



Český model
amerického kongresu

Ochrana osobních údajů v USA po vzoru GDPR

Zpráva Výzkumné služby Kongresu

Simona Petruž



1 Úvod

V dnešním světě o nás mohou moderní technologie shromažďovat velké množství informací – od oblíbené hudby přes polohu až po naše osobní vize a hodnoty vyjádřené skrze obsah, který na sítích konzumujeme. Osobní údaje jsou odrazem naší osobní identity¹ a v dnešním světě mají **vysokou cenu**: s jejich pomocí lze totiž efektivně prodat produkt, ale i vyhrát volby.² Zájmy subjektů, které osobní údaje shromažďují a dále využívají, přitom nemusí být vždy v souladu se zájmem společnosti jako celku. Málo regulovaná manipulace s osobními daty, jejich prodej a zneužívání často probíhá **bez nejmenšího tušení lidí, kteří jsou jejich nositeli**.³

Události posledních několika let ukázaly, že obava ze závažného zneužití osobních údajů není pouze hypotetická. Manipulace s osobními údaji může být **nebezpečná jak pro jednotlivce**, jejichž osobní údaje jsou zneužívány, **tak pro společnost jako celek** – prostřednictvím cílené manipulace lze šířit propagandu či fake news tak, aby se dostala k těm nejnáchylnějším jedincům a vyvolala ve společnosti určitou náladu. Nejen z těchto důvodů bylo na půdě Evropské unie schváleno Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation – GDPR), kterým se nyní chce inspirovat i americký Kongres.

1.1 Základní informace o osobních údajích

Osobní údaje jsou definovány různě, a to i v rámci Spojených států amerických. Federální obchodní komise (Federal Trade Commission) považuje za osobní údaj **každou informaci, která může být přiměřeně použita pro rozpoznání nebo kontaktování osoby**, včetně IP adres a identifikačních kódů.⁴ Právní systém každého státu v rámci federace však má osobní údaj definovaný jinak.

Dle evropské legislativy lze za osobní údaj považovat jakoukoliv informaci, která umožňuje identifikovat konkrétní fyzickou osobu.^{5 6} Při určování toho, co je a co není osobní údaj, se přitom často pohybujeme na tenkém ledě, protože **záleží na kontextu**, v jakém je údaj uveden a množství a charakter dalších

¹ Proč potřebuje Evropa lepší ochranu osobních dat. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>.

² Cambridge Analytica: Facebook row firm boss suspended. BBC [online]. [cit. 2019-01-08]. Dostupné z: <https://www.bbc.com/news/uk-43480048>.

³ GDPR se blíží, ale veřejnost se ochranou osobních údajů příliš netrápí. *Ekonomický deník* [online]. [cit. 2019-01-08]. Dostupné z: <http://ekonomicky-denik.cz/gdpr-se-blizi-ale-verejnost-se-ochranou-osobnich-udaju-prilis-netrapi/>.

⁴ Data protection laws of the world. *Definition of personal data - United States* [online]. [cit. 2018-12-30]. Dostupné z: <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US>.

⁵ What is personal data? European Commission [online]. [cit. 2018-12-26]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.

⁶ Jste připraveni na GDPR? Kropáček LEGAL, advokátní kancelář [online]. [cit. 2018-12-26]. Dostupné z: <https://pravopropodnikatele.cz/jste-pripraveni-na-gdpr/>.



informací, které mají potenciál původní údaj konkretizovat.⁷ Platí, že např. pouze na základě adresy nelze identifikovat konkrétního člověka, pokud na této adrese žije více lidí. Pokud však víme adresu a zároveň i jméno, již se o osobní údaj jedná.

Mezi nejtypičtější osobní údaje ve většině právních systémů patří jméno a příjmení, datum narození, adresa, rodné číslo, telefonní číslo nebo třeba e-mailová adresa.⁸

Ochraně osobních údajů se v poslední době dostává velké pozornosti zejména z toho důvodu, že jsou **čím dál snadněji zneužitelné**. Tzv. chytrá zařízení uloží nejen ty osobní údaje, které jim jejich uživatel poskytne dobrovolným zadáním do systému, ale i ty, které o svém uživateli zjistí, např. prostřednictvím určování polohy, vyhledávání na internetu a mnoha dalších nástrojů.⁹

1.2 Zneužívání osobních údajů – kauza Cambridge Analytica

V dnešní době jsou **online ukládány a v reálném čase analyzovány** údaje o chování, poloze, zájmech, vztazích velké části světové populace.¹⁰ Bohatým zdrojem informací o svých uživateli se stávají zejména smartphony, ale i notebooky, tablety, chytré hodinky, fitness náramky a další. Údaje o každodenním životě uživatele potom nemíří pouze do Googlu či Applu a poskytovatelům různých aplikací, ale zároveň do **mnoha partnerských společností**.¹¹

