dalším důležitým krokem je stanovit plán informování zpracovatelů o změnách nebo smazání údajů u jednotlivých subjektů. Tento plán by měl obsahovat seznam externích zpracovatelů spolu s typovými osobními údaji, které zpracovávají a stanovit prováděcí předpis jakým způsobem budou informování a do jak dlouhé doby.

Vede organizace dokumentaci o lokacích uložení osobních údajů?

Neexistuje evidence osobních údajů uchovávaných v listinné ani elektronické podobě. Organizace by měla mít dobrou povědomost o tom, kde se jaké osobní údaje nachází a to z důvodu jejich ochrany a také k zajištění práv subjektů údajů. Zároveň by mělo být zakázáno ukládat osobní údaje na interní úložiště firemních počítačů a vedení soukromých databází údajů.

Vede organizace dokumentaci o posouzení vlivu na ochranu osobních údajů (DPIA)?

Nevede. Povinnost vést DPIA je ve většině případů nejasná a to zejména kvůli nepřesným výkladům zákona. Okolnosti, které by mohly vést k povinnosti vypracování DPIA jsou velkokapacitní monitorování veřejného prostoru a zpracování při využití „nových technologií“. Vzhledem k této situaci je více než doporučené raději posouzení vlivu na ochranu osobních údajů neboli DPIA zpracovat.

Vede organizace záznamy o činnostech zpracování?

Nevede. Povinnost vést záznamy o činnostech zpracování nemají podniky malé a střední, které zaměstnávají méně než 250 zaměstnanců. Vzhledem k tomu, že společnost PRAKAB zaměstnává přibližně 350 zaměstnanců, tak se ho tato povinnost týká. Bližší informace ohledně povinnosti vypracování záznamů o činnostech zpracování lze nalézt v kapitole 3.2.14.2 Povinnost vést záznamy o činnostech zpracování.

Vede organizace evidenci oprávnění zaměstnanců na přístup k osobním údajům?

Nevede. Vzhledem ke kontrole přístupů, pomoci při detekci případného bezpečnostního incidentu a udělení zodpovědnosti zaměstnancům za svěřená data, je doporučené vést evidenci oprávnění zaměstnanců na přístup k osobním údajům. Tento dokument by měl obsahovat lokace uložení osobních údajů, ať již v listinné nebo elektronické podobě spolu s výpisem konkrétních typů osobních údajů a jmen zaměstnanců, kteří k datům mají přístup a kteří za dané údaje odpovídají. Toto doporučení úzce souvisí s doporučením v otázce číslo 10 a může být výhodné opatření provést v rámci jednoho dokumentu.

Má organizace likvidační a spisový řád?

Nemá. Osobní údaje zpracovávané ať již na základě souhlasu nebo jiného legitimního důvodu popsaného v kapitole 3.2.7 Souhlas se zpracováním, mají stanovenou lhůtu pro možnou délku uchování. Délka uchování se pro jednotlivé případy liší a to na zákonné lhůty, na lhůty dané organizačními předpisy a na lhůty stanovené v souhlasu se zpracováním. Po uplynutí stanovené doby je nutné dokumenty a veškeré soubory s osobními údaji zlikvidovat. Tento proces vyžaduje sepsání likvidačního a spisového řádu a je pro soulad s GDPR významně doporučen.

Má organizace definováno, jak bude provádět aktualizaci, výpis a výmaz údajů?

Nemá. Specifikovat jakým způsobem budou vymahatelná práva subjektů údajů je důležitý předpoklad pro splnění souladu s obecným nařízením. Subjekt údajů musí mít možnost vymáhat svá práva na osobní údaje stejně jednoduchým způsobem, jakým osobní údaje předal správci. V případě žádosti o výpis mu musí být navíc poskytnut tento dokument ve strojově čitelném kódu. Pro splnění tohoto požadavku může organizaci velmi pomoci právě spis lokací uložení osobních údajů zmíněný v otázce 10.

Zpracovává firma osobní údaje na základě souhlasu se zpracováním?

Ano, ale omezeně. Organizace dále neaktualizovala znění smluvních dodatků a souhlasů se zpracováním. Jelikož nové nařízení je relativně přísné při zpracování osobních údajů na základě souhlasů se zpracováním, je třeba souhlasy upravit na základě požadavků zmíněných v kapitole 3.2.7 Souhlas se zpracováním. V případě, že probíhá zároveň zpracování některých osobních údajů na základě starého souhlasu se zpracováním, tak je nutné, aby fyzické osoby podepsaly také nově upravený souhlas se zpracováním. V opačném případě není možné jejich osobní údaje dále zpracovávat.

4.2.2 Technická část

Obsahem této části analýzy je přezkoumání technického stavu a IT vybavení společnosti a to zejména s ohledem na zpracování, ochranu, manipulaci, ukládání a zálohování osobních údajů. Průběh celé analýzy je obsahem přílohy 2 – Vstupní analýza GDPR v sekci technické dotazy. Zde budou probrány pouze takové pasáže, kterými je nutné se zabývat v souvislosti s povinnostmi a doporučeními obecného nařízení.

Provádíte monitorování zaměstnanců?

Je používán systém GPS pro služební vozy a čipy pro příchody a odchody zaměstnanců. Na GPS systémech v automobilech lze přepínat mezi soukromou a služební cestou. V systému je potom zobrazeno trasování pouze pro služební cesty. Záznamy odchodů a příchodů slouží pro vyhodnocení docházky.

Má organizace vypracovanou IT směrnici?

Ano, její poslední revize je z července 2014. Vzhledem k velkým změnám technologií v IT infrastruktuře a změnám legislativy je doporučena její revize.

Řídí se organizace standardy ISO 27000?

Neřídí. ISO 27001, někdy také známý pod ISMS, je celosvětově uznávaný standard, který může pomoc organizacím s dodržením souladu obecného nařízení a to zejména v oblasti IT na organizační a bezpečnostní úrovni. Jeho implementace je doporučená minimálně na úrovni souladu s GDPR bez nutnosti získat certifikaci.

Vede organizace evidenci bezpečnostních incidentů?

Nevede. Dokumentace bezpečnostních incidentů může být oporou při zpětném dohledávání a vyhodnocování problémů a také může pomoci s předcházením dalších bezpečnostních incidentů.

Má organizace vypracována krizový plán v případě bezpečnostního incidentu?

Nemá. Krizový plán je důležitou součástí převážně pro velké IT týmy, kde vzniká jeho vytvořením částečná zastupitelnost. Jeho dalším přínosem je však také rychlé dohledání řešení a přesně stanovené postupy, které vedou k rychlé obnově výpadku služeb nebo k řešení bezpečnostního incidentu.

Využívá organizace Identity and Access Management (IAM)?

Nevyužívá. IAM je nástroj, který zajistí lepší správu a přehled nad přidělováním oprávnění v organizaci a to od schvalování práv nadřízenými přes přidělování práv podle oddělení a rolí až po okamžité odebírání práv v případě rozvázání pracovněprávního vztahu.

Využívá organizace Data Loss Prevention (DLP)?

Nevyužívá. DLP je prostředek, který zamezí uživatelům neoprávněně manipulovat se soubory označenými speciálními tagy. DLP je jeden ze základních nástrojů, které mohou významně přispět k prokázání schody s obecným nařízením. Reálně však systém nedokáže zabezpečit veškeré možnosti manipulace s citlivými soubory, a to například přepis údajů na papír nebo jejich focení bez použití počítače. Každé opatření, které alespoň částečně omezí možnost incidentu je přínosem.

Využívá organizace nástroje pro IT audit, monitoring sítě nebo sbírání logů?

Ano, využívá Netwrix, PRTG a poté omezeně Graylog a Aktivity. Logovací nástroj, který dokáže sbírat záznamy z veškerého provozu na síti, je dalším základním prostředkem, který může přispět k prokázání shody s obecným nařízením. Důležitá je však jeho plná funkčnost a pravidelné vyhodnocování logů. Netwrix je nástroj na IT audit, který mimo jiné dovede sledovat připojování uživatelů k serverům a zaznamenávat veškeré manipulace se soubory.

Provádí organizace revize oprávnění uživatelů?

Ano, ale revize se provádí pouze na Active Directory (AD). V případě, že společnost nepoužívá IAM zmíněný v otázce číslo 7 je nezbytné, aby byly v pravidelných intervalech

stanovených IT směrnicí revidovány oprávnění minimálně v AD a v ERP systému, ideálně však ve všech systémech společnosti.

Využívá organizace nějaké další způsoby ochrany osobních údajů?

Ano, využívá šifrování koncových stanic BitLocker a je prováděno pravidelné zálohování serverů na magnetické pásky. Šifrování koncových stanic je však prováděno pouze u přenosných počítačů. U stolních počítačů sice nehrozí takové riziko jako u přenosných, ale je doporučené šifrovat všechny disky a externí paměťová média. Zařízení, která by měla být dále chráněna, jsou mobilní telefony a to alespoň u těch uživatelů, kteří mají z mobilního telefonu přístup k firemnímu emailu. Minimálním zabezpečením telefonu je jeho odemykání číselným kódem, heslem nebo gestem. Ideálním zabezpečením však je spravovat telefon pomocí nástroje MDM neboli Mobile Device Management, který nám mimo jiné umožní v případě ztráty telefonu zařízení vzdáleně restartovat do továrního nastavení.

Provádí organizace pravidelné penetrační testy?

Neprovádí. V organizaci nebylo prováděno penetrační ani jiné testování. Provedení penetračních testů s úspěšným výsledkem dokazuje dobrou bezpečnostní ochranu nejen osobních údajů fyzických osob, ale i dalších důležitých firemních informací.

Využívá firma vzdálený přístup VPN?

Ano, ale zařízení interních uživatelů nejsou nijak kontrolovány a tudíž se uživatel může připojit z kteréhokoli zařízení, což představuje jisté bezpečnostní riziko. V rámci zmírnění rizika by bylo vhodné povolit připojení VPN pouze na firemních počítačích nebo zařízeních prověřených IT administrátory. Pro zařízení externích společností je využíván osobní certifikát.

4.2.3 Existující opatření

Organizace se řídí následujícími organizačními bezpečnostními hledisky:

- Pravidelné roční školení zaměstnanců.
- Interní i externí audity.
- Dobré zabezpečení archivních dokumentů.
- Minimalizace zpracování osobních údajů.

- Minimalizace archivování dokumentů s citlivými údaji fyzických osob.

Organizace využívá následující bezpečnostní technologie a opatření:

- firewall,
- firewallové IDS / IPS,
- ISE IEEE 802.1X,
- antivir,
- zálohování na pásky,
- nástroj pro IT audit,
- logovací nástroje,
- šifrování disků notebooků.

4.2.4 Povinnosti a zlepšovací návrhy

Důležité

- Posouzení vlivu na ochranu osobních údajů (DPIA).
- Vedení záznamů o činnostech zpracování.
- Úprava souhlasů se zpracováním a smluvních dodatků podle obecného nařízení.

