VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

METODIKA ZÁLOHOVÁNÍ V SOULADU S OBECNÝM NAŘÍZENÍM O OCHRANĚ OSOBNÍCH ÚDAJŮ - GDPR

THE METHODOLOGY OF DATA BACKUP IN ACCORDANCE TO GENERAL DATA PROTECTION REGULATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Miloslav Smutka**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Jiří Kříž, Ph.D.**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Miloslav Smutka**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Jiří Kříž, Ph.D.**
Akademický rok:	2018/19

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

Metodika zálohování v souladu s Obecným nařízením o ochraně osobních údajů – GDPR

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je vypracování metodiky pro zálohování dat v malých a středních firmách, která bude naplňovat požadavky kladené Obecným nařízením o ochraně osobních údajů.

Základní literární prameny:

BUCHALCEVOVÁ, Alena. Metodiky vývoje a údržby informačních systémů: kategorizace, agilní metodiky, vzory pro návrh metodiky. Praha: Grada, 2005. 163 s. ISBN 80-247-1075-7.

MELICHAR, Josef. Řízení rizik ve firmách a jiných organizacích. Univerzita Obrany. Ústav Strategických Studií. Obrana a Strategie [online]. Brno: University of Defence, 2015, 2015(1), 84-87 [cit. 2019-02-28]. DOI: 10.3849/1802-7199.15.2015.01.084-087. ISSN 12146463. Dostupné z: http://search.proquest.com/docview/1707745523/

PECINOVSKÝ, Josef. Archivace a komprimace dat: jak zálohovat data, jak komprimovat soubory WinRAR, WinZip, WinAce, Windows a nástroje komprese dat, jak archivovat data ve Windows. Praha: Grada, 2003. 116 s. ISBN 80-247-0659-8.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. července 2017

Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive)

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

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

Abstrakt

Tématem diplomové práce je vytvoření metodiky pro zálohování dat v souladu s obecným nařízením o ochraně osobních údajů. Na základě rozboru jednotlivých bodů nařízení budou definovány postupy a metody zálohování v souvislosti s různými zálohovacími technikami a médii. Pro jejich použití pak bude vypracována metoda řízení změny.

Abstract

The main topic of this thesis is creating a methodology for data backups in compliance with the General Data Protection Regulation (GDPR). After analysis of individual regulation sections, processes and methods of proper data backups will be defined. The thesis will also concern itself with different backup media types and related technology. Outcome of the text will be the creation of a specific method useful for change control.

Klíčová slova

GDPR, obecné nařízení o ochraně osobních údajů, zálohování, komprese, šifrování, PEST analýza, analýza 7S, SWOT analýza, řízení rizik, Lewinův model

Key words

GDPR, General Data Protection Regulation, backup, compression, encryption, PEST analysis, 7S analysis, SWOT analysis, risk management, Lewin model

Bibliografická citace

SMUTKA, Miloslav. *Metodika zálohování v souladu s Obecným nařízením o ochraně osobních údajů - GDPR* [online]. Brno, 2019 [cit. 2019-05-09]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/120074. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Jiří Kříž.

Čestné prohlášení

Prohlašuji, že svoji diplomovou práci na téma „Metodika zálohování v souladu s obecným nařízením o ochraně osobních údajů – GDPR“ jsem vypracoval samostatně s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Brně dne 10. Května 2019

…… podpis student

Poděkování

Rád bych poděkoval svému vedoucímu práce Ing. Jiřímu Křížovi, Ph.D. za odborné a cenné rady a vstřícnou spolupráci při vypracování této diplomové práce. Dále bych chtěl poděkovat své rodině a přátelům, kteří mě během mého studia a především psaní diplomové práce velmi podporovali. Za jazykovou korekturu bych chtěl poděkovat Bc. Davidovi Sloukovi. Za cenné právní rady potom Ondřeji Drahorádovi.

Obsah

ÚVOD

Dle údajů[1] poradenské firmy Bureau Veritas se nové nařízení o ochraně osobních údajů (GDPR, dále též nařízení) dotýká v České republice zhruba jednoho milionu subjektů. Týká se všech společností[1] a dále živnostníků, kteří zpracovávají osobní údaje. Nařízení se svým podáním a obsahem liší od běžných zákonů, které vydává parlament ČR. V kombinaci s jeho širokým rozsahem se jedná o záležitost, které je třeba věnovat dostatečnou pozornost, neboť při jejím neplnění hrozí vysoké pokuty.

Jedním z prvků, které nařízení stanovuje, je zabezpečení všech osobních dat nejenom proti odcizení, ale též proti ztrátě. Nejen proto je v zájmu všech správců osobních údajů data zabezpečit tak, aby nedošlo k jejich ztrátě například v případě živelné pohromy, selhání úložných médií, zlovolnému jednání třetí strany či chybě vlastního zaměstnance.

Cílem této práce je představit ucelenou metodiku, která čtenáře seznámí se všemi náležitostmi vyplývajícími z GDPR, a to zejména v oblasti, která se týká zálohování a dále možností zálohování a jeho využitelností v souladu se stávající legislativou. V dalších kapitolách je představen stručný model řízení změn a konkrétní postup, jaký by měl být zvolen pro co nejjednodušší přechod na zálohovací systémy, které budou splňovat všechny zákonné náležitosti.

[1] V dalším textu je pro podnik užito i označení firma či společnost, a to vzhledem k dlouhodobě zavedené terminologii užívané širokou veřejností i výkladovými slovníky, i přes to, že v novele obchodního zákoníku došlo ke změně v právní definici pojmu firma, který nyní znamená název, pod kterým je společnost vedená, a nikoliv podnik sám.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

GDPR nabývající účinnosti v květnu roku 2018 definuje pojmy, práva a povinnosti zúčastněných stran při zpracovávání osobních údajů. Zejména se týká správců a zpracovatelů osobních údajů a fyzických osob, kterým tyto údaje náleží. Správcem osobních údajů je každý subjekt, který provádí jejich shromažďování, zpracovávání a uchovávání. Správcem může být fyzická i právní osoba. Zpracovatelem osobních údajů je pak subjekt, který zpracovává osobní údaje jménem správce takovým způsobem a v takovém rozsahu, jaký mu určil správce.

Hlavním cílem práce bude vytvořit metodiku, s jejíž pomocí bude možné v malých a středních firmách zahájit, řídit a úspěšně ukončit proces změny, který je nevyhnutelný pro zajištění souladu s nařízením.

Nařízení má za cíl sjednotit současnou legislativu napříč všemi členskými státy EU. První část této práce je proto věnována rozboru nařízení, zejména částí, které se týkají správců a zpracovatelů a těch, které se přímo či nepřímo týkají zálohování. Důležité či nejasné body jsou doplněny vysvětlujícími komentáři a některé nové pojmy jsou vysvětleny v samostatných podkapitolách tak, aby z nich bylo možné vyvodit jednoznačné důsledky pro činnost subjektu správce a zpracovatele.

Následující kapitola se věnuje současným technologiím zálohování dat a uvádí je do souvislosti s nařízením. V této kapitole lze najít návrhy řešení aplikovatelná na současná zálohovací média takovým způsobem, aby bylo dosaženo souladu s GDPR.

V kapitole zabývající se návrhem řešení je nastíněn postup řízené změny, na jejímž konci by měl být stav, kdy je subjekt, který zpracovává osobní údaje plně připraven zálohovat tyto údaje v souladu s nařízením. Pro řízení změny jsou popsány nástroje a metodiky, které by měly zařídit co nejhladší průběh této změny. Na závěr jsou vypsány některé specifické techniky, které lze pro zálohování využít.

1 TEORETICKÁ VÝCHODISKA PRÁCE

Na úvod budou zmíněny záměry, které by mělo nařízení naplňovat. Nařízení není nijak převratné, většina členských zemí EU již dříve aplikovala zákony pro ochranu osobních dat. Nařízení pouze tyto zákony sjednocuje a stanovuje jasná pravidla jejich porušení. Dále definuje jednotné pojmy pro všechny členské státy. Pro lepší představu bude nyní rozebrána historie zákonů pro ochranu osobních dat v EU.

1.1 Historie ochrany osobních údajů v EU

Prvním dokumentem, který v Evropě sjednocoval zpracovávání a uchovávání osobních údajů byla *Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat*, vyhlášená pod *č. 115/2001 Sb. m. s.* Tato Úmluva zavazuje státy, které ji ratifikovaly (nevztahuje se na soukromé objekty), aby přijaly opatření k ochraně soukromí prostřednictvím pravidel, která budou nastavena pro zpracování osobních údajů. Dále státům ukládá, aby nekladly překážky pro volný pohyb dat mezi nimi.

Úmluva má k dnešnímu dni celkem 51 signatářů, kromě členů Evropské unie mezi ně patří primárně další členové Rady Evropy, jako je Gruzie, Turecko nebo Rusko. Úmluvu mohou přijmout kterékoliv státy, proto se mezi signatáři vyskytují i státy mimo Evropu, jako je například Tunisko či Senegal. Česká republika smlouvu ratifikovala 9. července 2001 a vstoupila v platnost dne 1. listopadu 2001.

Tato Úmluva sjednocuje definice klíčových pojmů, jako je osobní údaj, zpracovávání či správce údajů. Dále ukládá konkrétní úkoly signatářským státům. Štrasburský soud dovodil, že ochrana osobních údajů je nedílnou součástí práva na soukromí dle čl. 8 Úmluvy o ochraně lidských práv a svobod a že porušení Úmluvy 108 může představovat porušení práva na soukromí. Státy ratifikující tuto Úmluvu se zavazují, že umožní volné předávání údajů mezi signatářskými státy. Tato Úmluva se stala první, která se snaží tvořit evropský standard ochrany osobních údajů a tím stanovit stejná práva a povinnosti všem subjektům v rámci EU i dalším, jejichž státy smlouvy podepsaly.

Smlouva stanovuje práva a povinnosti subjektů a fyzických osob. Dále stanovuje procesní náležitosti a nástroje, které by měly státy implementovat do svých zákonů podle uvážení jejich zákonodárných orgánů. V současném znění Úmluva připouští výjimky či naopak rozšíření.

Smlouva byla vytvořena v době, kdy nikdo nemohl předvídat revoluci v informačních technologiích, která nastala v následujících letech. Proto zdaleka nestačila pro pokrytí potřeb rychle se rozrůstající světové sítě a všech zúčastněných subjektů a v roce 2012 byl na zasedání Evropské Rady představen první návrh modernizace. Finální úpravy byly dokončeny a konečný text zveřejněn 18. května 2018.

Tyto úpravy se dotýkají zejména lepší definice pojmů a detailnějšímu přístupu k pravidlům pro zpracování údajů, práv a povinností fyzických a právnických osob, jak zpracovávajících, tak zpracovávaných. Dále stanovují státům povinnost svěřit kompetenci nad touto oblastí konkrétním úřadům a definují, jak by tyto úřady měly svou funkci zastávat a jaké procesy by měly implementovat.

V současnosti (květen 2019) se očekává reakce signatářských států, které by měly modernizovanou Úmluvu ratifikovat. Úmluva nabude účinnosti ve chvíli, kdy ji ratifikuje 5 signatářských států původní úmluvy. Po úpravách se text velice blíží GDPR a jedná se vlastně o nadřazený dokument, z kterého GDPR vychází, z čehož je patrné, že pro členské státy ratifikující GDPR nebudou změny nikterak významné. Kde však určitě dojde ke změnám jsou státy mimo EU. Díky tomu by mělo být v budoucnu ještě snazší získat osobní data subjektů ze států, které ratifikují tuto smlouvu, a to i přesto, že nejsou v Evropské unii, neboť po úpravách dojde ke větší jednotnosti v oblasti zpracovávání údajů. Dále díky jasně vymezeným kompetencím, které musí být jasně přiřazeny konkrétním úřadům, bude vylepšen i jednotný přístup na komunikační úrovni, který proces zpřístupnění či vyžádání osobních údajů dále zjednoduší.

V rámci Evropské Unie byla do května 2018 platná směrnice *95/46/ES o ochraně údajů* z roku 1995[2]. Tato směrnice byla doplněna rámcovým rozhodnutím *2008/977/SVV*[3]. Směrnice i rámcové rozhodnutí naplňují *Úmluvu Rady Evropy* a zaměřují se na ochranu základního práva na ochranu údajů a zaručují volný pohyb osobních údajů mezi členskými státy.

Tyto právní předpisy byly navrženy a vypracovány v době, kdy nebylo možné předvídat směr, kterým se uberou počítačové sítě a celkově správa osobních údajů, proto už dlouho bylo jasné, že je třeba je přepracovat. V době jejich návrhu nikdo nemohl vědět, že se budou uplatňovat, pro sociální sítě, cloudová úložiště či chytré telefony, shromažďující o svých nositelích data, která bude třeba chránit. Navíc se ukázalo, že osobní data mohou být strategickou komoditou a jako taková je třeba je chránit i před vnějšími hrozbami, například snahami některých států získávat osobní data občanů Unie ve velkém a následněje zneužít pro vlastní účely.

1.2 Vznik Obecného nařízení o ochraně osobních údajů (GDPR)

První konzultace začaly probíhat 9. července 2009 a skončily 31. prosince téhož roku. Další konzultace probíhaly od 4. listopadu 2010 do 15. ledna 2011.

První prohlášení o chystané změně nastalo v roce 2010, kdy Evropská komise zveřejnila své sdělení *Komplexní přístup k ochraně osobních údajů v Evropské unii*, ve kterém deklaruje sjednotit politiku ochrany osobních údajů pro všechny členské státy.

Po řadě dalších jednání a zpráv byl představen první návrh o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů 25. ledna 2012. Následovalo opakované projednávání v jednotlivých institucích Evropské unie a ve členských státech. Finální dohoda mezi Radou Evropské unie, Evropskou komisí a Evropským parlamentem byla dosažena 15. prosince 2015. Výsledný podpis proběhl po několika dalších jednáních 27. dubna 2016.

1.3 Historie ochrany osobních údajů v Československu a České republice.

První snahou zavést ochranu osobních údajů do legislativy České republiky byl zákon *č. 40/1964 Sb. Občanský zákoník*. Zde jsou v několika paragrafech zmíněny základní principy ochrany soukromí. Konkrétně můžeme považovat za důležitý §11, kde se dočteme následující:

Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.

V §12 je specifikováno, co se považuje za projevy osobní povahy:

(1) Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.[4]

Dále se v tomto paragrafu specifikují dvě výjimky, pro zákonem nařízené účely a pro vědecké a umělecké práce, a pro tiskové, filmové a podobné využití.

V §13, §14, §15, §16 a §17 se upřesňují práva občanů pro případ porušení a právo na odstranění nevyžádaného zveřejnění takových údajů. Dále se upřesňují dědická práva takovýchto údajů.

I přesto, že jsou formulace velmi nekonkrétní, je toto prohlášení revoluční v tom, že poprvé v historii Československa připouští fakt, že osoba má právo na ochranu soukromí, specifikuje, co se tímto soukromím myslí a uznává právo na napravení škod, vzniklých zveřejněním takových údajů.

Zákon *40/1964 Sb.* fungoval bez výraznějších úprav až do 31. prosince 2013, kdy jej nahradil nový občanský zákoník (Zákon *č. 89/2012 Sb.*). Mezitím však byl přijat roku 1992 zákon *č. 256/1992 Sb.,* platný od 1. června 1992. Tento zákon specificky upravuje ochranu osobních údajů v informačních systémech[5] a stanovuje povinnosti a odpovědnost subjektů zpracovávajících osobní data pomocí informačních systémů. Definuje také pojmy jako uživatel, zprostředkovatel, zveřejnění informace nebo zpracování informace.

Zákon *256/1992 Sb.* však nebyl v souladu s *Úmluvou Rady Evropy č. 108/1981* na ochranu osob se zřetelem na automatizované zpracování osobních údajů[6] a pro ratifikaci této úmluvy Českou republikou bylo nutné tento zákon přepracovat. Tuto úmluvu Česko naplnilo zákonem *č. 101/2000 Sb. o ochraně osobních údajů*.

Kromě výše zmíněných zákonů se o právu na ochranu osobních údajů zmiňují ještě dva zákony:

1) Nový občanský zákoník[7], který definuje obecnější problematiku soukromí:

   §3, odstavec 2) bod a):

každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí

Či například §84:

Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.

2) Dále je právo na soukromí zaručeno v Listině základních práv a svobod[8], konkrétně například v článku 10, bodu 3:

Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

1.4 Předcházející legislativa

Nejdetailněji však zpracovává problematiku zpracování osobních údajů právě zákon *č. 101/2000 Sb.*, který je v současném znění platný od 25. června 2000[9].

Tento zákon určuje zejména následující:

1) Vymezuje vlastní působnost, na veškeré subjekty, zpracovávající osobní údaje a to i v případě automatizovaného zpracovávání.
2) Vymezuje pojmy, v souladu s Úmluvou Rady Evropy č. 108 a to zejména následující: Osobní údaj, citlivý údaj, zpracování osobních údajů, uchování osobních údajů, zpracovatel, správce, zveřejněný osobní údaj, souhlas subjektu, příjemce
    a. Osobním údajem se myslí jakákoliv informace, která dokáže přímo či nepřímo identifikovat subjekt údajů
    b. Citlivým údajem se myslí údaj o původu, politických postojích, náboženství, odsouzení za trestný a mezi dalšími i biometrické údaje, které mohou vést k jednoznačné identifikaci subjektu
3) Povinnosti správce osobních údajů, zejména následující:
    a. Stanovit účel, k němuž mají být osobní údaje zpracovány.
    b. Stanovit prostředky a způsob zpracování osobních údajů.
    c. Zpracovávat pouze přesné osobní údaje, v případě potřeby je aktualizovat či v opačném případě je zlikvidovat.

d. Shromažďovat osobní údaje odpovídající pouze stanovenému účelu, po dobu k tomu nezbytnou a pouze v nezbytném rozsahu.
e. Nesdružovat osobní údaje získané k různým účelům.

4) Správce a zpracovatel může osobní údaje zpracovávat pouze se souhlasem subjektu údajů, při kterém musí být informován o účelu zpracování, nebo pokud splňuje některou z následujících podmínek:
   a. Pokud ho k tomu zavazuje jiný zákon
   b. Jestliže je zpracování nezbytné k plnění či budoucímu uzavření smlouvy mezi správcem a subjektem údajů
   c. Pokud je to v zájmu životně důležitých zájmů subjektu údajů
5) Pro účel nabízení obchodu či služeb lze použít jméno, příjmení a adresu, pokud byly získány z veřejného seznamu nebo v souvislosti s činností zpracovatele.
6) Kdykoliv lze vyslovit písemný nesouhlas se zpracováváním osobních údajů. Potom lze tyto údaje uchovávat pouze pro to, aby subjekt nebyl dále kontaktován.
7) Pokud o to subjekt požádá, musí dostat informaci o zpracování svých osobních údajů, včetně účelu a rozsahu zpracování
8) Správce i zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě či jinému zneužití a to i po ukončení zpracování.
9) Je nutné zaznamenávat, komu byly osobní údaje předány
10) Zaměstnanci jsou povinni zachovávat mlčenlivost o osobních údajích, které zpracovávali a to i po ukončení pracovního poměru.
11) Po pominutí účelu zpracování či na žádost subjektu je zpracovatel provést likvidaci osobních údajů.
12) Zákon stanovuje oznamovací povinnost
   a. Kdokoliv se jako správce chystá zpracovávat osobní údaje, je povinen tuto skutečnost písemně oznámit Úřadu pro ochranu osobních údajů
   b. V oznámení musí být mimo jiné následující:
      i. Identifikaci správce
      ii. Účel zpracování
      iii. Místo a způsob zpracování

c. Zpracování je možné zahájit po 30 dnech po oznámení a pouze v případě, že Úřad nezahájí řízení

13) Subjekt údajů může kdykoliv požádat správce o vysvětlení zpracování jeho osobních údajů a v případě nesouladu se zákonem může žádat nápravu
14) Předání osobních údajů do cizích států se řídí mezinárodními smlouvami (zejména Úmluvou Rady Evropy č. 108)
15) Definuje přestupky proti tomuto zákonu a pokuty z nich vyplývající, které mohou nabývat výše až 5 milionů korun pro fyzické osoby a 10 milionů korun pro osoby právnické a podnikatele

Dále tento zákon zřizuje Úřad pro ochranu osobních údajů (ÚOOÚ) a stanovuje jeho kompetence. Tento úřad je nezávislým orgánem, který dohlíží na dodržování povinností vyplývajících z tohoto zákona. Dále vede registr, do kterého je povinen se registrovat každý, kdo chce zpracovávat osobní údaje. Úřad též podniká kontroly pro odhalení porušení zákona, při kterých jsou inspektoři tohoto úřadu oprávněni se seznamovat se zpracovávanými osobními údaji, a dále projednává přestupky proti tomuto zákonu a uděluje pokuty.