Nejznámější kauzou v nedávné době se stalo **zneužívání osobních údajů společností Cambridge Analytica**, díky níž dle jejich vlastních slov **vyhrál Donald Trump v roce 2016 americké prezidentské volby**.¹² Fungování firmy bylo založeno na tom, že si na základě psychologického testu zprofilovala každého dospělého Američana na Facebooku,¹³ a to podle míry jeho otevřenosti, pečlivosti, extravertizace, ochoty a neuroticismu, čímž Cambridge Analytica získala velice dobrý přehled o osobnosti většiny jednotlivců.

⁷ Co je, co není a co bude osobní údaj podle GDPR. Frank Bold Advokáti [online]. [cit. 2018-12-25]. Dostupné z: <https://www.fbadvokati.cz/cs/clanky/541-co-je-co-neni-a-co-bude-osobni-udaj-podle-gdpr>.

⁸ Tamtéž.

⁹ How safe is your personal data collected by your smart devices? The Business Times [online]. [cit. 2018-12-25]. Dostupné z: www.businesstimes.com.sg/opinion/how-safe-is-your-personal-data-collected-by-your-smart-devices.

¹⁰ Corporate Surveillance in Everyday Life. Cracked Labs [online]. [cit. 2018-12-26]. Dostupné z: <https://crackedlabs.org/en/corporate-surveillance>.

¹¹ CHRISTL, Wolfie. How companies use personal data against people. Cracked Labs [online]. [cit. 2018-12-26]. Dostupné z: https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf.

¹² BBC: Facebook data: How it was used by Cambridge Analytica [online]. [cit. 2018-12-30]. Dostupné z: <https://www.bbc.com/news/av/technology-43674480/facebook-data-how-it-was-used-by-cambridge-analytica>.

¹³ Tamtéž.



Jak je to možné? **Jen prostřednictvím „lajkování“ příspěvků na Facebooku lze zjistit typ osobnosti velice přesně** – průměrně stačí 10 lajků u různých příspěvků, aby algoritmy určily osobnost člověka lépe než jeho kolegové, 150 lajků pro poznání člověka lépe než jeho vlastní rodiče a 300 lajků, aby znaly člověka lépe než jeho životní partner.¹⁴

Jakmile Cambridge Analytica sesbírala tyto údaje, **vytvořila pro každý typ osobnosti jiný druh reklamy tak, aby reklamy vždy nejvíce apelovaly na to, co je danému člověku blízké**. Takto cílená reklama má potom na jednotlivce zákonitě **větší dopad** než obecné sdělení adresované všem a může tak přerůst v manipulaci.

Výše zmíněné jednání by nebylo nelegální, pokud by Cambridge Analytica pracovala s údaji získanými legálně, což se nedělo. Aplikace, jejichž prostřednictvím společnost osobní údaje nasbírala, požadovaly po svých uživateli **poskytnutí souhlasu s uložením osobních údajů, ovšem nejenom jejich, ale i všech jejich přátel na Facebooku**.¹⁵ K poskytnutí takového souhlasu přirozeně neměli daní lidé právo. Cambridge Analytica se však takto dostala ke statusům, lajkům, ale v některých případech i soukromým zprávám velice širokého spektra lidí, a to **bez souhlasu drtivé většiny z nich**.¹⁶

2 Osobní údaje v USA

Ve Spojených státech **neexistuje na federální úrovni žádný zákon**, který by jednotně upravoval ochranu osobních údajů. Úprava této problematiky tak zůstává rozkouskovaná v různých federálních, ale především státních zákonech, které si navíc někdy protiřečí.¹⁷ Federální zákony potom upravují problematiku **pouze částečně**, např. pouze ohledně jedné kategorie osobních údajů (finanční, zdravotní elektronické atp.) nebo ohledně jedné aktivity (zasílání marketingových e-mailů).¹⁸

Mezi zákony upravující dílčí problematiku v oblasti ochrany osobních údajů se řadí: The Federal Trade Commission Act (1914), The Financial Services Modernization Act (1999), The Health Insurance Portability and Accountability Act (1996) či the Privacy Act (1974). Zákonů, které se lehce celé problematiky dotýkají, je více, uvedený seznam slouží jako **ukázka toho, že osobní údaje jsou na federální úrovni v USA řešeny opravdu spíše vágně**, naopak neslouží jako komplexní výčet úpravy osobních údajů v USA. Bližší informace a další zákony lze případně nalézt [zde](#).