Doporučené

- Sepsání směrnice nebo předpisu pro nakládání s osobními údaji.
- Sepsání likvidačního a spisového řádu.
- Zahrnout do ročního školení také bezpečnost a ochranu osobních údajů.
- Úprava smluv s externími firmami.
- Předpis na zajištění práv subjektů údajů a o informování externích firem (výmaz, výpis, aktualizace,…).

- Vedení evidence lokací uložení osobních údajů obsahující typové osobní údaje, přístupy zaměstnanců, odpovědnou osobu.
- Revize IT směrnice.
- Implementace Data Loss Prevention (DLP).
- Provádění revizí oprávnění na všech systémech společnosti.
- Zabezpečení mobilních telefonů administrativních pracovníků.
- Provedení penetračních testů.
- Zabezpečení VPN připojení.

Volitelné

- Implementace ISO 27001.
- Vedení evidence bezpečnostních incidentů.
- Vypracování krizového plánu pro IT.
- Implementace Identity and Access Managementu (IAM).
- Šifrování disků stolních počítačů.

4.3 Technická analýza rizik

Předpokladem prokázání souladu s obecným nařízením o ochraně osobních údajů fyzických osob je zajištění korektního a legitimního zpracování osobních údajů, ale také zajištění celkové bezpečnosti. Každý systém je zabezpečený přesně podle toho, jak je bezpečný jeho nejslabší článek. Z tohoto důvodu je velmi důležité najít veškeré slabé články systému a provést potřebná opatření, která povedou ke zvýšení celkové bezpečnosti organizace. Průběh celé analýzy je obsahem Přílohy 3 – Technická analýza rizik, vzhledem k ochraně a „know-how“ podniku nejsou jmenovány konkrétní technologie. Zde budou probrány a popsány pouze nejrizikovější zranitelnosti. Postup analýzy vychází z kapitoly 3.3.3 Technická analýza rizik.

4.3.1 Stanovení rozsahů hodnot

Parametry	Nejnižší ohodnocení	Nejvyšší ohodnocení	Nejmenší hodnotu má	Požadovaná hodnota	Poznámka
Hodnota aktiva	1	5	nejnižší ohodnocení	-	-
Pravděpodobnost incidentu	1	20	nejnižší ohodnocení	co nejnižší	-
Dopad	1	5	nejnižší ohodnocení	co nejnižší	maximální hodnota je dána hodnotou aktiva
Riziko	1	100	nejnižší ohodnocení	co nejnižší	-

Tabulka 1 – Stanovení rozsahů hodnot technické analýzy rizik

Hodnoty byly stanoveny na základě doporučení z kapitoly 3.3.3 Technická analýza rizik a na principu odhadu nejvhodnější stupnice pro stanovení rizika. Klíčovým parametrem analýzy je riziko, které udává pravděpodobnost, s kterou nastane daná zranitelnost a jaký bude mít celkový dopad na podnik. Maximální hodnota rizika je 100, pokud zvolíme 3 stupňové ohodnocení, tak dostaneme stupnici pro míru rizika a to nízkou, střední a vysokou.

Hodnota rizika	1 - 33	34 - 66	67 - 100
Míra rizika	nízká	střední	vysoká
Poznámka	přijatelné riziko	zvýšené riziko	vyžaduje okamžitou nápravu

Tabulka 2 – Stupnice pro míru rizika

Pravděpodobnosti zranitelností jsou stanoveny na základě subjektivního odhadu autora práce. Dopad zranitelnosti je také subjektivně odhadnut autorem na základě hodnoty aktiva. Dopad zranitelnosti může být oprati hodnotě aktiva snížený dvěma způsoby. Může existovat opatření, které snižuje dopad zranitelnosti na aktivum nebo může dopad konkrétní zranitelnosti způsobit pouze částečné poškození aktiva.

4.3.2 Nízká rizika

Z technické analýzy rizik vyplívá, že v organizaci je 90 zranitelností s nízkým rizikem. Tyto zranitelnosti nepředstavují pro organizaci vážné nebezpečí, a tudíž nemá smysl se jimi zabývat. Jejich případná náprava by pro organizaci ve většině případů znamenala vyšší finanční výdaje než by byl případný dopad této hrozby, navíc v souvislosti s pravděpodobností, s kterou by zranitelnost mohla nastat. Blíže vysvětleno v kapitole 3.3.3 Technická analýza rizik v souvislosti s Obrázkem 2 - Nákladový model bezpečnostního opatření.

4.3.3 Střední rizika

Tato rizika již pro organizaci znamenají určité nebezpeční, které může mít za následek vynaložení značných finančních prostředků. U některých zranitelností je však stále nutné zvážit, zdali by jejich náprava nebyla finančně náročnější, než dopad případné hrozby. Další možností je alespoň částečné omezení pravděpodobnosti dopadu například organizačním předpisem či směrnicí nebo jiným způsobem, který by pro organizaci nebyl nadměrnou finanční zátěží. Zranitelností se středním rizikem je v organizaci 14. Sloupce tabulek jsou pojmenovány zleva a obsahují aktivum, hodnotu, hrozbu, zranitelnost, pravděpodobnost incidentu, dopad, riziko a existující opatření. Celou analýzu lze nalézt v Příloze 3 – Technická analýza rizik.

Zálohovací řešení	**2**	Porucha SW	Velmi nízká spolehlivost SW	17	2	34	-

Tabulka 3 – Střední riziko: zálohovací řešení

Výměnou stávajícího zálohovacího softwaru s nízkou spolehlivostí za nový lze snížit pravděpodobnost výskytu této hrozby.

Připojení k internetu	**4**	Výpadek operátora	Porucha na straně operátora	9	4	36	Duální připojení - kabelové, bezdrátové

Tabulka 4 – Střední riziko: připojení k internetu

Zranitelnost lze odstranit zřízením internetového připojení od dvou operátorů. Toto řešení je však značně nákladné a pravděpodobně by převýšilo výdaje spojené s případným výskytem hrozby.

Call manager	**4**	Výpadek konektivity	Porucha na straně operátora	9	4	36	-

Tabulka 5 – Střední riziko: call manager

Z technických důvodů by v tomto případě nepomohlo zřízení internetového připojení od více operátorů. Omezit riziko je možné pořízením mobilních telefonů pro všechny klíčové zaměstnance.

Active Directory a uživatelské účty	**4**	Zneužití uživatelského účtu	Včasné neodebrání práv uživatelům	13	3	39	-

Tabulka 6 – Střední riziko: active directory a uživatelské účty

Tento problém lze vyřešit implementací IAM (Identity and Access Managementu) v případě dostatečných finančních prostředků anebo úpravou IT směrnice. V IT směrnici je odebírání práv částečně popsáno, avšak chybí zde časové lhůty a bližší popis.

File server	**4**	Neoprávněný přístup a manipulace se soubory	Včasné neodebrání práv uživatelům	13	3	39	Auditní SW file serveru
		Krádež a zneužití citlivých souborů	Prodej informací zaměstnancem firmy	12	3	36	Skupiny přístupů v AD, auditní SW file serveru
			Prodej informací administrátorem	12	4	48	Auditní SW file serveru

Tabulka 7 – Střední riziko: file server

Neoprávněným přístupem a manipulací se soubory jsou myšleny zejména případy, kdy zaměstnanec přechází z jedné pracovní pozice na druhou a nejsou mu bezodkladně revidována oprávnění do všech firemních systémů. Problém lze opět řešit implementací IAM (Identity and Access Managementu) nebo lepšími komunikačními procesy mezi HR a IT oddělením. Krádež a zneužití citlivých souborů zaměstnanci je problém, který byl již v rámci jiných společností několikrát probírán v médiích. Lidská složka patří mezi nejrizikovější bezpečnostní hrozby a je velmi důležité tento faktor nepodcenit. Jedním z nástrojů, který může snížit pravděpodobnost výskytu této hrozby je DLP (Data Loss Prevention).

Osobní počítače	**3**	Napadení škodlivým softwarem (únik, smazání, pozměnění, zašifrování dat a inforamcí)	Emailové přílohy a jiné komunikační kanály	16	3	48	Emailový filtr, antivir
Notebooky	**3**	Napadení škodlivým softwarem (únik, smazání, pozměnění, zašifrování dat a inforamcí)	Emailové přílohy a jiné komunikační kanály	16	3	48	Emailový filtr, antivir

Tabulka 8 – Střední riziko: osobní počítače a notebooky

Napadení počítače škodlivým softwarem nemusí zabránit ani ten nejlepší antivir. Počítač může být infikován mnoha způsoby, ať již pomocí různých komunikačních kanálů anebo přenositelných médií. Primárním řešením tohoto problému by mělo být pravidelné roční školení IT bezpečnosti pro zaměstnance pracující s počítačem. Další možností je také krátké každoroční online studium doplněné o prověřovací testy.

Mobilní telefony	**3**	Krádež telefonu (přístup k firemním datům)	Neexistuje HW zabezpečení	18	3	54	Zodpovědnost uživatelů za převzatý HW

Tabulka 9 – Střední riziko: mobilní telefony

Krádež nebo ztráta telefonu s přístupy zejména k firemnímu emailu a kontaktům může být vážný problém. Hrozící nebezpečí je jak z hlediska GDPR tak z pohledu konkurenčního boje a to zejména pokud se jedná o mobilní telefon některého ze zástupců obchodního oddělení. Minimálním možným řešením je stanovení povinnosti zamykat mobilní telefony administrativních zaměstnanců. Ideálním řešením však je implementace MDM (Mobile Device Management).

Docházkový systém	**3**	Neoprávněný přístup	Neexistují minimální požadavky na heslo interních účtů	12	3	36	-
Ekonomický systém	**4**	Neoprávněný přístup	Neexistují minimální požadavky na heslo interních účtů	12	3	36	-

Tabulka 10 – Střední riziko: docházkový a ekonomický systém

Jedná se zejména o účty administrátorů a správců, u kterých nejsou systémově ani směrnicí stanoveny minimální požadavky na heslo, čímž může dojít k jeho prolomení a neoprávněnému přístupu do zmíněných firemních systémů.

Připojení VPN	**4**	Krádež dat a informací zaměstnancem	Možnost vzdáleného připojení z kteréhokoli zařízení	9	4	36	Auditní SW file serveru
		Zneužití přístupu cizí osobou	Osobní zařízení uživatelů nemusí být chráněna	11	4	44	-

Tabulka 11 – Střední riziko: připojení VPN

Poměrně závažným bezpečnostním rizikem je možnost připojit se do firemní sítě pomocí VPN z kteréhokoli zařízení. Zařízení, z kterých se uživatelé do sítě připojují, by měla být přinejmenším schvalována pracovníky IT oddělení, ideálně by však připojení mělo být možné pouze z firemních notebooků. Hrozí zde nebezpečí krádeže dat a informací zaměstnancem firmy, ale i případnou cizí osobou za pomoci napadeného osobního počítače zaměstnance.

