**Univerzita Hradec Králové**

**Fakulta informatiky a managementu**

**Katedra informačních technologií**

Obor: Aplikovaná Informatika

**Technická opatření pro plnění GDPR**

BAKALÁŘSKÁ PRÁCE

Vypracoval: Leoš Karásek

Vedoucí: Mgr. Josef Horálek, Ph.D.

2017/2018

**Čestné prohlášení**

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Praze dne x. x. 2018 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Jméno a příjmení studenta

**Poděkování**

Děkuji Mgr. Josefu Horálkovi, Ph.D. za odborné vedení mé práce, věcné připomínky, dobré rady a vstřícnost při konzultacích a vypracovávání bakalářské práce.

Abstrakt

Cílem této práce je posouzení dopadů „*NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*“. Známe zejména jako směrnice „Evropské unie GDPR“. Na správce informačních systémů podniku, a možných technických opatření, vedoucích k naplnění této směrnice.

Povinnosti plynoucí z tohoto nařízení zasáhnout všechny podnikatelské i nepodnikatelské subjekty všech velikostí a napřič všemi obory. Práce si klade za cíl zorientovat se v nařízení GDPR a navrhnou možná technická opatření k nakládání s daty občanů EU vedoucích ke splnění podmínek plynoucích ze směrnice GDPR.

Hlavní přínos této práce spočívá v analýze směrnice a povinnosti z ní plynoucích. Následně v návrhu možných technických řešení ke splnění požadavků směrnice pro podnikatelské subjekty napříč obory.

Obsah

[1. Úvod 5](#_Toc502145461)

[2. Představení GDPR 5](#_Toc502145462)

[3. Analýza dopadových kritérií 5](#_Toc502145463)

[4. Analýza možných technických opatření 5](#_Toc502145464)

[5. Návrh a realizace tech. opatření 5](#_Toc502145465)

[6. Zhodnocení projektu 5](#_Toc502145466)

[7. Závěr 5](#_Toc502145467)

## Úvod

Dne 25. 5. 2018 vstoupí v platnost *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*“ dále GDPR. Známé spise jako nařízení GDRP.

Vzhledem ke stále se rozvíjející informační společnosti, se data o lidech stávají velmi žádaným a ceněním obchodním artiklem. Na druhou stranu tato data jsou osobní a velmi citlivá. Žádný subjekt by bez souhlasu dotyčného, anebo bez zákonné opory neměl taková data shromažďovat a využívat.

Jednotlivé státy Evropské unie tuto problematiku nejprve upravovali ve vlastních národních legislativách, nakonec se ale ukázala potřeba jednotné regulace této problematiky.

Historie

Přínosy obecně

Dopady obecně

## Představení GDPR

## Analýza dopadových kritérií

K analýze dopadových kritérii byla použita CS verze NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679.

V analýze nejsou řešeny různé výjimky a možnosti změkčení dopadu směrnice, které se většinou týkají státních či vědeckých institucí, nebo speciálních případu. Z výše uvedeného  tohoto dokumentu vyplývá, že nějaká technická opatření bude vhodné přijmout k naplnění souladu s následujícími články.

Technická dopadová kritéria vyplívají z následujících článků

**Článek 5 odstavec 1.**

písm. a**)** hovoří o zásadě „přesnosti“, to znamená, že organizace musí být schopna osobní údaje nějakým efektivním způsobem aktualizovat, mazat či opravovat a mít přehled jaké osobní údaje a u koho jsou vedeny. Organizace tedy budou muset vytvořit nějaký centrální nejlépe elektronický systém správy osobních údajů.

V písm. b) je organizacím dále ukládáno zpracovávat osobní údaje tak, aby byli náležitě zabezpečeny proti zneužití nebo ztrátou či poškozením tedy zásada „integrity“ a „důvěrnosti“ dat

**Článek 7.**

ukládá organizacím zejména povinnost být schopen prokázat, že subjekty údajů poskytly souhlas s uchováváním osobních údajů. Dále poskytovat a odvolávat souhlas musí být stejně snadné. V praxi to znamená vytvoření jednotného způsobu udělování a odvolávání souhlasu.

**Článek 8. odstavec 2.**

se týká, získává souhlasů se spravováním osobních údajů od dětí, tedy nezletilých osob. Dotčené organizace musí u osob mladších 16 let vyvinout přiměřené úsilí k ověření, zda osoba, která souhlas udělila, má rodičovskou zodpovědnost k dítěti. Tedy otázka je, co je to přiměřené úsilí. Při současném stavu technologii identifikace a neexistenci registrů obyvatelstva je nějaké automatické řešení zatím nereálné.

**Článek 11**

**Článek 12** řeší především informační povinnost organizace vůči subjektům údajů. Organizace je povinna poskytnou informace. Které jsou uvedeny ve článku 13 a 14 a dále informovat o právech subjektů dle článků 15 až 22. Organizace musí tyto informace zpřístupnit ve vhodné strukturované formě subjektu údajů. Dále bude vhodné informace uvedené v článcích 13 a 14 doplnit standardizovanými ikonami dle odstavce 7.

**Článek 15**

Projít směrnici a zamyslet se nad dopady

1. Databáze
2. Zálohy
3. Počítače zaměstnanců
4. Mobilní zařízení
5. BYOD zařízení

## Analýza možných technických opatření

Článek 32 směrnice GDPR říká

„1*.   S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:*

*a) pseudonymizace a šifrování osobních údajů;*

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

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

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

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

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

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

“ zdroj *Http://www.privacy-regulation.eu/cs/32.htm* [online]. [cit. 2018-01-19].

1. Databáze – šifrování, psedonymizace
2. Zálohy
3. počítače zaměstnanců – organizační opatření, směrnice, šifrování disků v počítačích, AntiThiev nástroje
4. Mobilní zařizení – MDM systémy, šifrování úložiště
5. BYOD - organizační opatření, směrnice, šifrování disků v počítačích, AntiThiev nástroje, Zákaz používání

## Návrh a realizace tech. Opatření

## Zhodnocení projektu

ddddddd

## Závěr

Dddddd

Seznam literatury:

Online:

*NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)* [online]. 27.4.2016 [cit. 2018-01-26]. Dostupné z: <http://eur-lex.europa.eu/eli/reg/2016/679/oj>

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