¹⁴ Tamtéž.

¹⁵ What is Cambridge Analytica scandal? YouTube [online]. [cit. 2019-01-08]. Dostupné z: <https://www.youtube.com/watch?v=Q91nvbJSmS4>.

¹⁶ Tamtéž.

¹⁷ Data protection in the United States. *Practical law* [online]. [cit. 2018-12-31]. Dostupné z: [https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhpc=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhpc=1).

¹⁸ Tamtéž.



2.1 The Federal Trade Commission Act (FTCA)

Zákon z roku 1914 byl přijat za účelem ochrany spotřebitele před nekalými praktikami obchodních a jiných společností.¹⁹ Mimo jiné se zde věnuje **nakládání firem s osobními údaji spotřebitelů** a obsahuje sankce za jejich nedodržování, a to zejména ve vztahu ke klamavým praktikám, ale také ke sledování chování spotřebitelů na internetu a související problematice²⁰ (např. mířené reklamě). Zákon také ustanovil Federální obchodní komisi, která na jeho dodržování dohlíží.

2.2 The Financial Services Modernization Act (GLB)

GLB byl přijat v roce 1999 a jeho primárním cílem je odstranění překážek a zastaralých pravidel v oblasti poskytování finančních služeb.²¹ Oblasti osobních údajů se věnuje spíše okrajově – stanovuje přísnější **pravidla pro zveřejňování soukromých informací fyzických osob** v souvislosti s poskytováním finančních služeb a také dává těmto osobám nástroje, jak se proti zveřejňování svých údajů bránit.²²

2.3 The Health Insurance Portability and Accountability Act (HIPAA)

Cílem tohoto zákona z roku 1996 je usnadnit lidem přístup ke zdravotnímu pojištění a zajistit bezpečnost jejich osobních údajů v souvislosti se zdravotnictvím.²³ Vztahuje se na zdravotnická zařízení, lékárny, poskytovatele zdravotního pojištění a další subjekty schraňující osobní údaje z oblasti zdravotnictví. Nastavuje **zvláštní ochranu pro údaje týkající se zdraví**, konkrétně jejich zpracování a nakládání s nimi.²⁴

¹⁹ What is the Federal Trade Commission Act (FTCA)?. *Business Law* [online]. [cit. 2019-01-01]. Dostupné z: https://business-law.freeadvice.com/business-law/trade_regulation/federal_trade.htm.

²⁰ Data protection in the United States. *Practical law* [online]. [cit. 2018-12-31]. Dostupné z: [https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1).

²¹ Financial Services Modernization Act of 1999. *Investopedia* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.investopedia.com/terms/f/financial-services-act-of-1999.asp>.

²² Data protection in the United States. *Practical law* [online]. [cit. 2018-12-31]. Dostupné z: [https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1).

²³ HIPAA: Health Insurance Portability and Accountability Act. *University of Pittsburgh* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.dental.pitt.edu/hipaa-health-insurance-portability-and-accountability-act>.

²⁴ Data protection in the United States. *Practical law* [online]. [cit. 2018-12-31]. Dostupné z: [https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1).



HIPAA byl v roce 2013²⁵ novelizován prostřednictvím tzv. „HIPAA Omnibus Rule“, který práva pacientů a dalších subjektů osobních údajů v oblasti osobních údajů v souvislosti se zdravotnictvím ještě **posílil a nastavil vyšší standardy pro zabezpečení těchto osobních údajů**.²⁶

2.4 The Privacy Act

The Privacy Act z roku 1974 se nejvíce blíží komplexnější úpravě ochrany osobních údajů na federální úrovni. **Obsahuje pravidla pro shromažďování, ukládání, manipulaci a šíření osobních údajů**, nicméně se týká **pouze záznamových systémů federálních institucí**.²⁷ Není tak aplikovatelný např. pro firmy, společnosti či školy.

Zákon zakazuje odhalování osobních informací z Federálního registru bez **písemného souhlasu** jedince, pokud není naplněna jedna (nebo více) z 12 výjimek.²⁸ Navíc dává jedincům právo a **možnosti přístupu** k údajům, které jsou o nich v Registru shromažďovány.²⁹

3 GDPR: Inspirace evropským nařízením

Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation – GDPR) je nařízení Evropské unie s účinností od 25. května 2018.³⁰ GDPR je dosud **nejucelenějším souborem pravidel v oblasti ochrany osobních údajů na světě**.³¹

3.1 Důvody přijetí GDPR

Důvody, které vedly státy Evropské unie k přijetí GDPR, mohou být v mnohém relevantní i pro Spojené státy americké. GDPR ve své preambuli uvádí 173 bodů, které jeho přijetí odůvodňují, nicméně hlavní tři příčiny by se daly shrnout následovně.

