**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 se snaží zodpovědět otázku, která možná technická opatření bude vhodné, či dokonce nutné přijmout ke splnění požadavků směrnice. A dále také navrhnout jednu z možných cest jak takové technické řešení může vypadat

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 spíše 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.

## Představení GDPR

## Analýza dopadových kritérií

Při analýze dopadových kritérii byla použita CS verze NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679. stažena z <http://eur-lex.europa.eu> dne 19. 10. 2017.

Nejsou brány v potaz různé výjimky a možnosti změkčení dopadu směrnice, které se většinou týkají státních či vědeckých institucí, nebo speciálních případů.

Z výše uvedeného  tohoto dokumentu vyplývá, že určitá technická opatření bude vhodné přijmout k naplnění souladu s následujícími články.

**Kapitola II**

**Článek 5 odstavec 1.**

Hovoří především o zásadách zpracování osobních údajů. Hned v písm. a) je poukazováno na nutnost data zpracovávat korektně a zákonným způsobem. Osobní údaje musí být shromažďovány za jasně definovaným a legitimním účelem a dle písm. c) musí být také minimalizovány na nezbytný rozsah.

písm. d**)** hovoří o zásadě „přesnosti“, to znamená, že organizace musí být dále schopna osobní údaje nějakým efektivním způsobem aktualizovat, mazat či jinak spravovat a mít přehled jaké osobní údaje a u koho jsou vedeny.

V písm. f) je organizacím ukládáno zpracovávat osobní údaje tak, aby byli náležitě zabezpečeni proti zneužití nebo ztrátou či poškozením tedy zásada „integrity“ a „důvěrnosti“ dat. Tedy organizace jsou zodpovědné za data, která uchovávají.

Organizace budou muset mít jednoznačný přehled, jaké osobní údaje jsou kde uchovávány a za jakým účelem. Jedna z cest by mohlo být vytvoření nějakého centrálního, nejlépe elektronického, systému správy osobních údajů.

**Článek 7.**

ukládá organizacím, přesněji jmenovaným správcům v těchto organizacích, povinnost být schopen prokázat, že subjekty údajů poskytly souhlas s uchováváním osobních údajů jednoznačně, a bez jakýchkoli podmínek

Následné odvolání souhlasu musí být stejně snadné, jako jeho udělení.

V praxi by to mohlo znamenat vytvoření jednotného způsobu udělování a odvolávání souhlasu a centrální evidence takovýchto souhlasů. Ev. případně vytvoření takového workflow, kde oba tyto úkony budou splňovat výše uvedené požadavky.

**Článek 8.**

Se svým obsahem se týká udělování souhlasů nezletilými osobami

Především odstavec 2. může mít dopad na technická opatření v organizacích. Ukládá totiž organizacím vyvíjet přiměřené úsilí k ověření rodičovských práv u osob, které udělují souhlas se spravováním osobních údajů u osob mladších 16 let. Tady se nabízí otázka, co je to přiměřené úsilí. Při současném stavu technologii identifikace osob a veřejně nepřístupných registrů obyvatelstva se nějaké automatické řešení zatím zdá být nereálné.

**Článek 11**

**Kapitola III, oddíl 1**

**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.

Jedná se o jednoduchou informaci o právech a povinnostech stran. Zde by mohla pomoci jednoduchá www stránka s požadovanými informacemi.

**Oddíl 2**

**Článek 15**

Dává právo občanům na informace o tom, zda jsou jejich osobní údaje zpracovávaný, neboli nějakým způsobem využívány a dále právo vědět jaké osobní údaje jsou o nich vedeny a jak je s nimi nakládáno. Organizace tedy musí mýt především přehled, jaké údaje u dotyčných zpracovává a jak s nimi nakládá. V praxi tento článek bude organizace především nutit mít ve vedených osobních údajích pořádek a přehled.

**Oddíl 3**

**Článek 16**

Opravňuje občany požadovat opravu osobních údajů, pokud zjistí, že jsou jeho vedené osobní údaje nepřesné, nebo neúplné. Organizace tedy musí být opět schopny osobní údaje spravovat a jednoznačně identifikovat. Opět se zde dostáváme k nutnosti nějakého sytému pro správu osobních údajů.

**Článek 17**

„Právo být zapomenut“ ukládá v odstavci 1 organizacím povinnost, za definovaných podmínek, například v případě odvolání souhlasu občanem, tyto údaje bezodkladně vymazat. V odstavci 2. je dokonce přidána povinnost informovat ostatní organice, jimž tyto údaje zákonným způsobem poskytl, o tomto odvolání občanem.