4.3.4 Vysoká rizika

Vysoká rizika představují pro organizaci velké nebezpečí, které může mít v určitých případech s vysokým dopadem na aktiva téměř likvidační důsledek. Pro zranitelnosti, které představují vysoké riziko, by měla být bez zbytečného odkladu sjednána náprava. V analyzované organizaci není situace nijak vážná, existuje zde pouze 1 zranitelnost, která hraničí se středním rizikem. Přesto je důležité situaci nepodcenit a sjednat nápravu co možná nejdříve. Sloupec tabulky je pojmenován zleva a obsahuje aktivum, hodnotu, hrozbu, zranitelnost, pravděpodobnost incidentu, dopad, riziko a existující opatření.

Podnikový informační systém	**5**	Zneužití oprávnění	Přidělování nadbytečných práv	17	4	68	-

Tabulka 12 – Vysoké riziko: podnikový informační systém

Vzhledem k implementaci nového podnikového informačního systému nejsou některé jeho součásti dopracovány, a proto je nezbytné udělovat nadbytečná práva uživatelům s nižšími pravomocemi k zajištění nepřetržitého fungování firmy. Úprava oprávnění pro uživatele by však měla mít vyšší prioritu pro dopracování, jelikož může mít za následek značné finanční ztráty.

4.4 Návrh procesů pro zpracování údajů

Podle nařízení evropského parlamentu a rady (EU) 2016/679 je možné zpracovávat osobní údaje fyzických osob pouze v případě existence legitimního důvodu nebo v případě udělení souhlasu. Dokazování legitimního zpracování je vždy na straně správce, který ze zákona určuje účel a způsob zpracování osobních údajů. Organizace tedy může podle kapitoly 3.2.7 Souhlas se zpracováním zpracovávat osobní údaje subjektů v následujících případech:

- Zpracování za účelem plnění smlouvy.
- Zpracování na základě souhlasu.
- Zpracování z titulu oprávněného zájmu správce.
- Zpracování z titulu plnění zákonné povinnosti.

V případě, že správce předává jemu svěřené osobní údaje třetím stranám (externím zpracovatelům), tak za tyto zpracovatele ručí. Správce musí dále zajistit, aby v případě

vymáhání práv subjektů údajů bylo těmto požadavkům vyhověno a aby byli zpracovatelé o změnách ve zpracování informováni. Práva subjektů údajů jsou podle kapitoly 3.2.8 Práva subjektů údajů následující:

- Právo na přístup k osobním údajům (pasivní právo).
- Právo na aktualizaci údajů.
- Právo být zapomenut.
- Právo na přenositelnost údajů.
- Právo vznést námitku proti zpracování osobních údajů.
- Právo nebýt předmětem rozhodnutí založeného na automatizovaném zpracování.

Ve společnosti PRAKAB s.r.o. se neprovádí žádné rozhodování o subjektech údajů založeném na automatizovaném zpracování. Toto právo tedy není součástí návrhu procesů. V následujících kapitolách budou probrány procesy zpracování osobních údajů odvozené od možností legitimního zpravování zmíněných výše. Veškeré návrhy jsou součástí Přílohy 5 – Návrh procesů zpracování osobních a byly vytvořeny v programu Camunda modeler od společnosti Camunda Services GmbH.

4.4.1 Lokace zpracování a uložení osobních údajů

Práva subjektů údajů jsou plněna na základě Přílohy 4 – Lokace zpracování a uložení osobních údajů, kde je popsáno na jakých místech ukládají jednotlivá oddělení firmy osobní údaje fyzických osob. V případě, že společnost přijme požadavek od subjektu údajů, je tento požadavek rozeslán na všechny oddělení společnosti zpracovávající osobní údaje, tedy na: HR, IT, obchod, nákup, finance, kvalitu, SCM a dále mistrům, asistentkám a vedoucím pracovníkům. Zástupci jednotlivých oddělení poté posoudí, zdali je žadatel zaměstnanec, externista, zákazník nebo dodavatel. V případě, že není známý vztah subjektu k firmě, jsou zkontrolovány veškeré používané systémy a dokumenty daného oddělení. Pokud je žádost podle GDPR oprávněná, je požadavku subjektu vyhověno. V případě nejasnosti zdali se jedná o oprávněnou či neoprávněnou žádost z pohledu GDPR je možné se informovat na oddělení HR. Po interním zpracování požadavku jsou změny ve zpracování oznámeny také případným externím zpracovatelům a výsledek požadavku je zaslán zpět žadateli.

4.4.2 Zpracování za účelem plnění smlouvy

Proces zpracování za účelem plnění smlouvy je znázorněn v Příloze 5 v bodu 1). Proces začíná přijetím údajů pro plnění smlouvy. Během plnění smlouvy a to nezávisle na tom, jakou organizace zastává roli (zákazník nebo dodavatel) může poskytovatel údajů respektive subjekt údajů vymáhat svá práva. V rámci zákona je však možné vymáhat pouze právo na aktualizaci, výpis anebo je možné vznést námitku na omezení zpracování. Tato práva jsou plněna podle kapitoly 4.4.1 Lokace zpracování a uložení osobních údajů. Právo na přístup je poskytnuto již při uzavření smlouvy, právo být zapomenut nelze využít po dobu plnění smlouvy a automatizované zpracování organizace neprovádí. Poté co dojde k vystavení nebo proplacení faktury je možné uchovávat pouze takové osobní údaje, které jsou součástí dokumentů archivovaných ze zákona. Po uplynutí doby archivace je však nutné tyto údaje také zlikvidovat.

4.4.3 Zpracování na základě souhlasu

Proces zpracování na základě souhlasu je znázorněn v Příloze 5 v bodu 2). Proces začíná vystavením souhlasu se zpracováním podle kapitoly 3.2.7 Souhlas se zpracováním a je předán subjektu údajů k podepsání. Pokud subjekt souhlas nepodepíše, jeho údaje není možné zpracovat a proces končí. V případě, že souhlas podepíše, tak jsou údaje zpracovány a využívány ke konkrétnímu účelu po dobu stanovenou v souhlasu. Subjekt však může kdykoli vymáhat svá práva na aktualizaci, výmaz (odvolání souhlasu) anebo výpis. Tato práva jsou plněna podle kapitoly 4.4.1 Lokace zpracování a uložení osobních údajů. Právo na přístup je poskytnuto již při podpisu souhlasu. Právo vznést námitku proti zpracování není relevantní podávat, když lze využít možnosti odvolat souhlas a automatizované zpracování organizace neprovádí. Po uplynutí doby pro zpracování je nutné veškeré údaje subjektu smazat.

4.4.4 Zpracování z titulu oprávněného zájmu správce

Proces zpracování z titulu oprávněného zájmu správce je znázorněn v Příloze 5 v bodu 3). Tento proces začíná vznikem jakéhokoli kontaktu subjektu se společností, při kterém jsou zpracovávány osobní údaje subjektu. Typickým příkladem tohoto zpracování je kamerový systém, který spadá pod zpracování osobních údajů za účelem ochrany majetku. Údaje se uchovávají po dobu stanovenou organizací v ideálním případě na základě interních předpisů.

Po uplynutí stanovené doby je nezbytné zpracovávané údaje zlikvidovat. V tomto případě zpracování nemusí být vždy právo na přístup poskytováno subjektům údajů již v počátku zpracování jejich osobních údajů. Subjekty mají tedy právo na aktualizaci, výpis, přístup k údajům anebo právo vznést námitku proti zpracování, která má v tomto případě velký význam. Tato práva jsou plněna podle kapitoly 4.4.1 Lokace zpracování a uložení osobních údajů. Právo být zapomenut je vymahatelné pouze přes námitku proti zpracování a automatizované zpracování organizace neprovádí.

4.4.5 Zpracování z titulu plnění zákonné povinnosti

Proces zpracování z titulu plnění zákonné povinnosti je znázorněn v Příloze 5 v bodu 4). Tento proces začíná kontaktem založeným na speciálním vztahu mezi subjektem a společností. Typickým případem je zpracování osobních údajů zaměstnanců. Údaje se zpracovávají na základě zákona, kde je stanovena povinnost pro zpracování a případná doba archivace pro konkrétní případ. Při rozvázání vztahu nebo uplynutí doby je nutné bezodkladně zpracovávané údaje zlikvidovat. Subjekt údajů může kdykoli během procesu vymáhat svá práva na aktualizaci, výpis, přístup anebo vznést námitku proti zpracování. Pasivní právo na přístup opět může, ale nemusí být součástí prvotního kontaktu. Tato práva jsou plněna podle kapitoly 4.4.1 Lokace zpracování a uložení osobních údajů. Právo být zapomenut je vymahatelné pouze přes námitku proti zpracování a automatizované zpracování organizace neprovádí.

5 Závěr

Hlavním cílem bakalářské práce bylo zhodnotit a popsat požadavky obecného nařízení vzhledem ke zpracování osobních údajů ve velkém výrobním podniku, jehož výstupem mělo být stanovení povinností a doporučení, která povedou k prokázání souladu s GDPR. Doplňkovým cílem bylo stanovení bezpečnostních opatření, které v případě implementace mohou vést ke zlepšení celkové ochrany IT infrastruktury. Dalším vedlejším cílem byl návrh procesů legitimního zpracování osobních údajů fyzických osob, které jsou v souladu s obecným nařízením.

V teoretické části práce byly popsány obecné požadavky nařízení, dále byly vylíčeny postupy GDPR analýzy a technické analýzy rizik, následoval průzkum organizačních a technických bezpečnostních opatření, které by umožnili prokázat soulad s nařízením a také celkově zabezpečit IT infrastrukturu. Závěrem teoretické části byl krátký popis procesního modelování. První kapitola praktické části poskytla čtenáři základní informace o společnosti, která byla předlohou bakalářské práce. Druhá kapitola se zabývala dotazníkovým šetřením stavu společnosti a posouzením souladu na základě povinností a doporučení plynoucích z GDPR. Otázky dotazníkového šetření byly zkonstruovány na základě znalostí získaných z teoretické části. Třetí kapitola se věnovala postupu a vyhodnocení technické analýzy rizik, která pomohla indikovat bezpečnostní nedostatky v organizaci. Poslední, čtvrtá kapitola popisuje veškeré procesy, za kterých je možné z legitimních důvodů zpracovávat osobní údaje.

Výsledkem bakalářské práce je zjištění, že za účelem prokázání souladu s minimálními povinnými požadavky GDPR, musí společnost zhotovit nebo upravit následující dokumenty: posouzení vlivu na ochranu osobních údajů (DPIA), vedení záznamů o činnostech zpracování a úprava souhlasů se zpracováním a smluvních dodatků. Je však vhodné zvážit také implementaci doporučení stanovených ve vstupní analýze. Z technické analýzy rizik vyplývá, že největší bezpečnostní zranitelností, je přidělování nadbytečných práv v podnikovém informačním systému. Je však žádoucí posoudit a zabývat se také středně vážnými zranitelnostmi v podniku, kterých je celkem 14. U všech zranitelností se středním a vyšším rizikem je v praktické části popsán způsob, jak toto riziko snížit. Závěrem jsou navrženy 4 procesy na základě shodného množství legitimních důvodů zpracování osobních údajů, za kterých může jakákoli organizace zpracovávat osobní údaje fyzických osob.