1.5 Motivace pro zavedení GDPR

Jak je patrné z předcházejících kapitol, evropská legislativa byla v oblasti ochrany osobních dat velmi nekonzistentní a zastaralá. *Úmluva Evropské Rady č. 108* byla sepsána v roce 1981, směrnice *EU 95/46/ES* o ochraně údajů začala platit v roce 1995. Jako další příklad může posloužit Velká Británie, která zavedla první zákon pro ochranu osobních údajů až v roce 1998, ale ještě v roce 2011 panovaly nejasnosti v jeho provádění[10],[11] nebo Francie, která až do 20. června 2018 užívala zákon z roku 1978[12].

Dalším důvodem je fakt, že tajné služby států mimo Evropskou Unii shromažďovaly či shromažďují velké objemy osobních dat občanů EU. S přihlédnutím k různým výkladům práva na soukromí v některých státech mimo Evropskou Unii bylo tedy nezbytné stanovit mechanismy pro ochranu práv občanů EU.

1.6 Obecné nařízení o ochraně osobních údajů

Pro pochopení nařízení je třeba věnovat důkladnou pozornost samotnému nařízení a z něj vyplývajícím důsledkům. Dalším důležitým prvkem bude tzv. adaptační zákon[13], který lépe integruje nařízení do legislativy České republiky. Tento zákon byl 5. prosince 2018 schválen Poslaneckou sněmovnou a nyní je třeba, aby ji schválil Senát a podepsal prezident. Protože se jeho finální podoba se může ještě měnit a navíc v současné podobě modifikuje pouze okrajové části, nebudu se jím v práci dále zabývat.

1.6.1 Základní pojmy podle nařízení

Zde je uvedeno několik pojmů, které nařízení zavádí nově či odlišně od běžného užití.

1) Osobními údaji dle GDPR se rozumí:

   Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

   Z toho vyplývá, že osobními údaji se myslí jakékoliv údaje, které mohou sloužit k identifikaci osoby ať už samy o sobě, tak v kombinaci s jinými údaji.

2) Souhlasem se rozumí jakýkoli informovaný a jednoznačný projev vůle.
3) Zavádí se nový pojem „porušení zabezpečení osobních údajů“, což zahrnuje poškození, zničení či zpřístupnění osobních dat neoprávněnými osobami.
4) Omezení zpracování: stav, kdy jsou údaje stále uloženy u zpracovatele, ale jsou označeny, aby se omezilo jejich zpracování v budoucnu.

1.6.2 Některé další důležité body z nařízení

Zde uvádím další body z nařízení, zejména ty, které jsou nové oproti českému zákonu o ochraně osobních údajů či upravují některé již používané postupy.

1) Zpracovávané osobní údaje musí být přesné a musí být zpracovávány v minimálním rozsahu vzhledem k účelu zpracovávání
2) Správce zodpovídá za bezpečnost osobních údajů a je povinen použít přiměřenou míru zabezpečení
3) Pro zpracování dat je nutné splnit alespoň jednu z následujících podmínek:
    a. Subjekt údajů udělil se zpracováním souhlas
    b. Zpracování je nezbytné ze zákonných důvodů
    c. Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu či jiné osoby
    d. Zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany
4) Správce je povinen doložit důkaz, že alespoň jedna podmínka byla splněna
5) Subjekt má právo kdykoliv svůj souhlas odvolat
6) Správce je povinen poskytnout subjektu údajů tyto informace:
    a. Totožnost správce údajů
    b. Účely zpracování
    c. V případě, že se jedná o zpracování na základě oprávněných zájmů, pak o jaké zájmy se jedná
7) Subjekt má právo kdykoliv získat přístup ke svým zpracovávaným osobním údajům a dále krom údajů, které mu je správce povinen poskytnout i plánovanou dobu, po které bude osobní údaje zpracovávat a zdroj osobních údajů
8) Poskytnutí osobních údajů musí být zdarma
9) Subjekt má právo, aby byly jeho údaje bez zbytečného odkladu opraveny, pokud jsou nepřesné či vymazány, pokud již neexistují důvody pro jejich zpracování. K tomu může dojít i odebráním souhlasu.
10) Správce oznamuje subjektům veškeré opravy a výmazy jejich údajů
11) Každý správce vede záznamy o činnostech zpracování
12) Při porušení zabezpečení je to správce povinen o tom nejpozději do 72 hodin povinen informovat dozorový úřad, a pokud se lze domnívat, že porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, také subjektu údajů.

13) V případě, že zpracování údajů vyžaduje rozsáhlé, pravidelné a systematické monitorování, je správce i zpracovatel povinen jmenovat pověřence pro ochranu osobních údajů
14) Každý členský stát stanoví jeden nebo více nezávislých orgánů, které jsou pověřený monitorováním uplatňování tohoto nařízení
15) Je na každém členském státu, jaké zavede právní předpisy na ochranu osobních údajů v souvislosti se svobodou projevu, přístupu veřejnosti k informacím, zpracováním národních identifikačních čísel, v souvislosti se zaměstnáním a za účely archivace

1.6.3 Hlavní změny

Na základě zjištění učiněných v předchozích kapitolách je třeba identifikovat hlavní změny, které přináší zavedení nového nařízení do českých právních norem, protože právě ty způsobí nutnost zásahu do současného automatizovaného zpracování dat informačními systémy.

1) Se zavedením nařízení platí stejné povinnosti pro správce i zpracovatele osobních údajů. O plnění nařízení se nově musí starat oba.
2) Nově se za osobní údaje považuje i e-mail, IP adresa či tzv. cookies
3) Subjekt údajů dostává následující nová práva
    a. Právo odebrat souhlas se zpracováním osobních údajů jinak než písemně
    b. Právo být zapomenut, pokud neexistuje zákonný důvod pro další držení údajů
    c. Právo na přenos osobních údajů
    d. Právo na přístup ke svým osobním údajům, nejlépe online
4) Povinnost nahlásit příslušným orgánům a případně subjektům údajů porušení bezpečnosti dat
5) Ruší se ohlašovací povinnost, plynoucí z §16 zákona o ochraně osobních údajů
6) Místo ohlašovací povinnosti se zavádí záznamy o činnostech zpracování
7) Pro společnosti, zabývající se rozsáhlými systémy pro správu osobních dat je třeba jmenovat pověřence pro ochranu osobních údajů

1.7 Důsledky nařízení pro tvůrce softwarových služeb

Ze změn, které nové nařízení vnáší do legislativ plynou novinky, podle kterých se musí zařídit správci a nově i zpracovatelé osobních údajů. Do kategorie zpracovatelů osobních údajů spadají provozovatelé informačních systémů, pokud tyto systémy zpracovávají osobní údaje. Pro správce a zpracovatele osobních údajů platí od zavedení nového nařízení zejména tyto změny:

1) Provozovatel informačního systému je povinen zvážit nebezpečí úniku osobních údajů a na základě toho zvolit přiměřenou úroveň zabezpečení
2) Provozovatel společně se správcem jsou povinni umožnit subjektu údajů odebrat souhlas stejně snadno, jako jej udělil. Pokud jej například udělil tlačítkem v informačním systému, mělo by jít obdobně i souhlas odebrat
3) Správce musí umožnit smazat osobní data z informačního systému na základě přání subjektu údajů. Pokud by to narušilo integritu dat, je povinen anonymizovat údaje tak, aby z nich žádnou zpětnou transformací nebylo možné získat původní údaje, nejlépe tedy nahradit náhodným unikátním řetězcem
4) Provozovatel systému musí umožnit zobrazit subjektu údajů veškeré údaje, které jsou o něm zpracovávány. Správce pak musí být schopen určit dobu, po kterou se data budou zpracovávat.
5) Provozovatel systému musí kontrolovat případné úniky dat, aby o nich mohl správce informovat příslušný úřad, případně subjekty údajů.
6) Provozovatel musí zaznamenávat veškerou manipulaci a čtení osobních údajů, které byly v informačním systému provedeny.

1.7.1 Důsledky na zálohování

Zálohováním dat se myslí vytváření záložních kopií dat pro případ ztráty dat původních. Je jedno, zda se jedná o údaje na originálních úložištích či na záložních médiích, k obojímu je třeba přistupovat stejně. I pro zálohy tedy platí následující:

1) Je třeba nastavit přiměřenou úroveň zabezpečení, která zamezí neoprávněnému užití dat

2) Pokud subjekt údajů využije práva na to být zapomenut, je třeba zabezpečit, aby data byla smazána i ze záloh nebo aby se taková data nikdy nemohla dostat ani do systému ani do jiné podoby, kde by mohla být jakkoliv využita
3) V případě úniku záloh je třeba postupovat stejně, jako v případě úniku dat z primární databáze, pokud nejsou zálohy zašifrovány či jinak chráněny proti neoprávněnému užití
4) Veškerá manipulace a čtení záloh musí být zaznamenána

1.8 Praktické aspekty

Z hlediska způsobu, jakým je nové nařízení napsáno se liší od jiných právních norem, které jsou běžně uplatňovány v našem státě. Zatímco české zákony běžně obsahují normy a pokyny, které je třeba dodržovat pro zachování souladu se zákonem, v GDPR tyto aspekty chybí. Je proto třeba hledat další zdroje, jako jsou rozsudky soudů, které řešily žaloby spojené s těmito právními předpisy, výklady pracovních skupin a rady právních firem, které se zabývají výkladem Evropského práva.

Jedním z pramenů, kde lze najít cenné informace o výkladu, může být i preambule samotného nařízení. Ta obsahuje tzv. recitály, což jsou ustanovení předcházející vlastnímu textu nařízení. Z části slouží jakovýklad následujícího nařízení, obsahuj příklady, mohou sloužit jako výklad nejasně definovaných pojmů v textu samotného nařízení a lze je brát i jako zprávu o příčině zavádění opatření. V následujících bodech bude nastíněno vysvětlení některých pojmů, jejichž výklad by nemusel být po přečtení nařízení zcela jasný a pro jejichž vysvětlení lze nalézt oporu právě v preambuli.

1.8.1 Oprávněný zájem

Jak již bylo zmíněno v této kapitole, GDPR definuje právní základy, při kterých je zpracování osobních údajů legální. Pokud zpracovatel nenaplňuje ani jeden z nich, nesmí v žádném případě zpracovávat osobní údaje. Jeden z bodů, poskytujících legální základ pro zpracování osobních dat zní:

Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva

a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

(GDPR, Článek 6, odstavec 1. bod f)

Oprávněný zájem je novým pojmem, který směrnice zavádí do práva o ochraně osobních údajů. Tento bod zakládá právo zpracovat údaje na základě zájmů správce nebo třetí strany. V souvislosti s tímto bodem lze osobní údaje zpracovávat, pokud:

- Neexistuje jiný způsob, jak dosáhnout zájmu správce nebo třetí strany
- Zájmy a základní práva subjektu údajů nepřevažují nad zájmy správce údajů
- Subjekt může důvodně očekávat, že data budou tímto způsobem zpracována

Příklady, kdy může být tento právní základ využit pro zpracování osobních údajů, které udává přímo preambule nařízení, jsou zamezení podvodům a přímý marketing. Rozhodně však lze nalézt výrazně větší množství důvodů, které lze užít jako základ pro oprávněný zájem zpracovatele či třetí strany.

Jedním z typických příkladů může být ochrana majetku zpracovatele, ať už se jedná o kamerové systémy, systémy řízení přístupu do objektů či k zařízením. Ve složitějších případech doporučuje nezávislá asociace Data Protection Network (DPN) tři zkoušky[14], které zpracovateli mohou zodpovědět otázku, zda může použít oprávněný zájem jako základ pro zpracování osobních údajů.

1. Je zájem, kvůli kterému budou údaje zpracovávány, skutečně oprávněným zájmem správce?
2. Jaké konkrétní údaje budou zpracovávány? Je nevyhnutelné zpracovávat tyto údaje? Nelze se stejného výsledku dobrat i bez jejich zpracování?
3. Je oprávněný zájem dostatečný, aby vyrovnal omezení práv a svobod osoby, jejíž údaje se budou zpracovávat?

Tyto otázky by si měl zodpovědět každý, kdo bude chtít zpracovávat osobní data na základě oprávněného zájmu. V bodě jedna je třeba jasně definovat, co je zájmem budoucího správce údajů. Je třeba, aby byla provedena opravdu důkladná analýza s jednoznačným závěrem, jejíž výstupy budou zaznamenány a budou k nahlédnutí pro případ, že budou vyžádány ze strany ÚOOÚ. Dále by stručné závěry této analýzy měly být poskytnuty při sběru údajů a přístupné i později na vyžádání osob, jejichž osobní

údaje jsou zpracovávány. Pokud byly osobní údaje získány jinak, je třeba před jejich zpracováním informovat všechny dotčené osoby. Z toho vyplývá, že je nezbytné tuto analýzu vypracovat ještě před zahájením sbírání či zpracovávání údajů, v opačném případě se správce vystavuje riziku pokuty ze strany státních institucí dohlížejících na ochranu osobních údajů.

V druhém bodě je třeba analyzovat, které údaje jsou nevyhnutelné pro účely definované v předcházejícím bodě. Výstupem tohoto bodu je pak množina osobních údajů, která bude sloužit pro plnění definovaných cílů, která je dále neredukovatelná. V případě, že existuje více řešení, je správce povinen vybrat to, které zahrnuje co nejmenší množství osobních údajů. Větší množství osobních údajů než je nezbytně nutné je možné zpracovávat v případě, že by alternativní varianty způsobily správci nepřiměřené úsilí či náklady.

Ve třetí zkoušce je třeba zvážit, zda je zájem natolik závažný, aby vyvážil dopad na práva a svobody fyzické osoby, jejíž osobní údaje se budou zpracovávat. Vždy je třeba zvážit, jak důležité jsou pro správce zájmy, které naplní zpracováním osobních údajů v porovnání se zásahem, který bude učiněn do práv a svobod subjektu a jak citlivé osobní údaje budou zpracovávány. Dále je třeba na základě úrovně citlivosti osobních údajů určit, zda je správce schopen zajistit dostatečnou úroveň jejich ochrany.

1.8.2 Praktické případy užití oprávněného zájmu

Přímo v preambuli nařízení lze najít příklady, kdy lze užít oprávněný zájem správce pro zpracování osobních údajů. Tyto příklady pak mohou sloužit jako vodítka pro rozhodování, zda lze využít oprávněného zájmu či nikoliv. Obecně lze říci, že vždy záleží na tom, zda může subjekt osobních údajů očekávat, že se budou jeho osobní údaje zpracovávat tímto způsobem. Z toho například vyplývá, že například při podpisu smlouvy mohou být zpracovávány osobní údaje nejenom nezbytně nutné pro její plnění, ale i další, jejichž zpracování a užití může subjekt údajů důvodně očekávat. Je však nezbytné, aby správce vždy věděl, na jakém základě zpracovává které osobní údaje a byl schopen to doložit, například pro potřeby ÚOOÚ. Navíc se na údaje zpracovávané na různých základech vztahují různá pravidla.

Přímý marketing

Je-li zájem správce osobních údajů marketing jeho zboží či služeb, je potom možné užít

oprávněný zájem i pro potřeby přímého marketingu. I zde však platí pravidlo, že subjekt údajů musí být o zpracování informován a musí mít možnost vznést námitku. V případě vznesení námitky proti užití jeho osobních údajů pro potřeby přímého marketingu je správce povinen data bezodkladně smazat.

Předcházení podvodům

Dalším výslovným důvodem, který je uveden v preambuli nařízení, je zamezení podvodům. Je potom na správci, aby určil minimální množství osobních údajů, které poslouží pro splnění tohoto zájmu.

Předání osobních údajů v rámci skupiny

V případě skupiny podniků či institucí, může existovat oprávněný zájem, který dovoluje předávat osobní údaje mezi jednotlivými prvky struktury, zejména pro vnitřní administrativní účely. Toto se týká jak osobních údajů zaměstnanců, tak zákazníků.

Bezpečnost sítě a informací

Jedná se o snahu zabezpečit síť a informace na ní obsažené proti náhodným událostem, protiprávnímu či zlovolnému jednání, které ohrožuje dostupnost, pravost, správnost a důvěrnost údajů.

Samozřejmě výše vyjmenované příklady jsou jen část možných a oprávněný souhlas lze využít na širokou škálu zájmů vedoucích ke zpracovávání osobních údajů. Jako další lze uvažovat analytické účely, evidenci, personalizaci, monitoring pro zlepšování služeb atd.

1.8.3 Postup v případě námitky

Subjekt, jehož osobní údaje budou zpracovávány, má vždy právo vznést námitku. V takovém případě je správce povinen omezit zpracování těchto údajů a dále je nezbytné, aby prokázal oprávněnost zpracování těchto údajů. V tomto případě je nutné vycházet z analýzy, která musí předcházet zpracovávání osobních údajů na základě oprávněného zájmu. Pokud správce nebude schopen doložit oprávněnost svého zájmu, musí následovat výmaz osobních údajů či jejich anonymizace. Výjimku tvoří zpracování pro potřeby přímého marketingu. V takovém případě je správce povinen data přestat využívat a smazat je okamžitě, bez šance obhájit toto zpracování.

1.8.4 Oznámení subjektu údajů

V případě, že budou data subjektu zpracovávána na základě opravného zájmu, je správce povinen informovat jej již při sběru údajů, nebo, pokud data získá jinak, nejpozději do jednoho měsíce. Součástí informace by měly být stručné důvody, proč je to pro účely správce nezbytné a také zde musí být informace o možnosti vznést námitku proti tomuto zpracování.

1.8.5 Udělení souhlasu se zpracováním osobních údajů

Oprávněný zájem je v nařízení zaveden zejména z důvodu snížení počtu souhlasů se zpracováním osobních údajů, které musí každý jednotlivec udílet. S GDPR se však podmínky souhlasu zpřísňují. Konkrétně je jasně řečeno, že souhlas musí být svobodně daný, informovaný, oddělený od ostatních informací v textu, jasný a srozumitelný. Navíc souhlas musí být možné kdykoliv odebrat a to stejně jednoduše, jako byl udělený. To například znamená, že pokud byl souhlas udělen kliknutím na webu, měl by web obsahovat tlačítko, které tento souhlas automaticky odebere. Navíc by možnost odebrat souhlas měla být součástí všech dokumentů, skrz které se souhlas získává a všech písemností, zaslaných na základě tohoto souhlasu. V případě odebrání souhlasu je správce povinen data vymazat či anonymizovat.

Svobodný souhlas znamená, že souhlas nepodmiňuje libovolnou další akci, která přímo nesouvisí se zpracováním osobních údajů. Například tedy nelze vyžadovat souhlas se zpracováním osobních údajů před přihlášením se na Wi-Fi síť, možností účastnit se akce, pro kterou nejsou osobní data nezbytně nutná a podobně.

Dalším důležitým aspektem je zvážit, zda neexistuje jiný důvod pro zpracování osobních údajů a je opravdu nutné sáhnout po žádosti o souhlas. Souhlas je totiž z pohledu GDPR až poslední možnost a jsou na něj kladeny striktní požadavky. Navíc v případě, že existuje jiný právní důvod, například nezbytnost zpracování údajů pro účely plnění smlouvy mezi smluvními stranami, plnění úkolu prováděného ve veřejném zájmu či jiný oprávněný zájem, je vyžadování souhlasu dokonce v přímém rozporu s GDPR.