Podobně jako článek 16 nutí článek 17 organizace mít perfektní přehled o uchovávaných osobních údajích napříč všemi jeho systémy a přidává navíc povinnost mít přehled také o jejich pohybu. Na druhou Článek 17 stanovuje i přesně definované podmínky, kdy se právo být zapomenut neuplatňuje. Avšak je to vždy víceméně pouze ve veřejném zájmu a v komerční.

**Článek 18**

„Právo na omezené zpracovaní.“ Omezené zpracování je definováno v článku 4 odstavec 4 jako označení osobních údajů za účelem omezení jejich budoucího zpracování. V podstatě to znamená, že od okamžiku takového označení osobních údajů občana, nesmějí být nadále jakkoliv využívány a jsou pouze u organizace uloženy. Odstavec 3 organizacím navíc ukládá informační povinnost vůči občanům při aplikaci takovéhoto omezení. V praxi bude nutné takové údaje označit příslušným parametrem a nadále s nimi podle toho nakládat.

**Článek 19**

Obecně oznamovací povinnost. Směrnice nám dává určité zákonné možnosti, jak osobní údaje předávat dál jiným organizacím. Nicméně nám z tohoto článku vyplývá povinnost takovéto organizace informovat o jakýchkoli změnách v osobních údajích provedených na základě článků 16, čl. 17 odst. 1 a článkem 18. Tedy organizace jsou povinny, za přiměřeného úsilí informovat své partnery o změnách v osobních údajích, odvolání souhlasu a omezení zpracování. K tomu budou muset mít zejména přehled o takových změnách a také o pohybu osobních údajů.

**Článek 20**

V podstatě dává právo občanům si vyžádat vedené osobní údaje v nějakém strukturovaném, běžně strojově čitelném formátu. V praxi by se mohlo jednat o jednoduchý export dat např. ve formátu CSV, XML ev. XLS.

**Oddíl 4**

Tento oddíl se dotýká automatizovaného individuálního rozhodování a práva vznést námitku

**Článek 21**

„Právo vznést námitku.“ Tento článek dává občanům právo kdykoliv na základě jejich aktuální situace vznést námitku proti zpracování jejich osobních údajů. Organizace je povinna zpracovaní ihned přerušit min. do doby, kdy prokáže závažné a oprávněné důvody ve zpracovávání pokračovat. Tento článek ve svém důsledku může znamenat povinnost přestat se zpracováním v podstatě on-line, pokud občan vznese námitku. Technické řešeni by mohlo být zavedení příslušného parametru k označení osobních údajů nebo například použitím vhodné coockie v případě www stránek.

**Článek 22**

Právo nebýt předmětem žádného rozhodování založeného výhradně na automatizovaném zpracovaní. Směrnice GDPR zavadí pojem „Profilovaní“. Jinými slovy se jedná o vyhodnocení chování člověka a úpravě nabízeného obsahu- Jedná se například o ‚Personalizaci‘ v případě www stránek. Nebo reklamní bannery „na míru“ uživateli. Navíc článek 22 implicitně ve svém znění předpokládá, že občan s profilovaným nesouhlasí! Organizace budou tedy nuceny nejprve souhlas s profilovaním od občanů získat. Tedy opět doplnit vedené osobní údaje o příslušný parametr. Ev. souhlas evidovat opět pomocí vhodných coockies v případě www stránek.

**Kapitola IV, Oddíl 1**

**Článek 24**

**Článek 25**

„Ochrana osobních údajů“ týká se technických opatření k zabezpečení osobních údajů. Organizace je plně zodpovědná za údaje, která shromažďuje a musí přijmout přiměřená opatření, která zabrání jejich ztrátě či zneužití. Organizace budou muset zmapovat, kde všude se s osobními údaji nakládá a jak jsou zabezpečeny. Dále budou muset učinit opatření k jejich ochraně. Jedná se např. o šifrování dat, pseudonymizaci ale i minimalizaci ukládaných údajů a taková opatření, aby k osobním údajům měli přístup pouze oprávnění uživatelé.

**Článek 30**

**Oddíl 2.**

**Článek 32**

„Zabezpečené zpracování” předepisuje organizacím zabezpečit zpracovávání osobních údajů tak, aby byly údaje stále dostupné, integritní a zabezpečené. Vysloveně nařizuje, za předpokladu vynaložení úměrného úsilí, osobní údaje psedonymizovat a šifrovat. Dále bude vhodné zabezpečit pravidelné zálohování dat, vysokou dostupnost, nástroje k ověřování integrity dat a uchování historie operací provedených nad osobními údaji např. některý z nástrojů SIEM.

**Článek 34**

**Článek 89**

## Analýza možných technických opatření

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.