²⁵ What You Need to Know about the HIPAA Omnibus Rule. AAOS [online]. [cit. 2019-01-01]. Dostupné z: <https://www.aaos.org/AAOSNow/2013/Jul/managing/managing4/?ssopc=1>.

²⁶ HIPAA (Health Insurance Portability and Accountability Act). *SearchHealthIT* [online]. [cit. 2019-01-01]. Dostupné z: <https://searchhealthit.techtarget.com/definition/HIPAA>.

²⁷ Privacy Act of 1974. *The United States Department of Justice* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.justice.gov/opcl/privacy-act-1974>.

²⁸ Tamtéž.

²⁹ Tamtéž.

³⁰ 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). Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=CS>.

³¹ Co je GDPR a jak bude aplikováno v Česku. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>.



1. **Automatizované zpracovávání osobních údajů** ³² – s novými technologiemi dřívější předpisy o ochraně osobních dat nemohly počítat;
2. **Shromažďování osobních údajů občanů EU tajnými službami jiných států** ³³ – GDPR má za úkol stanovit standard, hranici legality a vyslat jasný signál o úrovni ochrany osobních údajů v Evropě;
3. **Rozšíření povědomí o problematice** ³⁴ – běžní občané nejsou o celé problematice dostatečně informováni, a to ani přes její vysokou relevantnost pro každého. Svůj podíl na tom měla i bagatelizace ze strany těch, kteří osobní údaje shromažďují.

3.2 Stručný obsah GDPR

GDPR stanovuje pravidla pro **každého, kdo shromažďuje, zpracovává nebo jinak nakládá s osobními údaji v rámci Evropské unie**.³⁵ Jedná se tedy o ty firmy, instituce a další subjekty, které mají sídlo v Evropské unii a o ty, které ač mají sídlo mimo EU, nakládají s osobními údaji občanů Evropské unie.³⁶ Pokud by např. asijská firma operovala jak na asijském, tak na evropském trhu, musela by pravidla GDPR aplikovat pouze na svoje evropské zákazníky. Pokud by ovšem evropská firma operovala v Evropě i Asii, GDPR pravidla by musela aplikovat na všechny zákazníky.

Osobními údaji jsou podle GDPR **veškeré informace o identifikované nebo identifikovatelné fyzické osobě**.³⁷ Jsou to tedy informace, **se kterými lze samostatně anebo společně určit jednu konkrétní osobu** (tzv. subjekt osobních údajů). GDPR výslovně stanovuje jako osobní údaj IP adresu nebo tzv. cookies.³⁸ GDPR klade důraz na to, aby konkrétní **správci osobních údajů** (správci osobních údajů jsou subjekty, které určují účely a prostředky zpracování osobních údajů – např. e-shop, kterému sdělíme osobní údaje za účelem nákupu) získávali, ukládali a **pracovali pouze s těmi osobními údaji, které jsou pro ně třeba** (např. aby nepožadovali po svých zákaznících pro nákup naprosto irelevantní číslo občanského průkazu). Také stanovuje přísnější pravidla pro předávání osobních údajů správci **zpracovatelům** (zpracovatelé jsou subjekty, které nakládají s osobními údaji pro účely správce – v případě e-shopu by to byl např. dopravce).

³² Proč potřebuje Evropa lepší ochranu osobních dat. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>.

³³ Tamtéž.

³⁴ Tamtéž.

³⁵ *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*. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=CS>.

³⁶ Tamtéž.

³⁷ Tamtéž.

³⁸ Jaké zásadní změny GDPR přinese. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.gdpr.cz/gdpr/zmeny/>.



Správce či zpracovatel musí mít vždy **právní titul pro zpracování** (zpracováním se rozumí jakákoliv operace s osobními údaji) osobních údajů – těmi nejobvyklejšími jsou **splnění smlouvy** (např. v případě e-shopu), **splnění zákonných povinností** (např. pokud zákon nařizuje po určitou dobu uchovávat jména zákazníků), **výslovný souhlas** subjektu osobních údajů (souhlas se zasíláním reklamních sdělení na e-mail) a **veřejný zájem** (sem lze zahrnout přiměřené nakládání s osobními údaji v souvislosti s prací novinářů – zveřejňování fotografií v médiích, články o osobnostech atp.).

Zvláštní kategorií dle GDPR jsou tzv. **citlivé osobní údaje**, kterým nařízení uznává **vyšší ochranu** než běžným osobním údajům. Mezi citlivé osobní údaje patří např. údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení.^{39 40} **Patří sem ale také veškeré údaje dětí, dále genetické a biometrické údaje** (snímek obličeje, otisk prstu).