V případě, že jsou data zpracovávána na základě jiných právních důvodů, může žádost o souhlas evokovat, že k výmazu dat může dojít na základě jeho odebrání, což ale v takovém případě není pravda a jedná se tak o zavádějící a klamavou informaci.

1.8.6 Postup při úniku osobních údajů

V případě bezpečnostního incidentu, při kterém existuje vysoké riziko pro práva a svobody subjektu (či subjektů) údajů, vzniká správci povinnost informovat o této události subjekt (subjekty) údajů, a to bez zbytečných odkladů[15]. Správce není povinen subjekty informovat v případě, že by to vyžadovalo nepřiměřené úsilí. Dále pokud je pravděpodobné, že by incident mohl vést k riziku pro práva a svobody fyzických osob, je nutné jej ohlásit příslušnému dozorovému úřadu.

V oznámení by mělo být jasně a stručně vysvětleno, k čemu došlo, co na základě tohoto incidentu může hrozit a jaké kroky podnikl správce, aby minimalizoval dopad této situace. Dále je nezbytné, aby oznámení obsahovalo kroky, které může podniknout subjekt údajů pro zabezpečení ochrany před nepříznivými důsledky porušení. Oznámení musí být provedeno bez zbytečného odkladu, což znamená co nejdříve to bude možné.

Co se rozumí pod pojmem vysoké riziko pro práva a svobody subjektu? Je to na posouzení správce údajů. Výjimkami přímo zmíněnými v nařízení jsou taková data, která nemohou sloužit k identifikaci konkrétních osob, například data zašifrovaná, anonymizovaná, či upravená tak, aby neměla vazbu na konkrétní subjekt. Dále není třeba informovat v případě, kdy správce učiní následné kroky, které znemožní identifikaci konkrétních subjektů údajů či jinak zamezí vzniku situace s vysokým rizikem pro práva a svobody.

Naopak jednoznačně je riziko vysoké, pokud může incident vést k fyzické, hmotné nebo nehmotné újmě fyzických osob, u jejichž údajů bylo narušeno zabezpečení. Například je třeba zodpovědět otázku, zda na základě uniklých dat není možné, že by subjektu byla způsobena újma diskriminací, krádeží nebo zneužitím totožnosti či poškozením dobrého jména.

Dalším nejasným bodem je nepřiměřené úsilí. Může se jednat například o situaci, kdy byla data v důsledku bezpečnostního incidentu ztracena, takže není možné zpětně určit, koho je třeba informovat. V takovém případě je na zvážení správce, zda

nezvolit opatření, které by informovalo všechny potenciální subjekty, jako je například zpráva v médiích či na vlastních webových stránkách. Dále je možné poskytovat informace o porušení na vyžádání, což by mohlo být užitečné pro ty osoby, které mohou být porušením dotčeny, ale z důvodu ztráty kontaktních údajů se s nimi nelze spojit.

Pokud správce údajů rozhodne, že subjekty informovat nebude, musí přesně vědět, z jakého důvodu tak nečiní pro případ, že ses jej na to dotáže dozorový úřad (v Česku Úřad pro ochranu osobních údajů). Tento úřad může rozhodnout, že je třeba oznámení učinit bez ohledu na dodaný důvod a případně udělit sankce.

Posouzení rizika

S novou legislativou vzniká i nová povinnost pro správce údajů. Ten by po incidentu, který může vést k riziku pro práva a svobody fyzických osob, měl nejen vhodně reagovat s cílem maximálně omezit škody, ale měl by také posoudit rizika, které z něj mohou plynout. Důvody, na kterých tento bod staví, jsou dobře identifikovatelné. Správce totiž nejlépe ví, jaká data unikla (či mohla uniknout) a je tedy kvalifikován posoudit, jak velké riziko pro dotčenou osobu z jejich kompromitace plyne.

Pracovní skupina WP29 zmiňuje následující oblasti, které by měly být vzaty v úvahu při hodnocení závažnosti incidentu:

1. Typ porušení – záleží na tom, o jaký typ porušení se jednalo. Například zcela jinou váhu má porušení, při kterém byla citlivá data poskytnuta neoprávněným osobám než to, kdy byla data pouze ztracena.
2. Povaha, citlivost a objem osobních údajů – čím jsou údaje citlivější, tím větší potenciální újma hrozí. Navíc je třeba zohlednit i další faktory, jako jsou například další data, která jsou o subjektu údajů již známá.
3. Snadnost zjištění totožnosti fyzických osob – záleží, zda uniklá data umožňují přímo identifikovat subjekt údajů, umožňují to v kombinaci s jinými daty nebo to není možné vůbec.
4. Závažnost následků pro subjekt údajů – důležitým aspektem je i to, zda si je správce vědom, že se údaje dostaly do rukou osob s neznámými či nebezpečnými záměry. V určitých případech lze určit nezáměrného příjemce dat za důvěryhodného, například v situaci, kdy se data dostala omylem do jiné části

organizace či známému dodavateli. V takovém případě si musí být správce jist, že na požádání budou data od nezáměrného příjemce smazána.

5. Zvláštní charakteristicky fyzické osoby – zejména v případě, že se jedná o děti či jinak zranitelné osoby.
6. Zvláštní charakteristiky správce údajů
7. Počet dotčených fyzických osob – čím více osob je dotčeno únikem dat, tím je vyšší míra rizika. Na druhou stranu i v případě úniku dat o jednotlivci může být tento únik zvlášť závažný, pokud naplňuje některé další body z tohoto seznamu
8. Všeobecné aspekty – obecně je na správci, aby zvážil potenciální míru dopadu a jeho pravděpodobnost. Pokud si správce není jist, je vhodnější incident nahlásit.

Dokumentace případů porušení

Každý bezpečnostní incident, bez ohledu na to, zda zakládá povinnost ohlásit jej, je třeba dokumentovat. Tato dokumentace musí být aktuální a Úřad pro ochranu osobních údajů si kdykoliv může vyžádat možnost do ní nahlédnout, proto se doporučuje vytvořit si centrální registr těchto záznamů.

V těchto záznamech musí být uvedeny podrobnosti týkající se porušení, a to včetně příčin a dotčených údajů. Dále by se zde měly vyskytovat kroky, které správce podnikl pro maximální snížení dopadu a zamezení opakování tohoto incidentu, například přesné znění a další dokumentace k oznámení, učiněného k subjektům údajů. Pokud incident nebyl ohlášen, je třeba zaznamenat důvod, proč tomu tak nebylo. Pokud došlo k oznámení se zpožděním, je třeba odůvodnit ve zprávě i toto zpoždění.

Přiměřená úroveň zabezpečení

Novým pojmem, se kterým je třeba se seznámit, je i přiměřená úroveň zabezpečení osobních údajů. GDPR ukládá každému správci i zpracovateli, aby zanalyzoval situaci a navrhl opatření, která budou vhodná pro zabezpečení konkrétních dat. Opět je to z toho důvodu, že právě správce a zpracovatel dokáží nejlépe posoudit, jak jsou uložená data citlivá s přihlédnutím k jejich povaze, rozsahu a účelem zpracování a jaká jsou vhodná technická a organizační opatření, která pro data na této úrovni poskytnou odpovídající zabezpečení.

Jako příklad lze uvést různou potřebu zabezpečení pro různě citlivá data. Například seznam jmen a příjmení lze označit za osobní údaje, ale pokud tato jména nebude možné spojit s dalšími citlivými údaji, například na základě povahy zpracovatele údajů, riziko jejich zneužití a z toho plynoucí fyzické, majetkové i nemajetkové ztráty pro subjekty údajů je nízké. Naopak v případě uchovávání medicínských dat je jasné, že při jejich úniku je riziko ztráty vysoké.

Jako zvláště citlivé osobní údaje jsou v nařízení uvedeny údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání, filosofickém přesvědčení, genetické či zdravotní údaje, údaje o sexuálním životě, odsouzení v trestních věcech a podobné informace, které by mohly subjekt údajů samy o sobě poškodit. V takovém případě lze tato data zpracovávat pouze v případě, že nastane některá z výjimek uvedených v článku 9 odstavci 2 nařízení.

Po analýze citlivosti údajů je potom na správci, aby stanovil patřičnou úroveň zabezpečení. Pokud pro správu najímá externího zpracovatele, je třeba, aby společným úsilím stanovili míru závažnosti případného úniku dat a nastavili odpovídající úroveň zabezpečení. Ani v případě nízkého rizika nelze zabezpečení zcela vynechat. Vždy je nutné volit ze současné nabídky bezpečnostních prvků takové, které budou data přiměřeně chránit.

Jedním z možných prvků zabezpečení je například pseudonymizace nebo šifrování. Pseudonymizací se rozumí činnost, při které se skryje identita subjektu údajů, a to tak, že se identita buď přímo odstraní, v případě, že ji není třeba pro účel zpracování znát (anonymizace), či se nahradí klíčem. Za použití tohoto klíče se dá identita subjektu dohledat, proto je nezbytné pro správnou funkčnost pseudonymizace uchovávat identitu odděleně od údajů s klíči. Šifrované údaje jsou takové, které jsou zašifrovány pomocí moderních technologií, které jsou v daném místě a čase považovány za bezpečné. Šifrované údaje jsou pak nečitelné pro kohokoliv, kdo nevlastní klíč. Tento klíč je třeba uchovávat odděleně od zdroje šifrovaných dat. V případě anonymizace se pak na data již nařízení nevztahuje, zatímco v ostatních výše zmíněných případech je třeba stále s daty nakládat v souladu s GDPR.

Nařízení dále upravuje i požadavky na smlouvy mezi správcem a zpracovatelem osobních údajů. Zpracovatelem je například i provozovatel cloudu, na kterém jsou data

uložena. Za bezpečnost přístupu ke cloudu pomocí účtů, které vytvořil správce údajů, pak sice odpovídá stále správce, ale provozovatel cloudu je v tomto případě odpovědný za to, aby nebylo možné k datům v cloudu přistoupit odjinud než z těchto účtů.

2 ANALÝZA SOUČASNÉHO STAVU

Tato kapitola bude zaměřena na současné metody zálohování, zejména na metody, které jsou vhodné a často využívané ve firmách, a dále rozebereme některé aspekty, které souvisejí s ochranou osobních dat v rámci těchto záloh.

2.1 Typy záloh dle způsobu vytvoření

Jedním z důležitých prvků, který je třeba zohlednit při posuzování přístupu k zálohování dat ve společnostech, je forma, jakým způsobem je zálohování provedeno. Každý typ má svá specifika, která určují, jakým způsobem je možné zálohy následně používat a má své výhody a nevýhody jak pro samotné ukládání, archivování a použití, tak i vzhledem k ochraně osobních údajů.

2.1.1 Nestrukturované zálohy

Jedná se o nejjednodušší způsob zálohování. Při tomto druhu zálohování se vytváří úplná kopie dat s minimem metadat, které by nesly informace o struktuře dat a umožnily tak práci s konkrétními částmi zálohy. Nahrání zálohy pak probíhá tak, že se nahrává celá. Pokud je třeba nahrát pouze část, je třeba manuálně tuto část najít a vložit do současných dat. Pro tento typ záloh nejsou žádné metodiky či programy, které by umožnily mapovat, která verze je v současnosti používaná. Tento systém se hodí pro menší části dat, například konkrétní pracovní stanice.

Pro data obsahující osobní údaje je tento způsob zálohování naprosto nevhodný. Protože není známo, jaká je povaha uložených dat, není možné určit, které informace jsou osobními daty, a proto při potřebě jakéhokoliv zásahu vycházejícího z povahy nařízení o ochraně osobních údajů není jiná varianta, než ručně zkontrolovat veškeré zálohy a provést úpravy, které jsou vyžadovány. Z důvodu neexistence dat o struktuře nelze zavést systémy, které by zaručily, že se údaje ze záloh, které mají být smazány či anonymizovány, nedostanou do aktuální verze.

Dále je třeba pro tyto zálohy nastavit pravidla, která zabezpečí kontrolu toho, kdy a jakým způsobem bylo k datům přistupováno a kdo k nim měl přístup. Opět neexistují jednotné systémy, které by toto zaručily, a je třeba důkladné nastavení firemních pravidel, které to zabezpečí. Rovněž je třeba nastavit pravidla tak, aby tyto

zálohy byly uloženy bezpečně, a to tak, aby nemohlo dojít k jejich odcizení, zpřístupnění třetím stranám či ztrátě. Navíc nastavení těchto pravidel musí být takové, aby pokud dojde ke ztrátě či odcizení těchto dat, bylo zaručeno, že tento incident neprojde bez povšimnutí, bude zaznamenán a bude možné provést odpovídající kroky, které vyžaduje nařízení. Jednou z variant, která se v tomto případě nabízí, je zabezpečit data tak, aby v případě ztráty byla nepoužitelná bez dalších informací, u kterých je zabezpečeno, že neuniknou. Jedná se tak například o šifrování, jehož úroveň je třeba nastavit na základě rizika plynoucího z úniku osobních dat pro fyzické osoby. Dále se může jednat o rozdělení dat tak, aby bez dalších interních informací nebylo možné určit, o kom data jsou, tzv. pseudonymizace.

Z výše zmíněných důvodů jsou nestrukturované zálohy vysoce nevhodné pro zálohování osobních údajů. Vždy je však třeba přihlédnout k přístupu založenému na riziku a postupu, který nebude přinášet nepřiměřené náklady.

2.1.2 Úplná záloha v kombinaci s inkrementální

Při tomto postupu je vytvořena kopie současného stavu a následně jsou v pravidelných intervalech zaznamenávány změny, které se vyskytly od poslední zálohy. Při návratu k některé z minulých verzí je nahrána do systému poslední úplná kopie stavu a následně postupně uplatněny všechny inkrementální změny až k požadované. Tento proces je poměrně náročný a jeho náročnost vzrůstá s počtem kroků, které je třeba provést od poslední úplné kopie. Zároveň se zvyšuje riziko ztráty zálohy, neboť chyba v kterémkoliv kroku znamená, že se již nikdy nebude možné plně vrátit k vyžadovanému stavu.

V případě, že je dobře zpracována správa metadat v tomto systému zálohování, může být vhodný pro zálohování osobních údajů. Důležité je, aby bylo zaznamenáno, která data jsou osobní a jakého druhu. V rámci firemních procesů je třeba nastavit taková pravidla, aby bylo možné zálohy smazat či anonymizovat osobní údaje v zálohách, pokud to bude vyžádáno na základě práva být zapomenut. Alternativně je možné nastavit procesy tak, aby se taková data ze záloh nikdy nemohla dostat do aktivní verze. Dále je nezbytné provést analýzu vhodné úrovně zabezpečení a na jejím základě nastavit pravidla, která zajistí, že veškerá manipulace se zálohami, včetně jejich součástí, bude zaznamenána.

2.1.3 Úplná záloha v kombinaci s rozdílovou

I v tomto případě je v pravidelných intervalech vytvářena úplná kopie současného stavu systému. V době mezi těmito intervaly je vytvářena záloha, kde zachytí všechny rozdíly mezi původní úplnou kopií a stavem v době zálohy. Tento systém je bezpečnější, neboť není třeba postupně aplikovat všechny kroky, ale aplikuje se pouze poslední. Nevýhodou oproti inkrementální verzi je pak větší velikost zálohovaných souborů.

Z hlediska ochrany osobních údajů není mnoho rozdílů mezi touto metodou a metodou inkrementální. Je nezbytné mít v rámci záloh metadata alespoň na takové úrovni, aby bylo jasně identifikovatelné, kde se nachází osobní údaje. Stejně tak musí být možné v zálohách mít možnost smazat či anonymizovat osobní údaje osob, které na to budou mít nárok a požádají o to. Stejně tak je třeba uplatnit firemní procesy pro omezení a monitorování přístupu. Zabezpečit je třeba jak úplnou kopii, tak i rozdílová data, pokud by z nich bylo možné jakýmkoliv způsobem získat data osobní.

2.1.4 Žurnálování

Při této metodě je každá změna zapsána do žurnálu, který plní funkci logu. Do tohoto žurnálu se většinou ukládají bloky dat namísto celých změněných souborů. To umožňuje vrátit se k libovolnému stavu systému na základě žurnálovaných dat.

I v tomto případě je ochrana osobních dat podobná jako u výše jmenovaných systémů. Je nezbytné zvolit systém, který dokáže rozlišit v žurnálech dle metadat položky obsahující osobní údaje. Je třeba mít možnost tyto osobní údaje smazat či anonymizovat. Nastavení firemních procesů by mělo být takové, že data budou přístupná pouze povolaným osobám a jejich čtení a změna bude vždy zaznamenána. Zabezpečení musí být takové, aby cizím osobám neumožnilo rekonstruovat z žurnálovaných dat žádné osobní údaje, které by mohly vést k identifikaci fyzických osob.

2.2 Média užívaná pro zálohování

Mezi další důležité prvky zálohování patří médium, na kterém se záloha nachází. Rychlost přístupu, možnosti změn na médiích, trvanlivost dat, přenosnost a další

parametry velice ovlivňují zálohování a je třeba je brát v úvahu při tvorbě strategie zálohování v souvislosti s nařízením. Pro všechna tato média platí zásada, že nachází-li se na nich data, která by mohla vést k identifikaci fyzických osob, je nezbytně nutné, aby nebyla přístupná nepovolaným osobám nebo byla ošetřena tak, aby v případě, že se k těmto osobám dostanou, nebylo možné přečíst plná data vedoucí k identifikaci fyzických osob. Toho lze dosáhnout například šifrováním či pseudonymizací. Dále musí být manipulace se zálohami zaznamenávána.

V následujících odstavcích budou rozebrána nejčastěji využívaná média a přístup, který by měla organizace implementovat pro vyhovění potřebám nařízení. V historii se pro zálohování užívalo větší množství médií a v některých společnostech se s nimi ještě stále lze setkat, pro potřeby této práce však byla zvolena pouze ta nejčastější. Pro libovolná média pak platí stejná pravidla, která se dají analogicky odvodit z následujících příkladů.

2.2.1 Magnetická páska

Jedná se o starší, ale stále velmi populární způsob zálohování a archivace dat. Jeho hlavní výhoda spočítá v nízké ceně médií a jejich dlouhé životnosti. Pro pásky standardu LTO (Linear Tape Open) se udává životnost 15 až 30 let. Bez povšimnutí by neměla zůstat ani vysoká spolehlivost páskových úložišť. Výše jmenované přednosti činní z páskových úložišť ideální média pro zálohování a zejména archivaci dat. Nevýhodou pak je vyšší režie při vytváření záloh i jejich čtení. Nevýhodou těchto úložišť je omezený počet zápisů na pásku.

Pro potřeby zálohování dat obsahujících osobní údaje jsou pásky použitelné, ale je třeba dodržet jistá pravidla. Zamezení přístupu k údajům lze dosáhnout jednoduše šifrováním, které může od standardu LTO-4 probíhat na hardwarové úrovni přímo ve čtecím zařízení, čímž se výrazně urychlí zpracování a následné čtení dat a zároveň zlepší datová integrita. V případě, kdy šifrování není použito, je důležité fyzicky zamezit přístupu třetích osob k páskovým úložištím, například uložením pásek v trezoru.

Samozřejmě i zde platí pravidla přístupu založeného na riziku, kde by úroveň fyzického zabezpečení pásek měla odpovídat citlivosti údajů na páskách. V případě šifrování je třeba mít šifrovací klíče uložené na bezpečných místech, kde k nim mohou

mít přístup pouze povolané osoby. Dále je třeba veškerou manipulaci s páskami zaznamenávat.

Je třeba mít na paměti, že z povahy nařízení může často docházet k žádostem o smazání či anonymizaci osobních údajů fyzických osob, kterým bude třeba vyhovět, v opačném případě bude následovat sankce. Plnění těchto žádostí je vzhledem k povaze páskových úložišť komplikované, protože počet přepisů pásky je omezený a s každým zápisem se zvyšuje riziko chyby.

