|  |  |  |
| --- | --- | --- |
| **Univerzita Hradec Králové**  **Fakulta informatiky a managementu**  **Katedra informačních technologií** | | |
| **Technická opatření pro plnění GDPR**  (podtitul práce)  Bakalářská práce | | |
| Autor: Leoš Karásek  Studijní obor: Aplikovaná Informatika | | |
| Vedoucí práce: Mgr. Josef Horálek, Ph.D.  Odborný konzultant: Titul, jméno, příjmení  Pracoviště | | |
| Hradec Králové | leden 2018 | |
| Prohlášení:  Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury. | | | |
| V Hradci Králové dne 4.2.2018 | | *vlastnoruční podpis*  Leoš Karásek | |
| Poděkování:  Děkuji vedoucímu bakalářské práce, Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, věcné připomínky, dobré rady a vstřícnost při konzultacích a vypracovávání bakalářské práce. | | | |

Anotace

KARÁSEK, Leoš. *Technická opatření pro plnění GDPR.* Hradec Králové: Fakulta informatiky a managementu Univerzity Hradec Králové, 2007. 87 s. Bakalářská práce.

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 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 napřič obory.

Annotation

Title: Název práce v anglickém jazyce

Obsah

[1 Úvod 1](#_Toc505004467)

[2 Cíl práce 2](#_Toc505004468)

[3 Metodika zpracování 3](#_Toc505004469)

[4 Představení GDPR 4](#_Toc505004470)

[5 Analýza dopadových kritérií 4](#_Toc505004471)

[6 Analýza možných technických opatření 8](#_Toc505004472)

[7 Návrh a realizace tech. Opatření 9](#_Toc505004473)

[8 Zhodnocení projektu 9](#_Toc505004474)

[9 Závěr 9](#_Toc505004475)

[9.1 Podkapitola 9](#_Toc505004476)

[9.1.1 Podřazená podkapitola 9](#_Toc505004477)

[10 Shrnutí výsledků 11](#_Toc505004478)

[11 Závěry a doporučení 12](#_Toc505004479)

[12 Seznam použité literatury 13](#_Toc505004480)

[13 Přílohy 15](#_Toc505004481)

Seznam obrázků

[Obr. 1 Název obrázku/grafu/fotografie. 3](#_Toc348517265)

Seznam tabulek

[Tabulka 1 Název tabulky. 3](#_Toc348517268)

# 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

# Cíl práce

Smysl a účel, výzkumné otázky.

# Metodika zpracování

Cíle, hypotézy/ výzkumné otázky, způsob hledání odpovědí na výzkumné otázky včetně metodiky vlastního výzkumu/šetření, literární rešerše.

# 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 mít 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**

Po prostudování směrnice GDPR se dají dopadová kritéria stanovit takto:

1. Organizace jsou plně zodpovědné za osobní údaje, která uchovávají. Musí mít o nich dokonalý přehled a mít možnost je kdykoli spravovat
2. Organizace musí získávat a evidovat souhlasy se zpracováním osobních údajů a být schopna je doložit.
3. Občané mají právo na opravu osobních údajů, právo být zapomenut a právo na omezené zpracování. Tato práva musí organizace zajistit a garantovat.
4. Organizace má také informační povinnost vůči třetím stranám, kterým osobní údaje zákonným způsobem poskytla. Jedná se zejména o případy z bodu 3.
5. Organizace také zodpovídají za nepřetržitou důvěrnost, integritu a dostupnost systémů zpracovávajících osobní údaje.

Některé body jsou podmíněny vynaložením přiměřeného úsilí a nákladů. V praxi se však na tuto formulaci nedá spoléhat. Není definováno, co jsou to přiměřené náklady a nakonec vždy bude rozhodovat úřední moc.

# Analýza možných technických opatření

Celá směrnice GDPR nutí především organizace udělat si pořádek ve shromažďovaných osobních údajích a následně je zodpovědně zpravovat. Pokud však chtějí organizace data řádně zpravovat, musí nejprve mít přehled, kde a jaká data shromažďuje a ukládá.

## Pořádek v datech

Zmapování dat nejedná se doslova o technické opatření, nicméně bez důkladného zmapování kde a jaká data se nacházejí, se budou přílišná citlivá data těžko spravovat. Užitečné mohou být v tomto směru závěry GAP analýzy.

Gap analýza, tedy v podstatě analýza mezer, řeší dvě základní otázky. Kde jsme? A Kam chceme dojít? Kde jsme, z pohledu dat, záleží především na stávajícím vedení organizace a jejím důrazu či nedůrazu na dodržování elementárních zvyklostí a pravidel pro nakládání s daty. Výhodu mají ty organizace, které implementovali předchozí směrnici EU o ochraně osobních údajů ev. Požadavky zákona č. 101/200 sb. [2]

Jednoznačně zde tedy vzniká nutnost tuto, dost často neoblíbenou práci, udělat a často i ručně zmapovat, kde se jaké osobní údaje nacházejí a kdo k nim má přístup.