Přínosem bakalářské práce je ucelený soupis pravidel a poznatků problematiky GDPR v teoretické části práce. Tento soupis může pomoci organizacím, které nemají časové možnosti a kapacity, aby hledaly jednotlivé požadavky obecného nařízení. Dalším přínosem je sestavení praktického postupu řešení, kterým se mohou firmy inspirovat při zavádění GDPR. Tento postup se skládá ze vstupní analýzy, technické analýzy rizik a návrhu procesů. Kromě již zmíněných obecných přínosů, které mohou využít organizace v České republice, má práce také přínos konkrétní, a to pro společnost PRAKAB. Pro tuto společnost byly stanoveny požadavky obecného nařízení, zjištěny zranitelnosti aktiv a jejich rizika a také navrženy procesy zpracování osobních údajů.

Závěrem lze konstatovat, že bezpečnostní stav analyzované organizace není zásadně kritický a že po zhotovení nebo úpravě relativně malého množství dokumentů lze prohlásit, že je společnost PRAKAB v souladu s GDPR.

6 Seznam použitých zdrojů

[1] ŠMÍD, V. Zákon č. 101/2000 Sb.: o ochraně osobních údajů a o změně některých zákonů (komentář). *FI Masarykova univerzita* [online]. Brno, 2000 [cit. 2018-03-08]. Dostupné z: https://www.fi.muni.cz/~smid/zood.htm

[2] ŠKORNIČKOVÁ, E. Co je GDPR?. *Obecné nařízení o ochraně osobních údajů: prakticky* [online]. Praha, 2016 [cit. 2018-03-08]. Dostupné z: https://www.gdpr.cz/gdpr/

[3] MARCÍN, V. GDPR v otázkách a odpovědích. *Úřad pro ochranu osobních údajů* [online]. Praha, 2017 [cit. 2017-11-07]. Dostupné z: https://www.uoou.cz/gdpr-v-nbsp-otazkach-a-nbsp-odpovedich/d-23790/p1=3938/

[4] ŠKORNIČKOVÁ, E. Citlivé osobní údaje. *Obecné nařízení o ochraně osobních údajů: prakticky* [online]. Praha, 2016 [cit. 2018-03-08]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/

[5] ŠKORNIČKOVÁ, E. Subjekt údajů. *Obecné nařízení o ochraně osobních údajů: prakticky* [online]. Praha, 2016 [cit. 2018-03-08]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/subjekt-udaju/

[6] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *EUR-Lex*. Brusel: EU, 2016, L 119/1. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS

[7] MARCÍN, V. GDPR a role ÚOOÚ. *Úřad pro ochranu osobních údajů* [online]. Praha, 2017 [cit. 2018-03-08]. Dostupné z: https://www.uoou.cz/gdpr-a-role-uoou/ds-4726/p1=4726

[8] KALÍŠEK, J. a P. VĚŽNÍKOVÁ. Pověřenec pro ochranu osobních údajů dle nařízení GDPR: Nové pokyny WP29 k výkonu funkce. *Epravo.cz* [online]. Praha, 2017 [cit. 2018-03-08]. Dostupné z: https://www.epravo.cz/top/clanky/poverenec-pro-ochranu-osobnich-udaju-dle-narizeni-gdpr-nove-pokyny-wp29-k-vykonu-funkce-104829.html

[9] VESECKÝ, Z. Jeden souhlas nestačí. Pro zpracování osobních údajů bude nutný double opt-in. *Podnikatel.cz: Průvodce vaším podnikáním* [online]. Praha, 2017 [cit. 2018-03-08]. Dostupné z: https://www.podnikatel.cz/clanky/jeden-souhlas-nestaci-pro-zpracovani-osobnich-udaju-bude-nutny-double-opt-in/

[10] ŠKORNIČKOVÁ, E. Souhlas se zpracováním osobních údajů. *Obecné nařízení o ochraně osobních údajů prakticky: prakticky* [online]. Praha, 2016 [cit. 2018-03-08]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/souhlas-se-zpracovanim-osobnich-udaju/

[11] DPO4U. *Oprávněný zájem* [online]. Pardubice, 2017 [cit. 2018-03-08]. Dostupné z: https://www.dpo4u.cz/l/opravneny-zajem/

[12] Asociace za lepší ICT řešení, o.p.s. *III. Kapitola: Práva subjektu údajů* [online]. Praha, © 2018 [cit. 2018-03-08]. Dostupné z: https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/gdpr-narizeni-iii-prava-subjektu-udaju/#13

[13] Asociace za lepší ICT řešení, o.p.s. *6. Práva subjektu údajů* [online]. Praha, 2017 [cit. 2018-03-08]. Dostupné z: https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/smernice-gdpr-otazky-6-prava-subjektu-udaju/

[14] ŠKORNIČKOVÁ, E. Zpracování osobních údajů. *Obecné nařízení o ochraně osobních údajů: prakticky* [online]. Praha, 2016 [cit. 2018-03-08]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/zpracovani-osobnich-udaju/

[15] Bohemiasoft s.r.o.: Webareal. *GDPR – nová právní úprava ochrany osobních údajů: Díl 4 – Omezení účelem a Minimalizace dat* [online]. 2017 [cit. 2018-03-08]. Dostupné z: https://blog.webareal.cz/gdpr-nova-pravni-uprava-ochrany-osobnich-udajudil-4-omezeni-ucelem-a-minimalizace-dat/

[16] CALDER, A. *EU GDPR: A Pocket Guide* [online]. (PDF). Cambridgeshire: IT Governance Publishing, 2016 [cit. 2018-03-08]. ISBN 978-1-84928-832-3. Dostupné z: http://www.datastax.com/wp-content/uploads/resources/whitepaper/GDPR-Pocket-guide-English.pdf

[17] MARCÍN, V. *11.* Sankce, pokuty. *Úřad pro ochranu osobních údajů* [online]. Praha, 2017 [cit. 2018-02-14]. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287

[18] GOLL, J. a I. SVOBODA. Detekce, analýza a řešení bezpečnostních problémů. *Průvodce ochranou osobních údajů*. Praha: Economia, a.s., 2017, s. 24-25.

[19] ŠKORNIČKOVÁ, E. Šifrování. *Obecné nařízení o ochraně osobních údajů: prakticky* [online]. Praha, 2016 [cit. 2018-03-08]. Dostupné z: https://www.gdpr.cz/blog/stitek/sifrovani/

[20] ESET, s.r.o. *Obecné nařízení o ochraně osobních údajů (GDPR)* [online]. (PDF). Severní Amerika: ESET, ©2018 [cit. 2018-03-08]. Dostupné z: https://encryption.eset.com/cz/wp-content/uploads/sites/25/2017/02/Deslock_Obecne-narizeni-GDPR_2017b.pdf

[21] ZACH, R. Správa a fungování Internetu: Šifrování. *Jak na internet* [online]. ČR: CZ.NIC, ©2018 [cit. 2018-03-08]. Dostupné z: https://www.jaknainternet.cz/page/1251/sifrovani/

[22] Asociace za lepší ICT řešení, o.p.s. *Směrnice GDPR – otázky: 10. Předávání osobních údajů do jiných zemí* [online]. Praha, 2017 [cit. 2018-03-08]. Dostupné z: https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/smernice-gdpr-otazky-10-predavani-osobnich-udaju-do-jinych-zemi/

[23] Hospodářská komora České republiky. *NOVÁ PRAVIDLA OCHRANY OSOBNÍCH ÚDAJŮ* [online]. (PDF). Praha: Hospodářská komora České republiky Odbor legislativy, práva a analýz, 2017 [cit. 2017-11-07]. Dostupné z: https://www.komora.cz/wp-content/uploads/2017/06/PriruckaGDPR_final.pdf

[24] ARTICLE 29: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. In: *DATA PROTECTION WORKING PARTY*. Brusel: WP29, 2017. Dostupné také z: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

[25] PECHANEC, I. 3. Nařízení GDPR z pohledu IT: činnosti vedoucí ke splnění nařízení GDPR. *Techbit.cz: život, vesmír, IT a vůbec...* [online]. 2017 [cit. 2018-03-08]. Dostupné z: https://www.techbit.cz/2017/3-narizeni-gdpr-z-pohledu-it-cinnosti-vedouci-ke-splneni-narizeni-gdpr/

[26] DOUCEK, P., L. NOVÁK a V. SVATÁ. *Řízení bezpečnosti informací*. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7

[27] SMEJKAL, V. a K. RAIS. *Řízení rizik*. Praha: Grada, 2003. Expert (Grada). ISBN 80-247-0198-7.

[28] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

[29] ŠKORNIČKOVÁ, E. Jednoduchý test: Jak jste na tom s přípravou na GDPR?. *Obecné nařízení o ochraně osobních údajů: prakticky* [online]. Praha, 2017 [cit. 2018-03-08]. Dostupné z: https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/

[30] POŽÁR, J. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

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

[32] TROST, R. *Practical intrusion analysis: prevention and detection for the twenty-first century*. Upper Saddle River, c2010. ISBN 0321591801.

[33] ManagementMania.com. *Audit* [online]. Wilmington, 2017 [cit. 2018-03-08]. Dostupné z: https://managementmania.com/cs/audit

[34] Antivirové centrum. *CHRAŇTE SVŮJ POČÍTAČ: Softwarové Firewally* [online]. Praha [cit. 2018-03-08]. Dostupné z: https://www.antivirovecentrum.cz/firewally.aspx

[35] Bezpečnýinternet.cz. *Ochrana osobního počítače* [online]. [cit. 2018-03-08]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/ochrana.aspx

[36] GAPP Systém, s.r.o. Propagační materiály. *Typizovaná technická opatření pro zajištění vysoké míry ICT bezpečnosti a souladu s GDPR*. Praha.

[37] Safetica Technologies, s.r.o. Propagační materiály. *Safetica Datasheet*. Brno.

[38] ROHLEDER, D. a V. LORENC. *802.1X - autentizace v počítačových sítích* [online]. (PDF). [cit. 2018-03-08]. Zpravodaj ÚVT MU. ISSN 1212-0901, 2008, roč. XIX, č. 1, s. 2-4. Dostupné z: http://webserver.ics.muni.cz/bulletin/clanky_tisk/590.pdf

[39] STEINER, F. Případová studie analýzy rizik informační bezpečnosti. *BPM téma* [online]. Plzeň: BPS Business Process Services, ©2007 [cit. 2018-03-08]. Dostupné z: http://bpm-tema.blogspot.cz/2007/11/ppadov-studie-analzy-rizik-informan.html

[40] PRAKAB PRAŽSKÁ KABELOVNA, s.r.o. *PROFIL SPOLEČNOSTI 2018* [online]. (PDF). In: Praha, 2018 [cit. 2018-03-08]. Dostupné z: https://www.prakab.cz/upload/prezentace_CZ.pdf

[41] ASUSTeK Computer Inc. *FAQ: Co je Mobile Device Management (MDM)?* [online]. Tchaj-pej 2016 [cit. 2018-03-08]. Dostupné z: https://www.asus.com/cz/support/FAQ/1018796/

[42] EXPERIA GROUP, s.r.o. *Penetrační testování.* [online]. Pardubice, ©2012 [cit. 2018-03-08]. Dostupné z: https://www.experia.cz/penetracni-testovani/

[43] Object Management Group, Inc. Object Management Group Business Process Model and Notation: Charter. *OMG: we set the standard* [online]. ©2018 [cit. 2018-03-08]. Dostupné z: http://www.bpmn.org/

[44] KLUG Solutions. *Diagram aktivit - BPMN* [online]. ©2015 [cit. 2018-03-08]. Dostupné z: http://www.klugsolutions.cz/znalostni-baze/objekty-diagramu-aktivit-BPMN.htm

[45] SOMMERVILLE, I. *Softwarové inženýrství*. Brno: Computer Press, 2013. ISBN 978-80-251-3826-7.