Největší nevýhody páskového úložiště v tomto směru lze odstranit vhodnou pseudonymizací, kde co největší množství dat bude uloženo pouze pod klíčovými označeními. Potom se mazání či anonymizace dat dotkne pouze těch pásek, které nesou klíče použitelné pro identifikaci konkrétních fyzických osob. Specifické postupy jsou blíže rozebrány v kapitole, která se věnuje praktické implementaci.

2.2.2 Pevné disky

Jedná se o elektromechanické zařízení pro záznam a čtení dat pomocí elektromagnetické indukce. Jeho hlavní výhodou je nízká pořizovací cena, dobrá přenositelnost, krátká přístupová doba a možnost připojení k široké škále koncových zařízení. Mezi nevýhody pak patří nižší životnost[16].

Vhodnou statistiku pro představu životnosti pevných disků poskytuje společnost Blackbaze, která provozuje datová centra pro zálohování. Tato datová centra obsahují velké množství disků. V roce 2018 se jejich počet pohyboval okolo čísla 25 000 plotnových disků. Společnost Blackbaze vede přesné statistiky o tom, jak dlouho disky vydrží. Z nich vyplývá, že poruchovost v prvním roce a půl se pohybuje na 5,1 % za rok. Dalších 18 měsíců se poruchovost drží na hodnotě 1,4 %. Poté se ovšem počet selhání výrazně zvyšuje na hodnotu 11,8 % za rok. Z toho plyne, že po čtyřech letech je funkčních pouze 78 % pevných disků. Delší statistiky zatím nejsou k dispozici.

Z důvodu této vyšší poruchovosti je při využití pevných disků pro zálohování vhodné použít řešení, které nabízí redundanci, kde je zapojeno více disků obsahujících stejná data, což v praxi znamená, že při poruše disku nebudou data ztracena. V angličtině se pro takové řešení užívá zkratka RAID (Redundant Array of Independent Disks) následovaná číslem, které udává úroveň zabezpečení dat na diskovém poli proti

ztrátě dat. V historii bylo vyvinuto mnoho takovýchto systémů redundance, většina z nich se ale již v praxi nepoužívá. Níže si rozebereme ty stále užívané.

RAID 0

Jedná se o stav, kdy neexistují žádná redundantní data, a proto se nejedná o bezpečný způsob ukládání dat. Při poruše jednoho disku jsou data, která na něm byla zaznamenána, nenávratně ztracena. Toto řešení se užívá pouze proto, aby byl prostor více disků adresovatelný jako jeden paměťový prostor.

Pro toto spojení paměťových prostorů se užívá dvou metod. Při první se disky zřetězí, takže po zaplnění prvního se data zapisují na druhý a tak dále. Výhodou je, že při ztrátě jednoho disku lze ještě zachránit data z disků ostatních.

Druhou metodou je prokládání, při kterém se data zapisují na disky střídavě po blocích pevné velikosti. Výhodou tohoto zapojení je vyšší rychlost při čtení velkých souborů, které jsou rozloženy mezi několika disky. Největší nevýhodou je naopak fakt, že při poruše jednoho disku budou dotčeny všechny soubory.

RAID 1

Jedná se o nejjednodušší ochranu, kde se zrcadlí data z jednoho disku na druhý. To znamená, že se stejná data zaznamenávají na dva disky najednou. V případě poruchy jednoho z disků lze stále přistupovat k druhému. Tento způsob ochrany dat je vysoce efektivní, nevýhodou pak mohou být vyšší pořizovací náklady.

RAID 5

Jedná se o systém, kde jsou použity alespoň tři pevné disky. Třetina kapacity této sestavy je pak vyhrazena pro samoopravné kódy, které umožňují v případě výpadku jednoho disku vypočítat ztracená data. Soubory jsou na discích rozloženy rovnoměrně po částech. Navíc tyto kódy umožňují i vyhledávání chyb. Výhodou je nižší redundance než v zapojení RAID 1, je pouze třetinová. Nevýhodou je pak pomalejší zápis, způsobený nutností výpočtu samoopravného kódu. Čtení je rychlejší, protože využívá stejné výhody jako RAID 0 při prokládané variantě.

RAID 6

RAID 6 je obdobou zapojení RAID 5 s tím rozdílem, že obsahuje dva samoopravné kódy, díky kterým umožňuje opravit systém po výpadku dvou disků. Kapacita odpovídající velikosti dvou disků je zde využita pro ukládání samoopravného kódu, takže toto zapojení je výhodné až při užití více než 4 disků. V opačném případě se doporučuje RAID 1.

Víceúrovňová disková pole

V praxi se často lze setkat s kombinováním výše uvedených metod v diskových polích. Tím lze získat výhody některých řešení a potlačit jejich nevýhody.

RAID 01 a 10

V tomto systému se disky spojí buď nejdříve do RAID 0 a tato spojení se zrcadlí na druhé spojení pomocí RAID 1, nebo se naopak dva disky zrcadlí pomocí RAID 1 a takto získaný paměťový prostor se propojí s dalšími pomocí RAID 0. Výhodou je dobrá rychlost čtení a zápisu jako při užití prokládaného RAID 1 s velmi robustním systémem ochrany proti výpadku disků. Nevýhodou je pak vyšší pořizovací cena, plynoucí z datové redundance, která činí 50 %, neboť polovina kapacity disků je využita pro zrcadlení.

RAID 50

Tento systém umožňuje zakombinovat větší množství diskových polí o třech discích do složitějších systémů. Pole 3 disků, zapojené pomocí RAID 5, se propojí s dalšími pomocí RAID 0, čímž vznikne jeden paměťový prostor.

Toto zapojení je odolné vůči výpadku jednoho disku z každého pole 3 disků spojených do pole RAID 5 a zároveň umožňuje rychlejší čtení dat, využívajíc metodu prokládání metody RAID 0. Navíc má jenom třetinovou redundanci. Nevýhodou pak může být nutnost použití minimálně 6 disků, což znamená, že toto řešení není vhodné pro malé množství dat.

RAID 60

Jedná se o pole zapojené podobným způsobem jako RAID 50, s tím rozdílem, že místo RAID 5 je využit RAID 6. To z tohoto zapojení činí jedno z nejbezpečnějších

zapojení, neboť je odolné vůči výpadku až dvou disků z každého pole RAID 6. Navíc využívá výhody rychlého čtení RAID 0 s použitým prokládáním. Nevýhodou je pak nutnost využití minimálně 8 disků, nejlépe však alespoň 10 pro rozvinutí plného potenciálu této metody.

Zálohování na pevné disky z pohledu GDPR

Pro zálohování dat obsahujících osobní údaje jsou pevné disky vhodné. Je však třeba dbát na dodržení souladu s nařízením. V první řadě je třeba nastavit přiměřenou úroveň zabezpečení tak, aby k datům neměly přístup neoprávněné osoby. To je možné například vhodným uložením disků v bance, trezoru a podobně.

Pro praktické užití je však tento způsob limitující, proto je možné disky používat i v datovém centru. Tam je však nutné, aby přístup k nim byl monitorován a omezen pouze na povolané pracovníky. V případě připojení takového centra do sítě, ať už interní či veřejné, je nezbytné, aby byla nastavena vhodná úroveň zabezpečení odpovídající obecné úrovni zabezpečení takových dat. Vhodné je též použít pseudonymizaci, šifrování či kombinaci obojího, což v případě úniku dat znemožní identifikaci konkrétních osob a nedojde tak k ohrožení fyzických osob. Síla šifrování by měla odpovídat technickým možnostem zpracovatele a citlivosti dat. Šifrovací klíče je pak nezbytné mít uložené na bezpečném místě a monitorovat jejich užívání.

V případě využití subjektu práva být zapomenut je nezbytné, aby firemní procesy umožnily toto právo bezezbytku splnit i v zálohách. Jednou z možností, kterou pevné disky umožňují, je smazání či anonymizace subjektu přímo v zálohovaných údajích. To však může být při rozsáhlejších úložištích problematické, proto je vhodné nastavit firemní procesy tak, aby se data o takovémto subjektu nemohla nikdy dostat zpět do aktuální verze. Opět zde platí přístup založený na riziku a taktéž postup nesmí způsobit správci ani zpracovateli dat nepřiměřené úsilí.

2.2.3 Optické disky

Tato kategorie zahrnuje široké spektrum médií, které slouží pro uchovávání dat. Pro zjednodušení budou v této kapitole uvažovány pouze disky typu kompaktní disk (CD), digital versatile disc (DVD) a blu-ray disk (BD). Tyto disky patří k nejrozšířenějším a je tedy nejpravděpodobnější, že budou využity k zálohování dat.

Na ostatní varianty disků se vztahují podobné závěry jako na tři vybrané, s přihlédnutím k jejich konkrétním specifikům a ke složitosti jejich čtecích a zápisových zařízení.

Obecně se jedná o kruhové disky, jejichž povrch umožňuje záznam a čtení pomocí laserové diody. Velikost jednotlivých médií se pohybuje od 0,7 GB pro jednovrstvá CD až po 128 GB u blu-ray disků. Stejně tak se v závislosti na médiu liší průměrná životnost média. Společnost Verbatim, jeden z největších výrobců optických disků na světě na svých stránkách[17] uvádí, že jejich CD a DVD při správném skladování při teplotě 20 až 25°C a relativní vlhkosti vzduchu 55 % vydrží až 100 let, a speciální MDISC blu-ray disky až 1 000 let. Tuto dobu ovšem velmi zkracují čtení či přepisy médií, stejně jako nečistoty a mechanická poškození, která u disků těchto typů mohou vzniknout velmi jednoduše. Dále hraje roli kvalita zapisovacího zařízení, pomocí kterého byl záznam na optickém disku vytvořen.

Z těchto důvodů je třeba přijmout zvláštní opatření pro zálohy na optických nosičích. Nejvhodnější je mít stejná data zálohovaná na více než jednom disku a tyto disky mít uloženy odděleně, pro případ události, která by ovlivnila všechny disky v jednom místě, například požár či povodeň. Dále je třeba disky pravidelně kontrolovat, zda nedošlo k poškození disku. V takovém případě je třeba vytvořit novou kopii z některé jiné zálohy. Výhodou je nízká pořizovací cena jak samotných nosičů, tak čtecích a zápisových zařízení.

Pro potřeby zálohování osobních údajů na optické nosiče platí podobná pravidla jako pro zálohování na magnetické pásky. Místo, kde jsou záznamy uloženy, by mělo být střeženo a přístup k němu monitorován. Pro případ odcizení disků by měla být data na discích šifrována s použitím standartu na odpovídající technologické úrovni s přihlédnutím k citlivosti uložených dat. Šifrovací klíče je třeba mít uložené na vhodném místě, kde k nim budou mít přístup pouze povolané osoby, a bude monitorován.

Dalším vhodným opatřením je pseudonymizace a následné rozdělení dat takovým způsobem, který sníží objem dat, na které se vztahuje nařízení, neboť data, která neumožní identifikaci fyzických osob, se nepovažují za osobní. Poté je třeba střežit pouze data, která obsahují klíče, které umožní spojit data tak, aby k identifikaci mohlo dojít.

Pro plnění práva být zapomenut je třeba stanovit vhodné procesy, které zabezpečí, že se osobní data nedostanou do aktuální verze systému a též nebude umožněno je kýmkoliv přečíst. Nastavení těchto procesů se blíže věnuje kapitola zabývající se konkrétními metodami řešení.

2.2.4 Přenosné flash paměti

Do kategorie přenosných flash pamětí spadají všechna zařízení, která obsahují paměť typu flash, která umožňuje uchovávat data a přenášet je mezi počítači. Mezi typické zástupce patří USB flash paměti a paměťové karty. Princip ukládání dat je v obou případech stejný, liší se pouze rozhraní, které je využito pro připojení k počítači. V případě USB flash disků je využito rozhraní USB, kterým jsou v dnešní době vybaveny prakticky všechny osobní počítače. Paměťové karty se pak umisťují do slotů přímo na zařízeních či do speciálních čtecích koncovek, které se připojují k počítačům.

Mezi hlavní výhody těchto pamětí patří dobrá přenositelnost[18], malá hmotnost a velikost, nízká cena, univerzálnost a snadnost použití. Mezi nevýhody pak patří nižší životnost, která se snižuje s počtem přepisů datového média. Společnost Verbatim uvádí, že doba uchování dat na jejich USB flash disku je 7 let. Stejně jako u dalších typů paměťových médií tak platí, že je zálohy třeba pravidelně kontrolovat a nespoléhat se pouze na jednu kopii, neboť k selhání může dojít kdykoliv.

I pro tyto druhy pamětí platí stejná pravidla jako pro ostatní zálohovací média. Je důležité si uvědomit, že ve chvíli, kdy se na flash disku objeví osobní údaje, je třeba při jeho nakládání přijmout standartní opatření, která vyplývají z nařízení. Manipulace s ním musí být zaznamenávána a je třeba zamezit, aby se dostal do držení nepovolaných osob. To může být v případě flash disků zaručeno uložením na bezpečném místě.

Pokud je to z povahy využití paměti nerealizovatelné – data se například přenáší mezi pobočkami či mimo firmu – je nezbytné, aby pracovník, který s daty manipuluje, neustále dohlížel na to, aby se k datům nemohly dostat nepovolané osoby. V případě méně citlivých osobních dat postačí, když bude mít disk neustále u sebe, případně jej bude odkládat pouze do zabezpečených prostor, u kterých bude mít záruku, že do nich nikdo nemůže vstoupit bez jeho vědomí.

V případě, že toho není možné dosáhnout nebo se jedná o citlivá osobní data, je nezbytné, aby byla šifrována na úrovni, která odpovídá technologickým standardům. Šifrovací klíče by pak měly podléhat stejné úrovni zabezpečení, jako by se jednalo o osobní data, neboť splňuj definici dat, která v kombinaci s jinými mohou vést k identifikaci fyzické osoby.

Dalším aspektem, který je třeba zvážit při používání flash pamětí pro zálohu dat, je možnost smazání dat. Běžným smazáním nejsou data odstraněna, je pouze odebrán záznam z tabulky, který odkazuje na jednotlivé soubory. I průměrně znalý uživatel je potom schopný data získat, pokud nedojde k jejich přepsání. Proto je při mazání dat nezbytné použít nástroj, který efektivně znemožní jejich následné znovuzískání. Tyto nástroje umožňují různou úroveň bezpečnosti smazání, kdy při již základní úrovni je pro běžného uživatele prakticky nemožné data přečíst. V závislosti na citlivosti dat je pak vhodné zvolit odpovídající úroveň bezpečnosti smazání dat.

V případě využití práva subjektu být zapomenut je nezbytné jeho údaje odstranit či anonymizovat. V souvislosti s tímto bodem je důležité dbát zejména na to, aby tak bylo učiněno ze všech uložišť, kde se data nacházejí. Platí to tak pro všechny disky, na kterých jsou tato data uložena, včetně těch, které se momentálně nachází v držení zaměstnanců a podobně. Pro splnění tohoto bodu je vhodné mít nastavené interní předpisy tak, aby to bylo zaručeno s jasnou definicí osob, které jsou zodpovědné za toto smazání a v jakém rozsahu.

2.2.5 Cloudové úložiště

Jedná se o stále častěji užívané řešení. V tomto případě se data ukládají vzdáleně přes síť na úložiště provozované třetí stranou. Provozovatel cloudového úložiště pak využívá některé z předcházejících řešení, ale správce osobních údajů neřeší konkrétní způsoby ukládání, pouze využívá služby, které jsou dodávány provozovatelem, a přes dohodnutá rozhraní k datům přistupuje, modifikuje je a podobně.

Většina cloudových úložišť je v dnešní době přístupná z webového prohlížeče, a proto jejich užívání nepředstavuje pro společnosti větší technologickou zátěž, než je běžný provoz. Některá úložiště však umožňují přístup i přes aplikační rozhraní, což výrazně usnadňuje jejich propojení s existujícím informačním systémem a s dalšími nástroji pro správu záloh a údajů.

Jako příklad provozovatelů a služeb pro vzdálené zálohování pak můžeme uvést například následující:

- Disk Google od společnosti Google
- Microsoft OneDrive a Microsoft Azure od společnosti Microsoft
- AWS od společnosti Amazon
- Acronis Backup od společnosti Acronis
- Dropbox od společnosti Dropbox, Inc.
- Comodo BackUp od společnosti Comodo
- Mozy od společnosti Carbonite

Samozřejmě existuje velké množství dalších služeb, které lze využít pro stejné účely. Pro všechny však budou platit stejná pravidla. První tři služby slouží i pro synchronizaci dat pro kooperaci více členů týmu a obsahují množství dalších nástrojů. Naopak další dvě služby se zabývají primárně zálohováním a obsahují tak nástroje, které se dají dobře integrovat do firemních procesů. Jedná se například o možnost spouštět zálohování automaticky v předem vybrané časy, či možnost krom vzdáleného úložiště ukládat ještě na další lokální místa, čímž se výrazně zvyšuje bezpečnost a spolehlivost celého řešení.

Všechny služby jsou v základní variantě zdarma pro určitý objem dat a další úložnou kapacitu je možné pořídit za poplatek. Vhodnost služby pro konkrétní řešení pak záleží primárně na požadavcích konkrétního podniku na velikost úložiště, dostupnost a související služby.

Z pohledu GDPR se jedná o stav, kdy se provozovatel vzdáleného úložiště stává zpracovatelem osobních dat. Jako takový musí s daty manipulovat pouze v rámci pokynů, které mu zadá správce osobních údajů. Navíc se stává spoluzodpovědným za dodržování nařízení a bezpečnost osobních údajů, což je novinka v porovnání s dosavadní praxí, kde za bezpečnost dat v celé šíři ručil pouze jejich správce.

V praxi je vhodné uzavřít smlouvu, která definuje, do jaké míry je která ze stran zodpovědná za konkrétní události. Provozovatel úložiště je bezpochyby zodpovědný za bezpečnost dat na svojí straně. Musí zaručit, že se k nim nedostane nikdo jiný, než správce (případně jeho zaměstnanci a další pověřené osoby) z účtů, které budou pro tento účel vytvořeny. Je na zvážení zpracovatele po případné konzultaci se správcem

určit úroveň zabezpečení, která bude dostatečná s přihlédnutím k citlivosti osobních údajů uložených na jeho zálohovacím řešení a současným technologickým možnostem.

Pokud to není nevyhnutelné, potom by ani zpracovatel a jeho zaměstnanci neměli být schopní data číst. Správce je pak povinen vybrat zpracovatele tak, aby vybral vhodného dodavatele cloudového úložiště, který splňuje nutná kritéria pro konkrétní případ. Jednou z doporučených podmínek je vybrat takovou službu, která se nachází na území EU a tím spadá do jurisdikce evropského práva. Z dříve uvedených služeb společnosti Microsoft[19] a Google[20] vydaly prohlášení o shodě s nařízením GDPR.

Mezi další povinnosti správce potom bezpochyby patří bezpečnost dat z jeho strany, což obsahuje především vhodné nastavení firemní politiky pro účty a nastavení přístupových práv pro ně tak, aby se k osobním datům dostaly pouze osoby povolané. Je vhodné zvážit politiku správy hesel, jejich složitost a frekvenci změn. Dále je na zvážení, zda umožnit zaměstnancům a dalším osobám možnost přihlašovat se mimo firemní síť. Zaměstnanec nesmí umožnit, aby se k osobním datům mohly dostat třetí osoby. Stejně tak je správce zodpovědný za takové nastavení firemních procesů, které umožní bezezbytku provést vymazání osobních údajů či jejich anonymizaci v případě, že subjekt využije svého práva být zapomenut.

I pro tato řešení platí, že veškerá manipulace a čtení osobních údajů musí být zaznamenána. Některá výše jmenovaná řešení obsahují i nástroje, které toto řeší automaticky a je tak možné pro oprávněné osoby nahlédnout do záznamů, kdy a kdo měl k údajům přístup nebo je modifikoval a jakým způsobem, zatímco v případě jiných je nezbytné, aby toto zajistil správce v rámci nastavení svých interních firemních procesů.

