VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

NEJČASTĚJI POUŽÍVANÉ RETENČNÍ DOBY V INFORMAČNÍCH SYSTÉMECH A JEJICH SOULAD S GDPR

THE MOST COMMONLY USED RETENTION PERIODS IN INFORMATION SYSTEMS AND THEIR COMPLIANCE WITH GDPR

ODBORNÁ PRÁCE

AUTOR PRÁCE — **AUGUSTIN MACHYŇÁK**
AUTHOR

CVIČÍCÍ — **Mgr. Ing. PAVEL OČENÁŠEK, Ph.D.**
INSTRUCTOR

BRNO 2022

Abstrakt

Tato práce se zabývá problematikou doby uchovávání dat v informačních systémech. Při řešení této otázky je kladen důraz na GDPR a jiné zákony týkající se zpracování osobních údajů. Retenční doba se totiž odvíjí od mnoha faktorů a bude odlišná v podstatě ve všech informačních systémech.

Abstract

This text deals with the issue of data retention in information systems. In addressing this issue, emphasis is placed on GDPR and other personal data processing laws. The retention time depends on many factors and will be different in virtually all information systems.

Klíčová slova

Retenční doba dat, informační systémy, GDPR

Keywords

Data retention, information systems, GDPR

Citace

MACHYŇÁK, Augustin. *Nejčastěji používané retenční doby v informačních systémech a jejich soulad s GDPR*. Brno, 2022. Odborná práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Cvičící Mgr. Ing. Pavel Očenášek, Ph.D.

Nejčastěji používané retenční doby v informačních systémech a jejich soulad s GDPR

Prohlášení

Prohlašuji, že jsem tuto odbornou práci vypracoval samostatně. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Augustin Machyňák
26. dubna 2022

Obsah

Kapitola 1

Úvod

Tato odborná práce se zabývá problematikou doby uchovávání dat v informačních systémech. Důvodů k uchovávání dat může být velké množství, avšak důvodů k jejich vymazání příliš není. V dnešní době je možné uchovávat osobní údaje o velkém množství uživatelů bez toho, aniž by bylo nutné se obávat nedostupnosti úložných prostorů. Uchovávání těchto dat však představuje bezpečnostní riziko. K únikům osobních dat nedochází příliš často, ale když k tomu dojde, následky můžou být velmi nepříjemné. Není možné vytvořit informační systém, který bude odolný vůči jakémukoliv (efektivnímu) útoku, který by mohl vést k úniku osobních údajů, protože vždy bude existovat ta největší zranitelnost pro systém - člověk. Z (nejen) tohoto důvodu je nutné se těchto dat pravidelně zbavovat a o tomto tato odborná práce pojednává.

Práce je rozdělena na 5 kapitol. Kapitola 2 se zabývá pojmem retenční doba obecně. Kapitola 3 pojednává o GDPR a proč je nutné ho brát v potaz pro nalezení nejčastěji používaných retenčních dob. V kapitole 4 jsou probrány některá omezení pro zpracování osobních údajů pro státy mimo EU, které mají vliv na retenční dobu. Na konec kapitola 5 obsahuje krátké shrnutí této práce a dosažených výsledků.

Kapitola 2

Retenční doba

Retenční dobou rozumíme dobu, po kterou budou data v informačním systému (dále jen IS) uchovávána. Obecně není možné říci, jaká retenční doba je nejčastěji používána, jelikož tyto doby můžou být různé v každém IS.

Retenční doba se může lišit například podle [1]:

- Osoby, o které jsou data uchovávána (uživatel IS, zaměstnanec, ...)
- Typu dat (daňové záznamy, záznamy o úrazech na pracovišti, ...)
- Státu (vyžadováno zákony apod.)
- ...

Na základě typu údaje je rozhodnuto, jaká bude jejich retenční doba, což není však pravidlem. Důvodem, proč je dobré tyto data rozdělit dle jejich účelu, je to, aby bylo dodrženo GDPR.

Kapitola 3

Retenční doba a GDPR

Následující sekce čerpají a interpretují informace z [2], které byly považovány za podstatné k úvodu do problematiky. Informace uvedené v { } odkazují na jednotlivé pasáže v tomto dokumentu.

3.1 GDPR

GDPR (*General Data Protection Regulation*) je nařízení Evropského parlamentu (dále jen nařízení), jehož účelem je ochrana fyzických osob v souvislosti se zpracováním osobních údajů. Nařízení mimo jiné definuje i důvody k jeho zavedení, subjekty, na které se vztahuje a jeho cíle. Důvodem k zavedení jsou výzvy, které s sebou přinesl rychlý technologický rozvoj a globalizace {(6)}, což vyžaduje pevný a soudržnější rámec pro ochranu osobních údajů v (Evropské) Unii, jenž by se opíral o důsledné vymáhání práva, a to s ohledem na nezbytnost nastolit důvěru {(7)}. Ochrana poskytována nařízením by se měla týkat zpracování osobních údajů fyzických osob bez ohledu na jejich státní příslušnost nebo bydliště {(14)}.

3.2 Vliv GDPR na retenční dobu

Nařízení mimo jiné omezuje dobu, po kterou je možné uchovávat osobní údaje následovně {Článek 5, 1.e)}:

Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů ***po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány****; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);*

Dále má vliv na retenční dobu {Článek 15, 1.e)}:

Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má (...) (právo) ***požadovat od správce opravu nebo výmaz osobních údajů*** *týkajících se subjektu údajů nebo omezení jejich zpracování a nebo vznést námitku proti tomuto zpracování;*

Tento článek následně doplňuje Článek 17 - Právo na výmaz ("právo být zapomenut"), který udává, ve kterých případech má subjekt právo k vymazání osobních údajů.

Z těchto článků je zřejmé, že osobní údaje je možné ukládat pouze po dobu nezbytně nutnou nebo dokud subjekt údajů nepožádá o jejich vymazání. Otázkou tedy zůstává, jak dlouhá doba je *nezbytně nutná doba*. Odpověď závisí na množství faktorů - subjektu, typu dat, aj. (viz Kapitola 1). Je nutné také brát v úvahu zákony země, ve které osoba zodpovědná za zpracování údajů působí. Pokud zákon stanoví, že konkrétní údaj je nutné mít uložen pouze po určitou dobu, tak je možné předpokládat, že tato doba odpovídá *nezbytně nutné době* a po této době je tedy nutné údaj vymazat pro dodržení GDPR.

V nařízení není nikde zmíněno, že by správce (osoba zodpovědná za zpracování osobních údajů) byl povinen zveřejňovat konkrétní dobu, po kterou budou data uchovávána.

Kapitola 4

Retenční doba v zemích mimo EU

Problematika se stává komplikovanější, jakmile se na ní podíváme v celosvětovém měřítku. Státy regulují a upravují retenční dobu dle svých potřeb, například:

- Austrálie - poskytovatelé telefonních služeb musí uchovávat určité metadata o uživatelích po dobu 2 let [6](187C(1)(a)(ii))
- Rusko - upravuje [5](Ch.2, Art.5, 7.). Stejně jako u GDPR můžou být osobní údaje uchovávány pouze po nezbytně nutnou dobu, avšak pouze v případě, že není dáno jinak jinými federálními zákony.
- Čína - upravuje CSL (Cybersecurity Law), PIPL (Personal Information Protection Law) a DSL (Data Security Law). Dle autorů [4](7.7) je však retenční doba dána stejná jako u GDPR.
- USA - nemá žádné omezení týkající se doby zpracování osobních údajů. Pro státní podniky upravuje FISMA (Federal Information Security Modernization Act). Pro finanční instituce BSA (Bank Secretary Act), který vyžaduje retenční dobu 5 let. [3]

Kapitola 5

Závěr

Je zřejmé, že nejčastěji používané retenční doby v IS nelze přímo určit - není jednotná. Odpověď může záviset například na:

- Zemi působnosti - zákony upravují retenční doby různě
- Instituci - pro státní instituce můžou být retenční doby velmi odlišné
- Typu dat - například osobní údaje můžou být uloženy po kratší dobu než daňové záznamy
- Subjektu - například data o zaměstnancích internetového obchodu budou pravděpodobně uchovávána delší dobu než data o návštěvnících stránky
- Oblast podnikání - stejný typ dat může být uložen po jinou dobu
- Vnitřních předpisech

Kritérií může být samozřejmě i více. Pokud se podíváme na všechny tyto kritéria, dle kterých je možné určit retenční dobu, tak je zřejmé, proč bylo dospěno k tomuto závěru.

Literatura

[1] Dunne, B. *How long should you retain your employee data under GDPR?* [online]. 2018 [cit. 2022-04-24]. Dostupné z: https://www.siliconrepublic.com/enterprise/gdpr-data-retention.

[2] Evropský parlament a Rada Evropské unie. *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016* [online]. 2016 [cit. 2022-04-24]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679.

[3] FFIEC Bank Secrecy Act/Anti-Money Laundering InfoBase. *BSA/AML MANUAL* [online]. 2021 [cit. 2022-04-24]. Dostupné z: https://bsaaml.ffiec.gov/manual/Appendices/17.

[4] Luo, D. a Wang, Y. *China - Data Protection Overview* [online]. 2021 [cit. 2022-04-24]. Dostupné z: https://www.dataguidance.com/notes/china-data-protection-overview.

[5] Rada federace. *Federal Law of 27 July 2006 N 152-FZ ON PERSONAL DATA* [online]. 2006 [cit. 2022-04-24]. Dostupné z: https://pd.rkn.gov.ru/docs/Federal_Law_On_personal_data.doc.

[6] The Parliament of Australia. *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* [online]. 2015 [cit. 2022-04-24]. Dostupné z: https://www.legislation.gov.au/Details/C2015A00039.