Běžné osobní údaje	Citlivé osobní údaje	Nejsou osobními údaji
Jméno a příjmení	Zdravotní stav	Údaje o zemřelých osobách
Datum narození	Údaje o rase a původu	Anonymizované údaje
Zaměstnání	Fotografie či video	

Tabulka č. 1: příklady kategorií osobních údajů dle GDPR

Subjekty osobních údajů by měly být ze strany správců řádně **informovány** o svých právech v souvislosti s osobními údaji,⁴¹ ale i např. jakým způsobem jsou jejich osobní údaje zpracovávány a kterým zpracovatelům jsou předávány. Dále mají také tzv. **právo být zapomenut**⁴² – možnost požádat o úplné vymazání osobních údajů, v čemž je dotýčný správce či zpracovatel povinen vyhovět, pokud mu v tom nebrání jiný zákonný důvod (např. povinnost uchovávat jména zákazníků).

GDPR také klade zvýšené požadavky na **zabezpečení osobních údajů**. Důležitým ustanovením nařízení je také povinnost **nahlásit do 72 hodin od zjištění** příslušnému úřadu (v ČR Úřadu pro

³⁹ Tamtéž.

⁴⁰ Co považuje GDPR za osobní údaje. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>.

⁴¹ Jaké zásadní změny GDPR přinese. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.gdpr.cz/gdpr/zmeny/>.

⁴² Tamtéž.



ochranu osobních údajů) **narušení bezpečnosti údajů**, což je snaha o předcházení zatajování velkých úniků osobních údajů, které v minulosti vyšly najevo i s několikaletým zpožděním.⁴³

Důležitým institutem je dále **Pověřenec pro ochranu osobních údajů** (Data Protection Officer – DPO), kterého musí někteří správci a zpracovatelé jmenovat⁴⁴ (zejm. jedná-li se o veřejnou instituci nebo probíhá-li zpracování osobních údajů ve velkém rozsahu⁴⁵). Tento pověřenec má za úkol monitorovat faktické nakládání s osobními údaji a posuzovat zda-li probíhá v souladu s GDPR a poskytovat poradenství.

GDPR však obsahuje mnoho dalších práv a povinností v souvislosti s ochranou osobních údajů. **Za jejich nedodržování potom stanovuje opravdu vysoké pokuty** – maximální částkou je 20.000.000 eur nebo 4 % z celkového ročního obrátu společnosti (vyšší z obou možností). GDPR se **nevztahuje na osobní údaje zemřelých osob, anonymizované údaje a údaje nabyté při neobchodním a neinstitucionálním styku** (pokud si např. kamarádi vymění svoje čísla).⁴⁶

3.3 Výhody a nevýhody nařízení

Pravděpodobně největší nevýhodou Obecného nařízení o ochraně osobních údajů jsou podstatně **zvýšené náklady na administraci**.⁴⁷ Pokud správci či zpracovatelé zpracovávají osobní údaje na základě souhlasu, musí být schopni tyto souhlasy doložit, správci a zpracovatelé musí v souladu s GDPR správně informovat o osobních údajích nejen zákazníky, ale např. i svoje zaměstnance.

Jednoznačnou nevýhodou je také **velké množství nových povinností** naráz, ve kterých se mnoho správců a zpracovatelů (např. malé firmy) nedokáže samo zorientovat a musí vynakládat náklady na právní či jiné poradenství. Naplňování všech povinností může být zejména pro malé a střední firmy finančně, časově i administrativně nákladným úkolem, a přitom u nich ve většině případů velké ohrožení osobních údajů nehrozí.

Jako u většiny zákonů, i zde platí, že velké firmy (kde jsou osobní údaje nejvíce ohrožovány), obzvláště Google či Facebook, na které bylo nařízení prvotně mířeno, **dokáží pravidla všemožně obcházet**, případně získat od svých uživatelů souhlasy se zpracováním pro nejrůznější účely aniž by si je dotyční vůbec přečetli.

⁴³ Tamtéž.

⁴⁴ DPO čili Pověřenec pro ochranu osobních údajů. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.gdpr.cz/gdpr/dpo/>.

⁴⁵ Tamtéž.

⁴⁶ Co považuje GDPR za osobní údaje. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>.

⁴⁷ Jaké zásadní změny GDPR přinese. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.gdpr.cz/gdpr/zmeny/>.