2.3 Obecné postupy při zálohování

Pro potřeby zálohování se užívá množství technik, které nezávisí na způsobu záloh ani na jejich médiu a umožňují zrychlení zálohovacího procesu, obnovení záloh z úložiště či zvyšují bezpečnost. Některé z nich jsou pouze volitelné, jiné lze považovat za základní prvky bezpečných záloh.

2.3.1 Komprese dat

Komprese dat je proces, který sníží velikost dat tak, aby zabrala menší prostor v cílovém úložišti. To je vhodné zvláště v případech, kdy je velikost cílového média limitována či pro snížení nákladů spojených s velikostí dat.

Hlavními nevýhodou je to, že data je třeba nejprve dekomprimovat před jejich čtením a případným použitím v systému, což může výrazně zkomplikovat například vyhodnocení těchto dat při využití práva subjektu na to být zapomenut. Při kompresi dat je proto dobré zvolit vhodný způsob pseudonymizace, který zajistí, že bude třeba dekomprimovat a zkontrolovat pouze část obsahující údaje o subjektu a jeho klíčích, a nikoliv celou databázi. Pro zálohování osobních dat je nezbytné užít bezztrátovou kompresi, neboť dle GDPR správce osobních údajů zodpovídá i za úplnost a uchování osobních dat a musí tedy zaručit vhodnými technologickými prvky, že nedojde k jejich ztrátě. Užití ztrátové komprese, tj. takové, při níž je část původní informace ztracena, je přípustné, pokud se jedná například o obrazová data. Pak ale ztrátová komprese smí snížit kvalitu obrazu pouze natolik, aby byl stále použitelný k původním účelům.

Některé z níže uvedených nástrojů obsahují možnost komprese dat. V ostatních případech je na zvážení, zda je vhodné data zkomprimovat. Zde jsou uvedeny pro příklad dva nástroje[21, s. 53], které to umožňují, včetně stručného přehledu jejich vlastností.

7-Zip

Jedná se o program šířený pod open source licencí, což jej umožňuje používat bezplatně. Navíc podporuje širokou škálu kompresních formátů a lze jej užívat na široké škále platforem.

WinRAR

Jeden z klasických kompresních programů, umožňující kompresi a dekompresi velkého množství různých formátů. Jedná se o placený program.

2.3.2 Šifrování

Při procesu šifrování jsou data transformována do podoby, která je nečitelná a nevyužitelná pro původní účel dat. Převod zpět je možný pouze se znalostí užitého

kryptografického algoritmu a klíče, který byl užit k jejich šifrování. Šifrování slouží k tomu, aby se k původním datům nedostaly nepovolané osoby v případě, že není možné zajistit jejich bezpečnost jinak, například při posílání přes veřejnou síť či uložení na veřejně přístupném místě. Šifrování je pro určité postupy při zálohování dat naprosto nezbytné.

Jeho hlavní nevýhoda je podobná jako v případě komprese, šifrování a dešifrování totiž zvyšuje přístupovou dobu k datům. Proto je vhodné v případě šifrovaných záloh užít pseudonymizaci a mít vytvořenou vhodnou strukturu metadat, která umožní snadno určit, kde se která data nachází i bez jejich dešifrování.

Při šifrování je dobré pamatovat, že šifrovat je nutné pouze data, která jsou důvěrná, nebo je z jiného důvodu nezbytné zamezit třetím osobám v přístupu k nim. Například data označená pouze klíčem, bez kterého nelze identifikovat fyzikou osobu bez dalších dat, která již zašifrovaná jsou, je zbytečné šifrovat. Šifrování je pak vhodné i pro případ, kdy administrátor nemá mít přístup k datům uživatelů systému.

Do firemních procesů spravujících šifrování spadá i politika hesel. Heslo je obvykle krátký řetězec, jehož znalostí se ověřuje totožnost uživatele. Vhodně zvolené heslo je jedním ze základních bezpečnostních prvků a proto by správě hesel měla být věnována zvláštní pozornost.

Heslo by mělo být přiměřeně dlouhé, aby jej nebylo možné prolomit pomocí útoku hrubou silou, kdy útočníci vyzkouší v krátké době velké množství kombinací alfanumerických znaků a zároveň by nemělo být možné jej jednoduše uhádnout. Hesla by neměla být nikde zapsána, uživatel by si je měl pamatovat. Stejně tak by neměl používat jedno heslo k více účtům, a to pro případ úniku hesel, ke kterému může dojít v případě, že služba zanedbává základní bezpečnostní prvky.

I v případě vhodně zvoleného hesla je nezbytné jej v pravidelných intervalech měnit, pro případ, že jej někdo například zahlédne při psaní na klávesnici a podobně. V takovém případě je i silné heslo prolomeno snadno. Frekvence změny hesla záleží na důležitosti a citlivosti systému, ke kterému je pomocí něj přistupováno.

Vzhledem k tomu, že na kvalitu hesla jsou kladeny značné nároky a zároveň by heslo mělo být pouze v paměti uživatele, který si jich většinou musí pamatovat značné množství, existují nástroje, které správu hesel výrazně usnadňují.

Při volbě nástroje je důležité zvolit takový, který implementuje nejmodernější bezpečnostní standardy, protože v případě prolomení zabezpečení budou kompromitována všechna hesla zde uložená. Zároveň z přístupu založeném na riziku plyne, že hesla k nejcitlivějším osobním údajům není vhodné ukládat ani do těchto vysoce zabezpečených databází.

Tyto nástroje umožňují uložit hesla a přihlašovací jména do libovolných služeb. Dále často umožňují propojení s dalšími aplikacemi, například webovým prohlížečem a díky tomu tak mohou hesla přímo vyplňovat. Většinou umožňují i vygenerovat nové heslo požadované délky a vlastností, které zároveň okamžitě uloží, aby nemohlo dojít k jeho ztrátě.

V případě užití těchto nástrojů na úrovni celé společnosti jejich největší výhoda spočívá v možnosti nastavení obecné politiky hesel. V rámci této politiky lze nastavit pro uživatele a systémy jak silná je třeba užívat hesla, kolik mají mít znaků a jakého typu a jak často se musí měnit.

2.3.3 Správa záloh

Pro manipulaci a správu záloh platí určitá pravidla, která vznikla na základě dlouholetých zkušeností firem i jednotlivců, kteří se šifrováním zabývají. Pro správnou funkčnost zálohovacího procesu je vhodné na ně pamatovat a používat je. Jejich implementace výrazně zvyšuje bezpečnost systému a snižuje riziko ztráty dat.

Geografické oddělení záloh

Jedním z velmi důležitých prvků je fyzické rozmístění zálohových médií. Zálohy na jednom místě jsou vystaveny nebezpečím nečekaných událostí, jako je například požár či záplavy. V takovém případě totiž i přes vhodně zvolená média a zálohovací média může dojít ke ztrátě všech médií najednou a tím i důležitých dat.

Proto je vhodné mít zálohy minimálně na dvou, ideálně však na ještě více místech, která jsou od sebe přiměřeně vzdálená. V případě subjektů vyskytujících se ve více zemích je vhodné, pro případ politických problémů, mít alespoň jednu z těchto záloh umístěnou v jiné zemi než ostatní. Samozřejmě i zde platí zásada přiměřenosti nákladů v závislosti na citlivosti dat a zejména přiměřenému riziku.

Průběžná kontrola

Dalším nezbytným prvkem zálohování je průběžná kontrola dat. Ať už kvůli vadám při výrobě, nebo vlivem běžného opotřebení materiálu, je nezbytná pro bezpečnost záloh jejich pravidelná kontrola. V závislosti na typu média a jeho uložení je třeba vhodně zvolit frekvenci kontrol a ty pak pravidelně provádět. V případě, že je zjištěn jakýkoliv problém s daty uloženými na záloze, je nezbytné, aby byla data nahrána znovu z jiné zálohy, případně bylo médium nahrazeno za jiné, v závislosti na jeho typu, stáří, kvalitě, historii chyb a dalších parametrech.

V případě vynechání kontrol se majitel záloh vystavuje riziku, kdy v případě ztráty jedné zálohy zjistí, že druhá podlehla běžnému opotřebení způsobenému časem a o data tak nenávratně přišel, případně je nucen pokusit se data získat z poškozených nosičů pomocí specializované firmy. Obojí mu může přinést nemalé finanční náklady, kterým se mohl jednoduše vyhnout.

Katalogizace záloh

Naprosto nezbytné je udržet v zálohovaných datech pořádek. Proto je vždy nutné média obsahující zálohy popsat, aby bylo jasné, co se na nich nachází, a také uvádět datum či časové období, kdy byly zálohy pořízeny. Toto se samozřejmě týká primárně záloh na fyzických nosičích uložených v trezorech a podobně. Například optické disky a flash paměti je dobré popsat viditelně, například štítkem přilepeným na médiu či jeho obale. Dále je nezbytné udržovat organizační systém v souborech a složkách, které jsou uloženy na médiích, což se týká zejména větších logických celků, například diskových polí, ale samozřejmě nevyjímaje ani zálohy na optických discích a podobně. Zamezí se tím tak nežádoucí duplikaci stejných dat na jednom nosiči, stejně jako opačné situaci, kdy data, která by měla být zálohována, budou buď částečně nebo úplně chybět. Dalším důvodem pro tento postup je jednoduché vyhledávání dat v případě jejich potřeby, nebo naopak v případě, kdy je rozhodnuto, že určitá část již není třeba zálohovat a média je možné vymazat a použít pro jiné účely či zcela zničit.

Dalším důležitým prvkem jsou metadata. Jedná se o informace o datech zapsaných na médiích. Určují, které položky obsahují jaká data, v jakém formátu, kdy byla zapsána, kdy byla naposledy čtena, do jaké patří verze a podobně. Dobrý stav

těchto metadat výrazně zjednodušuje správu dat, neboť je na první pohled jasně viditelné, která data jsou osobní a která nikoliv.

3 NÁVRH ŘEŠENÍ

Na základě předchozích kapitol je jasné, že všechny společnosti, které se jakkoliv podílí na zpracování osobních údajů, musí při své další činnosti brát v úvahu nové nařízení. To s sebou ponese odpovídající změny ve struktuře firemních procesů, datových toků, informačních systémů, vzdělávání a odbornosti zaměstnanců. V některých případech může vést ke vzniku nových oddělení a dalším strukturálním změnám. Pro úspěšné řízení změn je třeba položit si množství otázek o společnosti i jejím okolí. Teprve po jejich zodpovězení je možné úspěšně zahájit změnové řízení, které povede k co nejhladšímu průběhu vytvoření, nasazení, otestování a používání nových pravidel a metod. Tato kapitola představuje vodítko pro provádění těchto změn od počáteční analýzy přes tvorbu samotné změny až po závěr věnovaný řízení rizik, která neodmyslitelně plynou z této změny.

3.1 Analýza vnějších faktorů pomocí metody PEST

Jako první je třeba si zodpovědět: jaké jsou faktory, které působí na firmu a mohou ji ovlivnit? Pro obdobné analýzy byla vypracována řada metodik, které lze využít k různým účelům. V této práci bude použita metoda PEST.

Pod zkratkou PEST se rozumí analýza vnějších faktorů, které působí na firmu. Konkrétně se jedná o následující:

- Politicko-právní (Political)
- Ekonomické (Economic)
- Společenské (Social)
- Technologické (Technological)

Na podnik totiž působí velké množství vnějších vlivů, které nelze měnit a je třeba je akceptovat a zohlednit při tvorbě všech rozhodnutí. Proto je pro management firmy nevyhnutelné tyto vlivy znát, aby bylo možné dosáhnout souladu mezi strategií společnosti a okolím. Tyto faktory je nezbytné neustále sledovat a korigovat podle nich strategická rozhodnutí. To umožňuje se snáze zaměřit na hlavní činnost podnikání a tím získat konkurenční výhodu.

Při rozboru každého faktoru je třeba položit si následující otázky:

- Které z faktorů mají vliv na firmu?
- Co mohou tyto vlivy způsobit?
- Které z nich jsou nejdůležitější v krátkém časovém horizontu?

3.1.1 Politicko-právní faktory

Všechny společnosti podnikající na území České republiky podléhají zákonům, vyhláškám a dalším nařízením vlády, které je nezbytné akceptovat a řídit se podle nich. Ty mohou různou měrou ovlivňovat podnikatele a společnosti.

Daňové zatížení

Jedná se o jednu z největších oblastí, které mají dopad na podnik. Základní sazba DPH je v České republice 21 %[22] a první snížená sazba 15 %, resp. druhá snížená sazba 10 %. Základní sazba je stejná již od roku 2013. Dále je třeba zohlednit daň z příjmů fyzických osob (15%) a právnických osob (19%)[23]. Celkové zatížení v ČR je dle OECD 34,9%[24], což nás řadí k průměrným zemím (průměr pro OECD je 34,2%). Důležitá je též časová náročnost spojená se správou daní. Dle stejné studie se ČR nachází na 171. pozici ze 183. zemí OECD v době potřebné pro správu daní. Střednímu podniku podle této analýzy zabere správa daní v průměru 178 hodin ročně.

Vstup na zahraniční trhy

Vstup na zahraniční trhy je značně usnadněn Evropským jednotným trhem, který je umožněný celní unií a zónou volného obchodu pro členské státy Evropské unie. GDPR navíc zavádí jednotný zákon pro správu osobních údajů pro všechny členské státy a používání jednotných termínů. To případně umožňuje jednoduchý vstup na evropské trhy, neboť systém splňující tato nařízení v rámci České republiky bude, s přihlédnutím k místním úpravám, stejná nařízení splňovat i v libovolném dalším státě Evropské unie. Navíc úmluvu, ze které nařízení vychází, budou postupně ratifikovat i další státy mimo EU, což umožní ještě větší možnosti expandování do zahraničí.

Legislativa

V ČR upravuje podnikání celá řada zákonů a další zákony věnující se ochraně osobních údajů. Uveďme si zde ty nejdůležitější:

- *Zákon č. 90/2012 Sb. Zákon o obchodních společnostech a družstvech* (zákon o obchodních korporacích), též nesprávně označován jako Obchodní zákoník. Upravuje postavení firem a nastavuje obchodní závazkové vztahy, jejich podobu, formu, smluvní typy pro oblast obchodu a podnikání a další zvláštní ustanovení pro mezinárodní obchod.
- *Zákon č. 563/1991 Sb. ve znění pozdějších předpisů*. Tento zákon definuje povinnosti, rozsah a postupy při vedení účetnictví pro zachování průkaznosti.
- České účetní standardy a prováděcí vyhlášky k zákonu o účetnictví. Jedná se zejména o zákon *č. 563/1991 Sb.* a *500/2002 Sb.* Jedná se o pravidla, kterými se společnost řídí při vedení finančního účetnictví pro udržení souladu v užívání účetních metod.
- Zákon *č. 262/2006 Sb. Zákoník práce*. Upravuje převážnou část českého individuálního pracovního práva.
- Zákon *č. 101/2000 Sb. ve znění pozdějších předpisů*. Zákon, který upravuje ochranu osobních údajů a definuje činnost Úřadu pro ochranu osobních údajů. Jeho základním smyslem je dohled nad zachováváním práva na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů.
- *Nařízení Evropského parlamentu a Rady (EU) č. 2016/679* ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Jedná se o nařízení, které stanovuje pravidla ochrany fyzických osob ve věci jejich práva na soukromí a upravuje pravidla zpracovávání jejich osobních údajů. Toto nařízení je platné pro celou Evropskou unii. Zároveň stanovuje pravidla pro volný pohyb osobních údajů v rámci EU.

Dalším politicko-legislativním faktorem je stálost nařízení a zákonů. Podle průzkumu Hospodářské komory České republiky[25] 80 % dotazovaných firem uvádí, že za rok 2016 se zvýšila regulatorní zátěž podnikatelů. Dále Hospodářská komora uvádí, že podnikání neprospívají ani časté změny zákonů. Do roku 2016 se zákon o správních poplatcích změnil více než 180krát. Dále například zákon o DPH se změnil za stejné období 70krát a zákon o daních z příjmů 140krát. Ne všechny změny se týkají všech

subjektů, ale neustálá potřeba kontrolovat legislativní novinky a reakce na ně nevytváří příliš dobré prostředí pro úspěšné podnikání.

3.1.2 Ekonomické faktory

Při analýze rizik je třeba přihlédnout k momentální finanční situaci státu i lokality, ve které se podnik nachází, a z ní vycházet při tvorbě plánů a odhadů do budoucna, protože tyto faktory mohou silně ovlivnit budoucí možnosti růstu.

Hrubý domácí produkt

Celkovou úroveň ekonomiky a příhodnost podmínek pro podnikání ukazuje tzv. hrubý domácí produkt (HDP), což je celková peněžní hodnota statků a služeb vytvořená na území státu. V Česku tato hodnota stoupala poměrně stabilně až do roku 2008, kdy přišla hospodářská krize. V tomto roce zatím ČR mělo nejvyšší hodnotu HDP (235 mld. Kč) v historii. Následoval postupný propad až na hodnotu 187 mld. Kč, což byl stav srovnatelný s rokem 2007. V současnosti je hodnota HDP opět na vzestupu, konkrétně se nyní nachází na hodnotě kolem 218 mld. Kč. Další vývoj je těžko předvídatelný. Jednu z variant nastiňuje například jedna z nejstarších společností na světě, která se zabývá finančními službami: J.P. Morgan Chase & Co. Podle analýz této firmy je třeba očekávat další finanční krizi kolem roku 2020[26]. Podle všeho by však neměla být tak silná, jako ta z roku 2008.

Nezaměstnanost

Nezaměstnanost je jedním z důležitých faktorů, který ovlivňuje příležitost firem při poptávání po pracovní síle. Vyšší nezaměstnanost působí na podniky pozitivně, protože uchazeči o práci nemají takové platové požadavky. V ČR byla obecná míra nezaměstnanosti dle Českého statistického úřadu ve 4. čtvrtletí roku 2018 2 % [27], což je historicky nejméně od vzniku samostatného českého státu.

Inflace

Inflací se rozumí nárůst všeobecné cenové hladiny zboží a služeb v ekonomice v určitém časovém období, způsobené snížením kupní síly peněz. Dopady inflace jsou různé; snižuje hodnotu peněžních prostředků na účtech a v pokladnách. To odrazuje od spoření formou ukládání peněz na účty, na druhou stranu však stimuluje investice do nefinančních produktů. V případě vysoké inflace se mluví o hyperinflaci, se kterou

v podmínkách střední Evropy není třeba počítat. Opakem inflace je deflace, což je zvyšování hodnoty měny. V současnosti je většinou ekonomů prosazován trend stabilní mírné inflace, která příznivě stimuluje ekonomiku, ale nezpůsobuje totální znehodnocování peněz[28, s. 3].

V roce 2018 byla průměrná míra inflace 2,1 %[29]. Průměrná inflace od roku 2003 do roku 2018 byla 1,79 %, takže rok 2018 byl nadprůměrný, ale pouze lehce. Např. v krizovém roce 2008 byla inflace 6,3 %, zatímco např. v roce 2003 byla inflace pouze 0,1 %.

Současná míra inflace způsobuje mírný, ale vytrvalý růst cen. Příznivě podporuje investice, což je velice výhodné, protože jednou z dobrých investicí podniků může být i investice do nového informačního systému. Nejvíce jí bývají ovlivněny firmy, které produkují potraviny a energie.

Úrokové sazby

S inflací úzce souvisí i vývoj úrokových sazeb. Jejich vývoj je primárně ovlivněn snahou České národní banky, která reguluje úrokovou míru poskytovanou komerčním bankám. Ty toto zvýšení promítají do zvýšení úroků z úvěrů. Vysoká inflace by neměla na společnost pozitivní vliv, protože pro její snížení by národní banka zvýšila úrokovou míru a tím by zhoršila příležitosti pro čerpání úvěrů u soukromých bank pro další společnosti, čímž by se zpomalilo tempo ekonomiky a mohl by dojít k poklesu zájmu o nová řešení informačních technologií.