7 Přílohy

Příloha 1 – Vybrané články obecného nařízení

Informace a přístup k osobním údajům

Článek 13

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

1. Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne správce v okamžiku získání osobních údajů subjektu údajů tyto informace:

a) totožnost a kontaktní údaje správce a jeho případného zástupce;

b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů;

c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;

d) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);

e) případné příjemce nebo kategorie příjemců osobních údajů;

f) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.

2. Vedle informací uvedených v odstavci 1 poskytne správce subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování:

a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

b) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

c) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;

d) existence práva podat stížnost u dozorového úřadu;

e) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;

f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

3. Pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace uvedené v odstavci 2.

4. Odstavce 1, 2 a 3 se nepoužijí, pokud subjekt údajů již uvedené informace má, a do té míry, v níž je má. [6, str. 40-41]

Článek 14

Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů

1. Jestliže osobní údaje nebyly získány od subjektu údajů, poskytne správce subjektu údajů tyto informace:

a) totožnost a kontaktní údaje správce a případně jeho zástupce;

b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů;

c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;

d) kategorie dotčených osobních údajů;

e) případné příjemce nebo kategorie příjemců osobních údajů; 4.5.2016 L 119/41 Úřední věstník Evropské unie CS

f) případný záměr správce předat osobní údaje příjemci ve třetí zemi nebo mezinárodní organizaci a existence či neexistence rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo v čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.

2. Kromě informací uvedených v odstavci 1 poskytne správce subjektu údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů:

a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

b) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);

c) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

d) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;

e) existence práva podat stížnost u dozorového úřadu;

f) zdroj, ze kterého osobní údaje pocházejí, a případně informace o tom, zda údaje pocházejí z veřejně dostupných zdrojů;

g) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

3. Správce poskytne informace uvedené v odstavcích 1 a 2:

a) v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;

b) nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo

c) nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

4. Pokud správce hodlá osobní údaje dále zpracovat pro jiný účel, než pro který byly získány, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace uvedené v odstavci 2.

5. Odstavce 1 a 4 se nepoužijí, pokud a do té míry, v níž:

a) subjekt údajů již uvedené informace má;

b) se ukáže, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí; to platí zejména v případě zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely s výhradou podmínek a záruk uvedených v čl. 89 odst. 1, nebo pokud je pravděpodobné, že uplatnění povinnosti uvedené v odstavci 1 tohoto článku by znemožnilo nebo výrazně ztížilo dosažení cílů uvedeného zpracování. V takových případech přijme správce vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů, včetně zpřístupnění daných informací veřejnosti;

c) je získávání nebo zpřístupnění výslovně stanoveno právem Unie nebo členského státu, které se na správce vztahuje a v němž jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektu údajů; nebo

d) osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu, včetně zákonné povinnosti mlčenlivosti. [6, str. 41-42]

Článek 83, odstavec 2

Obecné podmínky pro ukládání správních pokut

2. Správní pokuty se ukládají podle okolností každého jednotlivého případu kromě či namísto opatření uvedených v čl. 58 odst. 2 písm. a) až h) a j). Při rozhodování o tom, zda

uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se řádně zohlední tyto okolnosti:

a) povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena;

b) zda k porušení došlo úmyslně nebo z nedbalosti;

c) kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů;

d) míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedeným podle článků 25 a 32;

e) veškerá relevantní předchozí porušení správcem či zpracovatelem;

f) míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků;

g) kategorie osobních údajů dotčené daným porušením;

h) způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře;

i) v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízena opatření uvedená v čl. 58 odst. 2, splnění těchto opatření;

j) dodržování schválených kodexů chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 a

k) jakoukoliv jinou přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení. [6, str. 82]

Článek 32

Zabezpečení zpracování

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody

fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování osobních údajů;

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

3. Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je dodržování schváleného kodexu chování uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42.

4. Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu. [6, str. 51-52]

Článek 46

Předávání založené na vhodných zárukách

1. Jestliže neexistuje rozhodnutí podle čl. 45 odst. 3, správce nebo zpracovatel mohou předat osobní údaje do třetí země nebo mezinárodní organizaci, pouze pokud správce nebo zpracovatel poskytl vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů.

2. Vhodné záruky uvedené v odstavci 1 mohou být stanoveny, aniž je zapotřebí jakékoli zvláštní povolení dozorového úřadu, pomocí:

a) právně závazného a vymahatelného nástroje mezi orgány veřejné moci nebo veřejnými subjekty;

b) závazných podnikových pravidel v souladu s článkem 47;

c) standardních doložek o ochraně osobních údajů přijatých Komisí přezkumným postupem podle čl. 93 odst. 2;

d) standardních doložek o ochraně údajů přijatých dozorovým úřadem a schválených Komisí přezkumným postupem podle čl. 93 odst. 2;

e) schváleného kodexu chování podle článku 40 spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů; nebo

f) schváleného mechanismu pro vydání osvědčení podle článku 42 spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů.

3. S výhradou povolení od příslušného dozorového úřadu mohou být vhodné záruky uvedené v odstavci 1 rovněž stanoveny zejména pomocí:

a) smluvních doložek mezi správcem nebo zpracovatelem a správcem, zpracovatelem nebo příjemcem osobních údajů ve třetí zemi nebo v mezinárodní organizaci; nebo

b) ustanovení určených k vložení do správních ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektu údajů.

4. Dozorový úřad použije mechanismus jednotnosti v případech uvedených v čl. 63 odst. 3 tohoto článku.

5. Povolení členského státu nebo dozorového úřadu na základě čl. 26 odst. 2 směrnice 95/46/ES zůstávají platná až do chvíle, kdy je dozorový úřad v případě potřeby změní, nahradí nebo zruší. Rozhodnutí přijatá Komisí na základě čl. 26 odst. 4 směrnice 95/46/ES zůstávají platná až do chvíle, kdy je Komise podle potřeby změní, nahradí nebo zruší rozhodnutím přijatým podle odstavce 2 tohoto článku. [6, str. 62]

Příloha 2 – Vstupní analýza GDPR

Organizační dotazy

1. **Bylo provedeno zhodnocení, zda firma musí jmenovat DPO?**
   Ano, DPO není potřeba.

   a. **Pokud ano, byl tento DPO již jmenován?**
      Ne, není potřeba.

   b. **Pokud ne, byla stanovena kontaktní osoba?**
      Ano, HR director.

2. **Je organizace správce nebo zpracovatel?**
   Správce.

3. **Má organizace předpisy a směrnice pro ochranu osobních údajů?**
   Ne.

4. **Jak často se provádí aktualizace interních předpisů?**
   Pouze v případě legislativních změn.

5. **Provádí firma školení zaměstnanců?**
   Ano.

   a. **Pokud ano, jak často je školení prováděno?**
      Jednou ročně probíhá interní školení všech zaměstnanců. Odborné školení provádí externí firmy v intervalech daných zákonem.

   b. **Pokud ano, školení provádí jen interní pracovníci nebo i externí firmy?**
      Školení provádí i externí firmy.

   c. **Pokud ano, zahrnuje školení také poučení o nakládání s osobními údaji?**
      Ne.

6. **Provádí firma audity?**
   Ano.

   a. **Pokud ano, komu jsou audity reportovány?**
      Vedení společnosti a příslušným úřadům.

b. **Pokud ano, jsou prováděny interně nebo externě?**
   Interně i externě.

7. **Poskytuje organizace osobní údaje externím firmám - zpracovatelům?**
   Ano.

   a. **Pokud ano, byla provedena úprava smluv s externími firmami?**
      Ne.

   b. **Pokud ano, byl stanoven plán informování zpracovatelů o změnách nebo smazání údajů?**
      Ne.

8. **Poskytuje organizace osobní údaje do zahraničí?**
   Ano.

   a. **Pokud ano, komu?**
      Sesterským společnostem.

9. **V jaké formě organizace uchovává dokumenty s osobními údaji?**
   V elektronické i papírové formě.

   a. **Pokud v papírové existuje nějaké zabezpečení těchto dokumentů?**
      Ano, dokumenty jsou zabezpečeny za zamčenými dveřmi s omezeným přístupem.

10. **Vede organizace dokumentaci o lokacích uložení osobních údajů?**
    Ne.

    a. **Existuje evidence osobních údajů uchovávaných v elektronické podobě?**
       Ne.

    b. **Existuje evidence osobních údajů uchovávaných v listinné podobě?**
       Ne.

11. **Vede organizace dokumentaci o posouzení vlivu na ochranu osobních údajů (DPIA)?**
    Ne.

12. Vede organizace záznamy o činnostech zpracování?

Ne.

13. Vede organizace evidenci oprávnění zaměstnanců na přístup k osobním údajům?

Ne.

14. Má organizace likvidační a spisový řád?

Ne.

15. Má organizace definováno, jak bude provádět aktualizaci, výpis a výmaz údajů?

Ne.

16. Na jakých odděleních se zpracovávají osobní údaje?

HR, IT, obchod, nákup, finanční, kvalita, SCM, mistři, asistentky a vedoucí pracovníci.

17. Zpracovává organizace citlivé osobní údaje nebo údaje o dětech?

Ano, ale pouze z titulu plnění zákonné povinnosti.

18. Zpracovává firma osobní údaje na základě souhlasu se zpracováním?

Ano, ale omezeně.

a. Aktualizovala organizace znění smluvních dodatků a souhlasů se zpracováním?

Ne.

Technické dotazy

1. **Provádíte monitorování zaměstnanců?**

   Ano.

   a. **Pokud ano, jaké?**

      Je používán systém GPS pro služební vozy a čipy pro odchody a příchody.

2. ***Má organizace vypracovanou IT směrnici?***

   Ano

   a. **Pokud ano, kdy byla naposled revidována?**

      V červenci 2014.

3. **Řídí se organizace standardy ISO 27000?**

   Ne.

4. **Vede organizace evidenci bezpečnostních incidentů?**

   Ne.

5. **Má organizace vypracována krizový plán v případě bezpečnostního incidentu?**

   Ne.

6. **Provádí organizace automatizované zpracování a profilování osobních údajů?**

   Ne.

7. **Využívá organizace Identity and Access Management (IAM)?**

   Ne.

8. **Využívá organizace Data Loss Prevention (DLP)?**

   Ne.

9. **Využívá organizace nástroje pro IT audit, monitoring sítě nebo sbírání logů?**

   Ano, využívá Netwrix, PRTG a poté omezeně Graylog a Aktivity.