## Kontrola přístupových práv

Jedním ze znaků zodpovědného nakládání s daty v organizacích patři zásada minimálních práv. Tedy zaměstnanci mají, přistup k datům, která skutečně potřebují k plnění vlastních povinností, a přístup k ostatním datům je blokován. Pozornost je však potřeba věnovat taká administrátorům systémů. A to podle stejných zásad minimálních oprávnění.

SCAP pro identifikaci bezpečnostních hrozeb

Nástroje pro analýzu práv v AD

## Deduplikace dat

## Průběžný audit

**Centrálni správa**

Preferenční centrum?

**Bezpečnost dat**

Šifrování

Pseudoniminizace

Maskování sloupců

Zálohování

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

# Závěr

Seznam literatury:

Online:

[1] *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>

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

[3] OBERREITER, V. GUI nástroj na měření zranitelností systémů pomocí knihovny OpenSCAP [online]. Brno: Vysoké učení technické v Brně. Fakulta informačních technologií. 2011.

Vlastní řešení dokládá student zpravidla v několika kapitolách. Podle charakteru práce musí student uvážit, zda informace netextové povahy (data, tabulky, obrázky atd.) bude uvádět přímo v textu, nebo je zařadí až za celou práci ve formě příloh, či bude kombinovat oba způsoby.

Více podrobností viz Metodické pokyny pro vypracování bakalářských a diplomových prací (zveřejňované formou výnosů děkana) a v kurzu MES – Metodologický seminář.

## Podkapitola

Vlastní text práce.

Tabulka 1 Název tabulky.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Zdroj: citace zdroje, nebo autor, vlastní zpracování

### Podřazená podkapitola

Vlastní text práce.



Obr. 1 Název obrázku/grafu/fotografie.

Zdroj: citace zdroje, nebo autor, vlastní zpracování

# Shrnutí výsledků

Souhrn vlastních výsledků získaných v průběhu řešení problému.

# Závěry a doporučení

Kritická diskuze nad výsledky, ke kterým autor dospěl (soulad výsled-ků  literaturou či předpoklady; výsledky a okolnosti, které zvláště ovlivnily předkládanou práci atd.). Je vhodné naznačit i případné další (popř. alternativní) možnosti zkoumání dané problematiky a otevřené problémy pro další studium.

# Seznam použité literatury

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

1. PŘÍJMENÍ, Jméno. Název knihy : podnázev. Vydání. Místo vydání : Název nakladatelství, rok vydání. Počet stran. ISBN.
2. Název. Název odpovědné korporace, instituce. Roky vydání (od-do), ročník (od-do).Místo vydání : Název nakladatelství. Standardní číslo (ISSN).
3. Jméno autora. Název zdrojového dokumentu. Označení vydání. Číslo části.Místo vydání : Název nakladatelství, rok vydání. Rozsah díla. Standardní číslo. Lokaceve zdrojovém dokumentu.
4. Autor příspěvku. Název příspěvku. In Název zdrojového dokumentu. Primární odpovědnost (autor) za zdrojový dokument. Vydání. Místo vydání : Název nakladatelství, rok. Lokace ve zdrojovém dokumentu.
5. Autor. Název článku. Název seriálu, rok vydání, ročník, číslo, strany od-do.
6. PŘÍJMENÍ, Jméno autora. Název monografie nebo www stránky (tag "title") : podnázev [druh média]. Vydání. Místo vydání : Vydavatel, datum publikování, datum poslední revize [citováno dne]. <dostupnost - URL adresa>. Standardní číslo.
7. PŘÍJMENÍ, Jméno autora. Název zdrojového dokumentu [druh média]. Vydání. Místo vydání : Vydavatel, datum publikování, datum poslední revize [citováno dne]. Označení části nebo kapitoly. Název části nebo kapitoly. <dostupnost -URL adresa>. Standardní číslo.
8. PŘÍJMENÍ, Jméno autora příspěvku. Název příspěvku [druh média]. In Název zdrojového dokumentu. Vydání. Místo vydání : Vydavatel, datum publikování, datum poslední revize [citováno dne]. <dostupnost -URL adresa>. Standardní číslo.
9. Název konference nebo fóra [druh média]. Místo vydání : Vydavatel, datum vydání [citováno dne]. <dostupnost -URL adresa>.

# Přílohy

*Oskenované zadání práce*