Vývoj mezd

Mezi další podstatné faktory patří též vývoj mezd. Ten určuje, kolik je třeba platit zaměstnancům, aby odváděli odpovídající a kvalitní práci.

Tabulka č. 1: Medián mzdy

	Medián mzdy v roce 2018
Medián mzdy v ČR	27 719Kč
Medián mzdy vývojářů	35 200Kč

Z tabulky je vidět, že programátorská práce je placena výrazně lépe než je průměr, a je třeba to zohlednit při projektech v rámci vývoje softwaru. Pokud je to možné, je dobré nezatěžovat programátory více, než je nezbytně nutné a veškerou ostatní práci nejlépe delegovat na pozice obsazené lidmi, jejichž primární pracovní náplní není vyvíjet software. Z toho plyne i fakt, že nová řešení v oblasti informačních technologií jsou poměrně drahá.

3.1.3 Společenské faktory

Společenskými faktory se míní vlivy, které jsou způsobeny složením a vlastnostmi obyvatel v dané zemi či regionu. Například je tedy třeba zohlednit počet obyvatel, hustotu osídlení, životní úroveň, úroveň a kvalitu vzdělání, spotřební zvyky, jazykovou vybavenost atp. V rámci zavádění nového nařízení o ochraně osobních údajů není pravděpodobné, že by společnosti byly příliš ovlivněny těmito faktory, ale i přesto alespoň některé z nich mohou hrát roli při plánování budoucího rozvoje, a proto si je uvedeme.

Demografické faktory

V rámci demografických faktorů můžeme uvést, že Česká republika má 10,58 milionů obyvatel[30]. S hustotou zalidnění 134 obyvatel na km^2 se řadí k nadprůměrně zalidněným státům. Úředním jazykem je čeština, u které se odhaduje počet mluvčích na 13,2 milionu[31].

Životní úroveň

Životní úroveň je důležitým faktorem, protože s vyšší životní úrovní se zvedá i poptávka po informačních technologiích. Podle průzkumu společnosti SEDA[32] se Česká republika umístila v žebříčku životní úrovně na 24. pozici ze 152 států a dá se tedy hodnotit jako země s vysokou životní úrovní. V žebříčku byl zahrnut ekonomický růst, jeho stabilita, situace na trhu práce, zdravotnictví, veřejná správa a další, včetně občanské spokojenosti.

Vzdělání obyvatelstva

Pravděpodobně nejdůležitějším společenským kritériem je kvalita a úroveň vzdělání. Vývoj softwaru je totiž činnost vyžadující kvalifikovanou pracovní sílu a při nabírání nových zaměstnanců je třeba k tomu přihlížet.

Podle studie OECD[33] má v ČR vysokoškolské vzdělání 30 % lidí ve věku 25-34 let, ale pouze 15 % ve věku 55-64 let. To ukazuje na trend, kdy se počet vysokoškolsky vzdělaných lidí v posledních letech výrazně zvedá. Výzkum dále předpokládá, že ČR dorovná průměr OECD a ve věku 25-34 let bude mít vysokoškolské vzdělání okolo 46 % obyvatel.

Co se kvality vzdělání týče, lze konstatovat, že v technických oborech má Česká republika dlouhou pověst kvalitních vysokých škol, včetně Vysokého učení technického v Brně, Českého vysokého učení technického v Praze, Masarykovy univerzity a Karlovy univerzity, jejichž technologické fakulty se pravidelně umisťují vysoko v žebříčcích nejlepších vysokých škol v Evropě[34].

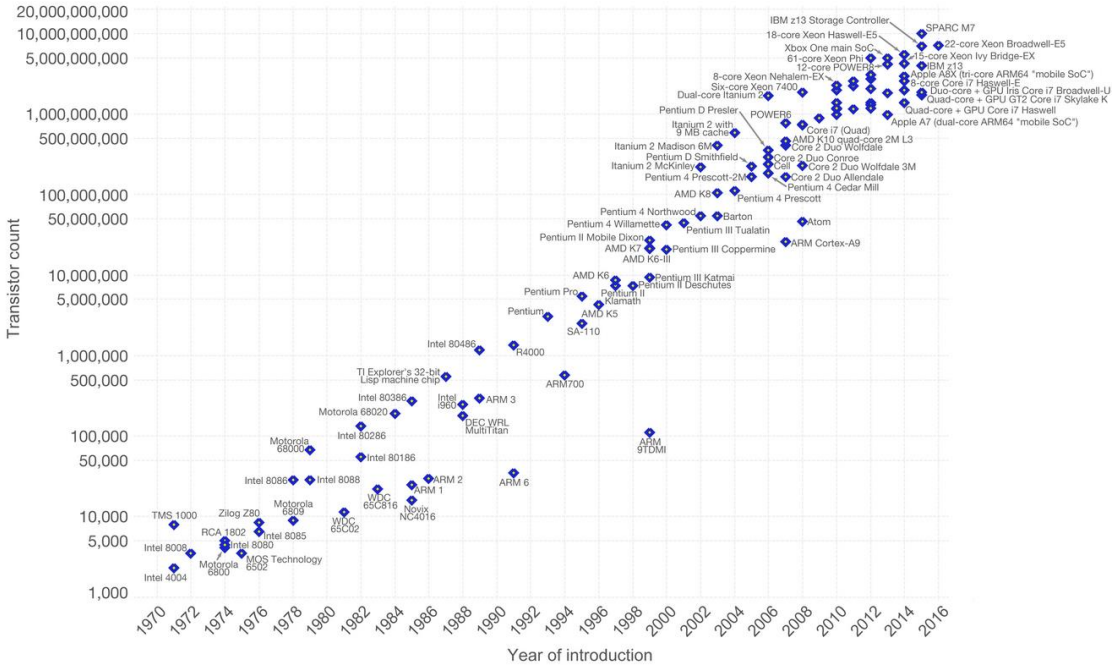
Z toho plyne, že v ČR je velké množství vysoce kvalifikovaných lidí, kteří mohou pracovat na vývoji webových informačních systémů, či na pozicích procesních inženýrů, správců internetových sítích a dalších pozicích, které budou ovlivněny nařízením či jejichž vznik si nařízení přímo vyžádá.

3.1.4 Technologické faktory

Informační technologie v poslední době tvoří to nejmodernější, co může současná technika nabídnout. Jedná se o velice rychle se vyvíjející segment, kde se novinky objevují prakticky denně a udržet krok v takto dynamickém prostředí není jednoduché. Veškeré faktory, které ovlivňují technologické zázemí takové společnosti jsou tedy klíčové pro nastavení směřování společnosti. Pojďme se zaměřit na nejdůležitější z nich.

Vývoj výkonu počítačů

Při zmínce o zrychlování počítačů nelze nevzpomenout na Moorův zákon. Ten říká, že se výkon počítačů každý rok až dva zdvojnásobí. Tento trend platí od roku 1965 až dodnes, jak ilustruje následující graf[35].



Obrázek č. 1: Zrychlování počítačů v čase

(Zdroj: 35)

Jeho svislá osa ukazuje v logaritmickém měřítku počet transistorů v procesorech, zatímco vodorovná osa ukazuje rok uvedení na trh. Jednotlivé body pak reprezentují konkrétní procesory. V současné době se začíná hovořit o tom, že toto tempo začne zpomalovat, ale zatím tomu tak není, a proto je třeba s tím počítat a být připraven na rychlejší a rychlejší počítače.

Zavádění internetu

Na to, jak byl v ČR zaváděn internet, odpovídá průzkum Českého statistického úřadu.

Tabulka č. 2: Zavádění internetu do domácností v ČR

Rok:	2013	2015	2017
Počet domácností s internetem (v %):	67	73,1	83

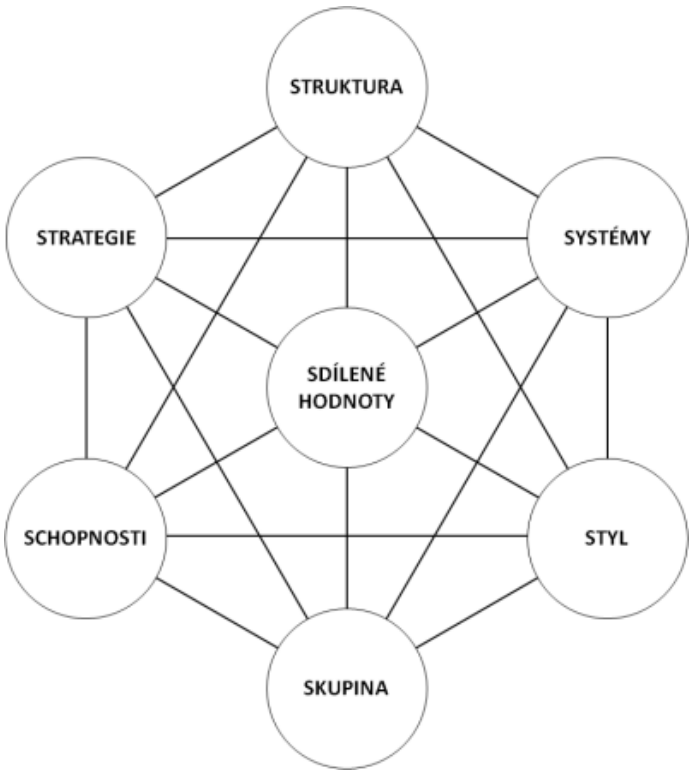
Z tohoto měření vyplývá, že v současnosti má internet většina domácností. Je tedy reálné předpokládat, že k systémům, které zpracovávají a uchovávají osobní data, bude mít přístup většina lidí a valná část se nebude připojovat pouze z práce, ale i

z domu, což jim umožňuje dostupné internetové připojení. Na druhou stranu je třeba to zohlednit při tvorbě strategie a plánování.

3.2 Analýza vnitřních faktorů pomocí metody 7S

Pro rozpoznání klíčových faktorů ovlivňujících změnu je nezbytné poznat firmu jako takovou. Existuje celá řada metodik, které vedou k rozboru a určení silných a slabých stránek uvnitř firmy, pro její lepší pochopení a následně jako zdroj pro tvorbu rozhodnutí. Tyto analýzy se většinou zaměřují na tzv. kritické faktory. Jsou to ty stránky řízení, které mají kritický význam pro směřování a úspěch firmy. Výzkum[36] T. J. Peterse a R. H. Watermana ukázal, že úspěšná firma je ovlivňována sedmi vnitřními, vzájemně se ovlivňujícími faktory. Pro úspěšnou firmu je klíčové, aby si udržovala povědomí o všech těchto faktorech a všechny je kontinuálně rozvíjela[37, s. 12].

Tyto faktory ukazuje následující obrázek:



Obrázek č. 2: Analýza 7s

(Zdroj: 37, s. 12)

Nyní je třeba si zodpovědět na klíčové otázky o společnosti, ve které bude prováděna změna a na jejich základě navrhnout plán pro zavádění změn. Tato analýza

umožní najít silné a slabé stránky firmy a tím určit, které aspekty lze použít jako stabilní výchozí body a na které je třeba se naopak zaměřit, neboť jsou potenciálně problémové.

3.2.1 Strategie firmy

Strategie firmy je základní kámen směřování firmy. Staví na vizi firmy, čímž se myslí představy majitelů a firmy o jejím vývoji a stavu, v jakém by se měla nacházet v horizontu několika let a na konkrétním poslání firmy, což je reálná situace poskytování služeb či tvorba výrobků. V rámci strategie firma definuje, jakým způsobem chce dosáhnout cíle či cílů, které si stanovila. Cílem se myslí konkrétní a měřitelný ukazatel, kterého chce společnost jednoznačně dosáhnout.

Cílem strategie je pomocí volných pokynů a rámcových popisů aktivit vytyčit směřování firmy tak, aby získala co největší konkurenční výhodu díky využití vnitřních zdrojů oproti jiným konkurenčním subjektům. Obecně se jedná o jakousi myšlenku či trend, kterým majitel či skupina vlastníků společnost řídí. Nejde pouze o definovanou strategii, ale zejména o to, jakým způsobem je realizována a vyhodnocována. Vyhodnocování je nezbytné, neboť bez něj je možné, že k naplnění cílů sice dojde, ale tyto budou již nerelevantní, neboť trh se posune jinam a zákazníci ztratí zájem.

Další důležitou věcí, kterou je třeba si uvědomit je, že strategie sama je vlastně sled strategií, které na sebe navazují v pyramidovém schématu.

Jako nejvyšší příčka pyramidy je označována firemní strategie, která určuje základní směr pro celou firmu, bez ohledu na to, zda se jedná o malý podnik o několika zaměstnancích či mezinárodní korporaci.

Na firemní strategii bezprostředně navazuje obchodní strategie, která určuje, jakým způsobem chce firma prezentovat a prodávat výrobky či služby zákazníkům. Také definuje segmenty zákazníků, které chce společnost primárně oslovit.

Na nejnižší příčce strategické pyramidy se nachází funkční strategie. Tyto strategie definují směřování jednotlivých segmentů společnosti, např. marketingu, výroby, managementu, financí atp.

Dělení strategií

Dle Porterova přístupu[37, s. 14] lze volit mezi dvěma konkurenčními výhodami, kterých se firma může snažit dosáhnout. Jedná se o strategii nízkých nákladů a strategii diferenciace. Jak už názvy napovídají, při volbě strategie **nízkých nákladů** se společnost snaží získat konkurenční výhodu tím, že bude nabízet výrobky srovnatelné kvality s konkurencí za nižší ceny. **Strategie diferenciace** se zaměřuje na poskytování jedinečných výrobků, které konkurence není schopna zákazníkům dodat.

Dále lze strategie rozdělit podle toho, zda se zaměřujeme na úzký či široký rozsah. Úzký rozsah znamená, že se zaměřujeme pouze na jeden či několik málo segmentů trhu, kde se snažíme dosáhnout vůdčího postavení. Široký rozsah pokrývá celé odvětví. Strategie cílené na úzký rozsah se nazývají strategiemi pozornosti.

V tomto bodě je třeba si zodpovědět následující otázky

- Čím se firma odlišuje od konkurence?
- Co je základním produktem, na kterém společnost vydělává?
- Jaké jsou segmenty, na které společnost cílí?
- Mají tyto segmenty nějaká specifika?
- Jaké jé území, na které společnost cílí?
- Má toto území (či jeho části) nějaké zvláštnosti? Lze na ně cílit?

3.2.2 Organizační struktura firmy

Organizační strukturou se myslí rozřazení pracovníku do hierarchie tak, aby bylo vždy jasně patrné, kdo komu přiděluje úkoly a kdo nese zodpovědnost za jaká rozhodnutí. Cílem organizace je optimalizace rozdělování úkolů tak, aby každý měl dostatek práce, ke které je kompetentní při minimalizaci režijních nákladů. S růstem velikosti organizace se organizační struktura stává složitější, čímž rostou náklady.

Nyní si ukažme některé nejčastější struktury, které se vyskytují ve firmách.

Liniová struktura

Nejjednodušší struktura, kde je jeden útvar přímo podřízený jednomu jinému. Výhodou jsou jasně definované pravomoci a vztahy nadřízenosti a podřízenosti a tím možnost rychlého rozhodování a pružná řešení. Nevýhodou pak poměrně velké režijní

náklady a nároky na ředitele každého útvaru, který musí mít znalosti v rámci celé společnosti, což vylučuje úzkou specializaci.

Funkcionální struktura

Tato struktura je v určitém směru opakem liniové struktury. Na stejné úrovni se nachází několik útvarů, kde každý vedoucí útvaru rozhoduje pouze o otázkách spadajících do jeho kompetence. Každý tak přesně ví, za co je zodpovědný, a může se specializovat na svoji odbornost.

Mezi nevýhody patří jednak vyšší režijní náklady, ale hlavně problematika koordinace útvarů na stejné úrovni. To způsobuje, že každému podřízenému je nadřízeno současně několik vedoucích, kteří jsou vůči sobě navzájem na stejné úrovni. To způsobuje, že vyšší management musí neustále řešit konflikt priorit či protichůdné příkazy a nemá čas se zaměřit širší pohled.

Liniově štábní struktura

Snaha o kombinaci předcházejících přístupů. Ve vedení je zachována liniová struktura, která jasně určuje zodpovědnosti a hierarchii. Na tu navazuje funkcionální struktura pro odborné složky společnosti. Provádění specializovaných úkolů je ponecháno na jednotlivých buňkách, tzv. štábech, které se za něj zodpovídají nadřízenému útvaru. Jedná se o pravděpodobně nejčastěji využívanou firemní strukturu.

Divizionální struktura

Jedná se o přístup, kdy se vytvoří relativně samostatné divize v závislosti na přirozeném členění společnosti. Například lze tedy dělit divize dle odvětví, cílové skupiny či geografické polohy. Každá divize je samostatná a obsahuje vše, co pro své fungování potřebuje. Největší nároky tato struktura klade na synchronizaci jednotlivých divizí, kde je třeba dohlédnout na správnou míru součinnosti pro předcházení redundantních činností.

Maticové organizační struktury

Kombinací divizionální a funkcionální struktury vzniká maticová organizační struktura. Jedná se o stav, kdy každý člověk má více, než jednoho nadřízeného. Většinou se jedná o dva, kdy jeden se zabývá odbornými otázkami problémů, zatímco druhý provozními. Pracovník se zodpovídá oběma a ti se zodpovídají svým nadřízeným.

Tyto struktury se vyznačují schopností pružné reakce na vnější změny a dobrou motivací pracovníků. Hlavní nevýhodou jsou dva vedoucí jednoho člověka, což může vést k neshodám, nejasnému určení zodpovědností a nejasnému stanovení priorit.

Samozřejmě existuje velké množství dalších organizačních struktur, které se vyvinuly podle potřeb konkrétních podniků a jejich zaměření. Většina z nich kombinuje některé z výše uvedených struktur nebo je různě modifikují. Navíc se každá struktura v průběhu času vyvíjí a mění dle potřeb trhu a prostředí.

Obecně by se měl management snažit o co nejmenší počet úrovní vedoucích struktur. Čím méně jich je (struktura je tzv. štíhlejší), tím je menší prostor pro chyby v komunikaci, lidská selhání či neporozumění. Nejdůležitější však je, že struktura musí být podřízená strategii firmy a je třeba, aby co nejlépe vyhovovala momentální situaci v dané firmě.

Otázky, na které je třeba si zodpovědět v tomto bodě:

- Jakou strukturu má společnost?
- Jaké je dělení v rámci jednotlivých úrovní struktury?
- Dochází zde k nějakým problémům?
- Má konkrétní struktura společnosti nějaká specifika, která je třeba zohlednit?

3.2.3 Informační systémy

Do tohoto bodu lze zahrnout veškeré systémy pro správu dat, které společnost využívá pro svoji práci. Může se jednat jak o systémy automatické správy dat, tak i systémy, které data zpracovávají více či méně automatizovaně. Většinou systémy na nejnižších úrovních používají maximální automatizované a autonomní zpracování dat tak, aby došlo na jejich rozklad na co nejmenší jednotky, které jsou jasně ohraničené a rovnou předložitelné zaměstnancům. Může se jednat o komplexní systémy pro podporu firemních procesů, které umožňují v jednom procesu přesouvat data od zaměstnance k zaměstnanci tak, aby každý znal přesně svoji část úlohy a byl odstíněn od všech pro něj nepodstatných aspektů. Stejně tak se využívají systémy pro správu jednotlivých úkolů, kdy úkol přechází celý od jednoho zaměstnance ke druhému a lze kdykoliv dohledat veškeré změny, které kdokoliv provedl.

Směrem k vyšším příčkám řídících struktur ubývá automatizovaného zpracování a je třeba větších zásahů ze strany lidského faktoru. Postupem se jednotlivé úkoly spojují do větších logických celků, kde se zanedbávají jednotlivé detaily úkolů a stále více se klade důraz na celková čísla, jako je počet úspěšných úkolů, počet reklamací atp. Na nejvyšší úrovni se tyto systémy využívají spíše jako zdroje dat pro tvorbu manažerských rozhodnutí.