10. **Využívá organizace nějaké technologie na ochranu proti průniku zvenčí?**

    Ano, využívá firewall, který sbírá také logy a má IDS/IPS.

11. **Využívá organizace nějaké interní bezpečnostní technologie?**

    Ano, je naimplementováno ISE IEEE 802.1X a antivir na uživatelských počítačích.

12. Provádí organizace revize oprávnění uživatelů?

Provádí revize pouze na Active Directory (AD).

13. Využívá organizace nějaké další způsoby ochrany osobních údajů?

Ano, využívá šifrování koncových stanic BitLocker a je prováděno pravidelné zálohování serverů na magnetické pásky.

14. Jaké komunikační nástroje se ve firmě používají?

Email, Facebook Workplace, Skype.

15. Kde všude jsou ukládána data s osobními údaji?

Zálohy, fileserver, exchange, docházkový, ekonomický a mzdový systém, ERP, CRM, GPS, kamerové systémy.

16. Provádí organizace pravidelné penetrační testy?

Ne.

17. Využívá firma vzdálený přístup VPN?

Ano.

a. **Jsou prověřována zařízení, z kterých se uživatelé na VPN připojují?**

   U externích společností je využíván osobní certifikát. U interních uživatelů zařízení prověřována nejsou.

Příloha 3 – Technická analýza rizik

Aktivum	Hodnota	Hrozba	Zranitelnost	Pravděpod. incidentu	Dopad	Riziko	Existující opatření
Virtualizační prostředí	**5**	Porucha HW	Nespolehlivost některých HW prvků	5	5	25	Duplikovaná paměť
		Porucha SW	Neočekávaná chyba	3	5	15	
Hlavní diskové pole	**4**	Porucha disků	Nadměrná zátěž	8	2	16	RAID ochrana, redundance v rámci pole
		Porucha HW	Neustálý provoz	5	3	15	Záložní diskové pole
		Fyzický přístup - odcizení, podvrhnutí dat	Nízké fyzické zabezpečení	4	3	12	Dvojté dveře na zámek, omezený přístup do areálu
		Síťový přístup - odcizení, podvrhnutí dat	Možné bezpečnostní hrozby	4	3	12	802.1X
Záložní diskové pole	**3**	Fyzický přístup - odcizení, podvrhnutí dat	Nízké fyzické zabezpečení	5	2	10	Přístup do serverovny na čip, omezený přístup do areálu
		Síťový přístup - odcizení, podvrhnutí dat	Možné bezpečnostní hrozby	4	2	8	802.1X
Zálohovací řešení	**2**	Porucha HW	Neustálý provoz	5	2	10	
		Porucha SW	Velmi nízká spolehlivost SW	17	2	34	
		Neúmyslný incident - špatné nastavení	Nedostatečné školení	6	1	6	
Zálohovací pásky	**3**	Odcizení - ztráta a zneužití dat	Nízké fyzické zabezpečení	4	2	8	Přístup do serverovny na čip, omezený přístup do areálu
		Přírodní a jiné katastrofy	Nízká fyzická odolnost média	3	2	6	
HW v hlavní serverovně	**5**	Vysoké teploty	Může dojít k přehřátí HW	6	4	24	Chlazeno klimatizací, vysoké teploty zasílány administrátorovi
		Přírodní a jiné katastrofy	Náchylnost elektronických zařízení	3	5	15	Vybudována záložní serverovna
		Úmyslné zničení zařízení	Nízké fyzické zabezpečení	3	5	15	Dvojté dveře na zámek, omezený přístup do areálu
HW v záložní serverovně	**3**	Vysoké teploty	Může dojít k přehřátí HW	8	2	16	Chlazeno klimatizací
		Přírodní a jiné katastrofy	Náchylnost elektronických zařízení	3	3	9	
		Úmyslné zničení zařízení	Nízké fyzické zabezpečení	3	3	9	Přístup do serverovny na čip, omezený přístup do areálu
HW na skladě	**3**	Krádež HW a disků s daty	Velmi nízké fyzické zabezpečení	3	3	9	Přístup přes prosklené dveře

Aktivum	Hodnota	Hrozba	Zranitelnost	Pravděpod. incidentu	Dopad	Riziko	Existující opatření
Switche v areálu	**3**	Náhodné nebo úmyslné vypnutí switche	Switche připojeny na společných pojiskách	15	2	30	
		Porucha switche	Velmi prašné prostředí	6	2	12	Switche umístěny v racích
		Změna konfigurace switche	Možné bezpečnostní hrozby	3	3	9	802.1X, chráněno heslem
		Připojení vlastního zařízení jiné osoby	Přístupné zásuvky v areálu	6	2	12	802.1X, vypínání nevyužívaných zásuvek
AP v areálu	**3**	Porucha HW	Vystaveno povětrnostním vlivům	10	2	20	AP umístěny v krabicích
			Záměrné zničení	3	2	6	AP umístěny v krabicích
		Neoprávněné připojení k síťi	Dobrá dostupnost GUEST účtů	13	2	26	802.1X, VLANa umožňující přístup pouze do internetu
			Možné bezpečnostní hrozby	8	2	16	802.1X
AP kontroler	**3**	Porucha HW	Neustálý provoz	3	3	9	
Kamerový systém	**2**	Zneužití záznamů	Přístupnost obsluhy k záznamům	5	2	10	Fyzická nepřístupnost k souborům se záznamy, záznamy je možné pouze prohlížet
		Porucha kamer	Vystaveno povětrnostním vlivům	10	1	10	Kamery průběžně servisovány
			Záměrné zničení	3	1	3	
		Porucha ostatního HW	Porucha switche na provoz kamer	5	2	10	Spravuje externí společnost
			Porucha serveru	5	2	10	Omezení zátěže - přístup pouze pro vrátnici
Připojení k internetu	**4**	Výpadek operátora	Porucha na straně operátora	9	4	36	Duální připojení - kabelové, bezdrátové
		Porucha interních prvků	Porucha firewallu	3	4	12	Duální firewall
Firewall	**4**	Porucha firewallu	Neustálý provoz	3	4	12	Duální firewall
		Průnik do sítě	Možné bezpečnostní hrozby	8	4	32	Firewallové IDS/IPS, sběr logů
Call manager	**4**	Porucha kontroleru	Neustálý provoz	3	4	12	Duální kontroler
		Výpadek Linux serveru	Neočekávaná chyba	3	4	12	Duální server
		Výpadek konektivity	Porucha na straně operátora	9	4	36	

Aktivum	Hodnota	Hrozba	Zranitelnost	Pravděpod. incidentu	Dopad	Riziko	Existující opatření
Tiskárny a služby tisku	**4**	Výpadek Windows serveru	Neočekávaná chyba	3	4	12	Připraven záložní server
		Výpadek služeb print serveru	Neočekávaná chyba	3	4	12	Spravuje externí společnost
		Porucha tiskárny	Prašné prostředí	9	2	18	Spravuje externí společnost
			Neustálý provoz	8	2	16	Spravuje externí společnost
			Odpojení tiskárny ze sítě	6	2	12	
		Krádež dat a informací	Zpětné vytištění dokumentů při neodhlášení uživatele na tiskárně	8	3	24	Nastavený timeout pro odhlášení
Active Directory a uživatelské účty	**4**	Výpadek Windows serveru	Neočekávaná chyba	3	4	12	Duální instalace serveru a propojení sesterských společností
		Zneužití uživatelského účtu	Včasné neodebrání práv uživatelům	13	3	39	
Exchange a emaily	**4**	Výpadek Windows serveru	Neočekávaná chyba	3	4	12	Propojení sesterských společností
		Podvržení emailového účtu	Podvodné emaily vydávající se za zaměstnanecké	4	3	12	Certifikace emailů klíčových uživatelů
		Zneužívání firemního emailu k soukromým účelům	Nedostatečné školení	14	2	28	
		Infikace počítače uživatele	Otevírání neznámých příloh - firemní email	7	3	21	Antivir, emailový filtr, firewallový IDS/IPS
			Otevírání neznámých příloh - soukromý email	10	3	30	Antivir, firewallový IDS/IPS, IT směrnice
		Infikace síťových disků	Otevírání neznámých příloh - firemní email	5	4	20	Antivir, emailový filtr, firewallový IDS/IPS
			Otevírání neznámých příloh - soukromý email	8	4	32	Antivir, firewallový IDS/IPS, IT směrnice

Aktivum	Hodnota	Hrozba	Zranitelnost	Pravděpod. incidentu	Dopad	Riziko	Existující opatření
File server	**4**	Neoprávněný přístup a manipulace se soubory	Včasné neodebrání práv uživatelům	13	3	39	Auditní SW file serveru
			Možné bezpečnostní hrozby	8	4	32	802.1X, auditní SW file serveru
		Náhodné smazání, úprava, přepis souborů	Lidská chyba	6	3	18	Pravidelné zálohování
		Krádež a zneužití citlivých souborů	Dobrá dostupnost souborů	7	3	21	Skupiny přístupů v AD, auditní SW file serveru
			Neprovádění revizí oprávnění	9	3	27	Skupiny přístupů v AD, auditní SW file serveru
			Prodej informací zaměstnancem firmy	12	3	36	Skupiny přístupů v AD, auditní SW file serveru
			Prodej informací administrátorem	12	4	48	Auditní SW file serveru
		Výpadek Windows serveru	Neočekávaná chyba	3	4	12	Real time kopie souborů včetně oprávnění na externí server
Databázové servery	**4**	Výpadek Windows serveru	Neočekávaná chyba	7	4	28	
		Zneužití a krádež informací	Přístup externí společnosti	6	3	18	Auditní SW
		Náhodné smazání, úprava, přepis záznamů	Lidská chyba	4	4	16	
Server webových služeb	**3**	Výpadek Windows serveru	Neočekávaná chyba	5	3	15	
		Zneužití a krádež informací	Přístup externí společnosti	6	2	12	Auditní SW - nahrávání přístupů
			Prodej informací zaměstnancem firmy	6	2	12	
		Výpadek služeb	Neočekávaná chyba	5	3	15	
			Přetížení serveru	9	2	18	
Ostatní servery	**3**	Výpadek Windows serveru	Neočekávaná chyba	5	3	15	
		Výpadek Linux serveru	Neočekávaná chyba	4	3	12	
Osobní počítače	**3**	Napadení škodlivým softwarem (únik, smazání, pozměnění, zašifrování dat a inforamcí)	Emailové přílohy a jiné komunikační kanály	16	3	48	Emailový filtr, antivir
			Infikované webové stránky	8	3	24	Firewall, antivir
			Infikovaná externí zařízení	7	3	21	Antivir
			Otevírání infikovaných souborů	5	3	15	Omezená práva uživatelů, antivir
		Krádež počítače nebo HDD	Neexistuje HW zabezpečení	4	3	12	Zodpovědnost uživatelů za převzatý HW, kontroly na vrátnici
		Krádež dat a informací zaměstnancem	Možnost připojit externí zařízení	8	3	24	
			Možnost zaslat emailem a jinými komunikačními kanály	7	3	21	

Aktivum	Hodnota	Hrozba	Zranitelnost	Pravděpod. incidentu	Dopad	Riziko	Existující opatření
Notebooky	**3**	Napadení škodlivým softwarem (únik, smazání, pozměnění, zašifrování dat a inforamcí)	Emailové přílohy a jiné komunikační kanály	16	3	48	Emailový filtr, antivir
			Infikované webové stránky	8	3	24	Firewall, antivir
			Infikovaná externí zařízení	7	3	21	Antivir
			Otevírání infikovaných souborů	5	3	15	Omezená práva uživatelů, antivir
		Krádež notebooku	Neexistuje HW zabezpečení	9	3	27	Zodpovědnost uživatelů za převzatý HW, šifrování disků - BitLocker
		Krádež dat a informací zaměstnancem	Možnost připojit externí zařízení	8	3	24	
			Možnost zaslat emailem a jinými komunikačními kanály	7	3	21	
Mobilní telefony	**3**	Krádež telefonu (přístup k firemním datům)	Neexistuje HW zabezpečení	18	3	54	Zodpovědnost uživatelů za převzatý HW
Podnikový informační systém	**5**	Zneužití oprávnění	Přidělování nadbytečných práv	17	4	68	
		Zneužití a krádež informací	Přístup externí společnosti	6	4	24	Smlouva o mlčenlivosti
			Prodej informací zaměstnancem firmy	7	4	28	
			Prodej informací administrátorem	8	4	32	
Docházkový systém	**3**	Zneužití informací	Přístup externí společnosti	4	2	8	
		Neoprávněný přístup	Neexistují minimální požadavky na heslo interních účtů	12	3	36	
Ekonomický systém	**4**	Neoprávněný přístup	Neexistují minimální požadavky na heslo interních účtů	12	3	36	
		Krádež dat a informací zaměstnancem	Prodej informací nebo poškození firmy	7	3	21	
Mzdový systém	**4**	Neoprávněný přístup	Neexistují minimální požadavky na heslo	10	3	30	
		Krádež dat a informací zaměstnancem	Prodej informací nebo poškození firmy	5	3	15	
Projektový systém	**3**	Neoprávněný přístup	Neexistují minimální požadavky na heslo	5	2	10	
		Krádež dat a informací zaměstnancem	Prodej informací nebo poškození firmy	6	2	12	
CRM systém	**4**	Neoprávněný přístup	Neexistují minimální požadavky na heslo interních účtů	8	3	24	
		Krádež dat a informací zaměstnancem	Prodej informací nebo poškození firmy	7	4	28	
Připojení VPN	**4**	Krádež dat a informací zaměstnancem	Možnost vzdáleného připojení z kteréhokoli zařízení	9	4	36	Auditní SW file serveru
		Zneužití přístupu cizí osobou	Osobní zařízení uživatelů nemusí být chráněna	11	4	44	

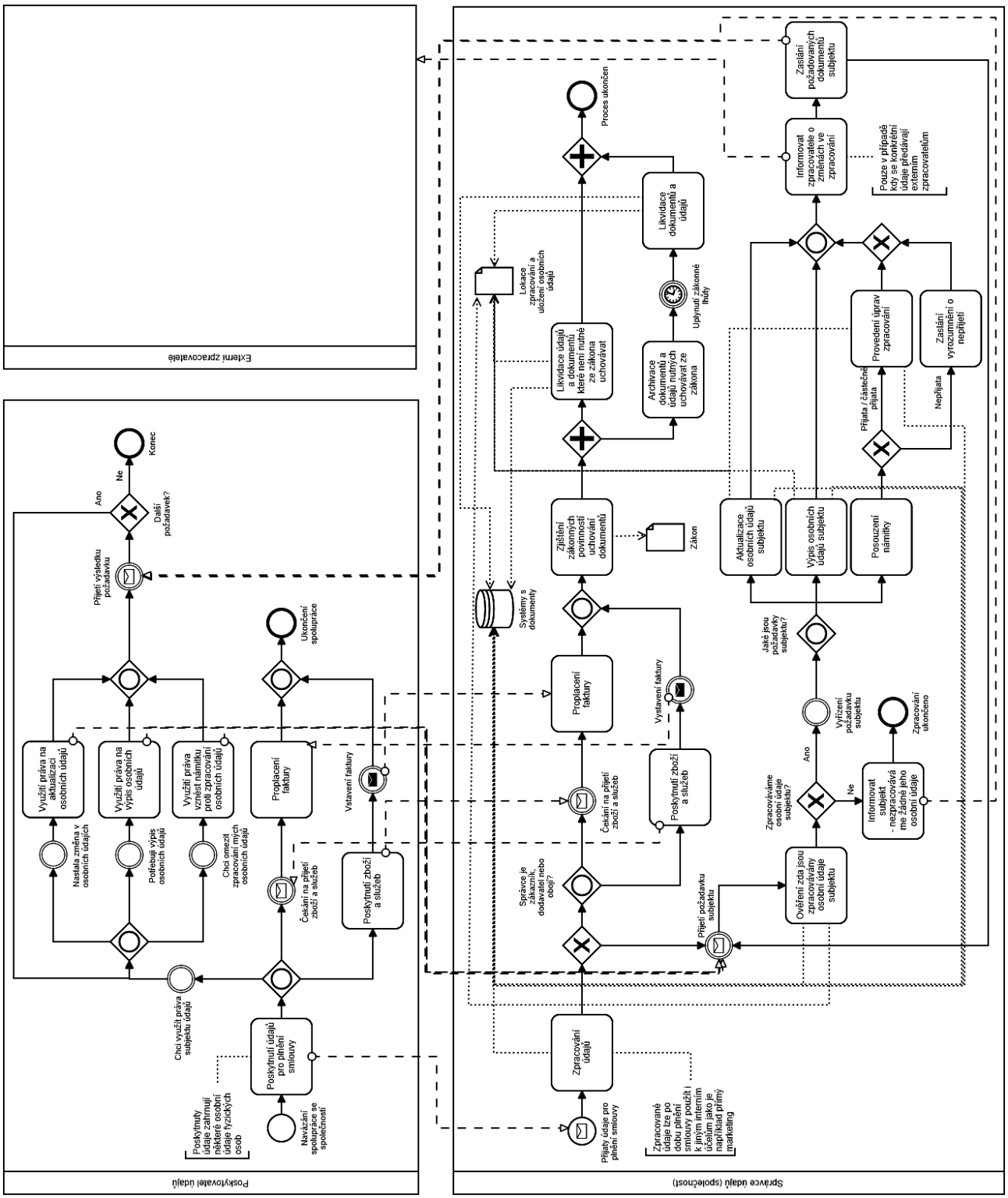
Příloha 4 – Lokace zpracování a uložení osobních údajů

Oddělení	Subjekty	Způsob uložení	Zpracování / Uložení
HR	Zaměstnanci	Elektronicky	Docházkový SW
			Mzdový software
			Síťové disky
			Externí paměťová média
			Lokální záznamy na PC
			Intranet WEB
			Firemní WEB
			Linkedin
			Vímvíc.cz
			Mobilní telefony
			Outlook
		Papírově	Archiv
			Šanony a dokumenty
	Externisté	Papírově	Šanony a dokumenty ostraha
IT	Zaměstnanci	Elektronicky	Active directory
			Exchange
			Informační systém
			Evidence IT prostředků
			Firemní sociální síť
			Call manager
			CRM
			Správa SIM karet
			Interní výrobní programy
			Firemní WEB
			Mobilní telefony
			Outlook
		Papírově	Šanony a dokumenty s předávacími protokoly
Obchod	Zaměstnanci	Elektronicky	Linkedin
			Intranet WEB
			Firemní WEB
			Síťové disky
			Zařízení pro marketing
			Brožury pro marketing
	Externisté	Elektronicky	Linkedin
			Intranet WEB
			Síťové disky
			Mobilní telefony
			Outlook
	Zákazníci	Elektronicky	Linkedin
			Intranet WEB
			Síťové disky
			CRM
			Mobilní telefony
			Outlook
Nákup	Dodavatelé	Elektronicky	Informační systém
			Mobilní telefony
			Outlook
		Papírově	Šanony a dokumenty

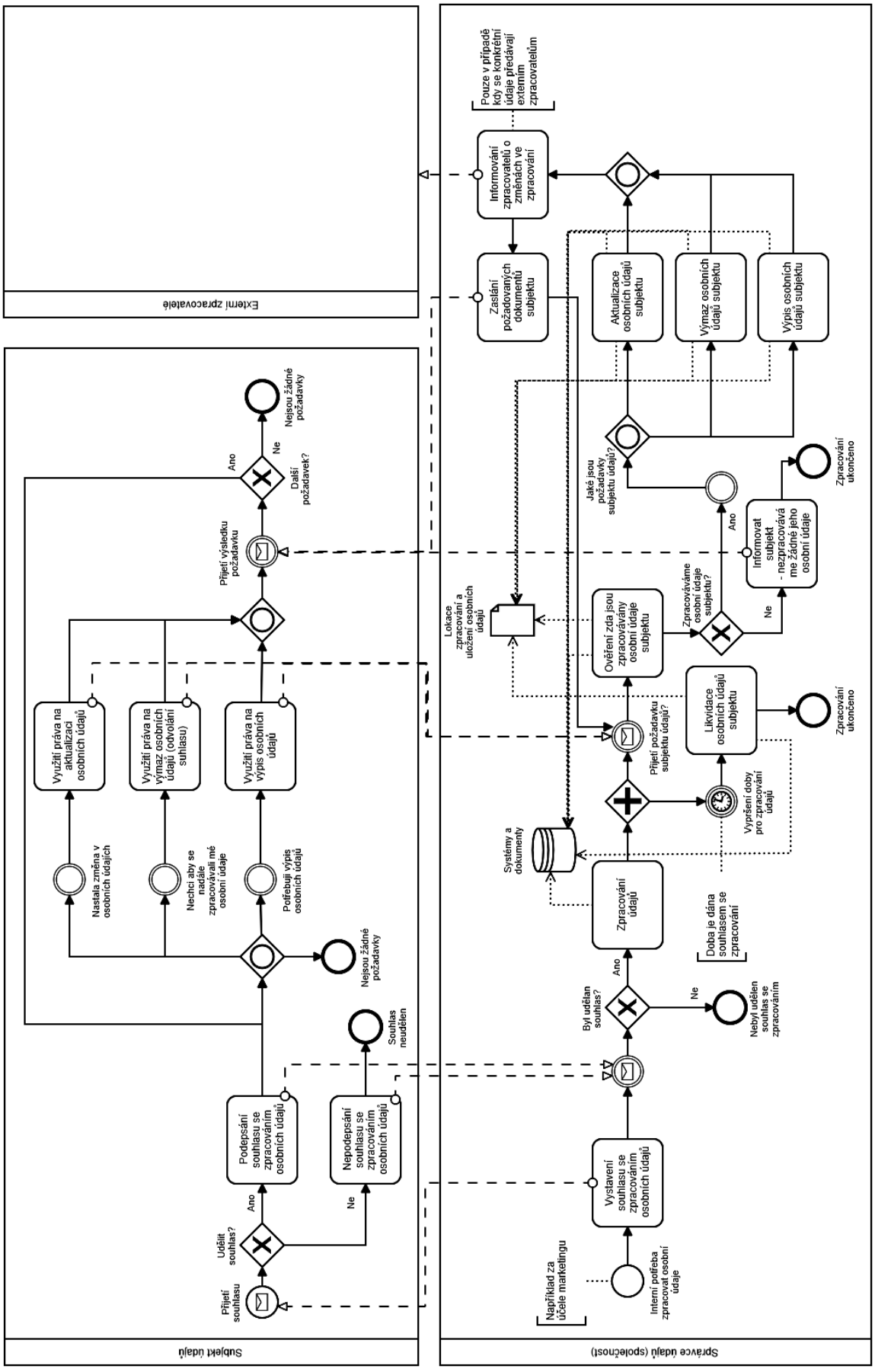
Oddělení	Subjekty	Způsob uložení	Zpracování / Uložení
Finanční	Zaměstnanci	Elektronicky	Knihy jízd WEB
			Finanční systém
			Outlook
			Aplikace pro interní spotřebu paliv
			Síťové disky
		Papírově	Šanony a dokumenty
	Externisté	Elektronicky	Finanční systém
			Účetní systémy
			Síťové disky
			Outlook
		Papírově	Šanony a dokumenty
Kvalita	Zaměstnanci	Papírově	Šanony a dokumenty
	Externisté	Elektronicky	Mobilní telefony
			Outlook
			Síťové disky
		Papírově	Šanony a dokumenty
SCM	Zaměstnanci	Elektronicky	Síťové disky
			Outlook
			Mobilní telefony
			Lokální záznamy na PC
		Papírově	Šanony a dokumenty
	Externisté	Papírově	Šanony a dokumenty
Mistři	Zaměstnanci	Elektronicky	Mobilní telefony
			Síťové disky
			Lokální záznamy na PC
			Outlook
		Papírově	Šanony a dokumenty
Vedoucí a asistentky	Zaměstnanci	Elektronicky	Knihy jízd WEB
			Mobilní telefony
			Síťové disky
			Lokální záznamy na PC
			Outlook
		Papírově	Šanony a dokumenty

Příloha 5 – Návrh procesů zpracování osobních údajů

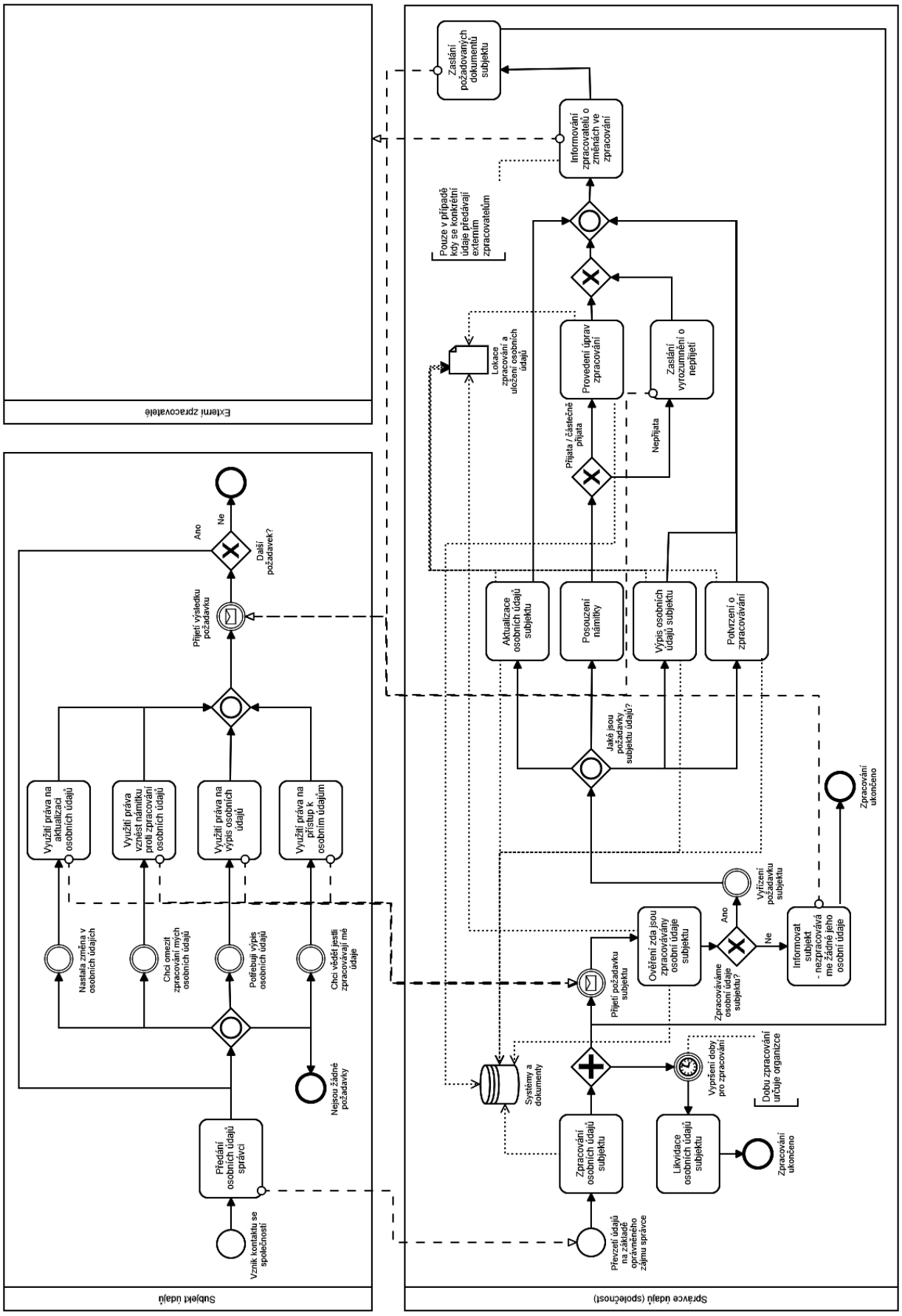
1) Zpracování za účelem plnění smlouvy:



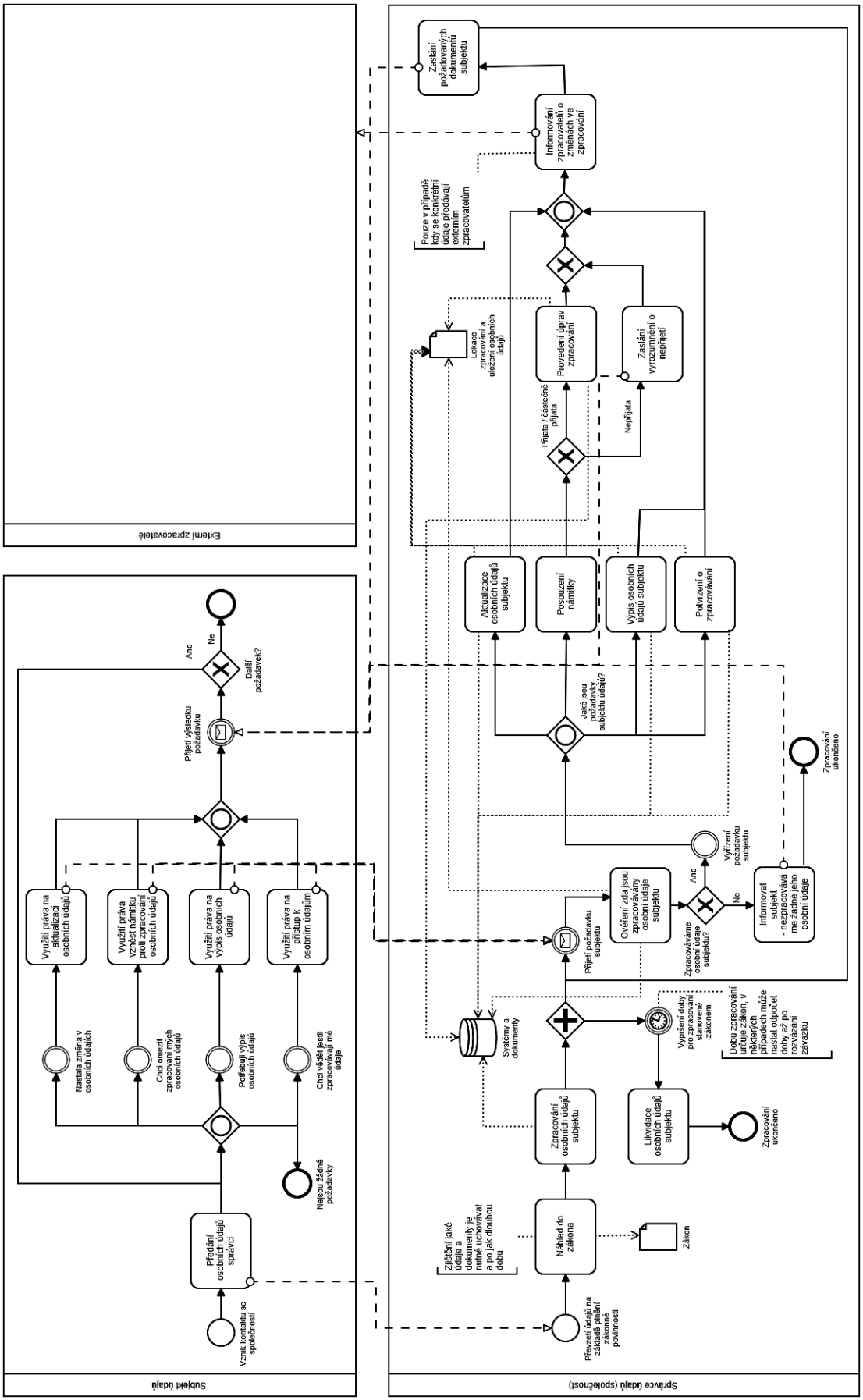
2) Zpracování na základě souhlasu:



3) Zpracování z titulu oprávněného zájmu správce:



4) Zpracování z titulu plnění zákonné povinnosti:



Příloha 6 – Základní prvky procesního modelování BPMN

Prvky modelu jsou převzaty z programu Camunda modeler od společnosti Camunda Services GmbH používaného v této bakalářské práci.

Události:

Brány:

Brána použita jako rozdělující:

- **Exkluzivní brána –** tok směřuje právě do jedné větve.
- **Inkluzivní brána** – je aktivována alespoň jedna výstupní větev.
- **Paralelní brána** – jsou aktivovány všechny výstupní větve.
- **Komplexní brána** – chování je vyjádřeno pomocí výrazů.
- **Událostní brána** – při výskytu události dochází ke spuštění nové instance.

Brána použita jako slučující:

- **Exkluzivní brána –** k odeslání toku dojde z jakékoli vstupní větve.
- **Inkluzivní brána** – ke sloučení příchozího toku dojde až ve chvíli, kdy přiteče signál ze všech aktivních větví.
- **Paralelní brána** – k aktivaci brány dojde až po příchodu signálů ze všech vstupů. [44]