Naopak mezi výhody patří mnoho z již zmiňovaného – povinnost ohlásit úniky osobních dat do 72 hodin, lepší zabezpečení, vyšší informovanost subjektů osobních údajů, jejich práva na získání osobních údajů, které jsou o nich zpracovávány a právo na jejich výmaz. GDPR však také přesněji vymezuje, co jsou osobní údaje (nově mezi ně zahrnuje e-mail, IP adresu či cookies), stanovuje vyšší standard jejich ochrany a vyděluje ty, které si zaslouží ještě zvláštní ochranu (citlivé osobní údaje).

Kromě dlouhodobých změn v nakládání s osobními údaji, které jsou spíše abstraktního charakteru může být očividné a okamžité zlepšení kvality života obyvatel EU alespoň částečná eliminace různých nevyžádaných obchodních sdělení mající příčinu v nekontrolovaných prodejkách databází dat.⁴⁸ Od GDPR se také očekává **zvýšení informovanosti občanů Evropské unie**, kteří často svá práva v souvislosti s osobními údaji neznali.

Velkým pozitivem je také prostřednictvím GDPR zavedené **právo na přenositelnost údajů**, které dává subjektům osobních údajů právo na **převedení osobních údajů, pokud změní poskytovatele služeb** – např. při přechodu k nové bance tedy subjekt osobních údajů již nemusí vyplňovat nové formuláře, instituce jsou povinny si tyto informace mezi sebou předat.⁴⁹

3.4 EU – US Privacy Shield

Mezi státy EU a Spojenými státy funguje intenzivní obchodní styk.⁵⁰ Předávání osobních údajů mimo EU je však podle GDPR důležité zvláště ošetřit tak, aby byla **při předávání i po něm zajištěna stejně vysoká úroveň ochrany osobních údajů**, což by mohlo být pro americké firmy problematické. Aby nedošlo k omezování obchodu mezi oběma velmocemi, byl vypracován tzv. **Privacy Shield** (Štít soukromí).

Privacy Shield byl schválen 12. července 2016. Program stanovuje americkým firmám, které se do programu přihlásí, **podobné povinnosti jako ty vyplývající z GDPR**: povinnost firem informovat subjekty o zpracování jejich osobních údajů, povinnost užívat osobní údaje pouze pro účel pro který byly získány, povinnost důkladného zabezpečení osobních údajů a jejich vymazání poté, co vyprší

⁴⁸ Pozitiva neprávem ocerňovaného GDPR. Norma pomáhá proti obtěžujícím telefonátům i zneužití sociálních sítí. *Investujeme.cz* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.investujeme.cz/tiskove-zpravy/pozitiva-nepravem-ocernovaneho-gdpr-norma-pomaha-proti-obtezujicim-telefonatam-i-zneuzeni-socialnich-siti/>.

⁴⁹ Tamtéž.

⁵⁰ Předávání osobních údajů do USA – štít soukromí ("Privacy Shield"). *Úřad na ochranu osobních údajů* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.uoou.cz/predavani-osobnich-udaju-do-usa-stit-soukromi-quot-privacy-shield-quot/ds-5068/p1=5068>.



právní titul k jejich zpracování a další.⁵¹ Všechny tyto firmy mají povinnost se registrovat u amerického Ministerstva obchodu, které má na americké straně na starost správu programu.⁵²

Účelem celého programu je **usnadnit americkým firmám naplňování povinností dle GDPR**. Pokud se společnosti nepřihlásí do programu Privacy Shield, jsou povinny poskytnout vhodné záruky podle čl. 46 GDPR (např. právně závazný nástroj vymáhání).⁵³

3.5 ePrivacy

Speciální úpravu ohledně bezpečí na internetu bude mít na starost **nařízení o soukromí a elektronických komunikacích**, tzv. ePrivacy. ePrivacy mělo být původně účinné společně s GDPR od května 2018, nicméně na začátku roku 2019 se na něm stále pracovalo a vzhledem ke květnovým volbám do Evropského parlamentu bude nakonec schválené pravděpodobně až v roce 2020.⁵⁴

ePrivacy bude zaměřené především na **bezpečnost na internetu**, bude podrobněji upravovat telekomunikace, internetový marketing, cookies a další. Myšlenkou ePrivacy je **vytvořit ekvivalent listovního tajemství i v internetových komunikacích**.⁵⁵

4 Podpora v Kongresu

V Kongresu i ve společnosti ⁵⁶ panuje **obecná shoda na tom, že zákon o ochraně osobních údajů by měl být v nějaké podobě přijat**. 43% voličů demokratů a 37% voličů republikánů si dokonce myslí, že by to měla být v roce 2019 priorita Kongresu, a to mj. kvůli nedávným kauzám.⁵⁷

⁵¹ GUIDE TO THE EU-US PRIVACY SHIELD. *European Commission* [online]. [cit. 2019-01-03]. Dostupné z: https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pdf.

⁵² Tamtéž.

⁵³ Předávání osobních údajů do USA – štít soukromí ("Privacy Shield"). *Úřad na ochranu osobních údajů* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.uoou.cz/predavani-osobnich-udaju-do-usa-stit-soukromi-quot-privacy-shield-quot/ds-5068/p1=5068>.

⁵⁴ Nařízení ePrivacy zřejmě tento rok platit nebude. *Podnikatel.cz* [online]. [cit. 2019-01-05]. Dostupné z: <https://www.podnikatel.cz/clanky/narizeni-eprivacy-zrejme-tento-rok-platit-nebude/>.

⁵⁵ Méně známý příbuzný GDPR. Co přinese nařízení ePrivacy?. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-05]. Dostupné z: <https://www.gdpr.cz/blog/mene-znamy-pribuzny-gdpr-co-prinese-narizeni-eprivacy/>.

⁵⁶ Pluralities of Democrats and Republicans Want Congress to Focus on Data Protection. *Morning Consult* [online]. [cit. 2019-01-03]. Dostupné z: <https://morningconsult.com/2018/11/07/pluralities-democrats-republicans-want-congress-focus-data-protection/>.

⁵⁷ Tamtéž.



Nová právní úprava zaměřená na ochranu osobních údajů je však více v zájmu demokratů.⁵⁸ Při projednávání lze očekávat neshody na obsahu mezi oběma stranami⁵⁹ – zatímco demokraté se budou pravděpodobně snažit o co nejvyšší úroveň ochrany práv občanů, republikáni budou usilovat především o co nejmenší náklady na administrativu spojenou se zákonem.

Lze také očekávat silné **lobbování ze strany společností jako Google a Facebook**, ale i dalších, např. obchodních firem. Vedle nových povinností v oblasti administrativy bude nová legislativa pro technologické giganty s největší pravděpodobností znamenat omezení příjmů z prodeje osobních údajů.

5 Závěr

Ochrana osobních údajů je důležitým aspektem globalizovaného světa. Kauzy jako Cambridge Analytica ukázaly, že zneužívání osobních údajů může být nebezpečné pro celou společnost. Evropská unie se s tímto problémem vypořádala prostřednictvím GDPR, které budí kontroverze a jeho reálný dopad je stále nejasný. A ačkoliv je nyní moc brzy na zhodnocování dopadů GDPR, je jasné, že i Spojené státy úpravu ochrany osobních údajů v nějaké podobě potřebují. Otázkou pro jednání zůstává, jak přísně budou pravidla nastaveny, jak vysoké budou sankce za jejich nedodržování a čeho se vlastně Spojené státy snaží jednotným zákonem o ochraně osobních údajů dosáhnout.

6 Doporučené zdroje ke studiu

- Jednoduchý průvodce obsahem GDPR (CZ): <https://www.gdpr.cz/gdpr/>
- Podrobná studie o ochraně osobních údajů v USA (EN):
[https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1)
- Jak fungují cookies – video (EN): <https://www.youtube.com/watch?v=I01XMRo2ESg>
- Celé znění GDPR (CZ): <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=CS>
- Krátké video o kauze Cambridge Analytica (EN):
<https://www.youtube.com/watch?v=Q91nvbJSmS4>
- O čem je ePrivacy (CZ): <https://www.gdpr.cz/blog/mene-znamy-pribuzny-gdpr-co-prinese-narizeni-eprivacy/>

⁵⁸ After the midterm elections, the odds improve a little for a US data privacy law. *C net* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.cnet.com/news/after-the-midterm-elections-the-odds-improve-a-little-for-a-us-data-privacy-law/>.

⁵⁹ Tamtéž.



7 Zdroje

Proč potřebuje Evropa lepší ochranu osobních dat. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>.

Cambridge Analytica: Facebook row firm boss suspended. BBC [online]. [cit. 2019-01-08]. Dostupné z: <https://www.bbc.com/news/uk-43480048>.

GDPR se blíží, ale veřejnost se ochranou osobních údajů příliš netrápí. Ekonomický deník [online]. [cit. 2019-01-08]. Dostupné z: <http://ekonomicky-denik.cz/gdpr-se-blizi-ale-verejnost-se-ochranou-osobnich-udaju-prilis-netrapi/>.

Data protection laws of the world. *Definition of personal data - United States* [online]. [cit. 2018-12-30]. Dostupné z: <https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US>.

What is personal data? European Commission [online]. [cit. 2018-12-26]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.

Jste připraveni na GDPR? Kropáček LEGAL, advokátní kancelář [online]. [cit. 2018-12-26]. Dostupné z: <https://pravopropodnikatele.cz/jste-pripaveni-na-gdpr/>.

Co je, co není a co bude osobní údaj podle GDPR. Frank Bold Advokáti [online]. [cit. 2018-12-25]. Dostupné z: <https://www.fbadvokati.cz/cs/clanky/541-co-je-co-neni-a-co-bude-osobni-udaj-podle-gdpr/>.

How safe is your personal data collected by your smart devices?. The Business Times [online]. [cit. 2018-12-25]. Dostupné z: www.business-times.com.sg/opinion/how-safe-is-your-personal-data-collected-by-your-smart-devices.

Corporate Surveillance in Everyday Life. Cracked Labs [online]. [cit. 2018-12-26]. Dostupné z: <https://crackedlabs.org/en/corporate-surveillance>.

CHRISTL, Wolfie. How companies use personal data against people. Cracked Labs [online]. [cit. 2018-12-26]. Dostupné z: https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf.

BBC: Facebook data: How it was used by Cambridge Analytica [online]. [cit. 2018-12-30]. Dostupné z: <https://www.bbc.com/news/av/technology-43674480/facebook-data-how-it-was-used-by-cambridge-analytica>.

What is Cambridge Analytica scandal? YouTube [online]. [cit. 2019-01-08]. Dostupné z: <https://www.youtube.com/watch?v=Q91nvbJSmS4>.

What is the Federal Trade Commission Act (FTCA)? *Business Law* [online]. [cit. 2019-01-01]. Dostupné z: https://business-law.freeadvice.com/business-law/trade_regulation/federal_trade.htm.

Financial Services Modernization Act of 1999. *Investopedia* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.investopedia.com/terms/f/financial-services-act-of-1999.asp>.

HIPAA: Health Insurance Portability and Accountability Act. *University of Pittsburgh* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.dental.pitt.edu/hipaa-health-insurance-portability-and-accountability-act>.

Data protection in the United States. *Practical law* [online]. [cit. 2018-12-31]. Dostupné z: [https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1).

What You Need to Know about the HIPAA Omnibus Rule. AAOS [online]. [cit. 2019-01-01]. Dostupné z: <https://www.aaos.org/AAOSNow/2013/Jul/managing/managing4/?ssopc=1>.

HIPAA (Health Insurance Portability and Accountability Act). *SearchHealthIT* [online]. [cit. 2019-01-01]. Dostupné z: <https://searchhealthit.techtarget.com/definition/HIPAA>.

Privacy Act of 1974. *The United States Department of Justice* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.justice.gov/opcl/privacy-act-1974>.



Co je GDPR a jak bude aplikováno v Česku. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>.

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). Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=CS>.

Jaké zásadní změny GDPR přinese. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.gdpr.cz/gdpr/zmeny/>.

Co považuje GDPR za osobní údaje. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-01]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>.

DPO čili Pověřenec pro ochranu osobních údajů. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.gdpr.cz/gdpr/dpo/>.

Předávání osobních údajů do USA – štít soukromí ("Privacy Shield"). *Úřad na ochranu osobních údajů* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.uoou.cz/predavani-osobnich-udaju-do-usa-stit-soukromi-quot-privacy-shield-quot/ds-5068/p1=5068>.

GUIDE TO THE EU-US PRIVACY SHIELD. *European Commission* [online]. [cit. 2019-01-03]. Dostupné z: https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pdf.

Nařízení ePrivacy zřejmě tento rok platit nebude. *Podnikatel.cz* [online]. [cit. 2019-01-05]. Dostupné z: <https://www.podnikatel.cz/clanky/narizeni-eprivacy-zrejme-tento-rok-platit-nebude/>.

Méně známý příbuzný GDPR. Co přinese nařízení ePrivacy?. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-01-05]. Dostupné z: <https://www.gdpr.cz/blog/mene-znamy-pribuzny-gdpr-co-prinese-narizeni-eprivacy/>.

Pluralities of Democrats and Republicans Want Congress to Focus on Data Protection. *Morning Consult* [online]. [cit. 2019-01-03]. Dostupné z: <https://morningconsult.com/2018/11/07/pluralities-democrats-republicans-want-congress-focus-data-protection/>.

After the midterm elections, the odds improve a little for a US data privacy law. *Cnet* [online]. [cit. 2019-01-03]. Dostupné z: <https://www.cnet.com/news/after-the-midterm-elections-the-odds-improve-a-little-for-a-us-data-privacy-law/>.