Otázky, na které je třeba si odpovědět:

- Jaké informační systémy společnost používá?
- Kdo je jejich dodavatelem?
- Jakým způsobem funguje tvorba změn v těchto systémech?
- Uchovávají se v těchto systémech osobní data?
- Jak jsou tyto systémy zabezpečeny?
- Které firemní procesy jsou řízeny pomocí těchto systémů?
- Není možné použít stávající systémy pro řízení dalších procesů?

3.2.4 Styl řízení

Stylem řízení se myslí přístup, který má vedení ke svým zaměstnancům. Určuje, do jaké míry je vedení autoritativní. Čím vyšší je míra autority, tím menší prostor mají podřízení pro prosazování vlastních názorů, a zároveň tím vyšší má manažer zodpovědnost. Způsobů řazení je mnoho, ale zde si uvedeme nejzákladnější systémy.

Direktivní styl vedení

Tento přístup v podstatě neumožňuje podílet se ostatním pracovníkům na řízení firmy. Veškeré příkazy pochází od vedení společnosti. Informace manažer získává od svých podřízených.

Demokratický styl

Manažer nechává i ostatním prostor pro vyjádření svých názorů a deleguje část odpovědnosti na podřízené. Stále má však poslední slovo v důležitých otázkách a zůstává mu proto značná část odpovědnosti. Při tomto stylu řízení manažer vysvětluje své postoje a komunikuje je směrem k podřízeným, kteří mají možnost se vyjádřit. Problémy se řeší přímo diskuzí mezi jednotlivými názorovými stranami.

Liberální styl

Manažer se zříká valné části odpovědnosti, skupina má volnost v tom, kdo bude co řešit a kdy. Klade velké nároky na členy týmu, kteří spolu musí být schopní komunikovat. Někdy je po úkolu vhodné s podřízenými probrat, co udělali dobře a čemu se příště vyhnout.

Otázky, na které je třeba si odpovědět:

- Jaký styl řízení firma uplatňuje?
- Uplatňuje se tento styl na všech úrovních?
- Jaké výhody a nevýhody plynou z tohoto stylu řízení?
- Jaké jsou odpovědnosti na jednotlivých pozicích?

3.2.5 Skupina

Do této kategorie spadá veškerá činnost spojená s nabíráním nových zaměstnanců, jejich udržováním ve firmě, dalším vzděláváním a podobně. Lidé jsou totiž základním kamenem úspěšné firmy.

Zároveň tato kategorie zahrnuje i to, co motivuje zaměstnance v setrvávání na pracovní pozici a odvádění své práce nejlépe, jak umí. Nejedná se pouze o finanční stránku práce a s ní související případné benefity, které jsou vlastně pouze jakýmsi substitutem finančního ohodnocení (např. možnost využívat firemní automobil znamená v první řadě to, že zaměstnanec nemusí řešit svoji dopravu vlastním vozem, jehož pořízení a provoz by ho stálo peníze). Důležitým prvkem je také osobní sounáležitost pracovníků s podnikovým kolektivem. V ideálním případě se považují za členy podnikové rodiny a firmu berou jako součást nejen své kariéry, ale i života. Takové zaměstnance je třeba identifikovat a podporovat tuto tendenci.

Tohoto stavu se dá dosáhnout vhodným jednáním se spolupracovníky a jejich řízením, ale zejména budováním firemní identity a možnostmi osobního růstu pro tyto lidi. To vytváří vhodnou motivaci ke kvalitní a tvůrčí práci.

Pro řízení změn jsou klíčoví řídící pracovníci, kteří dokáží nadchnout své kolegy pro změnu, čímž způsobí, že se jejich kolegové budou dobrovolně chtít na změně

podílet a tím si k ní vytvoří vztah už během jejího zavádění. To výrazně snižuje problémy při akceptaci změny po jejím zavedení.

Tito pracovníci by měli být, kromě schopnosti vést a motivovat lidi, schopní též předvídat problémy, které při změně mohou nastat a reagovat na ně buď ještě předtím, než nastanou, nebo v případě nepředvídatelných komplikací je dynamicky řešit tak, aby nedošlo k paralýze celého změnového řízení. Toho dosahují tím, že vidí možnosti i tam, kde se zdá, že žádné nejsou. Pokud už se pro nějakou příležitost rozhodnou, dokáží na ní vytrvale pracovat společně s celým týmem, který vedou.

Otázky, na které je třeba si odpovědět:

- Jaký je kolektiv ve firmě?
- Jaká panuje mezi kolegy atmosféra?
- Motivuje tento kolektiv k práci?

3.2.6 Sdílené hodnoty (kultura) firmy

Firemní kultura nebo též korporátní identita úzce souvisí s lidmi pracujícími ve firmě. Jedná se o soubor pravidel, která určují jednak jakým způsobem společnost přistupuje ke svému okolí, zákazníkům a obecné veřejnosti, tak také k vnitřním regulím, ať už psaným či nepsaným, které definují jednání společnosti s vlastními zaměstnanci. Vše je motivováno snahou o odlišení se od ostatních firem. To je důležité ze dvou důvodů: Jednak pro zákazníky, kteří pak při výběru pravděpodobněji sáhnou po povědomém; ale neméně důležitě ovšem též pro zaměstnance, pro které tak firma není jenom zdroje příjmů, který je možné kdykoliv nahradit, ale stává se nedílnou součástí jejich života, kterou není tak snadné opustit. Navíc ve chvíli, kdy jsou zaměstnanci osobně zainteresovaní, jsou daleko více motivováni podávat kvalitní výkony.

Firemní kultura zahrnuje celý charakter společnosti, atmosféru, pracovní normy, představy, přístupy a hodnoty jejich zaměstnanců na všech pozicích. Projevuje se napříč vzorci chování všech pracovníků a je jedinečná a charakteristická.

Otázky, na které je třeba si odpovědět:

- Jaké jsou hodnoty firmy?
- Jak se chce firma prezentovat svým klientům?

- Jaké je vnitřní prostředí firmy?

3.2.7 Schopnosti

Do této kategorie spadají klíčové schopnosti vedoucích pracovníků. Na těch totiž záleží, jakým směrem se bude společnost ubírat a do značné míry tak ovlivňují úspěch. Pojďme si uvést základní schopnosti, vlastnosti a znalosti, které by měl mít úspěšný manažer a které jsou základem úspěšné společnosti:

1. **Schopnost vytyčit si cíle** a cílevědomě za nimi jít. Je nezbytné, aby manažer přesně věděl, čeho chce dosáhnout a jakými metodami toho docílí. Následně musí být připraven tuto cestu hájit v případě problémů, ale zároveň musí být schopen pružně reagovat na neočekávané změny a překážky.
2. **Znalost ekonomického prostředí** společnosti je dalším klíčovým prvkem. Bez této znalosti není možné efektivně určovat cíle a směřovat společnost na nejlepší možnou cestu.
3. **Znalost oboru** a možností firmy.
4. **Povědomí o řízení společnosti.** Manažer by v první řadě měl být vůdce firmy. Jako takový musí znát teoretická východiska jejího řízení a mít představu o povinnostech, které mu ukládá zákon.
5. **Dovednost vhodně delegovat.** Nikdo nedokáže zastat práci na všech pozicích a obsáhnout všechny vědomosti ohledně oboru. Proto dobrý manažer musí vědět, kterou práci přenechat svým podřízeným a kdy se jich zeptat na názor.
6. **Lidské kvality.** Sem patří schopnost empatie, přijímat a dávat zpětnou vazbu, jednat s lidmi, smysl pro humor, morální hodnoty, otevřenost, schopnost pracovat v týmu, objektivita, umění nadchnout ostatní pro svoji věc a další vlastnosti, které jsou nepostradatelné pro jednání s lidmi.
7. **Dobré organizační schopnosti.** Neboť organizace času, ať už svého, tak podřízených, je základní náplní práce manažera.
8. **Schopnost sebereflexe a snaha se trvale zlepšovat.** V současné, stále rychlejší době je nezbytné, aby manažer znal své silné a slabé stránky a rozvíjel je tak, aby byl své firmě co nejužitečnější.

Otázky, na které je třeba si zodpovědět:

- Kdo jsou skuteční firemní lídři?
- Jaké mají vlastnosti?
- Jaké vlastnosti jim naopak chybí?
- Lze je nějak podpořit v jejich zlepšování?

3.3 Závěrečná analýza pomocí metody SWOT

V tomto bodě je třeba zhodnotit celkové vnitřní i vnější prostředí firmy na základě předchozích analýz a identifikovat klíčové body, kterým je třeba se věnovat. Pro tento účel je nejvhodnější analýza SWOT (z anglického originálu Strengths, Weaknesses, Opportunities, Threats, v češtině silné stránky, slabé stránky, příležitosti, hrozby). Ta identifikuje čtyři klíčové oblasti, které potom slouží jako základní kámen rozhodnutí, zda změnu provést a pokud ano, čeho se přitom držet a na co si dát pozor. Prostor grafu je rozdělen dvěma osami na čtyři kvadranty.

Na vodorovné ose leží vlevo všechna pozitiva. Všechny faktory, které mohou naši společnost ovlivnit pozitivně, se píší vlevo. Naopak všechno, co může působit negativně (např. způsobit zmenšení tržeb, podílu na trhu, odchod zaměstnanců atp.) se na této ose nachází vpravo.

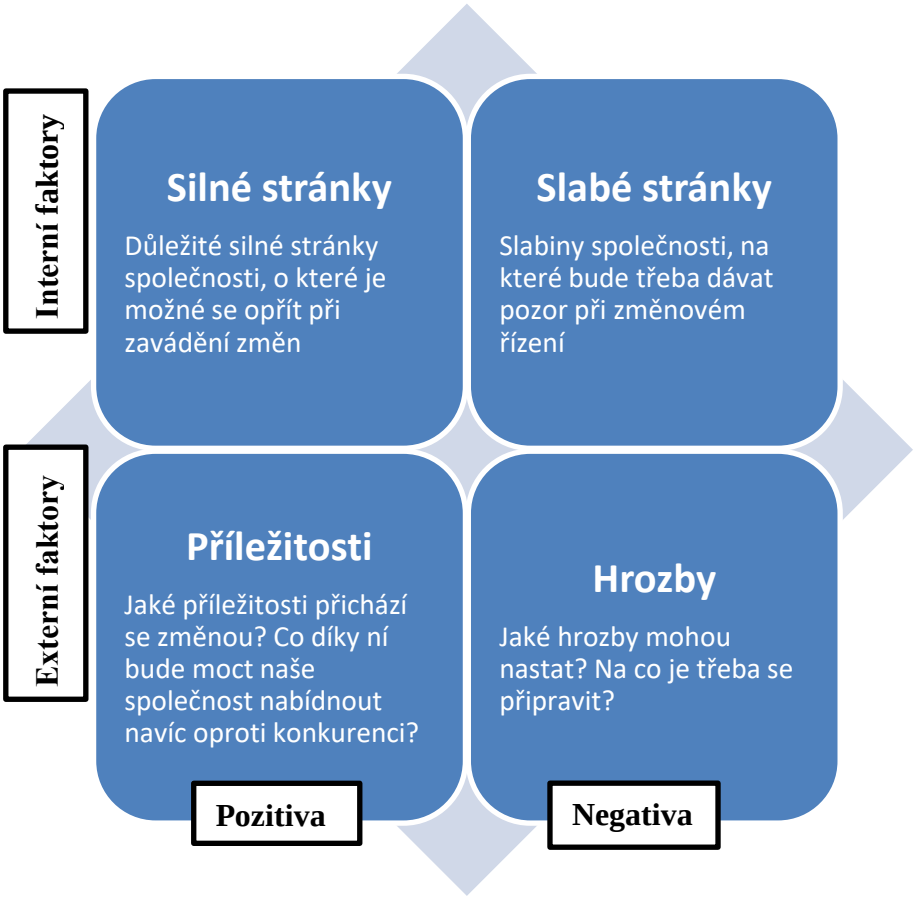
Svislá osa pak určuje, zda se jedná o interní faktory, které leží uvnitř samotné firmy a lze s nimi manipulovat, nebo faktory externí. V tom případě je nelze ovlivnit, ale lze se na ně připravit tak, aby nezpůsobily škody.

Tyto dvě osy pak dělí graf na 4 kvadranty. Kvadrant označený jako silné stránky definuje aspekty společnosti, ve kterých má něco navíc oproti konkurenci. Na těchto bodech lze stavět a je třeba jich maximálně využít pro maximalizaci zisku. Naopak v kvadrantu označeném jako slabé stránky jsou všechny prvky, které ve společnosti nejsou optimální a tak ji brzdí. Je důležité o těchto bodech vědět a soustavně na nich pracovat, aby se jich společnost zbavila, anebo z nich dokonce udělala své silné stránky.

Kvadrant označený jako příležitosti označuje všechny vnější vlivy, které mohou pozitivně ovlivnit vývoj společnosti, pokud jich vhodně využije. Na tyto body je třeba se připravit a cílit na ně při přípravě budoucí strategie. Naopak v posledním kvadrantu, označeném jako hrozby, jsou všechny okolnosti, které mohou působit negativně. Tyto vlivy je třeba zvážit a připravit se na jejich působení buď tak, že jim předejdeme, nebo

se připravíme na jejich negativní dopady. Tento kvadrant bude blíže rozpracován v kapitole zabývající se řízením rizik.

Jak může vypadat analýza SWOT zobrazuje následující grafika:



3.3.1 Vyhodnocení SWOT analýzy

V kroku vyhodnocení analýzy SWOT je třeba zhodnotit jednotlivé kvadranty a zejména jejich kombinace pro získání lepší představy o tom, kde leží největší problémy a kde naopak příležitosti, jak využít silných stránek společnosti pro vyřešení problémů a k co nejlepšímu využití příležitostí.

Doporučený postup vyhodnocení je následující:

- Jak využít silných stránek pro co největší zisk z příležitostí na trhu?
- Jak využít příležitostí k odstranění či snížení slabých stránek?
- Jak využít silné stránky k odvrácení hrozeb?
- Jak zapracovat na svých slabých stránkách, aby se společnost vyhnula hrozbám?

3.4 Návrh změny pomocí Lewinova modelu

V této části se zaměříme na konkrétní návrh strategie, která povede ke změně ze současného stavu, který nevyhovuje nové legislativě, do stavu nového, který bude vyhovující. Pro tento proces je vhodné použít Lewinův model[37, s. 30], který popisuje kroky vedoucí řízenou změnu.

Tento model se skládá ze tří částí:

1. **Rozmrazení –** Tato fáze obsahuje všechny kroky, které je třeba učinit před samotnou změnou. Obsahuje analýzy, které poskytnou teoretické informace, na jejichž základě můžeme činit rozhodnutí o směřování firmy a konkrétní podobě uskutečňované změny.
2. **Posun –** Zde dochází k samotné změně. Zahrnuje jak samotnou změnu a s ní spojené činnosti, tak monitoring a průběžné vyhodnocování.
3. **Zmrazení –** Jedná se o činnosti, které následují po posunu. Měly by vést ke standardizaci činností a vytvoření nové rovnováhy ve stavu po změně. Obsahuje též závěrečnou zprávu, která ukáže, nakolik byla změna úspěšná, zda se změnily požadované ukazatele a poslouží jako podklad pro příští změnové strategie.

3.4.1 Rozmrazení

Na začátku je třeba provést analýzu situace, která nám poskytne vodítka pro další kroky při řízení změny. Případně může vyjít najevo, že současný stav je vyhovující a není třeba jej měnit.

Jako první si na základě Lewinova modelu je třeba zodpovědět následující otázky:

Jaké síly inicializují změnu? Jak jsou intenzivní? Co způsobí?

V tomto případě je silou, která změnu požaduje, nová legislativa Evropské unie o ochraně osobních údajů. Konkrétní požadavky tohoto nařízení jsou vypsány ve druhé kapitole této práce. Pokuta za nedodržení tohoto nařízení může činit až 20 000 000 eur, kde i její zlomek by byl pro malý nebo střední podnik likvidační. Proto není možnost se této změně vyhnout a je třeba se na ni připravit.

Dobrým vodítkem pro tuto otázku může být analýza silového pole. I přesto, že se změna může zdát nevyhnutelná, může být aplikována na různé dílčí změny. Pokud je aplikována na celek, může být vodítkem pro určení, od kterých subjektů očekávat pomoc a kde naopak mohou nastat problémy.

Principem je vypsat všechny síly ve firmě i mimo ni, které působí pro změnu a budou ji podporovat a proti nim všechny síly, které budou změnu naopak komplikovat či bojkotovat. Následně se jednotlivým silám přidělí váhy dle závažnosti na škále od 1 do 10, kde 1 je síla téměř zanedbatelná, zatímco 10 je síla, která výrazně ovlivňuje realizovatelnost celé změny. Na závěr se udělá prostý součet sil působících pro a sil působících proti. Ze součtu je pak jasně patrné, které síly převažují a zda má změna více podpory či komplikací.

V případě, že je zjištěno velké množství či síla faktorů působících proti změně, je na místě se zamyslet, zda je změna vůbec realizovatelná a s jakými překážkami se bude muset firma potýkat. Pokud se i přesto rozhodne změnu podniknout, je dobrou cestou nejprve odstranit či zmírnit faktory působící proti změně.

Zde jsou uvedeny příklady sil, které mohou působit pro a proti změně zavádějící nové činnosti a firemní procesy plynoucí z nařízení.

Síly působící pro změnu

- Legislativa
- Vedení společnosti
- Zaměstnanci společnosti, v závislosti na tom, zda chápou důležitost ochrany osobních údajů a zavedení nové normy
- Udržení konkurenceschopnosti
- Získání nových klientů

Síly působící proti změně

- Finanční náklady
- Časová náročnost
- Zaměstnanci společnosti, zejména pokud se jedná o lidi konzervativní
- Riziko špatné implementace

Jak vypadá požadovaný stav, kterého chceme dosáhnout?

Cílovým stavem je samozřejmě bod, kdy všechny systémy budou splňovat nařízení. Platí to jak pro systémy interní, tak pro nově vytvářené systémy v případě společností, které dodávají systémy a figurují tak v roli zpracovatelů osobních dat. To samo o sobě však nestačí. Je třeba, aby se někteří zaměstnanci seznámili dle své odbornosti s nařízením natolik, aby podle něj byli schopní pracovat. Zaměstnanci na klíčových pozicích musí nařízení chápat dost na to, aby dokázali ve svých odděleních zavést vhodná opatření, která zajistí soulad s nařízením.

Kdo z firmy bude proces bojkotovat a kdo ho bude podporovat? Nositel změny

Vzhledem k závažnosti situace lze předpokládat, že většina zaměstnanců nebude mít se změnou přílišné problémy. Největší motivaci pro zavedení změn bude mít tým sestavený speciálně pro tento účel. Právě ten bude mít na starost získat pro změnu na svou stranu ostatní zaměstnance a provést ji. Určité problémy mohou nastat na základě nechuti některých konzervativních zaměstnanců k novým byrokratickým postupům. Zde je pak na realizačním týmu, aby jim předložil dostatečně jasně důležitost a smysl nových pracovních postupů.

Kde konkrétně bude provedena intervence? Jakým způsobem?

Změna bude iniciována na několika místech současně. V následující části se podíváme na každou část zvlášť:

1. **Studium nového nařízení.** Je třeba, aby každý v rozsahu své odbornosti věděl, co jemu přináší nová legislativa v rámci jeho úkolů a zodpovědností. Proto bude třeba zařídit školení. Tato školení budou rozdělena na řídící pracovníky a na řadové zaměstnance. Vedoucí oddělení totiž musí pochopit nařízení dostatečně na to, aby dokázali na svých odděleních zavést nezbytná opatření. Zaměstnancům pak stačí znát nové byrokratické postupy a rámcové pokyny v takové míře, aby byl jejich výstup v souladu s nařízením.

2. **Změna interních nástrojů společnosti.** Jedná se o vnitřní mechanismy firmy, které se používají pro správu úkolů a docházky. Je třeba zrevidovat, zda odpovídají novému nařízení, a odstranit případné nedostatky. Ze závěrů předcházejících kapitol ve vztahu k zálohování je nutné zvážit zejména následující body:
    - Je uložení dat bezpečné? Je zamezeno jejich ztrátě či zpřístupnění nepovolaným osobám?
    - Jsou zálohy pravidelně kontrolovány povolanými osobami?
    - Jsou firemní mechanismy nastaveny[38, s. 73] tak, aby se úroveň zabezpečení zlepšovala podle moderních bezpečnostních standardů?
    - Je možné dostát v plném rozsahu práva být zapomenut, jak vychází z nařízení?
    - Jsou firemní postupy nastaveny tak, aby bylo vždy jasné, kdo má právo manipulovat či nahlížet na konkrétní osobní údaje a bude to zaznamenáváno?
    - Je možné dostát všem povinnostem, které z nařízení vyplývají v plném rozsahu?
3. **Případná změna struktury.** V případě, že hlavní činností správce je rozsáhlé, pravidelné a systematické monitorování občanů, či zpracování zvláště citlivých osobních údajů, je nezbytné vytvořit novou pozici pověřence pro zpracování osobních údajů.

Operační modely

Před samotnou změnou je třeba nastavit operační modely, které budou reflektovat již splněnou část změny a ukazovat směr ještě nehotových součástí. Díky těmto modelům lze předvídat dobu trvání, po kterém lze předpokládat, že bude změna ukončena. Zároveň lze s nimi porovnávat nakolik bylo dosavadní plnění modelu úspěšné a případně upravit další směřování, pokud se ukáže, že původní odhad a navržený postup je nerealizovatelný.

Závěr analýzy

Při zvážení všech pro a proti je poměrně jasné, že změna je z důvodu nové legislativy nevyhnutelná. Výhodou je dobrá ekonomická situace spolu s dalšími

pozitivními vlivy okolí, které jsou rozebrány v analytické části. Rizika, které tato změna přináší, je třeba zohlednit a připravit se na ně, což bude obsahem samostatné kapitoly.

3.5 PERT

Pro řízení změny je nezbytné nastavit plán, který ukazuje, jakým činnostem se věnovat a definuje jejich priority. Pro řízení změn existuje velké množství metodik. Pro řízení změny zavedení nového nařízení je velmi vhodná například metoda PERT.

Metoda PERT (Program Evaluation and Review Technique – Metodika hodnocení a přezkoumávání procesu) je jednou z metod síťové analýzy. Jedná se o metodu založenou na metodě kritické cesty (CPM). Hlavním rozdílem oproti metodě CPM je to, že doba trvání úkolu je chápána jako náhodná proměnná, mající určité rozložení pravděpodobnosti. Doba trvání tedy není přesně známa, ale je určena pravděpodobnost jejího trvání. Pro rozdělení se nejvíce hodí rozložení beta, u kterého bylo dokázáno[39], že pro praktické procesy nejlépe vyhovuje.

Z metod síťové analýzy byla zvolena proto, že pro dané použití nejlépe odpovídá realitě. U úkolů totiž není vždy jasně dané, jak dlouho budou trvat, vždy je zde jistá míra nejistoty. Tato míra může být poměrně vysoká a může silně ovlivnit celkové trvání projektu. Metoda PERT však umožňuje s touto mírou nejistoty pracovat a dodat tak cenná data pro manažerská rozhodnutí.

Doba trvání jednotlivých činností je udána pomocí tří odhadů: optimistického, nejpravděpodobnějšího a pesimistického. Na základě těchto odhadů je vypočítána délka trvání jednotlivých činností a pravděpodobnost tohoto trvání.

Na základě těchto odhadů se sestaví nejpravděpodobnější doba trvání. Pomocí této doby je sestaven síťový graf činností. Jednotlivé hodnoty, potřebné pro každou činnost, se nachází v následující tabulce.

Základní charakteristiky metody PERT

Optimistický odhad	**a**
Realistický odhad	**m**
Pesimistický odhad	**b**

Deterministický model	$\mathbf{T_e}$	$\frac{a+4m+b}{6}$
Začátek možný	**ZM**	KM předchůdce
Konec možný	**KM**	ZM + t_{eij}
Začátek přípustný	**ZP**	KP – teij
Konec přípustný	**KP**	ZP následníka
Rezerva celková	**RC**	ZP – ZM
Rezerva volná	**RV**	ZM následníka – KM
Rozptyl	$\boldsymbol{\sigma^2}$	$\frac{(b-a)^2}{36}$

Následně se na základě vypočítaných hodnot sestaví kritická cesta. Jedná se o nejdelší cestu v grafu, která má nulovou rezervu a jejíž prodloužení způsobí prodloužení celé činnosti.

3.6 Analýza rizik

Každá změna s sebou nese rizika. Rizikem se myslí situace, která může s určitou pravděpodobností nastat a která potenciálně může způsobit ztrátu či neúspěch. Též představuje nebezpečí negativní odchylky od cílového stavu. S riziky je třeba pracovat, neboť vhodnou přípravou jim lze předcházet či výrazně snižovat jejich dopady.

Prvním krokem v procesu[37, s. 85] snižování rizik je jejich analýza. Jedná se o činnost, jejímž výstupem je seznam hrozeb, které mohou ovlivnit proces a hodnocení jejich pravděpodobnosti a závažnosti. To poskytuje vhodný základ k dalším manažerským rozhodnutím, která by měla vést ke snížení pravděpodobnosti či dopadu rizik. Pro potřeby řízení této změny je doporučena skórovací metoda, kde je každému riziku stanovena pravděpodobnost a dopad na škále 1 až 10, kde 1 je nejnižší pravděpodobnost/dopad a 10 nejvyšší. Vynásobením těchto čísel získáme celkovou hodnotu rizika, která nám umožní určit, jak závažné riziko je. V následující tabulce lze najít orientační přehled rizik, který může vyvstat při této změně.

3.6.1 Identifikace a ohodnocení rizik

Tabulka č. 3: Identifikace a ohodnocení rizik

Číslo rizika	Riziko
1	Chybné pochopení legislativy
2	Špatně vytvořené zadání pro změny v procesech
3	Špatná identifikace ovlivněných procesů
4	Špatně zacílené školení
5	Nepochopení školení ze strany zaměstnanců
6	Příliš pomalá reakce, pokuta
7	Překročení rozpočtu
8	Další legislativní změny
9	Zanesení chyb do stávajícího systému
10	Nečekaný výpadek klíčových pracovníků

3.7 Mapa rizik

Mapa rizik je dalším vhodným nástrojem pro analýzu rizik. Pomocí vizualizace rozděluje rizika do čtyř kvadrantů tak, aby bylo jasné, kterým je třeba věnovat nejvyšší pozornost.

Kvadrant kritických rizik

V tomto kvadrantu se nachází rizika, která s velkou pravděpodobností nastanou a budou mít velký dopad. Je naprosto nezbytné pro ně vypracovat opatření, která jim zabrání nebo jejich dopad zmírní.

Kvadrant významných rizik

Rizika, jejichž pravděpodobnost je nízká, ale pokud se přesto stanou, mohou mít vážné následky. I pro tuto kategorii je třeba vypracovat opatření. Typickým opatřením pro rizika z této kategorie bývá pojištění.

Kvadrant běžných rizik

Rizika s vysokou pravděpodobností výskytu, ale nízkým dopadem. Jedná se o rizika, která běžně nastávají v průběhu projektů. Při vytváření opatření je dobré zvážit hodnotu těchto opatření, aby nepřevyšovala hodnotu rizika. V určitých případech je přípustné riziko z této kategorie podstoupit.

Kvadrant bezvýznamných rizik

Jedná se o rizika s malou pravděpodobností výskytu a malým dopadem. Tato rizika mohou být podstoupena bez větších opatření.

3.8 Opatření

Na základě analyzovaných rizik se dá dobře stanovit, na která rizika je třeba se zaměřit v první řadě a věnovat jim zvýšenou pozornost. Opatření vhodná pro rizika představená v předchozí kapitole jsou přehledně zaznamenána v následující tabulce.

Tabulka č. 4: Opatření vzhledem k rizikům

Číslo rizika	Opatření
1	Detailní analýza, konzultace s právníky, případně s konkurencí
2	Detailní analýza problému, studium řešení v podobných firmách
3	Přesné zacílení na potřeby firmy
4	Školení pomocí externí firmy, která se zabývá daným odvětvím
5	Školení pomocí externí firmy, která se zabývá daným odvětvím
6	Dobrá příprava plánu, zaměření se na termíny
7	Dobrá příprava plánu
8	Návrh systému tak, aby byl dobře modifikovatelný
9	Průběžná kontrola systémů
10	Vypracování krizových plánů

Po zohlednění opatření je vhodné přehodnotit mapu rizik. Při analýze rizik pro konkrétní řešení se po zavedení opatření odpovídajícím způsobem upraví hodnoty pravděpodobnosti a dopadu rizika.

3.9 Použité techniky

V této kapitole budou rozebrána některá konkrétní řešení, která odpovídají na problematiku zálohování osobních údajů v určitých situacích. Tato řešení jsou aplikovatelná s přihlédnutím k jejich implementaci pro konkrétní zálohovací technologie a citlivost osobních údajů, pro která jsou užita.

3.9.1 Pseudonymizace

Velmi efektivním postupem při správě osobních dat je jejich pseudonymizace. Jedná se o postup, při kterém jsou data rozdělena tak, aby jednotlivé části nemohly být použity k identifikaci fyzické osoby, které se týkají. Nejtypičtějším příkladem je nahrazení jména, příjmení a případných dalších specifických údajů jako je rodné číslo či číslo občanského průkazu, vygenerovaným unikátním klíčem. Do samostatné tabulky jsou pak uloženy specifické údaje společně s vygenerovaným klíčem. Podmínky, které je nutné splnit pro ochranu osobních údajů, se poté vztahují pouze na tabulku obsahující specifické údaje. Ostatní data, označená pouze kódem, lze šířit zcela volně. Je však nezbytné mít jistotu, že ze zbylých údajů nepůjde, ani při jejich kombinaci s jinými volně dostupnými informacemi, určit identitu subjektu.

3.9.2 Anonymizace

V případě, že je třeba data smazat, například z důvodu využití práva být zapomenut či protože vypršela doba, po kterou je jejich uložení nezbytně nutné, mohlo by dojít k narušení integrity systému, neboť na data se mohou odkazovat jiná data z jiné části systému. Udržení integrity systému však nezakládá nárok na další uložení dat, proto je třeba přistoupit k jejich anonymizaci. To je proces, při kterém jsou data vedoucí k jednoznačné identifikaci fyzických osob nahrazena unikátními identifikátory, z kterých však již nelze, ani v kombinaci s jinými daty, nikdy zjistit původní údaje. V takovém případě se nařízení na data dále nevztahuje a zároveň je zachována celistvost systému.

3.9.3 Šifrování

Vhodně zvolené šifrování může sloužit jako nástroj pro plnění povinností vyplývajících z nařízení o ochraně osobních údajů. Jednou z možností je ukládat veškerá data o každé fyzické osobě do zvláštního archivu, který bude šifrován unikátním bezpečnostním klíčem. V případě, že subjekt využije právo být zapomenut, postačí změna tohoto klíče na náhodný, který nebude známý žádné osobě a nebude jej možné ani jinak získat, přečíst či zpětně vypočítat.

Pokud to možné není, protože například i v případě využití práva být zapomenut je nutné u subjektu udržovat údaje nutné pro plnění smluv, lze využít více šifrovacích klíčů pro jeden subjekt. V případě nutnosti smazání některých údajů pak postačí změnit konkrétní klíč, bez nutnosti ztráty ostatních údajů. Tato technika je zvláště vhodná pro případ zálohování na média, jejichž čtení a přepis je nákladný na režii a vystavuje média nepřiměřené zátěži, například magnetické pásky.

Šifrovací klíče je třeba mít uložené na bezpečném místě, dle bezpečnostních norem odpovídajícím dané lokalitě a čase. I tyto klíče je nezbytné zálohovat, ale jejich velikost může být řádově menší než velikost původních dat, a proto je jejich zálohování jednodušší a je možné přistoupit k dynamičtější formě záloh než v případě velkých objemů dat.

ZÁVĚR

Cílem této práce bylo seznámit čtenáře se všemi náležitostmi, které vyplývají pro zálohování z nového nařízení o ochraně osobních údajů. V první části byly určeny aspekty nařízení, které se přímo dotýkají zálohování a další body, které je dobré znát a věnovat jim pozornost. Dále byly předvedeny vhodné zálohovací metody, které mohou sloužit pro zálohování osobních údajů v souladu s nařízením. V závěru je stanovena metodika, která umožní využít nabyté znalosti pro co nejhladší přechod na systémy, které jsou v souladu s GDPR.

Jedním z cílů práce bylo šířit osvětu ohledně nového nařízení, neboť ve společnosti ohledně něj koluje množství zavádějících, neúplných nebo zcela špatných informací. Tato práce ukazuje, že vzhledem k původním zákonům České republiky nedochází k velkému počtu změn, navíc odpadají některé povinnosti a metodika správy osobních údajů nyní bude sjednocena napříč všemi státy EU.

SEZNAM POUŽITÉ LITERATURY

[1] Návrh zákona o zpracování osobních údajů je teprve meziresortním připomínkovém řízení. *Bureau Veritas* [online]. 2017 [cit. 2019-05-03]. Dostupné z: https://www.bureauveritas.cz/home/news/latest-news/gdpr-nepropadejte-panice

[2] *Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24 října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Special edition in Czech: Chapter 13 Volume 015 P. 355 - 374*

[3] *Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech*

[4] *Zákon ze dne 5. 3. 1964 č. 40/1964 Sb. Občanského zákoníku ve vyhlášeném znění*

[5] *Zákon ze dne 29. dubna 1992 o ochraně osobních údajů v informačních systémech*

[6] *Úmluva Rady Evropy č. 108 ze dne 28. Ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat*, vyhlášená pod č. 115/2001 Sb. m. s.

[7] *Zákon ze dne 3. února 2012, občanský zákoník.*

[8] *Úplné znění Ústavního zákona České národní rady č. 1/1993 Sb., Ústava České republiky: Úplné znění Usnesení České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky ; některé další související právní předpisy*. Vydání: třinácté. Praha: Armex Publishing, 2018. Edice kapesních zákonů. ISBN 978-80-87451-55-7.

[9] *Zákon ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů*, č. 101/2000 Sb.

[10] *"Cameron 'uneasy' about use of injunctions".*, dostupné online*:* *https://www.bbc.co.uk/news/uk-13158087 BBC. 2 April 2011*.

[11] *Leigh, David (12 October 2009). "Guardian gagged from reporting Parliament". The Guardian. UK. Archived from the original on 28 March 2010. Retrieved 26 March 2010.* Dostupné online*:* *https://www.theguardian.com/media/2009/oct/12/guardian-gagged-from-reporting-parliament*

[12] *78-17 on Information Technology, Data Files and Civil Liberties*

[13] *Zákon o zpracování osobních údajů č. 110/2019 Sb.*

[14] Legitimate Interests Guidance *DPN* [online]. [cit. 2019-05-01]. Dostupné z: https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/

[15] Guidelines on Personal data breach notification under Regulation 2016/679. *Iapp* [online]. 2018 [cit. 2019-04-16]. Dostupné z: https://iapp.org/media/pdf/resource_center/WP29-Breach-notification_02-2018.pdf

[16] Backblaze Hard Drive Stats for 2018. *Blackbaze* [online]. [cit. 2019-04-30]. Dostupné z: https://www.backblaze.com/blog/hard-drive-stats-for-2018/

[17] *Verbatim: Digital Media Storage Solutions* [online]. [cit. 2019-04-30]. Dostupné z: https://www.verbatim.com/

[18] Object of Interest: The Flash Drive *The New Yorker* 2018-07-23. [cit. 2019-05-02] Dostupné také z: https://www.newyorker.com/tech/annals-of-technology/object-of-interest-the-flash-drive

[19] Microsoft declaration of conformity with GDPR *Microsoft* 2018 [cit. 2019-04-15] Dostupné také z: https://www.microsoft.com/en-us/trustcenter/default.aspx

[20] Google declaration of conformity with GDPR Google 2018 [cit. 2019-04-15] Dostupné také z: https://privacy.google.com/businesses/

[21] PECINOVSKÝ, Josef. *Archivace a komprimace dat: jak zálohovat data: jak komprivovat soubory WinRAR, WinZip, WinAce : Windows a nástroje komprese dat: jak archivovat data ve Windows*. Praha: Grada, 2003. Snadno a rychle (Grada). ISBN 80-247-0659-8.

[22] Zákon č. 235/2004 Sb. o dani z přidané hodnoty

[23] Zákona č. 586/1992 Sb. o daních z příjmů

[24] OECD (2018), *Revenue Statistics 2018*, OECD Publishing, Paris, https://doi.org/10.1787/rev_stats-2018-en.

[25] Tisková zpráva Hospodářské komory ČR. *Hospodářská komora ČR* [online]. Praha, 2017 [cit. 2019-04-01]. Dostupné z: https://www.komora.cz/tiskova_zprava/podnikatele-trapi-caste-zmeny-zakonu-i-vysoke-odvody-za-zamestnance-ukazal-pruzkum-hospodarske-komory/

[26] 10 years after the financial crisis. *JPMorgan* [online]. [cit. 2019-04-01]. Dostupné z: https://www.jpmorgan.com/global/research/10-years-after-crisis

[27] ČESKÝ STATISTICKÝ ÚŘAD. Tab. Zaměstnanost, nezaměstnanost v r. 2018. *Český statistický úřad* [online]. 01. 04. 2019. [cit. 2012-01-29]. Dostupné z: https://www.czso.cz/csu/czso/zamestnanost-a-nezamestnanost-podle-vysledku-vsps-ctvrtletni-udaje-4-ctvrtleti-2018

[28] BERNANKE, Ben S.; MISHKIN, Frederic S. Inflation targeting: a new framework for monetary policy?. *Journal of Economic perspectives*, 1997, 11.2: 97-116.

[29] ČESKÝ STATISTICKÝ ÚŘAD Tab. Míra inflace v r. 2018. *Český statistický úřad* [online]. 01. 04. 2019. [cit 25. 3. 2019]. Dostupné z: https://www.czso.cz/csu/czso/mira_inflace

[30] EUROSTAT *Population on 1st January by age, sex and type of projection* [online]. 2019 [cit. 2019-04-04]. Dostupné z: https://ec.europa.eu/eurostat/web/products-datasets/-/proj_15npms&lang=en

[31] SIMONS, Gary F.; FENNIG, Charles D. *Ethnologue: Languages of the World. Twentieth edition.* [online]. Dallas, Texas: SIL International, 2017 [cit. 2017-11-29]. Dostupné z: https://www.ethnologue.com/language/CES

[32] *SEDA Sustainable Economic Development Assessment Rankings* [online]. Boston, 2019 [cit. 2019-04-04]. Dostupné z: https://www.bcg.com/publications/interactives/seda-2018-guide.aspx.

[33] Education at a Glance. *OECD* [online]. 2018 [cit. 2019-04-04]. Dostupné z: https://read.oecd-ilibrary.org/education/education-at-a-glance-2018_eag-2018-en

[34] QS EECA University Rankings 2019. *QS EECA* [online]. [cit. 2019-04-04]. Dostupné z: https://www.topuniversities.com/university-rankings/eeca-rankings/2019

[35] ROSER Max, Hannah RITCHIE. *Technological Progress*. [online] [cit. 2019-05-02] OurWorldInData.org, Dostupné z: https://ourworldindata.org/technological-progress

[36] PETERS, Thomas J. a Robert H. WATERMAN. *Hledání dokonalosti*. Praha: Svoboda-Libertas, 1993. ISBN 80-205-0313-7.

[37] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[38] BUCHALCEVOVÁ, Alena. *Metodiky vývoje a údržby informačních systémů: kategorizace, agilní metodiky, vzory pro návrh metodiky*. Praha: Grada, 2005. Management v informační společnosti. ISBN 80-247-1075-7.

[39] *Metoda PERT* [online]. [cit. 2019-05-09]. Dostupné z: http://books.fs.vsb.cz/SystAnal/texty/26.htm

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK