ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Diplomová práce

Internet a ochrana osobních údajů v EU

Roman Brožek

Plzeň 2019

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Katedra ústavního a evropského práva

Diplomová práce

Internet a ochrana osobních údajů v EU

Roman Brožek

Studijní program:	Právo a právní věda
Studijní obor:	Právo
Vedoucí práce:	Mgr. et. Mgr. Renáta Vokrojová katedra ústavního a evropského práva

Plzeň 2019

Čestné prohlášení

Prohlašuji, že jsem tuto diplomovou práci na téma „Internet a ochrana osobních údajů v právu EU“ zpracoval samostatně. Veškeré prameny a zdroje informací, které jsem použil, jsou řádně ocitovány v poznámkách pod čarou a uvedeny v seznamu použité literatury.

V Plzni 27. 3. 2019 .....

Poděkování

Na tomto místě bych rád poděkoval Mgr. et Mgr. Renátě Vokrojové za vedení práce a vstřícný přístup. Dále děkuji své rodině za podporu nejen při psaní této práce, ale i během celého studia.

Obsah

Seznam použitých zkratek a termínů

DPIA	Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment)
EHP	Evropský hospodářský prostor
ESD	Evrospký soudní dvůr
EU	Evropská unie
ePrivacy	Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.04.2016 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)
IoT	internet věcí (Internet of Things)
Kodex	Evropský kodex pro elektronické komunikace
LZPEU	Listina základních práv Evropské unie
Pracovní skupina WP29	Nezávislá pracovní skupina zřízená dle článku 29 směrnice č. 95/46/ES o ochraně osobních údajů.
SEU	Smlouva o Evropské unii
SFEU	Smlouva o fungování Evropské unie

Úvod

Růst uživatelů internetu, jakožto hlavního informačního pramene 21. století, se v poslední době již nijak rapidně nezvyšuje, tedy alespoň ne ve státech Evropy. Průzkum z roku 2017 ukazuje, že odhad uživatelů členských států EU majících přístup k internetu z domova činí přes 87 %.[1] Trendem posledních let je spíše mobilita internetového připojení, tedy přechod od stolních počítačů k mobilním zařízením. S tímto trendem se však pojí jistý paradox, neboť ačkoliv je internet rychlejší a dostupnější, přesto na něm uživatelé tráví více času, nežli tomu bylo dříve s pomalejším a hůře dostupným připojením. Mohou za to jednak nové možnosti, tedy i služby, které jsou poskytovatelé schopni nabídnout, a dále tento trend podporují zejména sociální sítě. Čím dál častěji se také hovoří o tzv. internetu věcí, který propojuje nové technologie poskytované přes internet do běžných zařízení. Jde například o monitorování a řízení městské infrastruktury, integrace internetu do energetických systémů budov, nebo třeba domácí spotřebiče používající Wi-Fi připojení pro možnost vzdáleného ovládání. Nástup těchto technologií s očekáváním vyhlížejí také lékaři, neboť budou moci využívat data o zdravotním stavu uživatele zaznamenaná chytrými hodinkami, která jsou uložena na vzdáleném serveru. Kromě získání podrobného přehledu o zdravotním stavu jedince mohou tato data pomoci také s upozorněním na nově vznikající zdravotní problémy.[2] Podobné trendy digitalizace lze zaznamenat také v průmyslu, pro které se ujal termín Průmysl 4.0, který označuje způsob automatizace výroby pomocí nových technologií. Tyto služby nabízejí svým uživatelům zcela nové možnosti a značně usnadňují běžné činnosti. Na druhou stranu je také třeba zdůraznit, že při využívání internetových služeb dochází k masovému přenosu dat včetně přenosu osobních údajů jejich uživatelů. Mezi tímto množstvím údajů se mohou vyskytovat také velmi citlivá data, jejichž

[1] Digital economy and society statistics - households and individuals. Eurostat [online]. Luxembourg [cit. 2018-04-08]. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#internet_access

[2] Podrobněji GOLD, Jon. *Lab makes data sharing easier so medical IoT devices can be smarter*. Network World [online]. Framingham: IDG Communications, 2018 [cit. 2018-10-09]. Dostupné z: https://www.networkworld.com/article/3295905/internet-of-things/lab-makes-data-sharing-easier-so-medical-iot-devices-can-be-smarter.html?utm_campaign=IoT%2BWeekly%2BNews&utm_medium=web&utm_source=IoT_Weekly_News_125

zveřejnění či zneužití by pro dotyčnou osobu mohlo mít neblahé důsledky. Na vzniklé riziko se snaží reagovat jednak legislativy členských států, ale také především unijní legislativa. Jedná se však o nerovnocený závod nově se vyvíjejících technologií a těžkopádně přijímané legislativy, která se snaží obecnými definicemi pojmout v budoucnu nově vzniklé technologie.

Poskytovatelům služeb nabízených skrze internet se tak do rukou dostává obrovské množství dat, které by nebylo vůbec možné jinými prostředky získat. Tato data jsou spravována a zabezpečována poskytovateli služeb, přičemž právě v jejich správě jsou spatřována obrovská rizika, která představují zejména úniky dat, o čemž jsme se mohli v minulosti přesvědčit již několikrát. K jednomu z nejmasovějších úniků dat došlo v srpnu roku 2013, kdy společnosti Yahoo unikla data celkem tří miliard účtů[3], nebo nedávný únik dat z Facebooku, který se měl týkat okolo 87 milionů uživatelů.[4] V rámci smluvních podmínek jejich poskytovatelé často zdůrazňují, že tyto osobní údaje mají primárně sloužit ke zlepšování nabízených služeb.[5] Je tedy oprávněným zájmem uživatele, aby tyto údaje byly v bezpečí u poskytovatelů těchto služeb a nedocházelo k jejich únikům. K tomuto výsledku se snaží dopomoci také evropská legislativa, která zavádí určitá omezení zabraňující takovýmto únikům dat či jejich zneužití. Poskytování služeb na internetu není ve většině případů omezeno pouze pro ten který stát, na němž daný správce údajů sídlí, ale nachází si uživatele i vně hranic. Vzhledem k tomu, že v případě internetu neexistují jakékoliv hranice jeho využití, lze shledat tendence k jednotné úpravě na území Evropské unie jako nadmíru žádoucí. Přestože většina velkých správců osobních údajů sídlí v USA, považuji jednotnou právní úpravu a tedy i přístup k dodržování určitých standardů v rámci EU jako jednu z klíčových oblastí unijní legislativy.

Článek 8 Listiny základních práv Evropské unie stanoví (dále jen „LZPEU“), že každý má právo na ochranu osobních údajů, které se ho týkají. Tuto deklarovanou ochranu se Evropská unie snaží zajišťovat skrze značné

[3] LARSON, Selena. *Every single Yahoo account was hacked - 3 billion in all*. In: CNN: tech [online]. 4. 10. 2017 [cit. 2018-04-08]. Dostupné z: http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

[4] KUCHLER, Hannah. Facebook chief admits ‘mistakes’ over data leaks. *FINANCIAL TIMES* [online]. London: Nikkei, 2019 [cit. 2018-09-17]. Dostupné z: https://www.ft.com/content/3130c420-3c0c-11e8-b9f9-de94fa33a81e

[5] Například zásady ochrany soukromí Googlu: https://www.gstatic.com/policies/privacy/pdf/20180525/853e41a3/google_privacy_policy_cs.pdf

množství sekundárních právních předpisů, které jsou zejména reakcí na nově se vyvíjející technologie. Tuto unijní úpravu zanalyzuji chronologicky, tak jak byla vydána, přičemž se nebude jednat o kompletní rozbor právních předpisů, nýbrž vyberu pouze ustanovení a principy vztahující se k problematice ochrany osobních údajů na internetu ovlivňující stávající úpravu. Zmíněny budou zejména zásady, jichž se jednotlivé právní úpravy poměrně striktně drží a tvoří tak základní prostředek pro interpretaci jednotlivých ustanovení. Rozeberu také Obecné nařízení o ochraně osobních údajů (dále jen „GDPR“)[6], neboť se jedná o doposud poslední účinný právní předpis EU v oblasti ochrany osobních údajů. Opět se nebude jednat o kompletní rozbor, ale pouze o nastínění důležitých institutů, které mají přímý dopad na ochranu osobních údajů na internetu. V rámci této práce bude poukázáno na to, jakým způsobem by správci měli splnit na ně kladené požadavky a jak toto nařízení změnilo internetové prostředí. Významná část práce bude věnována dosud ještě neúčinnému návrhu nařízení ePrivacy[7], které se bude týkat ochrany soukromí při využívání elektronických komunikací. To se především vztahuje na komunikační služby provozované přes internet, tedy například na Facebook Messenger, WhatsApp, Skype a další obdobné služby. Ačkoliv se ePrivacy dotýká ochrany důvěrného charakteru komunikací, tedy širšího rozsahu nežli je ochrana osobních údajů, přesto ho považuji za významný právní předpis v této oblasti, neboť zmíněný obsah komunikací je chráněn především z důvodu osobních údajů v něm obsažených. Tomuto nařízení není doposud věnována zdaleka taková pozornost, kterou si v minulosti získalo GDPR, proto považuji výklad o tomto nařízení přínosným. Nejdříve se však budu věnovat pojmu osobní údaj, a popíši, co vše lze považovat za osobní údaj v prostředí internetu a z jakého důvodu by měly být chráněny.

Práce si klade za cíl analyzovat, jakým konkrétním způsobem by měl správce osobních údajů postupovat při zpracovávání osobních údajů na internetu. Zároveň zkoumá, jaký dopad bude mít nařázení ePrivacy na internetové služby, zejména pak na komunikaci prováděnou skrze internet. S ohledem na takto stanovený cíl použiji především pragmatickou metodologii zkoumání, která se

[6] 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).

[7] Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).

zaměřuje na praktickou řešitelnost a užitečnost vyvstalých problémů. Tato metoda se jeví jako vhodná, neboť internet, potažmo služby na něm nabízené, se neustále vyvíjí kupředu a není tak možné lpět na obecných právních principech.[8] Další pomocnou metodou bude analýza a v případě rozboru jednotlivých právních předpisů komparace.

Vzhledem k absenci publikací věnujících se komplexně danému tématu použiji především vědecké práce a stanoviska, které se snaží na danou problematiku pružněji reagovat. Zaměřím se také na klíčová rozhodnutí Soudního dvora Evropské unie, která dále poodkryjí praktický výklad sporných ustanovení.

[8] Srov. POLČÁK, Radim. *internet a proměny práva.* Praha: Auditorium, 2012. Téma (Auditorium). ISBN 978-80-87284-22-3, str. 76 a dále.

1. Internet a osobní údaje

1.1. Osobní údaje na internetu a jejich ochrana

Stejně jako je v dnešní době snadné nahrát obsah na internet, tak je stejně tak snadné ho kopírovat, sdílet, či jinak přenášet. Ve chvíli nahrání jakéhokoliv obsahu na internet přestává mít nad ním uživatel okamžitou kontrolu v tom ohledu, že není prakticky zjistitelné, kde se daný obsah může nacházet. Na internetu existují dokonce služby, které kompletně monitorují internet a ukládají jeho obsah v čase. Je tak možné si otevřít webové stránky s obsahem, který již uživatel dávno smazal.[9] Je tedy nutno mít na paměti, že internet za žádných okolností nezapomíná.[10] To samé platí i pro osobní údaje, které uživatel předává poskytovateli internetových služeb.

Kromě obvyklých osobních údajů, které lze na internet umístit, jako je například jméno, adresa bydliště, nebo třeba rodné číslo, lze vystopovat i další skupinu osobních údajů. Tyto údaje povětšinou představují jakýsi identifikátor (soubor znaků), které mohou danou osobu nepřímo identifikovat. Jedná se o údaje, které nejsou na internet primárně ukládány a uživatelé o jejich záznamech ani nemusí mít povědomí, jde tak spíše o stopy v síti zanechané uživatelem. Tyto údaje lze také označit jako tzv. neperfektní identifikátory, neboť na jejich základě nelze danou osobu přímo určit a je nutné podniknout i další kroky k její identifikaci.[11] Na základě těchto údajů je možné přesně identifikovat zařízení, ze kterého byly zaznamenány. To neplatí bezvýhradně, neboť například v případě IP adres existuje tzv. VPN (Virtual Private Network) technologie, která umožňuje jejich skrytí. Podobné výjimky lze zaznamenat prakticky u všech níže uvedených typů osobních údajů, přesto je patrné, že takovéto služby běžní uživatelé internetu nevyužívají a je tak nezbytné, aby jim byla poskytována ochrana.

[9] DONÁT, Josef a Jan TOMÍŠEK. *Právo v síti: průvodce právem na internetu.* V Praze: C.H. Beck, 2016. ISBN 978-80-7400-610-4, s. 18-20.
[10] Ačkoliv se tomuto faktu snaží evropská legislativa ochrany osobních údajů postavit, není to vždy dobře možné. Více k této problematice bude pojednáno v kapitole 3.6. v rámci výkladu o sociálních sítích.
[11] MATEJKA, Ján. *internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6, s. 92 a následující.

Ve smyslu výše nastíněného lze dovodit, že legislativa v oblasti ochrany osobních údajů je formována právě díky vývoji nových informačních a komunikačních technologií. S nárůstem služeb poskytovaných přes internet narůstá i množství shromážděných osobních údajů, které mají poskytovatelé služeb ve své správě. Proto je nezbytné, aby byla nastavena jasná pravidla pro jejich sběr, uchovávání, ale zejména také předávání třetím stranám.

GDPR definuje ve svém článku 4 odst. 1 osobní údaj jako jakoukoliv informaci, která se týká určené nebo přímo či nepřímo určitelné fyzické osoby, nikoliv tedy právnické osoby, což je i zdůrazněno v bodě 14 recitálu GDPR. Výjimkou jsou v tomto ohledu právnické osoby mající oficiální název identifikující jednu či více fyzických osob.[12] Určitelnost fyzické osoby lze vykládat jako požadavek odlišení určité fyzické osoby od jiných, tedy jednoznačné určení té které osoby.[13] Jedná se o údaje, které samy o sobě nemusí určitelnou osobu přímo identifikovat. Důležitým je zde vztah osobního údaje k člověku, který může mít dopad do práv dané osoby, byť může být zanedbatelný.[14] Není tedy nutné rozlišovat osobní údaj, který je sám o sobě schopný určit předmětnou osobu a osobní údaj, který k identifikaci konkrétní osoby bude vyžadovat dalšího údaje. Nezbytné je rozlišovat, co je osobním údajem, soukromou informací a projevem osobní povahy (např. osobní dopis), neboť v každém z těchto případů budou rozdílně uplatňována práva osob. Ve druhé části článku 4 odst. 1 GDPR je pak uveden demonstrativní výčet osobních údajů, který se soustředí spíše na specifické osobní údaje (např. síťový identifikátor, zvláštní prvky fyziologické či genetické). Definice se příliš neliší od předchozí Směrnice 95/46/ES, až na důraz toho, že osobním údajem se rozumí pouze údaj o fyzické osobě. Obdobně je tomu i u nařízení ePrivacy, v rámci kterého je ochrana osobních údajů poskytována pouze fyzickým osobám, ačkoliv v případě ochrany důvěrnosti sdělení komunikace je osobní působnost rozšířena i na právnické osoby.

---

[12] Rozsudek ESD ze dne 9. listopadu 2010, Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) proti Land Hessen, za přítomnosti: Bundesanstalt für Landwirtschaft und Ernährung, ve spojených věcech C-92/09 a C-93/09, EU:C:2010:662, bod. 53. V rámci předběžné otázky soud řešil, zda mají jednátelé právnické osoby jež má jejich jména v názvu právo na ochranu dle čl. 7 a 8 LZPEU.

[13] MAŠTALKA, Jiří. *Osobní údaje, právo a my.* V Praze: C.H. Beck, 2008. Beckova edice ABC. ISBN 978-80-7400-033-1, s.14.

[14] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů.* Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3, s. 77-78.

1.2. Specifické osobní údaje v internetovém prostředí

V následujících kapitolách budou rozebrány osobní údaje specifické pro internet, které mají především tu zvláštnost, že ačkoliv se považují za osobní údaje, jedná se vlastně o údaje určitého zařízení, které daná osoba používá. Identifikace tohoto druhu nesměřuje přímo ke konkrétní fyzické osobě, ale k zařízení, přičemž nemusí být jisté, zda jej konkrétní osoba skutečně používala. Nemusí být dokonce jasné, zda vůbec některá osoba dané zařízení obsluhovala a nejednalo se tak o předem naprogramované chování zařízení. Je tedy nezbytně nutné posuzovat každý případ individuálně a v kontextu, aby bylo možné určit, zda tyto údaje jsou osobními údaji fyzických osob.[15] Vylíčení jednotlivých specifických osobních údajů poslouží zejména ke snazšímu pochopení výkladu v rámci třetí kapitoly.

1.2.1. Síťové identifikátory

Síťové identifikátory si lze představit jako určité číselné vyjádření konkrétního zařízení. Mezi síťové identifikátory lze zařadit např. IP adresu, což je unikátní číselný kód, který má přiděleno každé rozhraní (např. počítač, mobilní telefon). Každé rozhraní přitom může mít více než jednu adresu, ačkoliv většina má právě jednu. Tato čísla jsou přidělována celosvětově jednoznačně a jsou jedinečná, tedy alespoň v rámci veřejného internetu. Pokud uživatel využívá vlastní vnitřní síť, např. intranet v rámci obchodní společnosti, jsou zde IP adresy přiřazovány nezávisle od internetových IP adres.[16] Celosvětové přidělování IP adres má na starosti organizace IANA.

Při každé návštěvě webových stránek je tento číselný kód odesílán na server, na kterém je webová stránka provozována. Obdobně je tomu tak i v případě aplikací, ať už počítačových či mobilních, které jsou zprostředkovávány skrze internet. Provozovatel služby může tyto údaje ukládat v tzv. logovacích datových souborech, ze kterých jsou patrné časové údaje návštěv jednotlivých IP adres.

[15] MATEJKA, Ján. *internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6, s. 90.
[16] KLEMENT, Milan. *IP adresace a směrování v počítačových sítích.* Olomouc: Univerzita Palackého v Olomouci, 2015. ISBN 978-80-244-4571-7, s. 6-13.

Rozslišovat je možné jednak statické IP adresy, které jsou přidělovány připojenému zařízení poskytovatelem internetového připojení (dále jen „ISP“) či správcem sítě v rámci intranetu. Statické IP adresy, jak z názvu vyplývá, budou vždy neměnné, a je tedy jasné, že je lze označit jako osobní údaj. Dále existují také dynamické IP adresy, které se mění při každém připojení zařízení do sítě (jak internetové, tak i lokální), příčemž stejnou dynamickou IP může mít při pozdějším připojení i jiný uživatel.

Předávání dynamických IP adres poskytovateli webových stránek řešil v rámci předběžné otázky Soudní dvůr Evropské unie (dále jen „ESD“) v případu Patrik Breyer proti Spolkové republice Německo.[17] P. Breyer v uvedeném případě napadal německé orgány, které uchovávaly jeho IP adresy spolu s datem otevření webové stránky a dalšími údaji, které Breyer na těchto stránkách uvedl, neboť dle jeho názoru neexistovala právní opora pro zpracování těchto údajů. ESD v daném případě zkoumal, zda lze i dynamickou IP adresu považovat za osobní údaj a poskytovat ji ochranu. Nakonec ve svém rozhodnutí uložil německým orgánům, aby se zdržely uchovávání dynamické IP adresy v tom rozsahu, v němž není nezbytné pro obnovení služby v případě poruchy, přičemž orgány dále mohly uchovávat pouze časy připojení. Soud se dále vyslovil, že i dynamická IP adresa je osobním údajem, pokud je zanechána na webu spolu s jiným osobním údajem, případně pokud má poskytovatel webu alespoň prostředky k identifikaci subjektu údajů. Soud však v daném případě nevyslovil, o jaké prostředky by se mohlo jednat, vyslovil se pro pouhý předpoklad, že by německé orgány mohly mít právní prostředky pro získání dalších údajů, zejména v souvislosti s ochranou proti kybernetickým útokům.[18] Obdobně rozhodl ESD již dříve ve věci Productores de Música de España (Promusicae) v Telefónica de España SAU[19], kde společnost Promusicae požadovala odhalení totožností osob, které nelegálně stahovaly hudební soubory skrze program pro výměnu dat (tzv. P2P software). Promusicae

[17] Rozsudek ESD ze dne 19. října 2016, Patrick Breyer proti Bundesrepublik Deutschland, C-582/14, EU:C:2016:779.
[18] NESPUREK, Robert, Richard OTEVŘEL a Monika MATYSOVÁ. *Breyer Ruling, And Dynamic IP Addresses As Personal Data.* Mondaq [online]. Copyright © 1994-2018 Mondaq ®, 2019 [cit. 2019-01-22]. Dostupné z: http://www.mondaq.com/x/677894/data+protection/Breyer+Ruling+And+Dynamic+IP+Addresses+As+Personal+Data
[19] Rozsudek ESD ze dne 29. ledna 2008, Productores de Música de España (Promusicae) v. Telefónica de España SAU, EU:C:2008:54.

disponovala právě IP adresami a časy připojení těchto uživatelů, přičemž se ESD vyslovil, že se jedná o osobní údaje.[20]

Obdobné principy platí i u MAC adresy, což je identifikátor síťového zařízení, jenž je přidělován již při výrobě zařízení (např. telefonu či chytrých hodinek). Jedná se tak o neměnný identifikátor v rámci síťové komunikace. Informace o tomto číselném identifikátoru neputují mimo síť v rámci níž je zařízení připojeno, slouží tak pouze ke komunikaci se zařízeními v rámci jedné sítě.

Stejně tak lze považovat za osobní údaj i číselný identifikátor IMEI. Jedná se o identifikátor, který přiděluje výrobce mobilním telefonům, přičemž každý telefon má svůj unikátní číselný identifikátor.[21] IMEI je nutné považovat za osobní údaj z toho důvodu, že je možné ho zaznamenávat zejména k marketingovým účelům nebo např. k měření návštěvnosti určitého místa. Ačkoliv běžný správce (nikoliv operátor) tohoto údaje nemá reálnou možnost zjistit totožnost vlastníka zařízení, je ho však možné zjistit pomocí orgánů činných v trestním řízení, které si mohou dané údaje vyžádat a následně vyžadovat identifikace těchto IMEI u mobilního operátora, čímž mají možnost identifikovat danou osobu.[22]

1.2.2. Lokalizační údaje

S rozšiřováním poskytování nejrůznějších služeb na internetu vznikla potřeba znát polohu uživatelů, jež má opět sloužit ke zlepšení poskytování služeb, jako jsou například webové stránky v národním jazyce, nabídka služeb specifických přímo pro danou lokalitu, nebo třeba poskytování zpravodajství pro určité území. Tuto potřebu ulehčilo bezdrátové Wi-Fi připojení, které usnadnilo možnost vysledování zařízení, která jsou na ni připojeny. Lokalizační údaje jsou tak údaje, které určují zeměpisnou polohu koncového zařízení. Zeměpisná poloha

[20] Podobný přístup zaujímá i Kanada v rámci ochrany osobních údajů s tím rozdílem, že identifikace musí vést k soukromému zařízení. IP adresa či např. email společnosti nebude považována za osobní údaj, ačkoliv by ho používal pouze jeden zaměstnanec. Podrobněji: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/

[21] MATEJKA, Ján. *internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6, s. 93-95.

[22] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 80.

se bude týkat zejména mobilních zařízení, které má uživatel stále při ruce a aktivně je využívá po celý den. Problematická budou zejména často navštívená místa, neboť z nich bude patrné, kde subjekt údajů bydlí, či kde pracuje. Data o často navštěvovaných místech mohou dokonce odhalit velmi citlivé osobní údaje, kterými může být náboženské vyznání či sexuální orientace. Například Google umožňuje zaznamenávat na mapě veškerá místa, která uživatel navštívil, pokud měl zapnutou GPS navigaci, přičemž ani přímé připojení k internetu není nutné, neboť data jsou odeslána až po připojení k internetu.[23] Pokud by se souhrn těchto lokalizačních údajů dostal do cizích rukou, mohlo by to mít pro uživatele velmi neblahé důsledky.

1.2.3. Cookies

Cookies lze označit jako malé soubory, které jsou ukládány na pevný disk zařízení při návštěvě webových stránek. Jejich základní funkcí je identifikace uživatele, který se na web vrací, přičemž tuto opakovanou návštěvu zjednodušují např. tím, že uživatel nemusí již vypisovat heslo při vstupu na emailovou adresu, nebo při přidání položek do nákupního košíku v rámci internetového obchodu, v němž tyto položky zůstanou i při opakované návštěvě.[24] Z pohledu ochrany osobních údajů jsou nejdůležitější tzv. sledovací cookies, které monitorují uživatelovo chování v rámci navštívené webové stránky. Tyto informace poté může poskytovatel webové stránky využívat zejména k marketingovým účelům, tedy např. úpravě webu, ale může také docházet k individualizaci nabídek či reklamních sdělení.[25] Soubory cookies mohou obsahovat různé informace, např. společnost Google ve svých smluvních podmínkách[26] uvádí, že soubory obsažené v cookies ukládá do protokolů na svých serverech, které obsahují webový požadavek, datum a čas požadavku, IP adresu, typ prohlížeče a jazyk prohlížeče. Ze souborů cookies tak lze snadno zjistit, jakým jazykem uživatel hovoří, jaké výrazy na webu vyhledává, nebo jak často navštěvuje konkrétní webové stránky.

[23] Více na https://maps.google.com/locationhistory.
[24] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 92
[25] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7., s. 72-73.
[26] Ochrana soukromí a smluvní podmínky Google: https://policies.google.com/technologies/ads?hl=cs

Problematická může být samotná ochrana těchto souborů, neboť na pevném disku zařízení nejsou standardně nijak chráněny. Z výše naznačeného je tedy patrné, že i tyto údaje mají velmi úzkou souvislost se soukromím uživatele. Přesto jsou cookies považovány za osobní údaje pouze v určitých případech, konkrétně při jejich sběru a následném profilování uživatele, případně pokud jsou cookies ukládány spolu s dalšími informacemi o fyzické osobě.[27] Pokud totiž tyto informace nejsou součástí profilování a nejsou uloženy s informacemi o uživateli, pak je možné je označit jako anonymní, neboť není prakticky možné vystopovat souvislost s konkrétním uživatelem.

1.2.4. Metadata

Metadata lze označit jako data, která poskytují informace o dalších datech, konkrétně o jejich vlastnostech. Jedná se tak o data o digitálních objektech, obsahujících zejména název autora objektu, jazyk dokumentu, čas uložení, místo vzniku nebo třeba název vydavatele. Jednoduše si lze představit digitální fotografii, která může být zcela abstraktního charakteru, avšak právě z metadat lze vyčíst podrobnější informace, jako je jméno autora či čas pořízení, případně u fotoaparátů s integrovanou GPS také místo pořízení. Ačkoliv se jedná spíše o prostředek, kterým se lze dostat k dalším osobním údajům autora, je nutné považovat metadata za osobní údaj jako celek. Metadata se tak budou týkat zejména cloud computingu o kterém bude pojednáno v kapitole 3.3., případně také obsahu v rámci elektronické komunikace. V rámci samotné komunikace mohou metadata prozradit IP adresu zařízení, čas odeslání zprávy, místo odeslání apod.

1.3. Zvláštní kategorie osobních údajů

Určité osobní údaje mohou být pro jedince natolik citlivé, že jim legislativa propůjčuje vyšší ochranu nežli běžným osobním údajům. Jde o citlivé údaje, které by mohly vést k diskriminaci osob ve společnosti, nebo jejich vážnému poškození v běžném životě. Konkrétně se může jednat o údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení, sexuální orientaci, zdravotním stavu či členství v odborech. V rámci GDPR jsou do této skupiny zahrnovány nově také

[27] Bod číslo 30 recitálu GDPR.

genetické či biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby. Biometrické údaje jsou až na výjimky jedinečné identifikační údaje, které identifikují přímo konkrétní osobu. Jedná se např. o otisk prstu, sítnice oka či geometrie tváře. ESD již v minulosti považoval otisky prstů za osobní údaj, neboť umožňují jedinečnou identifikaci fyzické osoby[28], přičemž právě od nabytí účinnosti GDPR jim je poskytována vyšší úroveň ochrany. Vzhledem k unikátnosti těchto údajů, jsou tato data využívána zejména jako bezpečnostní prvek pro přístup do určitého objektu, případně pro přístup k datovému úložišti skrze internet. Pro toto využití musí být biometrické údaje zaznamenány a uloženy do přístupového zařízení, které tyto uložené údaje poté porovnává s těmi, které uživatel zadává při pokusu o přístup.

Naopak za citlivé osobní údaje nelze obecně považovat fotografie, ačkoliv i ony mohou vyzradit citlivé údaje. Fotografie je však považována za citlivý osobní údaj pouze v případě, pokud je zpracována technickými prostředky umožňujícími jedinečnou identifikaci fyzické osoby.[29] Toto ovlivnilo zejména sociální síť Facebook, která vzhledem k obrovskému množství nahraných fotografií na této sociální síti vyvinula technologii, která je schopna rozpoznat osobu na nahrané fotografii a umožňuje její rychlé označení. Právě díky přijetí obecné právní úpravy na ochranu osobních údajů (GDPR) musel Facebook využít souhlas jako právní titul pro využívání této technologie, viz příloha č. 1.[30]

Zpracování takovýchto údajů může způsobovat vážné ohrožení základního práva na soukromí. Z tohoto důvodu jsou vyžadovány zvláštní požadavky na zákonnost zpracování takovýchto údajů, jako je ochrana životně důležitých zájmů subjektů údajů, výkon nebo obhajoba právních nároků, pro účely preventivního nebo pracovního lékařství apod.[31] Výjimku v tomto ohledu mají také neziskové organizace, nadace a sdružení, které mohou zpracovávat citlivé údaje svých současných či bývalých členů či podporovatelů, a to bez právního důvodu. Podmínkou však je, že tyto údaje nesmí být dále nijak zpřístupňovány.[32] Členské

[28] Rozsudek ESD ze dne 17. října 2013, Michael Schwarz proti Stadt Bochum, C-291/12, EU:C:2013:670, bod 27.
[29] Bod 51 recitálu GDPR
[30] KELION, Leo. *Facebook seeks facial recognition consent in EU and Canada.* BBC [online]. London [cit. 2019-03-01]. Dostupné z: https://www.bbc.com/news/technology-43797128.
[31] Srov. článek 9 odst. 2 GDPR.
[32] NAVRÁTIL, Jiří. *GDPR pro praxi.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 151.

státy mohou stanovit výjimky pro zákaz zpracování zvláštní kategorie osobních údajů, pokud přijmou vhodné záruky na ochranu osobních údajů a jiných základních práv, nebo pokud jsou zpracovávány ve veřejném zájmu. V současném vládním návrhu českého zákona o ochraně osobních údajů však nebyly vymezeny žádné výjimky.

2. Právní úprava ochrany osobních údajů v EU

V následujících kapitolách stručně popíši vývoj evropské legislativy týkající se ochrany osobních údajů. Jejich cílem je uvést čtenáře do souvislostí vývoje legislativy a představit některé klíčové instituty, které daný předpis zavedl, a jsou i nadále využívány novějšími předpisy. Nejedná se o komplexní analýzu přijaté legislativy, neb to není ani cílem této práce.

2.1. Původ ochrany osobních údajů

Právo na ochranu osobních údajů lze odvodit od práva na informační sebeurčení člověka. Pojem informační sebeurčení člověka byl poprvé použit německým ústavním soudem, který jím rozuměl způsobilost člověka určit dostupnost a užití jeho osobních údajů. Jedná se o úhrnné označení různých informačních práv člověka, která se v průběhu času a s rozvojem informační společnosti mění.[33] Tento pojem v sobě zahrnuje kromě ochrany osobních údajů a práva na soukromí také právo na vzdělání (tedy příjem informací), právo na informace veřejného sektoru a také svobodu projevu.[34] Toto právo tedy znamená, že člověk se může svobodně rozhodnout, jaké informace o sobě poskytne svému okolí, a které informace bude přijímat. Ochranu osobních údajů lze podřadit pod pasivní složku informačního sebeurčení člověka.[35]

S tím souvisí i tzv. informační stopa, kterou za sebou člověk zanechává jak už v reálném životě, tak čím dál častěji na internetu. Vzniká tak potřeba tyto informace chránit, zejména pokud byly svěřeny pouze určitému okruhu osob či správci osobních údajů.[36] V minulosti některé právní řády členských států (např. Rakousko a Itálie) poskytovaly ochranu osobních údajů i právnickým osobám,

[33] Polčák informační společnost chápe jako společnost, která si postupně uvědomuje důležitost informací a která ke zvýšení své informovanosti využívá možností daných moderními informačními a komunikačními technologiemi. POLČÁK, Radim. *internet a proměny práva.* Praha: Auditorium, 2012. Téma (Auditorium). ISBN 978-80-87284-22-3 s. 274.
[34] POLČÁK, Radim. *internet a proměny práva.* Praha: Auditorium, 2012. Téma (Auditorium). ISBN 978-80-87284-22-3 s. 324-328.
[35] POLČÁK, Radim. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8, s. 21.
[36] Správce osobních údajů bude blíže rozebrán v kapitole 2.6.1. Pro představu stačí nyní uvést, že dle dikce GDPR se jedná o každý subjekt, který určuje účel a prostředky zpracování osobních údajů, přičemž za tímto účelem provádí jejich shromažďování, zpracování a uchování. Tímto správcem tak může být např. poskytovatel e-mailové schránky (např. Google, Seznam.cz).

ačkoliv to odporovalo znění Směrnice 95/46/ES, které poskytovalo ochranu osobních údajů pouze osobám fyzickým.[37]

Obecně ochrana soukromí jedince je v EU jako základní lidské právo postaveno na poměrně vysoké úrovni, již v článku 7 LZPEU je stanoveno: *„Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace"*.[38] Listinu lze zařadit mezi primární právní předpisy, neboť jí byla přisouzena ekvivalentní právní síla jako podepsaným komunitárním smlouvám, a to díky přijaté Lisabonské smlouvě podepsané dne 13. prosince 2007. Právo na ochranu soukromí bývá také označováno jako právo být ponechán sám o samotě (angl. right of the individual to be let alone), které pochází z USA. Právo být ponechán sám o samotě představuje negativní složku pojmu soukromí, přičemž tu pozitivní představuje právo osoby znát, jaké osobní údaje jsou o ní evidovány a mít možnost tyto údaje opravit.[39] Tomáš Sobek pak dokonce chápe právo na soukromí jako právo na skrývání své osobní slabosti.[40]

Problematická může být i otázka výkladu pojmu soukromí, neboť tento pojem má v historickém vývoji zcela rozdílný rozsah, stejně tak ale bude rozdílně pojímán v odlišných kulturách, neboť s ohledem na vývoj informačních technologií nelze poskytovat absolutní ochranu soukromí, pokud by tedy osoba nebyla zcela o samotě a nevyužívala žádných komunikačních technologií. Ochrana soukromí je tak velmi dynamicky měnícím se odvětvím, které je neustále ovlivňováno vývojem nových technologií. Pojem soukromí lze chápat jako vlastní kontrolu nad informacemi o svých osobních záležitostech, přičemž osoba toto soukromí ztrácí už v momentě, kdy netuší, jakým způsobem může být naloženo s jejími osobními informacemi a to i v případě, že s nimi nijak nakládáno není.[41] Soukromí je pak také chápáno jako sféra myšlení a jednání, které je nezávislé od

[37] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 109.
[38] Toto ustanovení bylo převzato z Evropské úmluvy o ochraně lidských práv a základních svobod z roku 1950. Nahrazen byl pouze pojem korespondence širším pojmem komunikace, který reaguje na možnost využití širší škály komunikačních kanálů, nežli bylo možné využívat v roce 1950. Ostatně i další práva odpovídají Úmluvě, přičemž EU chtěla vytvořením vlastní Listiny více umocnit poskytovaná lidská práva a umocnit hodnoty, kterými se bude řídit.
[39] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, str. XX.
[40] ŠIMÍČEK, Vojtěch, ed. *Právo na soukromí.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3, s. 43.
[41] Viz tamtéž, s. 41.

státního zásahu.[42] Osobní soukromí v sobě zahrnuje i rozhodování o své osobní integritě. Kriticky se k ochraně soukromí staví např. Richard Posner, který pohlíží na problematiku z ekonomického hlediska, jakožto na ochranu, která je ekonomicky neefektivní. Tvrdí, že chráněny by měly býti takové informace, jejichž zpřístupnění veřejnosti by znamenalo ztrátu na hodnotě. Také podotýká, že selektivní zpřístupnění informací může manipulovat s veřejností. Posner se tak spíše než k ochraně soukromí fyzických osob klaní k ochraně soukromí obchodních společností, jelikož jejich ochrana může zlepšit ekonomickou situaci společnosti. Kriticky se k ochraně soukromí staví také Judith Jarvis Thomson, která zamýšlí, že ochrana soukromí je jen souhrnem již exitujících práv jako je např. vlastnické právo, svoboda, právo na život.[43] Domnívám se, že tento kritický pohled není na místě, neboť tímto způsobem by bylo možné přistupovat i k jiným právům, jako je např. vlastnické právo, které v sobě zahrnuje právo držby, užívání věci, užívání plodů z věci a právo volně s věcí nakládat. Ačkoliv pojem soukromí není zcela jednoznačný, jeho ochrana jakožto souhrnu určitých práv je z hlediska koncepční soudržnosti důležitá. V tomto duchu je i vydávána dosavadní legislativa, neboť s tímto pojmem operuje, přičemž podrobnější výklad je ponechávána na rozhodovací praxi soudů, popřípadě na výkladu dozorových úřadů.

Právo na ochranu soukromí je relativní právo, může být tedy omezeno, pokud vstoupí do kolize s jiným ústavně zaručeným právem. V takovém případě však musí být dodržen princip proporcionality, neboť omezení takového práva je možné pouze v případě, kdy je to nezbytně nutné a spravedlivě požadovatelné a to tak, aby byl naplněn účel omezení, a zároveň není k dispozici žádný mírnější zásah do práv dané osoby. Dále platí, že čím se jedná o intimnější informace z osobní sféry člověka, tím spíše musí být kladeny přísnější nároky na proporcionalitu takového omezení.[44] V rámci informační společnosti dochází stále častěji ke konfliktu mezi různými základními právy (např. ochranou osobních údajů a práva na informace). Přičemž právě konflikt těchto práv neznamená, že by tato práva měla být určitým způsobem oslabena, ba spíše naopak v rámci

[42] WALDO, James, Herbert LIN a Lynette I MILLETT. *Engaging privacy and information technology in a digital age.* Washington, D.C.: National Academies Press, c2007. ISBN 978-0-309-10392-3, s. 376.
[43] DECEW, Judith. Privacy. *Stanford Encyclopedia of Philosophy* [online]. Kalifornie: The Metaphysics Research Lab, 2016, 14.5.2002 [cit. 2018-09-29]. Dostupné z: https://plato.stanford.edu/entries/privacy/#CriPri.
[44] ŠIMÍČEK, Vojtěch, ed. *Právo na soukromí.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3, s. 60-62.

argumentace pro to či ono právo by měla plnit svůj účel a smysl. Problematická může být i definice pojmu informační společnost, protože to jsou právě informace, které drží každou společnost pohromadě. Pojem tedy není možné vykládat pouze jako organizovanou společnost, nýbrž jako společnost, která si je vědoma důležitosti informací, přičemž ke zvýšení své informovanosti využívá nových technologií.[45]

Domnívám se, že ochrana soukromí, potažmo osobních údajů, je v rámci EU klíčová. Jedná se o jednu z oblastí, kterou je vhodnější řešit na unijní úrovni, nežli pouze v rámci legislativy členských států. Díky internetu a moderním technologiím není možné zabezpečit, aby osobní údaje nebyly předávány vně hranic. Je tedy proto žádoucí, aby ochrana osobních údajů byla sjednocena nejen v celé Evropě, ale aby se vedl i dialog mezi ostatními státy ohledně ochrany osobních údajů a byly tak sbližovány jednotlivé legislativy států, které by poskytovaly obdobné standardy. Spolupráce je nutná zejména s USA, neboť většina velkých technologických společností má sídlo právě zde. Harmonizovaná legislativa by měla především poskytovat stejnou právní ochranu osobních údajů na celém území, ale také by měla sjednocovat sankce a jejich vymahatelnost.

S ohledem na postavení ochrany soukromí a rozsáhlosti sekundární legislativy lze usoudit, že EU poskytuje nejvyšší úroveň ochrany soukromí na celém světě. Sekundární předpisy EU dokonce inspirují některé státy k tvorbě vlastní legislativy na ochranu soukromí. Příkladem může být čínský zákon o internetové bezpečnosti, který zcela nově zavedl v čínské legislativě určité standardy ochrany osobních údajů a zavedl jasná pravidla, jakým způsobem mohou obchodní společnosti získávat, uchovávat či předávat osobní údaje.[46]

2.2. Počátek ochrany osobních údajů

Za první právní dokument v Evropě lze označit Úmluvu č. 108 Rady Evropy z roku 1981, která si předeslala chránit osobní údaje občanů států

[45] MATEJKA, Ján. *internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6, s. 37-38.
[46] China's data privacy standard came into effect this May - inspired by GDPR. Computerworld UK [online]. London, 2018 [cit. 2018-09-11]. Dostupné z: https://www.computerworlduk.com/data/how-chinas-data-privacy-law-was-inspired-by-gdpr-3678918/.

ratifikujících Úmluvu. Ačkoliv se nejedná o vůbec první dokument[47] týkající se ochrany osobních údajů na území Evropy, jeho důležitost tkví v tom, že se jedná o první právně závazný předpis.[48] Úmluva reagovala na nové technologie umožňující automatické zpracování osobních údajů, přičemž stanovovala zejména určité mantinely používání automatického zpracování. Vydání tohoto dokumentu nám dokazuje, že legislativa v oblasti ochrany osobních údajů reaguje zejména na nové technologické možnosti a soustřeďuje svou pozornost na ochranu obrovského množství dat proudících po síti. Již v této Úmluvě bylo stanoveno účelové omezení zpracování osobních údajů, tedy že osobní údaje mohou být zpracovány pouze pro určité, výslovně vyjádřené a legitimní účely.[49]

Úmluva determinovala tzv. zvláštní kategorii osobních údajů, které požívají zvláštní ochranu. Jedná se o osobní údaje, které mohou významně poškodit danou osobu, dle dikce Úmluvy jde o barvu pleti, politické názory, náboženské či jiné vyznání, údaje o zdravotním stavu, sexuálním životě a kriminálních záznamech. Úmluva především zakazovala jejich automatické zpracování.[50]

Ochranu osobních údajů jakožto základní lidské právo reagující na rozvoj informačních a komunikačních technologií zakotvuje v právu EU článek 8 LZPEU. Evropská unie si dále předsevzala v článku 16 Smlouvy o fungování Evropské unie (dále jen jako „SFEU“) přijmout pravidla o ochraně fyzických osob při zpracování osobních údajů, přičemž odkazuje na článek 39 Smlouvy o Evropské unie (dále jen jako „SEU“), ve kterém vymezuje, že dodržování této ochrany bude vykonáváno nezávislými orgány. V České republice je tímto orgánem Úřad pro ochranu osobních údajů, který vykonává dohled nejen nad dodržováním vnitrostátní úpravy, ale dohlíží i nad úpravou práva EU dle zmíněného čl. 39 SEU.

---

[47] Tím jsou Pokyny k ochraně osobních údajů vydané Organizací pro hospodářskou spolupráci a světový rozvoj z roku 1980.

[48] *Cross-border issues under EU data protection law with regards to personal data protection.* Taylor & Francis Online [online]. Londýn: Informa UK Limited, 2018, 24.05.2017 [cit. 2018-09-17]. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1330740.

[49] Article 29 Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf., s. 6-8.

[50] Automatickým zpracováním se dle čl. 2 písm. c) Úmluvy rozumí operace, kdy se zcela či částečně automaticky data ukládají, provádí aritmetické či logické operace na těchto datech, jejich změna, vymazání, vyhledávání či šíření.

2.3. Směrnice 95/46/ES

Potřeba jednotného rámce ochrany osobních údajů v rámci EU dospěla k přijetí Směrnice 95/46/ES[51], která měla být implementována do právních řádů členských států do 24. října 1998. V České republice se jednalo o přijetí zákona č. 101/2000 Sb., o ochraně osobních údajů, který před vstupem do EU doznal mnoha novelizací.[52] V rámci EU se jednalo o první závazný sekundární předpis v oblasti ochrany osobních údajů. Směrnice zakotvila řadu principů, přičemž tím hlavním je, že osobní údaje mohou být zpracovávány pouze pro specifický, výslovně vyjádřený a legitimní účel. Zároveň platil zákaz zpracovávat osobní údaje v rozporu s tímto účelem. Také došlo k definici citlivých osobních údajů a zpřísnění jejich ochrany. Zavedena byla povinnost informovat subjekt údajů o zpracování osobních dat, konkrétně o způsobu jejich zpracování, povinnost identifikace zpracovatele a určení účelu jejich zpracování.[53] Zaveden byl termín správce osobních údajů, tedy osoby, která má osobní údaje ve správě a určuje jejich účel a prostředky zpracování. Jednalo se o právní předpis, který měl vzhledem k rozdílným právním předpisům členských států v oblasti ochrany osobních údajů zabránit nemožnosti jejich volného pohybu mezi členskými státy. Komise vydala pracovní program pro lepší provádění Směrnice 95/46/ES, v rámci kterého vyhodnocovala, jak členské státy aplikují směrnici. Nutno shrnout, že ačkoliv došlo ke sblížení ochrany osobních údajů, nebyly cíle zcela naplněny. Proto při vydávání nového právního předpisu v oblasti ochrany osobních údajů (GDPR) byla zvolena forma nařízení, která by tohoto cíle měla dosáhnout lépe.

Zároveň došlo k přijetí speciální směrnice týkající se ochrany osobních údajů a ochrany soukromí v telekomunikačním sektoru.[54] Vzhledem k rychlému technologickému vývoji došlo brzy k přijetí nové směrnice pod číslem 2002/58/EC, která se zabývala zejména lokalizačními údaji vznikajícími důsledkem vzdálené komunikace.

---

[51] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[52] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 41
[53] ZEVENBERGEN, Jaap. *European Privacy Law and its Effect on Location Information* [online]. Delft, the Netherlands, 2004 [cit. 2019-03-03]. Dostupné z: http://www.otb.tudelft.nl/fileadmin/Faculteit/Onderzoeksinstituut_OTB/Over_OTB/Medewerkers/alle_medewerkers/doc/jaapz.pdf. Delft University of Technology.
[54] Směrnice 97/66/EC Evropského parlamentu a Rady z 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v telekomunikačním sektoru.

2.4. Nařízení 45/2001/ES

V roce 2000 došlo ke schválení Nařízení 45/2001/ES[55], jehož cílem bylo zajistit dodržování ochrany osobních údajů i mezi orgány členských států a institucí Společenství pří výkonu jejich pravomocí. V každém orgánu měl být ustanoven inspektor ochrany osobních údajů, jehož povinností bylo dohlížet na dodržování zpracovávání osobních údajů. Zřízen byl úřad inspektora ochrany osobních údajů, jehož úkolem je dohled nad zpracováním osobních údajů ze strany orgánů EU, poskytování poradenství orgánům EU, vyřizování stížností a sledování nových technologií, majících dopad na ochranu osobních údajů.[56] Volební období inspektora je pětileté a v současnosti funkci zastává italský politik Giovanni Buttarelli.

2.5. Strategie pro jednotný digitální trh

Strategie pro jednotný digitální trh je projekt Evropské komise, jehož cílem je v rámci jednotného trhu sbližovat evropské státy v oblasti digitálního prostoru. Strategie byla přijata 6. května 2015 a sestává ze tří pilířů. Prvním pilířem je zlepšení přístupu spotřebitelů k digitálnímu zboží a službám v Evropě, druhým je rozvoj digitálních sítí a služeb a posledním pilířem je maximalizace růstového potenciálu digitální ekonomiky. V rámci prvního pilíře by mělo dojít k odstranění bezdůvodných překážek, zlevnění přeshraniční dopravy, ochrana zákazníků nakupujících online a celková podpora přeshraničního digitálního trhu. V současnosti již bylo přijato nařízení, které zakazuje bezdůvodné blokování uživatelů na základě zeměpisné polohy. Již by tedy nemělo docházet k blokování služeb poskytovaných skrze internet v některých zemích. V roce 2021 by zároveň mělo dojít k přijetí nových daňových pravidel, které by měly více zpřístupnit a zjednodušit digitální trh v EU. V rámci rozvoje digitálních sítí a služeb bude podporován rozvoj 5G sítě v EU, veřejné organizace by měly nabízet Wi-Fi připojení zdarma a také přijetí evropského kodexu pro elektronické komunikace,

[55] Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů

[56] *EUROPEAN DATA PROTECTION SUPERVISOR* [online]. Brussels, 2019 [cit. 2019-03-17]. Dostupné z: https://edps.europa.eu/edps-homepage_en.

který právně upraví vše výše uvedené.[57] V rámci třetího pilíře by měl být zajištěn volný pohyb neosobních údajů v rámci EU a to zejména s ohledem na podporování cloudových služeb a zároveň také na ochranu dat v cloudu uložených. Mělo by dojít k rozvoji online služeb nabízených orgány veřejné moci. V rámci Strategie pro jednotný digitální trh mělo dojít k přijetí řady legislativních předpisů, jako jsou modernější pravidla pro autorské právo a elektronické obchodování, harmonizace daňových pravidel a také k přijetí nařízení GDPR a ePrivacy.

Evropská komise předesílá, že by projekt měl zpřístupnit zejména začínajícím společnostem a podnikatelům oslovit širší okruh spotřebitelů skrze technologie, čímž by mělo docházet k vytvoření nových pracovních míst a rozvoji služeb. Jedná se tak o projekt naplňující článek 26 SFEU, v rámci kterého by mělo kromě volného pohybu zboží, služeb a kapitálu, přibýt i volný pohyb dat, který by měl zaručit nové obchodní příležitosti zejména pro malé a střední podniky, ale také pro jednotlivce. V rámci jednotného digitálního trhu by mělo dojít ke zlepšení konektivity internetu po celém území EU, zabráněním bezdůvodného zeměpisného blokování v rámci internetu, zvýšení kybernetické bezpečnosti, ale také ochraně dat v podobě přijetí nových pravidel v rámci nařízení ePrivacy.[58]

2.6. Nařízení GDPR

Důvodem přijetí nového Nařízení GDPR bylo dle úvodních článků recitálu GDPR snaha sjednotit právní úpravu v rámci členských zemí EU, ale také rychlý technologický rozvoj, tedy rozvoj internetu a sdílení osobních údajů pomocí internetu. Ačkoliv měla být právní úprava sjednocena již předchozí směrnicí 95/46/ES, forma směrnice nezajistila jednotu v rámci právních úprav členských zemí při implementaci. Z tohoto důvodu byla použita forma nařízení dle čl. 288 SFEU, které je závazné ve všech svých částech a přímo aplikovatelné ve všech členských státech.[59] Přestože není potřeba nařízení transponovat do právního řádu členského státu, GDPR předpokládá přímou implementaci národním právním

[57] *Right environment for digital networks and services.* European Commission [online]. 2018 [cit. 2019-02-10]. Dostupné z: https://ec.europa.eu/digital-single-market/en/right-environment-digital-networks-and-services.
[58] *Digital single market.* European Commission [online]. 2018 [cit. 2019-02-10]. Dostupné z: https://ec.europa.eu/commission/priorities/digital-single-market_en.
[59] TICHÝ, Luboš. *Evropské právo. 5., přeprac. vyd.* V Praze: C.H. Beck, 2014. Academia iuris (C.H. Beck). ISBN 978-80-7400-546-6, s. 201-202.

předpisem a v čl. 23 uvádí určité mantinely, v rámci kterých se může legislativa jednotlivých států s přihlédnutím k nezbytnosti, přiměřenosti a s respektem k lidským právům pohybovat. Členské státy jsou povinny nařízení přímo aplikovat, ačkoliv nepřijaly do doby účinnosti nařízení, tedy ke dni 25. května 2018, vlastní národní úpravu. Samotné nařízení dále ruší povinnost oznamovat dozorovému úřadu[60] zpracování osobních údajů, ale spíše se soustředí na provádění dokumentace podniknutých kroků správců v oblasti ochrany osobních údajů pro prokázání souladu s právními předpisy. Domnívám se, že tento krok může vést k nadměrnému zatížení správců a to zejména s ohledem na vypracovávání rozsáhlých analýz ze strachu před sankcemi, které mohou dosahovat až 20 000 000 EUR nebo 4 % celosvětového ročního obratu[61], přičemž je otázkou, zda při vypracovávání evidenčních dokumentů budou opravdu zvažovány jednotlivé procesy zpracování osobních údajů, nebo je budou správci vytvářet, jen aby prokázali předstíranou snahu o prokázání souladu s požadavky GDPR.

Předmětem nařízení je stejně jako u předchozí směrnice ochrana fyzických osob v souvislosti se zpracováním osobních údajů, což zajišťuje kromě přiznání určitých práv fyzickým osobám, také zejména stanovení určitých povinností správcům osobních údajů.[62] Došlo také k rozšíření místní působnosti, neboť GDPR se vztahuje na správce a zpracovatele i mimo území EU, pokud zpracovávají osobní údaje subjektů nacházejících se na území EU. To se týká zejména poskytovatelů služeb skrze internet majících sídlo mimo území EU (zejména v USA). Problematické však může být vymáhání ochrany osobních údajů u subjektů nemající na území EU žádný majetek.

2.6.1. Správce, zpracovatel a subjekt údajů

Pro další výklad je nezbytné si definovat jednotlivé strany, které v rámci předávání osobních údajů vystupují. Správcem se dle článku 4 GDPR rozumí: *fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních*

[60] V ČR je jím Úřad pro ochranu osobních údajů, jakožto ústřední správní úřad vykonávající dohled nad oblastí ochrany osobních údajů, který byl zřízen zákonem č. 101/2000 Sb., o ochraně osobních údajů dne 1. 6. 2000 spolu s účinností uvedeného zákona.
[61] ČR využila možnosti snížení maximální výše sankce pro orgány veřejné moci, která dle návrhu zákona o zpracování osobních údajů představuje částku ve výši 10 000 000 Kč.
[62] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů.* 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7., s. 59-61.

údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení. Ačkoliv tato definice může vypadat poněkud zvláštně a nelogicky, pak by z ní mělo být patrné, že samotný správce osobní údaje nemusí vůbec zpracovávat. Může tak zcela pověřit zpracovatele, aby za něho zpracovával osobní údaje, přičemž na správci zůstává odpovědnost za jejich zpracování, pokud není smluvně dohodnuto jinak. Stejně tak je odpovědný za dodržování veškerých zásad pro zpracování. Správcem může být např. provozovatel internetového obchodu, zaměstnavatel, lékař, nebo třeba škola. Jde tak o subjekty, které se rozhodly pro určitou činnost, jejíž nezbytnou součástí je zpracování osobních údajů, přičemž samotné zpracování mohou provádět samy, zcela pověřit zpracovatele, či přenést jen část své zpracovatelské činnosti na zpracovatele.

Pod pojmem zpracování osobních údajů nelze rozumět jejich pouhé získávání, ale jakýkoliv systematický úkon, který provádí správce či zpracovatel. Kromě sběru dat, jde o jejich kopírování, vyhledávání, třídění, výměnu, jakékoliv používání, ale i jejich publikování na webových stránkách.[63]

Zpracovatelem dle GDPR je: *"fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce"*. Zpracovatel nemusí být určen pouze na základě smlouvy, ale může být zvolen zákonným zmocněním a to zejména ve veřejné sféře. Jedná se například o katastrální úřady, které jsou zmocněny katastrálním zákonem.[64] V případě, že se správce rozhodne dobrovolně využít služeb zpracovatele, je nezbytné, aby s ním uzavřel písemnou smlouvu o zpracování osobních údajů. Smlouva o zpracování osobních údajů musí obsahovat veškeré náležitosti, které jsou uvedeny v čl. 28 GDPR. Zpracovatel v rámci zpracování osobních údajů musí dodržovat mlčenlivost, zajistit bezpečnostní opatření k ochraně osobních údajů, smazat či vrátit veškeré osobní údaje při pokynu správce a dále je povinen poskytnout správci veškeré informace potřebné k doložení splnění zákonných povinností. V případě že by zpracovatel sám mimo smlouvu určil účel či prostředky zpracování, pak je zpracovatel považován za správce. V rámci zpracovatelské smlouvy může být i ujednáno, že zpracovatel může ke zpracování osobních údajů využít i další

[63] Rozsudek ESD ze dne 6. listopadu 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596, bod. 25.
[64] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7., s. 91-93.

zpracovatele, přičemž je nutné, aby zpracovatel o každém využití dalšího zpracovatele informoval správce. Pokud by toto explicitní svolení nebylo ve smlouvě uvedeno, je nutné, aby mezi správcem a zpracovatelem došlo k písemné dohodě o využití dalšího zpracovatele.

Jako subjekt údajů je dle GDPR označována fyzická osoba, k níž se osobní údaje vztahují. Aby měly tyto osoby nárok na ochranu svých osobních údajů, je nezbytné, aby se jednalo o žijící osoby v EU, neboť je vyloučena ochrana osobních údajů zesnulých osob. Právní předpisy v oblasti ochrany osobních údajů těmto osobám přiznávají řadu práv. Jde zejména o právo být zapomenut, na výmaz a opravu osobních údajů, nebýt předmětem automatizovaného rozhodování, vznést námitku ke správci či obrátit se na dozorový úřad.

2.6.2. Pověřenec pro ochranu osobních údajů

Každý správce či zpracovatel má možnost pověřit jím určenou osobu, která bude dohlížet na ochranu osobních údajů při jejich zpracování. Subjekty veřejné moci (s výjimkou soudů), osoby provádějící rozsáhlé pravidelné a systematické monitorování, nebo jejíž hlavní činností je zpracování zvláštních kategorií údajů, mají povinnost tuto osobu ustanovit. Může se jednat buď přímo o zaměstnance, případně se výkonem pověřence může smluvně zavázat třetí osoba, přičemž by nemělo docházet ke střetu zájmů. Je přípustné, aby služby pověřence poskytovala právnická osoba, avšak i v takovém případě je nutné zvolit jednu konkrétní fyzickou osobu, která bude funkci pověřence vykonávat.[65] Pověřenec při výkonu své činnost nesmí dostávat pokyny ke konkrétním krokům a musí působit zcela nezávisle. V současnosti jsou již takové služby komplexně nabízeny obchodními společnostmi či advokátními kancelářemi. U externích společností lze jako výhodu shledávat vyšší odbornost v oblasti ochrany osobních údajů, zároveň i podstatně nižší možnost střetu zájmů a ovlivňování správce.

Jeli správcem nebo zpracovatelem orgán veřejné moci, může být s ohledem na velikost těchto orgánů jmenován pouze jeden pověřenec pro ochranu osobních údajů, který provádí činnost pověřence pro zvolený okruh orgánů. V případě obchodních společností, které jsou tvořeny vícero entitami, může být jmenován jediný pověřenec pro všechny tyto dílčí společnosti. U ostatních

[65] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4, s. 42.

společností, které nemají povinnost ustanovit pověřence pro ochranu osobních údajů lze doporučit, aby takovouto osobu jmenovaly dobrovolně, neboť tím bude dosaženo zajištění dohledu nad zpracováním. Jedná se i o pozitivní signál vůči dozorovému úřadu, že správce nebere ochranu osobních údajů na lehkou váhu. Pro snazší rozhodování zda má správce povinnost jmenovat pověřence pro ochranu osobních údajů, či nikoliv, lze doporučit, aby správce vypracoval analýzu, kde budou popsány důvody, pro které není pověřenec jmenován. Tímto dokumentem by správce následně prokazoval dozorovému úřadu soulad s právními předpisy na ochranu osobních údajů.[66] Náplní práce pověřence je především dohlížet na soulad zpracování s právními předpisy a poskytovat správci či zpracovateli rady ohledně ochrany osobních údajů. V případě jmenování pověřence však nedochází k přenesení odpovědnosti a nadále to tak bude správce či zpracovatel, kteří jsou odpovědni za dodržování právních předpisů v oblasti ochrany osobních údajů.

Pověřenec ochrany osobních údajů není zcela novým institutem, nýbrž byl již zahrnut v různých legislativách členských zemí, včetně Slovenska. Pověřenec by měl fungovat jako zcela nezávislý orgán, který není v oblasti ochrany osobních údajů nikým vázán. Při jeho agendě by tak nemělo docházet ke střetu zájmů, které by mohly narušit správný výkon funkce. Pověřenec by dle GDPR měl dosahovat patřičné úrovně odbornosti a profesních kvalit, a to zejména s ohledem na rozsah zpracování osobních údajů a míru citlivosti údajů. Předpokládá se zejména vysoká úroveň znalostí národních a evropských předpisů na ochranu osobních údajů. Konkrétní znalosti či dovednosti nejsou v GDPR vymezeny, neboť budou rozdílné u každého správce osobních údajů. Přesto je vhodné, aby osoba byla dostatečně kvalifikována a aby rozuměla procesům zpracování a aby se nadále vzdělávala a absolvovala vhodná školení.[67] Taková osoba by měla ovládat na patřičné úrovni alespoň jeden úřední jazyk EU, aby byla schopna komunikovat se zahraničními dozorovými úřady. V současném návrhu zákona o ochraně osobních údajů se počítá s tím, že akreditační orgán Český institut pro akreditaci, o.p.s. bude vydávat akreditace, na základě kterých budou moci být udělovány certifikáty pro

[66] NEŠPŮREK, Robert, Jaroslav ŠUCHMAN a Ján JAROŠ. Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?. *Epravo.cz magazine* [online]. 2018, 2018(1), 41-43 [cit. 2019-03-08]. Dostupné z: https://www.epravo.cz/_dataPublic/data/E-pravo_mag/2018_E1_web.pdf.
[67] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 361-370.

pověřence, jenž by měly sloužit jako prokázání profesních kvalit pro výkon správce. Po jmenování pověřence by správce či zpracovatel měl zveřejnit jeho kontaktní údaje a dále je sdělit dozorovému úřadu. Údaje musí být zveřejněny takovým způsobem, aby jej na základě nich mohl dozorový úřad či subjekt údajů snadno kontaktovat. S dozorovým úřadem je pověřenec povinen v případě potřeby komunikovat.

2.7. Nařízení ePrivacy

Od vydání Směrnice 2002/58/ES, známé jako „Cookie směrnice“, uplynula již značná doba a od roku 2002 technologický pokrok zejména v online prostředí pokročil výrazným tempem. Z tohoto důvodu shledala Evropská komise v rámci Strategie pro jednotný digitální trh za nezbytné, přezkoumat nyní ještě účinnou Směrnici o soukromí a elektronických komunikacích. Nový návrh nařízení ePrivacy reaguje především na správce osobních údajů, kteří poskytují komunikační služby přes internet. Jedná se o služby VoIP, instant messaging, nebo třeba emailové služby (dále jen „OTT služby“)[68], jež Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 nezahrnovala do své působnosti. Nařízení ePrivacy by mělo zaručovat, aby poskytovatelé OTT služeb poskytovali obdobné standardy při komunikaci, které musí poskytovat telekomunikační operátoři. Jedná se zejména o důvěrnost komunikace a tedy ochranu jejího obsahu, včetně osobních údajů. Předmět Nařízení je tedy širší v tom smyslu, že nechrání pouze osobní údaje, ale i samotný obsah komunikace. Kromě obsahu zpráv dopadá nařízení na zanechané stopy na internetu a metadata (např. doba hovoru, místo hovoru apod.). Přirozeně návrh ePrivacy vyvolal u poskytovatelů OTT služeb značnou vlnu kritiky, nicméně je třeba, aby byl určitým způsobem chráněn obsah komunikace přenášené skrze internet a nespoléhat se pouze na samoregulaci poskytovatelů služeb.

Dalším důležitým bodem by mělo být zjednodušení pravidel při využívání cookies. V současnosti jsou webové stránky plné vyskakovacích pop-up oken vyzývajících uživatele k souhlasu se zpracováním cookies. Ve většině případů uživatelé netuší jak cookies fungují a zbytečně je tyto výzvy k udělení souhlasu obtěžují. Mělo by dojít k odpadnutí potřeby vyžadování souhlasu na všechny typy

[68] Z angl. Over the Top, značí přenášení textového, zvukového či obrazového obsahu mezi dvěma a více uživateli přes internet.

cookies. Oproti předchozí úpravě byla stejně jako u GDPR zvolena forma nařízení, neboť vzhledem k přímé aplikovatelnosti by měla zajistit stejný režim ochrany ve všech členských státech, což nyní ještě účinná směrnice nečiní, neboť umožňuje nastavit členským státům různá pravidla.[69] Cíle a principy původní směrnice jsou však zachovány, pouze došlo ke změně způsobu ochrany s ohledem na technologické a hospodářské změny. Ochrana dat dle nařízení bude zajišťována stejně jako u GDPR pověřeným orgánem.[70] Nařízení ePrivacy mělo původně nabýt účinnosti stejně jako GDPR dne 25. května 2018, ale vzhledem k značenému množství připomínek se tomu tak nestalo, přičemž v současné době je stále veden trialog nad zněním nařízení. Dle slov současného Evropského inspektora ochrany osobních údajů Giovanni Buttarelliho je ePrivacy posledním základním dílkem skládačky představujícím ochranu dat a soukromí v EU.[71] Tato dualita právní úpravy v oblasti ochrany osobních údajů je již v právu EU tradiční, neboť i v minulosti byla oblast ochrany dat v telekomunikacích vždy upravena samostatně.[72] Jedná se o celkem logické rozdělení úpravy ochrany osobních údajů, neboť povaha a způsob, kterým jsou data chráněna v rámci komunikačních služeb, jsou odlišné. Rozdílný je také rozsah subjektů, neboť v rámci ePrivacy jsou chráněny taktéž právnické osoby, což vyplývá přímo z bodu č. 3 recitálu nařízení, kde je tato skutečnost zdůvodněna tím, že data elektronických komunikací mohou odhalit též obchodní tajemství či jiné citlivé informace.

Nařízení ePrivacy bude fungovat jako *lex specialis* vůči GDPR v oblasti ochrany osobních údajů. Tam, kde nebude konkrétně upraveno zpracování osobních údajů, budou použita ustanovení GDPR. Současně se ePrivacy opírá o definice pojmů uvedené v evropském kodexu pro elektronické komunikace.[73]

Nařízení ePrivacy je zaměřeno zejména na poskytovatele OTT služeb, přičemž je zároveň stanovena negativní působnost, která z působnosti ePrivacy

[69] K srovnání například články 17,21,23,36, 44 a řada dalších, které mají formu spíše určitých návrhů možností řešení, které mohou členské státy využít. Neurčitost a nejednoznačnost byla mimo jiné shledána i hodnocením REFIT vztahující se k této směrnici.
[70] *Proposal for an ePrivacy Regulation. European Commission* [online]. 2018 [cit. 2019-02-10]. Dostupné z: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.
[71] YUN CHEE, Foo. *Exclusive: EU privacy chief expects first round of fines under new law by year-end.* Reuters [online]. New York: Thomson Reuters, 2019 [cit. 2019-02-11]. Dostupné z: https://uk.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUKKCN1MJ2AY.
[72] Konkrétně Směrnicí 97/66/EC a Směrnicí 2002/58/EC
[73] Směrnice Evropského parlamentu a Rady 2018/1972, ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace.

vylučuje činnost orgánů, institucí a agentur Unie, na něž se vztahují zásady a povinnosti stanovené v Nařízení Evropského parlamentu a Rady č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů. OTT služby bývají poskytovány převážně zdarma, přičemž za jejich užívání se uživatelům zobrazují reklamy, případně poskytují své osobní údaje pro další zpracování. Tyto služby se často prolínají spolu se službami pro přenášení obsahu, sociálními sítěmi, či třeba platebními službami (NFC platby).[74]

Nařízení v duchu principu proporcionality a subsidiarity dle čl. 5 SEU stanovuje pouze určitý rámec nezbytné úpravy, který členské státy mohou dle potřeby doplnit. V České republice je Směrnice 2002/58/ES transponována do zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) a lze tak očekávat, že po přijetí ePrivacy dojde k novelizaci tohoto zákona a zároveň k přijetí dalších opatření.

2.7.1. Výsledky posuzování REFIT

Iniciativa REFIT (The Regulatory Fitness and Performance) sleduje, zda právní předpisy EU naplňují zamýšlený cíl, zda zbytečně nezatěžují podniky a jedince a také zkoumá ekonomický dopad právních předpisů. V lednu roku 2017 vydala Evropská komise dokument, který hodnotí předchozí směrnici 2002/58/EC.[75] Hodnocení této směrnice sloužilo jako jeden z hlavních podkladů pro tvorbu nového nařízení ePrivacy. Směrnice 2002/58/EC si stanovila následující tři cíle:

1. Zajistit stejnou úroveň ochrany soukromí a důvěrnosti s ohledem na zpracování osobních údajů v rámci elektronických komunikací po celém území EU, která je poskytována i právnickým osobám.
2. Zajistit stejnou úroveň ochrany s ohledem na zpracování osobních údajů v odvětví elektronických komunikací s cílem zajistit základní právo na ochranu osobních údajů.

[74] POLČÁK, Radim. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8, s. 536.
[75] Commission staff working document, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, SWD(2017) 5 final. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0005&from=GA.

3. Zajistit volný pohyb osobních údajů vznikajících užíváním elektronických komunikací v rámci vnitřního trhu a volný pohyb koncových zařízení a služeb.

Tyto cíle mají i nadále význam, proto jsou aktuální i pro ePrivacy. Shledáno však bylo, že nástroje, které směrnice nabízí, jsou s ohledem na technologický pokrok a změny již zastaralé. Jedním z hlavních problémů, je skutečnost, že směrnice nezahrnuje poskytovatele OTT služeb, přičemž tyto služby jsou dle průzkumu Eurobarometru využívány 74% občanů členských států denně. Průzkum zároveň ukázal, že si občané členských států přejí stejnou ochranu v rámci komunikací, kterou zajišťují telekomunikační operátoři.[76] Jako zastaralý a neefektivní byl shledán požadavek, kdy jsou uživatelé při procházení webových stránek neustále vyzýváni k vyjádření souhlasu se zpracováváním cookies, čímž je snižován komfort při jejich procházení. Směrnice navíc nereaguje na nové možnosti, jakými jsou např. otisky prstů. Efektivitu vyžadování souhlasu se zpracováváním cookies navíc snižují i zvýšené náklady na zřizování bannerů vyzývajících k souhlasu. Nakonec byla problematickým shledána rozdílná implementace některých ustanovení v různých členských státech.

Dle výsledků posuzování REFIT by tak uvedené cíle měly být nadále relevantní, přičemž by v rámci nařízení ePrivacy mělo dojít ke změnám, které těchto cílů budou lépe dosahovat.

2.7.2. Kritika ePrivacy

Současný návrh nařízení ePrivacy je kritizován zejména s ohledem na zásadu důvěrnosti komunikace, kde je v čl. 5 stanoveno, že by měl mít přístup k datům komunikace pouze koncový uživatel. Takto vymezené zásadě mohou snadno vyhovět telekomunikační operátoři využívající tradiční komunikační sítě, avšak v případě OTT služeb to může být složité, neboť jejich úspěšnost tkví zejména v tom, že využívají obsah komunikací pro poskytování vedlejších služeb, které poskytují uživatelům komfort při jejich využívání.[77] ePrivacy je v určitých ustanoveních v rozporu se zněním GDPR, když například v čl. 6 ePrivacy je vyžadován souhlas pro zpracování osobních údajů i pro zpracování založeném na

[76] Eurobarometer průzkum z července 2016, č. 443 (SMART 2016/079), dostupný z: ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82290.
[77] ePrivacy může ohrozit technologické inovace. Sdružení pro internetový rozvoj [online]. Praha [cit. 2019-03-16]. Dostupné z: http://www.spir.cz/eprivacy-muze-ohrozit-technologicke-inovace.

plnění smluvní povinnosti, přičemž čl. 6 GDPR to považuje jako samostatný právní titul, u kterého není vyžadován další souhlas. V rámci recitálu ePrivacy zcela absentuje odůvodnění pro tuto odchylku. ePrivacy dále shledává legitimní a užitečné nástroje pro analýzy webu, přesto pro ně nestanovuje výjimky pro získání souhlasu. Požadavek souhlasu by tyto nástroje činil nepoužitelnými, navíc by byl v rozporu se snahou odstraňovat bannery vyžadující od uživatelů souhlas se zpracováním cookies.[78]

2.8. Základní zásady zpracování osobních údajů

Následující zásady jsou v oblasti ochrany osobních údajů významné, neboť s nimi pracují veškeré právní předpisy na ochranu osobních údajů a stejně tak výklad jednotlivých ustanovení má být v jejich souladu. Většina zásad již byla uvedena ve směrnici 95/46/ES, avšak v GDPR došlo k jejich zpřesnění. Nařízení ePrivacy jakožto *lex specialis* k GDPR na těchto zásadách také staví a některé i speciálně upravuje ve vztahu k ochraně osobních údajů v rámci elektronických komunikací. Zásady jsou v rámci legislativy týkající se ochrany osobních údajů velmi významnými, neboť řada ustanovení je velmi obecná a je třeba je vykládat v souladu s těmito zásadami. Správce je odpovědný za prokázání souladu s právními předpisy dozorovému úřadu, k čemuž mu mohou dopomoci právě uvedené zásady, které aplikuje na své procesy zpracování osobních údajů.

GDPR v čl. 23 umožňuje, aby tyto zásady byly v určitých důležitých případech omezeny. Jedná se např. o případy obrany státu, národní bezpečnost, odhalování trestných činů či k zajištění nezávislosti soudnictví. Mělo by se tak jednat o krajní možnost nezbytnou k vyvážení jiných významnějších práv či zájmů.

2.8.1. Zásada zákonnosti, korektnosti a transparentnosti

Zásady vycházející z článku 5 odst. 1 písm. a) GDPR lze označit jako nejdůležitější zásady ochrany osobních údajů vyjadřující, že by jakékoliv nakládání s osobními údaji mělo probíhat otevřeně vůči osobě, o jejíž údaje se jedná a tato osoba by měla znát účel jejich zpracování. Správce by měl subjekt

[78] HÄRTING, Niko. *STUDY ON THE IMPACT OF THE PROPOSED EPRIVACY REGULATION* [online]. Berlin, 2017 [cit. 2019-03-14]. Dostupné z: https://www.haerting.de/sites/default/files/downloads/study_on_the_impact_of_the_proposed_eprivacy_regulation.pdf. Studie. HÄRTING Rechtsanwälte.

údajů informovat, jakým způsobem bude s jeho údaji nakládáno a komu budou zpřístupněny. Musí být zajištěna rovnováha mezi tím, jaké údaje jsou zpracovávány a za jakým účelem.

Důležitá je zejména zásada zákonnosti, která stanovuje, že veškeré zpracování osobních údajů musí probíhat na základě některého z právních titulů, kterými mohou být:

- souhlas se zpracováním osobních údajů udělený subjektem údajů;
- zpracování osobních údajů v rámci uzavírání a plnění smluvních závazků;
- nezbytnost zpracování pro splnění zákonné povinnosti vztahující se na správce;
- nezbytnost zpracování pro ochranu životně důležitých zájmů;
- zpracování prováděné správcem, které je nezbytné pro splnění úkolů ve veřejném zájmu;
- zpracování z důvodu oprávněného zájmu správce.

V případě, že by správce hodlal zpracovávat citlivé osobní údaje, nestačí pouze jeden z uvedených právních titulů, nýbrž je nezbytné, aby byla splněna jedna z podmínek uvedených v čl. 9 odst. 2 GDPR. Jedná se např. o zpracování již zveřejněných osobních údajů, zpracování pro významný veřejný zájem, nezbytný výkon lékařských služeb a preventivního lékařství, pro vědecké a archivní účely, výkon a obhajoba právních nároků. Zpracovávat citlivé osobní údaje svých současných a bývalých členů mohou také nadace, sdružení či neziskové organizace, pokud zpracováním sledují politické, filzofické, náboženské či odborové cíle. Z výše uvedených právních titulů se jeví nejkomplikovanějšími zejména zpracování na základě souhlasu a z oprávněného zájmu správce.

Souhlas se zpracováním osobních údajů musí být vždy písemný a v případě, že je udělován v rámci jiného textu (především smlouvy), pak je nutné, aby takovýto souhlas byl viditelně oddělen od ostatní textace, přičemž by neměl být podmiňován k možnosti uzavření smlouvy, neboť by ho nebylo možné považovat za svobodný. Zároveň platí, že musí být srozumitelný a snadno přístupný, a to pod sankcí ztráty závaznosti takto uděleného souhlasu. Z pohledu správce je problematické zejména právo subjektu údajů na odvolání souhlasu, neboť v případě jeho uplatnění je správce povinen přestat zpracovávat osobní

údajů. Lze tak shrnout, že v případě, kdy má správce na výběr z několika možných titulů pro zpracování, pak by získání osobních údajů na základě souhlasu mělo být až poslední možností. V tom je patrný rozdíl oproti zákonu č. 101/2000 Sb., kde nebylo zpracování na základě souhlasu toliko zpřísněno a souhlas tak byl postaven na roveň ostatním právním titulům pro zpracování.

Zpřísnění podmínek použití souhlasu dle GDPR spočívá zejména v tom, že správce bude muset být schopen dozorovému orgánu doložit, že subjekt údajů jednoznačným projevem vůle udělil souhlas.[79] Proto například není správná současná praxe některých internetových obchodů, kde v případě dokončení nákupu je předzaškrtnuté políčko udělení souhlasu se zpracování osobních údajů (tzv. opt-out). Stejně tak je problematické, pokud je uživatel nucen zaškrtnout políčko, ve kterém je uvedeno, že nesouhlasí s předáním svých osobních údajů, jak je znázorněno v příloze č. 2. Získání osobních údajů na základě souhlasu také nesmí být ničím podmíněno. Tedy nelze kupříkladu vyžadovat zaškrtnutí políčka získání osobních údajů na internetovém obchodě určených k marketingovým účelům, bez kterého by nebylo možné dokončit objednávku. Kromě tzv. check-boxů existují i jiné metody. V aplikacích lze například souhlas udělit nakreslením určitého znaku či otočením chytrého telefonu. Vždy se však musí jednat o aktivní jednání. Stejně tak by měli býti zaměstnavatelé vůči zaměstnancům velmi zdrženliví v používání souhlasů pro zpracování osobních údajů, neboť s ohledem na nerovné postavení může být svoboda získání takového titulu lehce zpochybnitelná.

Pokud je to možné, měl by správce údajů co nejvíce užívat tzv. členěný souhlas, v rámci kterého si subjekt bude moci konkrétně vybrat, s jakými operacemi souhlasí. V případě dětí je nezbytné, aby pro účinnost souhlasu bylo dítěti alespoň 16 let.[80] V případě mladšího dítěte je možné souhlas udělit či schválit pouze zákonným zástupcem. Správce by měl vyvinout přiměřené úsilí s ohledem na dostupné technologie k ověření, že souhlas byl udělen zákonným zástupcem dítěte. V případě, že zákonný zástupce udělí rodičovský souhlas, je tento platný i po dosažení potřebného věku dítěte (tj. 16 let), přičemž jej může

[79] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 125-129.
[80] Současný návrh českého zákona na ochranu osobních údajů nahrazující zákon č. 101/2000 Sb. počítá se snížením věkové hranice pro souhlas na 15 let, přičemž GDPR v případě odchylné úpravy členských států požaduje věk alespoň 13 let.

samo vzít zpět či jej jinak upravit.[81] Správce osobních údajů může později zvolit jiný vhodnější titul zpracování, přičemž je povinen o této skutečnosti informovat subjekt údajů. Zvláštní povahu má výslovný souhlas vyžadovaný dle čl. 9 odst. 2 písm. a) GDPR pro zvláštní kategorii osobních údajů.

V online prostředí je typické, že řada služeb je poskytována zdarma, přičemž poskytovatelé výměnou za užívání služby požadují osobní údaje, které jsou často následně užívány pro marketingové účely. V takovém případě nelze souhlas se zpracováním osobních údajů považovat za protiplnění smlouvy a uživateli by měla služba být dostupná i v případě neposkytnutí osobních údajů, byť třeba v omezené funkcionalitě služby.[82]

Zpracování osobních údajů na základě oprávněného zájmu představuje nový titul pro zpracování, jenž je velmi flexibilním a požaduje důkladné určení zájmu, za jakým mají být údaje zpracovány. Správce by měl před použitím tohoto právního titulu důkladně zvážit, zda zájem na získání osobních údajů je dostatečný, resp. zda nad tímto zájmem nepřevažují zájmy, práva či svobody subjektů údajů a následně provést tzv. balanční test. V rámci balančního testu by správce měl zvážit váhu oprávněného zájmu, důsledky zpracování pro subjekt údajů a nakonec přijmout dostatečné záruky pro ochranu práv a svobod subjektů údajů. Obranným institutem vůči zneužívání tohoto titulu jsou námitky proti zpracování, které může subjekt údajů uplatnit vůči správci. Ten je následně povinen znovu poměřit zájmy a případně tyto údaje vymazat a zároveň o podniknutých krocích informovat subjekt údajů. V případě užití titulu oprávněného zájmu za účelem provádění přímého marketingu platí, že v případě podání námitek je správce povinen ihned zastavit zpracovávání osobních údajů. Další omezení spočívá v tom, že tento právní titul nesmějí používat orgány veřejné moci při plnění svých úkolů, přičemž musí využít jiného právního titulu pro zpracování.[83]

Pokud zpracování není prováděno na základě některého z legitimních titulů, pak je prováděno nezákonně. Zásada zákonnosti však neznamená pouze

[81] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 17/EN WP 259. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849, s. 27.
[82] Pokyny pracovní skupiny WP29 ze dne 28. listopadu 2017, WP259, s. 8.
[83] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 135-139.

soulad s GDPR, ale obecně s právním řádem jednotlivých členských zemí a EU (tedy i ePrivacy), případně i se smluvními podmínkami[84], pokud jsou údaje zpracovávány na základě smluvního podkladu.

Zásada transparentnosti se odráží zejména v tom, že správce údajů předem poskytne subjektům informace o zpracování jejich osobních údajů, a to stručným, srozumitelným a snadno dostupným způsobem. Zejména se bude jednat o uveřejnění zásad zpracování osobních údajů na webu. Správce je dále povinen dodržet informační povinnost dle článku 13 a 14 GDPR, když je povinen zejména při získání osobních údajů uvést kontaktní údaje správce (pověřence pro ochranu osobních údajů), účel zpracování, záměr předávat osobní údaje třetím osobám a identifikovat je. Dále pro dodržení zásady transparentnosti je povinen uvést v okamžiku získání osobních údajů po jakou dobu budou údaje uchovávány, informovat subjekt údajů o právu na změnu či výmaz osobních údajů, právu podat stížnost k dozorovému orgánu, informovat o tom, zda dochází k automatizovanému rozhodování či profilování a v případě, že je předání osobních údajů založeno na souhlasu, informovat o možnosti souhlas kdykoliv odvolat.

Bod číslo 10 recitálu k nařízení GDPR umožňuje členským státům pomocí právních předpisů konkretizovat pravidla pro zpracování osobních údajů a tedy upřesnit podmínky, za nichž je zpracování ještě v souladu se zásadou zákonnosti. Právní předpis členského státu může dokonce stanovit přísnější podmínky pro využívání právních titulů zpracování.

Tyto zásady zároveň souvisí s povinností oznamovat porušení zabezpečení osobních údajů dozorovému úřadu a to pokud možno do 72 hodin od okamžiku dozvědění se o porušení. Výjimkou jsou případy, kdy by porušení nepředstavovalo riziko pro práva a svobody fyzických osob. Správce by však měl mít stanovený jasný postup pro případný bezpečnostní incident. Každý incident by měl být následně zdokumentován a měla by být přijata opatření, která by zabránila jejímu opakování.[85]

[84] Viz tamtéž, s. 107-109.
[85] NAVRÁTIL, Jiří. *GDPR pro praxi.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 177.

2.8.2. Zásada účelového omezení

Tato zásada určuje, za jakým účelem mohou být osobní údaje zpracovávány. Ať již jsou osobní údaje zpracovávány na základě smlouvy, souhlasu či plnění zákonné povinnosti, musí být stanoven jasný účel zpracování těchto údajů. Pokud např. subjekt udělí poskytovateli emailových služeb své osobní údaje na základě souhlasu se zpracováním osobních údajů za účelem poskytování emailových služeb, pak není možné, aby správce svévolně tyto údaje využil k jiným účelům nežli poskytování emailových služeb. Účel by měl být specifikován dostatečně konkrétně, aby ho nebylo možné vyložit jiným způsobem. Není tedy možné požadovat souhlas se zpracováním osobních údajů pro „marketingové služby“, neboť se jedná o značně široký pojem a uživatel si pod ním nebude schopen představit, jakým způsobem budou data využita. Takovýto souhlas by byl neúčinný, jelikož by neodpovídal zásadě účelového omezení. V případě že by správce chtěl pokrýt vícero způsobů marketingu, je možné v souhlase všechny tyto způsoby popsat, neboť je možné zpracovávat osobní údaje pro více účelů, avšak musí být vždy dostatečně konkrétně specifikovány. Není však možné kumulovat více zcela rozdílných druhů účelu, tedy např. zasílání reklamních sdělení a plnění smlouvy.[86] Správce musí mít stanoven účel zpracování nejpozději při samotném shromažďování osobních údajů, přičemž s ohledem na výše uvedené lze shrnout, že účel musí být určitý, výslovně vyjádřený a legitimní.[87]

Nařízení přímo stanoví, v jakých případech lze tuto zásadu omezit, jedná se o případy zpracování za účelem archivace ve veřejném zájmu, vědecký či historický výzkum a statistické účely, přičemž pokud je to vhodné, pak by se v těchto případech měla co nejvíce uplatnit zásada minimalizace údajů a také pseudonymizace údajů. Tyto případy jsou v GDPR označovány jako tzv. další zpracování.

[86] Article 29 Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf., s. 15-19.
[87] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s.109-110.

2.8.3. Zásada minimalizace údajů

Minimalizace osobních údajů značí, že by údaje měly být shromažďovány jen v takovém rozsahu, v jakém je to nezbytné pro naplnění účelu, za jakým byly shromažďovány. Správce by měl průběžně zvažovat, zda nejsou některé údaje přebytečné pro naplnění účelu, za jakým jsou shromažďovány, a to i z hlediska časového. Nejedná se o povinnost snížit osobní údaje na nezbytné minimum pro činnost správce, nýbrž by měl správce zpracovávat osobní údaje přiměřeně k účelu zpracování. Tato zásada se aplikuje na zpracování na základě všech právních titulů, přičemž přísněji bude aplikována na zpracování na základě oprávněného zájmu, v rámci kterého je správce povinen přihlížet k balančnímu testu, ve kterém porovnává vlastní zájmy nad právy a svobodami subjektu údajů.[88] Správce by také měl vždy přihlížet, k jakému účelu jsou údaje zpracovány a nezpracovávat údaje, které zjevně s daným účelem nesouvisí.

2.8.4. Zásada přesnosti

Zpracované údaje musejí být přesné, tedy i zároveň aktuální. Pokud subjekt údajů zjistí, že správce o něm eviduje nepravdivý údaj, má právo žádat po správci, aby tyto údaje změnil. Zásada však nevyjadřuje to, že by správce měl neustále kontrolovat pravdivost údajů. V případě že subjekt poskytne správci nepravdivé údaje, pak správce neodpovídá za jejich nepravdivost. Veškeré údaje však nepochází přímo od subjektu údajů, např. poskytovatel emailových služeb spravuje i údaje o odeslaném či přijatém emailu. Subjekt není schopen tyto údaje ovlivnit a je na správci, aby tyto údaje byly přesné. Správce osobních údajů by měl v případě potřeby provádět průběžně aktualizace osobních údajů. Uvedené samozřejmě neplatí při uchovávání historických údajů, kde je účelem uchovat tyto údaje ve formě v jaké byly získány.

2.8.5. Zásady integrity, důvěrnosti a odpovědnosti

Jedná se o zásady, jejichž účelem je, aby osobní údaje byly náležitě zabezpečovány před neoprávněným zpracováním, ztrátou, zničením či poškozením. Při posuzování zabezpečení je nezbytné posoudit rizika, která při zpracování osobních údajů mohou vznikat. S ohledem na takováto rizika je nutné přijmout taková bezpečnostní opatření, která zmírní ona rizika s ohledem na stav

[88] PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář.* Praha: Leges, 2018. Komentátor. ISBN 978-80-7502-288-2, s. 64-65.

techniky, náklady na provedení, povahu a rozsah. Toto posuzování by mělo být prováděno v pravidelných intervalech, či při zavedení významnějších změn ve způsobu zpracování osobních údajů. Ačkoliv je dnes většina osobních údajů uchovávána na vzdálených serverech, nemělo by být zapomínáno i na fyzické uložení osobních údajů, či fyzické zabezpečení výpočetní techniky. Důraz je v nařízení kladen především na anonymizování osobních údajů, dále pak na šifrování, pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Anonymizování je proces, kdy dochází k úpravě údajů způsobem, který následně neumožní tyto údaje identifikovat s určitou fyzickou osobou. Důležité je, aby osoba po anonymizování zůstala neidentifikovatelnou, což může být u některých údajů problematické, neboť je není možné zcela anonymizovat. Mělo by být přihlíženo ke všem prostředkům, které by mohl správce či zpracovatel využít, aby mohl případné údaje odanonymizovat. V případě, kdy by bylo možné údaje odanonymizovat (např. pomocí šifrovacího klíče), nebylo by je již možné považovat za anonymizované osobní údaje. Pokud by určitá osoba obdržela soubor byť anonymizovaných údajů, přičemž by předavatel disponoval širšími informacemi, na základě kterých by bylo možné tyto anonymizované údaje rozklíčovat, jednalo by se spíše o pseudonymizované údaje. Pro úplnou anonymizaci by muselo dojít k úplnému odstranění původních dat. Při šifrování dochází k převedení údajů do určité podoby, která není bez šifrovacího klíče čitelná. Účelem šifrování je omezení přístupu k údajům a zároveň jejich ochrana před neoprávněným získáním.[89]

Zásadu důvěrnosti využívá nařízení ePrivacy, které rozšiřuje její uplatnění na celý obsah komunikace. Zajištění důvěrného charakteru komunikací je nezbytným předpokladem pro zajištění souvisejících práv, jako je svobodný přístup k informacím, svoboda projevu, myšlení, svědomí, náboženského vyznání, ale také zajišťuje ochranu osobních údajů. Jedná se o provedení článku 7 LZPEU, který mimo jiné zajišťuje respektování soukromí komunikace. Důvěrný charakter by měl být zajištěn tím, že informace, které si strany mezi sebou vymění, by neměly být vyzrazeny nikomu jinému. Důvěrný charakter sdělení by se měl uplatnit i na vnější údaje, tedy na údaje o tom, kdy a odkud bylo sdělení odesláno,

[89] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 117-121; 315-319.

jak dlouho trval hovor apod. Zásady důvěrnosti se uplatní kromě komunikačních služeb, rovněž na samotný přístup k internetu a zároveň na budoucí služby, které v budoucnu vzniknou. V rámci celého nařízení je patrná snaha určitým způsobem podchytit technologický pokrok a reagovat i na služby nabízené v budoucnu. Dle čl. 12 recitálu k ePrivacy by se měla zásada důvěrnosti vztahovat i na komunikaci mezi stroji. Jedná se tak o reakci na tzv. internet věcí (IoT), v rámci kterého zařízení mezi sebou vzájemně komunikují skrze síť elektronických komunikací.

Důvěrný charakter sdělení by měl být posílen u veřejně dostupných bezdrátových sítí, ke kterým lze získat snadno přístup. Jedná se zejména o Wi-Fi hotspoty umístěné např. v nákupních centrech, přepravních prostředích či veřejných budovách. Ačkoliv se nejedná o hlavní nabízenou službu, měla by přesto být zajištěna zásada důvěrnosti. Naopak se tato zásada neuplatňuje na komunikaci v rámci interní sítě (např. intranet obchodní společnosti).

Je zakázáno, aby jakákoliv jiná osoba zasahovala do dat elektronických komunikací. Tedy aby prováděla odposlech, monitorování, uchovávání, skenování, či jinak zachycovala, sledovala, či zpracovávala data elektronických komunikací. Oproti předchozí směrnici došlo k rozšíření zákazu zpracovávání elektronických komunikací, což může působit značné problémy, neboť zpracování dat je hlavní činností, kterou poskytovatel těchto služeb činí.[90] Kromě koncových uživatelů mohou data zpracovávat také poskytovatelé služeb, pokud je to nezbytné pro přenos komunikace a to pouze po dobu nezbytnou pro tento účel. Druhou možností zpracování těchto dat je nutnost zachování či obnovení bezpečnosti služeb a sítí elektronických komunikací nebo odhalení závad či chyb v přenosu komunikací.

Důvěrnost by měla být zajištěna u komunikace mezi zařízeními, pokud informace nebo metadata plynoucí z této komunikace se týkají osobních údajů. Metadata jsou považována za citlivé osobní údaje a musí být proto smazána či anonymizována, pokud k jejich dalšímu zpracování neudělil subjekt údajů souhlas, případně pokud nejsou nezbytná pro provedení vyúčtování za poskytnuté služby.

[90] HÄRTING, Niko. *STUDY ON THE IMPACT OF THE PROPOSED EPRIVACY REGULATION* [online]. Berlin, 2017 [cit. 2019-03-14]. Dostupné z: https://www.haerting.de/sites/default/files/downloads/study_on_the_impact_of_the_proposed_eprivacy_regulation.pdf. Studie. HÄRTING Rechtsanwälte.

Ačkoliv je zásada důvěrnosti charakteru sdělení hlavní zásadou, která prolíná celé nařízení, neobsahuje žádné ustanovení týkající se bezpečnosti dat jako je tomu u GDPR.

Každý správce je odpovědný za povinnosti, které vyplývají z výše uvedených zásad, přičemž je i odpovědný za to, že tyto skutečnosti bude schopen dozorovému orgánu doložit. V tomto ohledu došlo oproti zákonu o ochraně osobních údajů k rozšíření odpovědnosti za dokumentaci splnění povinností. Dokumentace by měla být pro dozorový orgán srozumitelná, což se bude týkat především velkých společností, kde bývá složitá struktura, čemuž může odpovídat i veškerá interní dokumentace.

2.9. Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů (dále jen jako "DPIA" - Data Protection Impact Assessment) je povinnost, kterou zavedlo GDPR. Správce musí DPIA provést vždy, když určitý druh zpracování osobních údajů bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, a to zejména při využití nových technologií. GDPR uvádí demonstrativní výčet rizikových zpracování:

- *systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,*
- *rozsáhlé zpracování zvláštních kategorií údajů (např. údajů o rasovém či etnickém původu, politických názorech či zdravotním stavu anebo biometrických údajů atd.) nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů; anebo*
- *rozsáhlé systematické monitorování veřejně přístupných prostorů.*[91]

Správce má možnost DPIA provádět zcela dobrovolně, což je vhodné zejména u větších společností, neboť posouzení může předcházet řadě možných rizik. DPIA by mělo obsahovat analýzu procesů zpracování a měly by být jasně

[91] Článek 35 odst. 3 GDPR

definovány účely zpracování. V rámci analýzy procesů správce popíše veškeré operace, které probíhají při zpracování osobních údajů. Dále by měl posoudit nezbytnost zpracování údajů a jejich rozsahu. Zvážena by měla být také plynoucí rizika a zároveň zvážit opatření, která by tato rizika měla eliminovat.[92] Správce by si před zpracováním DPIA měl vyžádat od pověřence pro ochranu osobních údajů jeho stanovisko a následně s ním konzultovat výsledky.

[92] NAVRÁTIL, Jiří. *GDPR pro praxi.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 97-104.

3. Dopady právní úpravy ochrany osobních údajů na internetu

V následujících kapitolách popíši, jaký konkrétní dopad má GDPR a v budoucnu i nařízení ePrivacy na technologie a služby, které jsou nabízeny přes internet. Dále analyzuji, jakým konkrétním způsobem by měl správce osobních údajů postupovat, pokud zpracovává osobní údaje skrze internetové služby. Zaměřím se také na specifickou ochranu osobních údajů dětí na internetu.

3.1. Komunikace skrze internet

Každý člověk má dle čl. 11 LZPEU právo na zastávání názorů, přijímání a rozšiřování informací nebo myšlenek bez zasahování veřejné moci a bez ohledu na hranice. V digitálním prostředí je to internet, jež je základním prostředkem interpersonální komunikace. Komunikace na internetu již dávno neprobíhá pouze skrze emailové zprávy, ale existují rychlejší způsoby komunikace, jako je například instant messaging, nebo hlasová komunikace (dále jen „VoIP“ - Voice over Internet Protocol). S četností poskytovatelů komunikačních služeb však roste možnost zneužívání jejich obsahu a to včetně osobních údajů. Jak již bylo v dřívějším výkladu uvedeno, nařízení ePrivacy reaguje na současnou situaci, kdy komunikační služby, jež nejsou založeny na identifikačních číslech (OTT služby) nemusí dodržovat stejné standardy jako poskytovatelé veřejných komunikačních sítí v rámci současně ještě účinné Směrnice 2002/58/EC. Nařízení ePrivacy poskytuje ochranu dat elektronických komunikací, která jsou zpracovávána v souvislosti s poskytováním a používáním služeb elektronických komunikací v EU, bez ohledu na to, kde dochází ke zpracovávání.

Dle evropského kodexu pro elektronické komunikace (dále jen jako "Kodex") se službou elektronických komunikací rozumí: *"Služba obvykle poskytovaná za úplatu prostřednictvím sítí elektronických komunikací, která s výjimkou služeb poskytujících obsah přenášený prostřednictvím sítí a služeb elektronických komunikací nebo vykonávajících redakční dohled nad tímto obsahem zahrnuje tyto druhy služeb:*

a) *služba přístupu k internetu*
b) *interpersonální komunikační služby*

c) *služby spočívající zcela nebo převážně v přenosu signálů, například přenosové služby používané pro poskytování služby komunikace mezi stroji a pro vysílání."*

Nařízení ePrivacy v tomto případě spoléhá na definici uvedenou v Kodexu, přičemž ta je již oproti původní směrnici rozšířena o komunikace prováděné právě skrze internet, čímž by mělo dojít k zajištění důvěrnosti dat elektronických komunikací.

Správce by při poskytování komunikačních služeb měl přihlížet k důvěrnému charakteru sdělení předávaných skrze OTT služby. Nesmí do nich jakýmkoliv způsobem zasahovat, a to ani automatizovanými prostředky. Do doby než adresát obdrží zamýšlený obsah, platí absolutní zákaz zachycování obsahu. Pod zachycováním obsahu si lze představit kopírování zpráv, jejich čtení, nebo v případě VoIP hovorů také jejich odposlouchávání. Za zachycování obsahu komunikací je také považováno monitorování navštívených webových stránek uživatelem, návyků chování na internetu či sledování jejich interakce s ostatními uživateli.[93] Obsah komunikace budou obvykle tvořit kromě samotného sdělení uživatelů, také lokalizační a provozní údaje, které mohou být zpracovávané pro potřeby přenosu nebo účtování zpráv. Zákaz zachycování obsahu komunikací představuje určitý ekvivalent listovního tajemství, který je zakomponovaný do prostředí elektronických komunikací. Oproti GDPR, které chrání v rámci čl. 5 odst. 1 písm. f) důvěrnost osobních údajů, je v rámci ePrivacy chráněn celý obsah komunikace a zároveň je také rozšířena osobní působnost i na právnické osoby.

Při poskytování služeb elektronických komunikací má správce obvykle přístup k samotnému obsahu komunikací. Tento obsah poskytovatelé využívají zejména k poskytování dalších služeb, které uživatelům zvyšují komfort při jejich využívání. Jedná se např. o automatizované třídění emailových zpráv, jejich filtrování, či označování určitých zpráv jako reklamní sdělení. Poskytovatel by měl mít dle čl. 7 ePrivacy povinnost obsah komunikace vymazat či data anonymizovat, a to v momentě, kdy je obsah komunikace doručen adresátovi. Odst. 1 článku 7 se tak zdá býti velmi problematickým, neboť tento postup by byl proti oprávněným zájmům uživatelů, jelikož by nemohli využívat všech služeb a zřejmě by bylo zároveň nemožné, aby správce ukládal jakoukoliv historii

[93] Bod č. 15 recitálu ePrivacy.

komunikace. Aby tyto zprávy mohly být tímto způsobem uživateli rozřazeny, je možné toho docílit pouze zpracováním obsahu zpráv. Obdobně pokud si uživatel zablokuje určité emailové adresáty, pak poskytovatel emailové služby zpracovává obsah zpráv ještě před tím, než je adresátovi doručen. Dle bodu 19 recitálu k ePrivacy je zpracování dat za účelem vytváření filtrů výše uvedených shledáno jako vysoce rizikové. Vzhledem k tomu, že tyto filtry nejsou nezbytné pro přenos komunikací, aplikuje se čl. 6 odst. 3 písm. b) ePrivacy, který stanoví povinnost, aby toto zpracování bylo nejdříve konzultováno s dozorovým úřadem, a zároveň aby správce získal od uživatele souhlas ke zpracování údajů za tímto účelem. Z článku však vyplývá, že by daný souhlas měli poskytnout oba koncoví uživatelé, například i zároveň zasílatel spamu. Těžko si však lze představit, že by zasílatel uděloval souhlas se zpracováním dat za tímto účelem a ještě každému poskytovateli emailových služeb, kterým zasílá sdělení. V rámci samotného GDPR lze zpracování dat pro účely emailových filtrů posuzovat jako zpracování nezbytné pro splnění smlouvy dle čl. 6 odst. 1 písm. b), čímž odpadá nutnost potřeby souhlasu.[94]

Domnívám se, že by ještě mělo dojít k přehodnocení odst. 1 čl. 7 ePrivacy, neboť je v zájmu uživatelů, aby správce uchovával historii komunikací, přičemž by to měl být uživatel, který by měl mít nad obsahem komunikace kontrolu. Jako právní základ pro zpracování osobních údajů poskytovateli elektronických komunikací nemusí být vždy pouze souhlas. Data je také možné zpracovávat, pokud je to nezbytné pro přenos komunikace a to po dobu nutnou pro tento účel a dále pak pro zachování nebo obnovení bezpečnosti služeb a sítí elektronických komunikací či odhalení technických závad.[95] Avšak v případě samotného obsahu elektronických komunikací je vždy vyžadován souhlas, který naplňuje požadavky GDPR. Oproti původní směrnici[96] tak došlo k požadavku získání souhlasu se zpracováním obsahu, což by mělo zaručit vyšší ochranu jejich uživatelům a posílit důvěrnost komunikací, zároveň by to však znamenalo nutnost získávání souhlasů od uživatelů, kteří by chtěli využívat vedlejších služeb.

[94] HÄRTING, Niko. *STUDY ON THE IMPACT OF THE PROPOSED EPRIVACY REGULATION* [online]. Berlin, 2017 [cit. 2019-03-10]. Dostupné z:
[95] Srov. čl. 6 odst. 1 písm. a) a b) ePrivacy.
[96] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

3.2. Cookies a webové prohlížeče

Poskytovatelé služeb elektronických komunikací mají často přístup k informacím z koncových zařízení jejich uživatelů. Tyto informace má zákaz zpracovávat jakýkoliv jiná osoba než samotný koncový uživatel, pokud není zpracování těchto dat nezbytné pro uskutečnění přenosu komunikace, poskytnutí služby požadované uživatelem či měření návštěvnosti webových stránek uživatelem. Poslední možností je zpracovávání koncových dat na základě souhlasu, který splňuje veškeré požadavky GDPR. Správcům je zakázáno využívat funkce koncového zařízení pro další zpracovávání a uchovávání dat.

Nařízením ePrivacy by mělo dojít ke zvýšení role webových prohlížečů, které budou muset rozšířit možnosti nastavení soukromí. Uživatel by si již při instalaci webového prohlížeče či jiného softwaru umožňujícího prohlížení webu, mohl nastavit rámec ochrany osobních údajů. Subjekt údajů bude mít zejména možnost nastavit, aby za něj prohlížeč dával automaticky souhlas se zpracováním cookies. Výchozí nastavení prohlížeče by však mělo zakazovat získávání souborů cookies třetích stran. Na získání permanentního souhlasu se zpracováním cookies udělený internetovému prohlížeči, by měly dopadat stejné požadavky jako na obecný souhlas, tedy svobodně poskytnutý, informovaný a jednoznačný. Zejména po přijetí GDPR došlo k tomu, že veškeré webové stránky využívající cookies požadují po uživateli udělení souhlasu s jejich předáváním. Pro uživatele se tato nutnost stálého udělování souhlasů stává velmi obtěžující a kazí plynulost procházení mezi jednotlivými stránkami. Díky možnosti integrování souhlasu přímo do webového prohlížeče by mělo dojít ke zvýšení komfortu uživatelů při procházení internetových stránek.

Na druhou stranu, pokud si uživatel nastaví absolutní zákaz předávání cookies, pak může být pro provozovatele webových stránek poměrně obtížné tento souhlas získat. Uživatelé by měli mít možnost si v prohlížeči nastavit, že souhlasí s ukládáním cookies pouze pro určitý účel, např. pro zapamatování si přístupových údajů či nastavení rozhraní webu. Poskytovatelé tak budou nadále využívat souhlasy např. pomocí bannerů či vyskakovacích oken jako tomu bylo doposud, což povede ke zvýšení komfortu procházení webových stránek pouze uživatelů, kteří udělí souhlas s předáváním cookies bez jakéhokoliv omezení.

Nastavení provedená ve webových prohlížečích by měla být závazná a vynutitelná vůči třetím stranám. Internetové prohlížeče by tak měly sehrát roli ochrany před předáváním dat ze zařízení, nebo jejich ukládáním. Uživatel po udělení souhlasu webovému prohlížeči by měl mít možnost kdykoliv tento souhlas vzít zpět či poupravit nastavení předávání cookies. Například by měl mít možnost vyjmout určité webové stránky, kterým by nebylo možné předávat cookies.

Změna v oblasti využívání cookies by měla přinést snížení nákladů poskytovatelům služeb a zvýšit komfort a ochranu dat uživatelů. Na druhou stranu, pokud by většina uživatelů nastavila v prohlížeči maximální možnou ochranu, pak bude pro poskytovatele velmi obtížné získat souhlas. To by mohlo vést až ke snížení efektivnosti reklam na internetu, ale také ke značenému omezení určitých nástrojů, jako je například Google Analytics sloužící k získávání statistických dat o návštěvnících webu.

3.3. Komunikace mezi zařízeními v rámci IoT

Internet věcí (Internet of Things, dále jen „IoT“) jakožto označení přístrojů připojených k internetu představuje pro oblast ochrany osobních údajů zcela nové výzvy. IoT je využíváno v řadě oblastí, ať už se jedná o inteligentní domácí spotřebiče, přes autonomní vozidla, až po využití v průmyslu. Zařízení v rámci IoT tvoří kombinaci procesorů, senzorů a sítě sloužící ke sledování a ovládání jednotlivých zařízení. Účelem IoT by měla být především úspora nákladů, zvýšení produktivity a komfortu při jejich využívání.

Zařízení využívaná jako IoT skrze senzory sbírají data, která samostatně vyhodnocují v určitých situacích, případně také mohou dlouhodobě vytvářet záznamy o těchto datech. Zařízení skrze internet vzájemně mezi sebou či s uživatelem komunikují, čímž dochází k vytváření osobních údajů. Jako u jiných technologií i v případě IoT může dojít k úniku dat, která mohou zahrnovat osobní údaje. Kromě útoků hackerů či krádeže může být také problematická správná konfigurace těchto zařízení, zejména je-li jich nasazeno větší počet, jež spolu mají vzájemně komunikovat.[97] Nařízení ePrivacy ve svém bodě 12 recitálu přímo

[97] PATHAK, P.B. internet of Things: A Look at Paradigm Shifting Applications and Challenges. *International Journal of Advanced Research in Computer Science* [online]. 2016, 7(2), 50-51 [cit. 2019-03-10]. ISSN 0976-2697. Dostupné z: www.ijarcs.info.

poukazuje na využívání IoT a zdůrazňuje, že i v případě komunikace mezi stroji je nezbytné dodržovat zásadu důvěrnosti.

Pokud se správce osobních údajů rozhodne využít IoT, pak je na místě vypracovat důkladné posouzení dopadů na práva osob. Při utváření analýzy je nezbytné se zaměřit na specifika, které IoT přináší. Správce by si při vytváření analýzy měl přizvat IT specialistu a prodiskutovat s ním jednotlivá rizika, která mohou při využívání IoT vznikat. Zejména v případě chytrých zařízení sloužících ke sledování zdravotního stavu uživatele by měl správce dbát zvýšené pozornosti, neboť mohou odhalit velice citlivá data subjektů údajů.[98] V případě že by správce shledal, že zpracování je vysoce rizikové, je povinen danou problematiku prodiskutovat ještě s dozorovým orgánem. Ačkoliv to právní předpisy nevyžadují, měl by správce vypracované posouzení vlivu na ochranu osobních údajů uveřejnit, neboť tím poskytne subjektům údajů další informace o procesu zpracování a uživatel bude moci zjistit, v čem spočívají nejvyšší rizika zpracování.[99] Je třeba přikládat zvýšenou váhu zásadě transparentnosti, tedy aby subjekt údajů přesně věděl, jaká data o něm jsou zpracovávána a za jakým účelem. Výrobce těchto zařízení by si toho měl být vědom a řádně o tom informovat subjekt údajů, včetně popsání procesu jakým způsobem jsou data zpracovávána a kde jsou uchovávána. Tyto informace by neměly být poskytovány příliš odborným jazykem, ale co nejjednodušeji, aby byly srozumitelné pro každého uživatele.

V případě že určité zařízení využívá více uživatelů, může být problematické zabránit jejich diskriminaci, neboť používání chytrého zařízení jedním uživatelem může ovlivnit chování zařízení při ovládání druhým uživatelem. Je tedy třeba, aby zařízení ovládalo takové algoritmy, které by nevedly k diskriminaci při jeho rozhodování. Správce by měl co možná nejvíce využívat anonymizaci dat a to zejména pokud data poskytuje třetí straně.[100]

[98] IoT regulation: IoT, GDPR, ePrivacy Regulation and more regulations. *I-SCOOP* [online]. Belgium: i-SCOOP, 2019 [cit. 2019-03-10]. Dostupné z: https://www.i-scoop.eu/internet-of-things-guide/iot-regulation/.
[99] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248 rev. 01. *Evropská komise* [online]. [cit.17. 3. 2019]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.
[100] WACHTER, Sandra. The GDPR and the internet of Things: a three-step transparency model. *Law, Innovation and Technology* [online]. 2018, 10(2), 266-294 [cit. 2019-03-10]. DOI:

Zejména ve zdravotnictví mohou být pro účely statistik určitá data velmi zajímavá a posloužit dalšímu výzkumu. V současnosti např. zdravotní pojišťovny v USA poskytují slevy na zdravotním pojištění těm, kteří poskytnou data ze svých chytrých hodinek, neboť mají podloženo, že uživatel sportuje, což může vést ke snížení zdravotních problémů a tedy zároveň k úsporám na vypláceném pojistném. Výrobce těchto zařízení by také měl zvážit, zda do zařízení nezabudovat funkci, která by zařízení zcela odpojila od internetu. Odpojením by sice došlo k omezení plného využití, ale uživateli by se tak dostala plná kontrola nad předáváním dat.[101]

U IoT může být problematické vymezení účelu zpracování, jelikož zařízení mohou pomocí senzorů zpracovávat i údaje, které nebudou nijak využity. Může se jednat třeba o pohybové senzory či kamery, které mohou zaznamenat určitou osobu. Je proto nezbytné, aby data, která nejsou nikterak využívána, byla ihned odstraněna s nemožností jejich obnovení. Důležitá je tedy zejména komunikace správce směrem k subjektu údajů, který by měl poskytnout co nejvíce informací o daném zařízení a subjekt údajů tak mohl posoudit, zda určité zařízení poskytuje dostatečnou ochranu jeho dat.

3.4. Přímý marketing na internetu

Přímým marketingovým sdělením se dle ePrivacy rozumí: *"jakákoliv forma reklamy, ať už písemná nebo ústní, která je zaslána jednomu nebo více identifikovaným nebo identifikovatelným koncovým uživatelům služeb elektronických komunikací, a to včetně využití automatických volacích a komunikačních systémů se zásahem člověka nebo bez něj, elektronické pošty, SMS atd."*[102] Pod reklamou dle Směrnice o klamavé a srovnávací reklamě[103] nutno rozumět předvedení zboží nebo služby, které má sloužit k jeho odbytu. Kromě klasické tržní podpory odbytu produktu zahrnuje přímý marketing také sdělení, která jsou zasílána politickými stranami za účelem podpory svých stran a stejně tak sdělení zasílaná neziskovými organizacemi.[104] Dle názoru pracovní skupiny

10.1080/17579961.2018.1527479. ISSN 1757-9961. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1527479, s. 273-283.

[101] Rolf H Weber and Romana Weber, *internet of Things: Legal Perspectives*, vol 49 (Springer Science & Business Media, 2010).

[102] Čl. 4 odst. 3 písm. f) ePrivacy.

[103] Čl. 2 písm. a) směrnice Evropského parlamentu a Rady č. 2006/114/ES ze dne 12. prosince 2006 o klamavé a srovnávací reklamě.

[104] Bod 32 recitálu ePrivacy

WP29 by zde mělo dojít ještě k úpravě, aby do tohoto výčtu byli zahrnuti i političtí kandidáti, kteří hodlají zasílat marketingová sdělení potencionálním voličům.[105] Formou provádění přímého marketingu může být zasílání SMS zpráv, provádění telefonních hovorů, ale taktéž sdělení prováděné skrze služby elektronických komunikací. Výhodami využívání přímého marketingu je jeho efektivnost, možnost personalizace a v případě internetového prostředí i nízké náklady. Zejména s ohledem na četnost využívání přímého marketingu se ePrivacy snaží reagovat na nové technologie využívané pro provádění přímého marketingu, které mají negativní dopad pro příjemce, a to zejména na zneužívání osobních údajů a nadměrné obtěžování příjemců reklamních sdělení (tzv. spamming).

S přijetím GDPR se ukázal problematickým jeho výklad ohledně přímého marketingu, neboť nebylo zcela jasné, zda lze provádět přímý marketing na základě oprávněného zájmu či zda je vyžadován souhlas se zpracováním. Oprávněného zájmu lze však využít pouze v případě, že dané reklamní sdělení bude subjekt údajů očekávat. Jedná se o případy, kdy vzniká mezi správcem a subjektem údajů zákaznický vztah. Správce je oprávněn využít získané osobní údaje pouze z uzavřené smlouvy v souvislosti s prodejem svého zboží či poskytnutí služeb (tzv. soft opt-in). Marketingová sdělení však musí souviset se zakoupeným zbožím, přičemž nesmí docházet k jejich nadměrnému zasílání. Subjekt údajů by měl mít možnost kdykoliv zasílání těchto sdělení odvolat.[106] Tento původně nejasný výklad zpřesňuje ePrivacy v bodě 33 recitálu, který stanovuje, že by se tato možnost měla vztahovat pouze na tutéž společnost, jež získala osobní údaje v souladu s nařízením GDPR. V případě, že si subjekt údajů nepřeje, aby mu byly zasílány reklamní sdělení na základě oprávněného zájmu, má možnost podat námitku, jež má absolutní povahu, tedy jakmile ji subjekt údajů vznese, musí správce přestat zpracovávat osobní údaje pro marketingové účely. O možnosti podat námitku musí být subjekt údajů informován a to již při

[105] Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 17/EN WP 247. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.
[106] HRADSKÝ, Jiří. *Přímý marketing ve světle nařízení eprivacy a GDPR.* Iurium [online]. iurium, [2018] [cit. 2019-02-20]. Dostupné z: https://www.iurium.cz/2018/12/15/primy-marketing-ve-svetle-narizeni-eprivacy-a-gdpr/.

shromáždění osobních údajů. Tato informace musí být uvedena odděleně od ostatních informací a být zřetelná.[107]

V ostatních případech bude muset správce získat souhlas se zpracováním osobních údajů (tzv. opt-in). Souhlas musí splňovat veškeré obecné požadavky GDPR, tak jak byly popsány v kapitole 2.8.1. Vzhledem k nutnosti prokázání získání souhlasu je vhodné v případě jeho získání na základě zaškrtnutého formulářového políčka na webové stránce si po subjektu údajů vyžádat ještě jeho potvrzení např. v rámci emailu. Tento způsob se sice může zdát zbytečně komplikovaný, avšak pro správce osobních údajů by pak mělo být mnohem snazší prokázat vůli subjektu k zasílání reklamních sdělení. Subjekt údajů by měl mít možnost tento souhlas odvolat, a to co možná nejjednodušším způsobem a zcela zdarma.[108] V případě elektronického sdělení by tomu tak mělo být lehce seznatelným odkazem, kterým subjekt údajů vezme zpět svůj souhlas se zpracováním osobních údajů, přičemž je zasílatel povinen tento odkaz připnout ke každému zaslanému marketingovému sdělení. Pokud subjekt údajů využije takového odkazu, měl by být následně informován, že mu již nebudou zasílána sdělení, a že jeho údaje byly odstraněny, případně anonymizovány. Dále by v rámci sdělení mělo být jasně patrné, který subjekt jej zasílá a mělo by být označeno, že se jedná o marketingové sdělení, např. slovy reklama, obchodní sdělení, akce apod.[109]

V rámci naplnění zásady transparentnosti by měl být subjekt údajů informován o době uchování údajů, o jeho právech a případně o informaci, zda jsou údaje zpracovávány automatizovaně.[110] Nutno říci, že již v současné době je tato praxe poměrně běžná a uživatel má možnost kontroly nad zasíláním reklamních sdělení. Správci často vyžadují odůvodnění odvolání souhlasu, přičemž je nutné, aby poskytování odůvodnění odvolání zůstalo zcela čistě na vlastní vůli subjektu údajů, neboť není přípustné, aby jím bylo podmiňováno odvolání souhlasu.

[107] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů.* 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 252-253.
[108] Článek 16 odst. 2 ePrivacy
[109] Srov. článek 16 odst. 6 ePrivacy
[110] ŠVEJDOVÁ, Martina. *Marketing ve světle ustanovení GDPR.* Epravo.cz [online]. Praha: epravo.cz, [2018] [cit. 2019-02-20]. Dostupné z: https://www.epravo.cz/top/clanky/marketing-ve-svetle-ustanoveni-gdpr-106977.html.

V případě telefonních hovorů by mělo být vždy zobrazeno číslo volajícího, případně ePrivacy doporučuje, aby členské státy zavedly zvláštní předponu pro marketingové hovory, kterou by museli volající využívat. Toto se samozřejmě netýká hovorů uskutečňovaných skrze VoIP, neboť platformy pro provádění hovorů neumožňují skrýt svoji identitu a zároveň obvykle vyžadují, aby byl volající nejdříve přidán do kontaktů.

Správcům osobních údajů využívajících přímý marketing lze doporučit, aby znovu zvážili, zda jejich souhlasy se zpracováním osobních údajů splňují požadavky ePrivacy a GDPR a případně je revidovali. Subjekt údajů musí přesně vědět, jaká sdělení bude na základě souhlasu dostávat a být tedy schopen posoudit, zda chce skutečně své osobní údaje správci předat. Správce by se měl také ujistit, zda veškerá sdělení skutečně obsahují možnost opt-out, tedy odvolat svůj souhlas. Pokud správce využívá více systémů pro zasílání marketingových sdělení, měl by být schopen odvolání souhlasu provázat do všech těchto systémů, aby tak po jeho odvolání skutečně nedocházelo k zasílání marketingových sdělení. Souhlasy získané před přijetím ePrivacy a GDPR lze nadále využít, pokud splňují jejich požadavky. Není proto nutné zasílat všem adresátům přímého marketingu výzvy k udělení nového souhlasu.

Vzhledem k tomu, že ePrivacy bude zvláštním právním předpisem vůči GDPR, tak nebude možné využít pro zpracování osobních údajů jiného právního titulu nežli souhlasu, čl. 16 odst. 2 ePrivacy tak bude mít přednost před čl. 6 odst. 1 GDPR, a to i přesto, že v bodě 47 recitálu GDPR je výslovně stanoveno, že zpracování osobních údajů pro přímý marketing lze považovat za zpracování prováděné v oprávněném zájmu správce.

S ohledem na ustanovení, že se ochrana poskytne koncovým uživatelům - fyzickým osobám, není zcela jasné, zda bude poskytována ochrana před přímým marketingem i fyzickým osobám při výkonu pracovních povinností, tedy pokud jim bude zasíláno reklamní sdělení do emailové schránky poskytnuté jim zaměstnavatelem. Domnívám se, že by tomu tak být nemělo, ačkoliv je smyslem úpravy ochrana fyzických osob před nevyžádanými reklamními sděleními, shledávám jako vhodné zasílání reklamních nabídek týkajících se předmětu

podnikání subjektu, neboť v opačném případě by mohlo dojít k určitému omezení svobody podnikání. Na druhou stranu by nemělo docházet k zasílání reklamních sdělení, které zcela nesouvisí s předmětem podnikání, např. zasílání nabídky exotických dovolených zaměstnancům průmyslové společnosti.

Lze shrnout, že ePrivacy přináší poměrně zásadní změny v případě využití přímého marketingu, a to zejména k nemožnosti využití přímého marketingu na základě oprávněného zájmu správce, tedy na základě předchozího nákupu zboží či služby.

3.5. Cloud computing

Koncepci cloud computingu lze zjednodušeně popsat jako vzdálený přístup k úložišti souborů či aplikacím, které jsou umístěny na vzdáleném serveru. Může se jednat o pouhý pronájem výpočetního zařízení, na kterém poběží vzdáleně vlastní aplikace, případně o vzdálené úložiště pro vlastní data, nebo také využívání vzdáleného softwaru, který je ve vlastnictví poskytovatele (označované také jako „SaaS“, tedy Software as a Service). Pro možnost využívání cloud computingových služeb je nezbytné stálé připojení k internetu.[111] Koncepce cloud computingu může zejména pro menší společnosti, ale i pro jednotlivce představovat výrazné snížení nákladů za využívané služby, neboť poskytovatelé skrze cloud computing hostují tyto aplikace, čímž uživatelům odpadá nutnost disponovat dostatečně výkonným zařízením pro chod těchto služeb. Prakticky se jedná o sdílení výpočetního výkonu mezi řadou uživatelů, kteří ho mohou využívat flexibilně dle jejich potřeb. Uživatelé mohou využívat cloud computingových služeb z jakéhokoliv místa a zařízení, a to vždy v jejich nejnovější verzi, přičemž odpadá jakákoliv nutnost instalace softwaru přímo do zařízení.[112] Vzdálený přístup však představuje zároveň rizika v podobě nefunkčnosti serverů a potažmo i aplikací, ale i závažnější problémy jako je ztráta dat či jejich odcizení. Nepochybně se mezi těmito daty mohou nacházet i osobní údaje fyzických osob. Kromě údajů, které uživatel přímo uloží na server, to mohou být i síťové identifikátory.

[111] Samotné slovo „cloud“ je metaforou pro internet, neboť v síťových diagramech se znázorňuje jako obláček. Odtud tedy i vznikl název cloud computing.
[112] VELTE, Anthony T., Toby J. VELTE a Robert C. ELSENPETER. *Cloud Computing: praktický průvodce.* Brno: Computer Press, 2011. ISBN 978-80-251-3333-0, s. 23-45.

Pracovní skupina WP29 ve svém stanovisku shledává problematickým používání cloudových technologií, zejména v ohledu zvýšených nákladů za přenesení dat k jinému poskytovali služeb, nebo znemožnění vůbec tato data přenést k jinému poskytovateli. Dále se může jevit problematickým počet operací, které poskytovatel může učinit v rámci své činnosti a to zejména s ohledem na možné propojení většího množství cloudových služeb. Z propojení více cloudových služeb může pramenit nedostatek informovanosti správců využívajících tyto služby, čímž nebudou schopni přijmout vhodná opatření k ochraně dat.[113] Pro poskytovatele těchto služeb sídlících v EHP platí absolutní povinnost dodržovat předpisy EU. Není tedy rozhodné, zda zpracovávají osobní údaje zákazníků z třetích zemí, neboť je jim poskytována stejná ochrana.

V případě že zákazník využívá cloudových služeb pro zpracovávání osobních údajů, pak je zde nutné jím rozumět zároveň správce, neboť takováto osoba zároveň určuje účel zpracování těchto údajů. Ve vztahu správce a poskytovatele by měly být stanoveny podmínky zpracování a obě strany by měly přijmout potřebná technická či organizační opatření. Smluvně by zároveň měla být stanovena jasná odpovědnost za porušení legislativy na ochranu osobních údajů. Nutno však konstatovat, že většina cloudových služeb je nabízena standardizovaně a správce (zákazník) tak nemá reálnou možnost vyjednat si rozdílné smluvní podmínky. Přesto je to správce kdo určuje způsob zpracování osobních údajů a stejně tak si vybírá ke své činnosti cloud computingové poskytovatele. Je proto nezbytné, aby správce volil takového poskytovatele, který zaručí soulad s právními předpisy na ochranu osobních údajů.[114] Vhodnou zárukou souladu s právními předpisy na ochranu osobních údajů může být například certifikace od nezávislé auditorské společnosti.

Služby cloud computingu jsou často propojovány s dalšími službami či se na zpracování podílí více zpracovatelů, v takovém případě musí všechny tyto subjekty dodržovat pokyny vydané správcem. Zároveň by mělo při řetězení zpracování dojít k uzavření smlouvy, která by reflektovala původní smlouvu se

[113] Article 29 Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN WP 196. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, WP196, s. 5-6.
[114] Stanovisko WP29, ze dne 1. července 2012, č. 05/2012, WP196, s. 7-9.

správcem.[115] V rámci smlouvy by měl být kladen důraz zejména na bezpečnostní opatření, která zpracovatel přijme, podmínky navrácení dat či jejich zničení, upřesnění informační povinnosti vůči správci a uvedení míst ve kterých budou data uchovávána.

V případě kdy se správce rozhodne využít cloudových služeb, jejich poskytovatel se tak stává zpracovatelem osobních údajů. Správce by měl před využitím cloudových služeb dobře zvážit, zdali jejich poskytovatel dokáže přijmout odpovídající záruky za ochranu osobních údajů a prokázat soulad s legislativou v oblasti ochrany osobních údajů. Správce musí mít dostatečnou představu nad tím, jakým způsobem a kde jsou údaje zpracovávány. Poskytovatelé větších cloudových služeb často využívají velké množství datových center, které mohou být umístěny v třetích zemích, což se může jevit jako problematické. Stejně tak jako správce, má i zpracovatel vůči subjektům údajů přímou odpovědnost za ochranu dat. Je tedy nezbytné, aby i poskytovatelé cloudových služeb vyvinuli úsilí a zavedli patřičná interní opatření, která budou chránit svěřené osobní údaje. S ohledem na princip integrity je nezbytné, aby byla přijata veškerá vhodná technická opatření k zabezpečení odpovídající možným rizikům.[116] Správce by tak měl být dostatečně informován kde a jakým způsobem mají být osobní údaje zpracovávány, a takovéto informace je pak povinen předat subjektům údajů. Například německá společnost SAP ve svých smluvních podmínkách přímo stanovuje, že data budou ukládána pouze na území EHP a Švýcarska, přičemž uložení mimo toto území podléhá písemnému souhlasu.[117] Takovéto ustanovení lze shledat jako jednu z vhodných záruk ochrany osobních údajů a posiluje správcovo povědomí o tom, kde jsou data fyzicky uložena. Zároveň má i možnost odmítnout zpracování dat mimo území EHP.

Poskytovatel by měl být schopen zaručit dostatečnou dostupnost zpracovávaných dat. Dále by měl být schopen zaručit při skončení smluvního závazku či na přání klienta zajistit absolutní výmaz veškerých dat včetně jejich

[115] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://www.pdpjournals.com/docs/88016.pdf, s. 29.
[116] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4, s. 251-256.
[117] https://www.sap.com/about/cloud-trust-center/cloud-service-level-agreements/cloud-services.html?search=Data%20Processing&sort=title_asc#pdf-asset=c634978e-027d-0010-87a3-c30de2ffd8ff&page=6

záloh. To je důležité zejména s ohledem na účelové omezení uchovávání dat a v případě pominutí účelu musí dojít k jejich úplnému odstranění. Správce by tak měl být dostatečně informován, jakým způsobem jsou data uchovávána a jakým způsobem jsou průběžně prováděny zálohy těchto dat.

Přístup k údajům může být ohrožen zejména neočekávanou ztrátou síťového připojení či kolísání výkonnosti serverů. Správce by měl při výběru poskytovatele cloud computingu přihlížet i k těmto aspektům a volit poskytovatele nabízející dostatečné záruky dostupnosti údajů, zejména využívající záložních zdrojů, záložního internetového připojení či zálohování dat. K předejití rizik by poskytovatel měl být schopen nabídnout správci rozsáhlou správu přístupů ke cloudu, přičemž by mělo být zabráněno, aby ani administrátor neměl přístup k celému cloudu. Pokud správce využívá více cloudových služeb může být velmi problematické sjednávat jednotlivé podmínky u každé služby zvlášť, proto je vhodnější využít poskytovatele, který nabízí vícero pro správce vhodných cloudových služeb.

Společnosti zvažující využívání cloud computingových služeb by nejdříve měly provést důkladnou analýzu rizik pro práva a svobody fyzických osob v rámci posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR, který by měli správci vytvářet zejména při zavádění nových technologií. Ačkoliv je posouzení vlivu na ochranu osobních údajů povinné pouze pokud správce zpracovává osobní údaje pro automatické rozhodování zakládající právní účinky, při rozsáhlém zpracování zvláštních kategorií osobních údajů, případně při monitorování veřejně přístupných míst, pak je i přesto vhodné analýzu rizik uskutečnit, neboť je to dobrý prostředek pro předcházení rizik spojených s únikem osobních údajů a zároveň pro zajištění schopnosti doložit soulad s právními předpisy dle čl. 24 GDPR. V rámci analýzy by mělo být důkladně popsáno, jaká rizika by mohla vzniknout, pokud by se takové údaje dostaly k nežádoucím osobám. Zejména v případě citlivých osobních údajů by správce měl dbát významnějšího zřetele. Při zhodnocení rizik jsou využívány tři stupně rizika pro práva a svobody fyzických osob. V případě, že správce vyhodnotí určité riziko jako nízké, může se zprostit povinnosti ohlašovat porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR. Pokud by bylo riziko shledáno jako vysoké, má správce povinnost provést kompletní posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR. V

takovém případě má správce povinnost provést konzultaci s dozorovým úřadem a v případě porušení zabezpečení osobních údajů je povinen o této skutečnosti informovat subjekty údajů.[118] Jako vysoce rizikové bude posuzováno zejména zpracování osobních údajů velkého množství subjektů údajů a to zejména, pokud budou zároveň zpracovávány citlivé údaje, případně bude využita zcela nová technologie, při níž bude pro subjekty údajů obtížnější uplatnit svá práva.[119] Ve výsledku je proto nutné zvážit míru rizika a prospěch, který může být získán zavedením cloud computingové služby. Správce by po zvážení rizik měl přijmout vhodná opatření k jejich zmírnění, zejména se tedy pokusit o sjednání výhodnější podmínek, případně využít anonymizaci dat, či jiná vhodná opatření. Analýzu rizik si správce může vyhodnotit sám, případně je vhodnější tuto činnost přenechat třetí straně, která pomůže správci nezávisle zvážit rizika a přispěje tak k transparentnosti celého procesu. Postup správce by měl být zvažován citlivě dle jeho velikosti, rozpočtových možností a zejména s ohledem na zpracovávané osobní údaje.

V rámci přílohy č. 3 je přiložena část vzorové analýzy rizik určené pro zdravotní organizace využívající cloudových služeb. V levé části jsou konkrétně popsána rizika, která mohou využitím cloudových služeb vzniknout. Jedná se například o zjištění uživatelem zapsaného hesla ke službě, stažení kopie dat do počítače, nebo třeba o nemožnost přístupu k datům. Dále je v tabulce uvedeno jakou míru rizika daný problém může představovat a jaký by mohl být jeho zdroj. Zvážena je také možnost výskytu a stávající metody kontroly daného rizika. Veškeré tyto informace by měly odpovídat skutečnosti a správce by při vytváření rizikové analýzy měl využít spolupráce svých zaměstnanců pro věrné zachycení skutečnosti. V pravé části tabulky jsou pak uvedeny postupy, které by měly být učiněny pro eliminaci definovaných rizik a jejich kontroly.

Lze shrnout, že každá smlouva o využívání cloud computingových služeb by minimálně měla obsahovat následující:

- informace o fyzickém místě uložení a zpracovávání dat po dobu trvání smlouvy,

[118] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů.* 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 270-271.
[119] Bod 91 recitálu GDPR

- výslovné prohlášení o tom, že data nebudou využívána poskytovatelem,
- uvedení, že správce má právo na kontrolu činností poskytovatele, zda jsou v souladu se smlouvou a právními předpisy, přičemž kontrolu může vykonávat i externí společnost,
- prohlášení, že správce údajů zůstává i nadále vlastníkem všech dat,
- ustanovení o přístupu subjektu údajů ke všem datům, možnost jejich úprav, včetně úplného odstranění.[120]

Zároveň je také vhodné, aby byly stanoveny určité principy, kterými se bude poskytovatel, ale i subjekt údajů řídit. V případě využívání cloudových služeb zaměstnavatelem by mohl poskytovatel vyžadovat i proškolení zaměstnanců, čímž by mělo dojít ke snížení rizika úniku dat. Dále by měla být citlivě stanovena odpovědnost za ztrátu, poškození či vyzrazení dat. Správce by se také měl informovat o tom, jaká metadata poskytovatel sbírá, jak jsou zabezpečována a zda k nim nemá přístup třetí strana. Pro poskytovatele je vhodné, aby soulad s legislativou na ochranu osobních údajů demonstrovali kupříkladu certifikátem ISO 27001 (systém řízení bezpečností informací), případně certifikátem ISO 27018 (Soubor postupů na ochranu osobních identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII).

3.6. Sociální sítě

Sociální síť je služba provozovaná skrze internet, která svým uživatelům umožňuje vytváření osobních profilů, které jsou alespoň částečně veřejné. Dále umožňuje vzájemnou komunikaci mezi uživateli, včetně sdílení obsahu. Toto jsou jen základní funkce sociálních sítí, které je neustále rozšiřují a propojují s dalšími službami. V současnosti sociální sítě umožňují také komplexní marketingové služby, poskytují zpravodajství, videoobsah, nebo třeba videohry. Kromě soukromé komunikace se na sociálních sítích užívá zejména veřejná hromadná komunikace mezi více uživateli. Jejich funkcí je naplňování potřeb svých uživatelů, jako je sebevyjadřování, komunikace a bytí součástí určité komunity.[121] V rámci jejich využívání se změnilo pojímání soukromí, neboť uživatelé mají možnost sdílení informací o své osobě po celém světě. Sociální sítě také začali v

[120] FAL, O. M. a V. F. KOZAK. *PERSONAL DATA PROTECTION PROBLEMS ASSOCIATED WITH CLOUD COMPUTING* [online]. USA: Springer US, 2014 [cit. 2019-03-04]. ISSN 1573-8337. Dostupné z: https://link.springer.com/article/10.1007/s10559-014-9667-8, s. 770.
[121] Grimmelmann, J. (2009) *Saving Facebook.* Iowa Law Review, 94, s. 159.

hojném počtu využívat podnikatelé k proklientské komunikaci a budování značky. V rámci sociálních sítí vstupují uživatelé do řady právních vztahů, kromě předávání osobních údajů může docházet k uzavírání smluv, nekalé soutěži, či zasahování do osobnostních práv.[122]

Poskytovatelé sociálních sítí sídlí často mimo území EHP, zejména v USA. Z tohoto důvodu vydala Komise rozhodnutí na základě směrnice 94/46/ES[123], jímž měla zajistit odpovídající ochranu poskytovanou dle zásad tzv. bezpečného přístavu. Dohoda Safe Harbour byla uzavřena mezi EU a USA po dvouletém vyjednávání a ukládala společnostem z USA, aby dodržovaly zásady na ochranu osobních údajů dle právních předpisů EU i v případě, že údaje nejsou zpracovávány na území EHP. Pokud se obchodní společnost v USA dobrovolně přihlásila k dodržování zásad v rámci Safe Harbour, mohla volně zpracovávat osobní údaje získané z EU. Toto bylo možné až do vydání přelomového rozhodnutí Soudního dvora EU ze dne 6. října 2015[124], v rámci něhož došlo ke zrušení programu Safe Harbour. Rakouský právník Maximillian Schrems podal na společnost Facebook Ltd. stížnosti k dozorovému úřadu, neboť se domníval, že Facebook Ltd. nedodržuje zásady ochrany osobních údajů, které se zavázala dodržovat na základě programu Safe Harbour. Schrems si již jako student práv vyžádal po Facebooku výpis osobních údajů, které o něm společnost shromažďuje. Facebook mu poskytl výpis o celkové délce 1200 stran, ze kterých bylo patrné, že Facebook o jeho osobě shromažďuje údaje, které již dávno ze svého profilu vymazal, a zároveň mu nebyly poskytnuty informace o fyzickém uložení dat. Úřad uložil společnosti, aby provedl určitá opatření, ty však Schrems považoval za nedostatečná a nakonec vzal stížnost zpět, neboť úřad odmítl věc dále projednávat.[125] V rámci jedné ze stížností požadoval, aby dceřiná společnost Facebook Ireland přestala předávat osobní údaje o jeho osobě do Spojených států, neboť právní předpisy v této zemi nezajišťují dostatečnou ochranu osobním

[122] JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. *internetové právo.* Brno: Computer Press, 2016. ISBN 978-80-251-4664-4, s. 351.
[123] Rozhodnutí Komise ze dne 26. července 2000, K(2000) 2441. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://www.uoou.cz/files/rk_26-07-00.pdf.
[124] Rozsudek Soudního dvora (velkého senátu) ze dne 6. října 2015, Maximillian Schrems proti Data Protection Commissioner, C-362/14, EU:C:2015:650.
[125] JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. internetové právo. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4, s. 376.

údajům. Komisař pro ochranu osobních údajů také tuto stížnost zamítl s tím, že je neopodstatněná, neboť se odvolávala pouze na zjištění učiněná ohledně činností zpravodajských služeb Spojených států, přičemž dle jeho názoru o tom neexistují důkazy. Schrems se s ohledem na způsob vyřízení stížnosti obrátil na soud, který v rámci projednávání položil ESD dvě předběžné otázky, a to zda je úřední osoba vázána rozhodnutím zajišťujícím program Safe Harbour i přesto, že by se mělo jednat o nezávislou osobu prosazující právní předpisy o ochraně osobních údajů. Druhou otázkou pak byla, zda taková osoba má provést vlastní šetření ve věci s ohledem na situaci ke které došlo od prvního zveřejnění Komise. Dle rozhodnutí ESD je takovéto rozhodnutí Komise závazné pro všechny členské státy a tedy i pro všechny orgány členských států. Ačkoliv členské státy tak nemohly přijmout opatření, která by odporovala tomuto rozhodnutí, přesto zůstává právo osoby domáhající se ochrany svých práv, aby se obrátil na příslušný orgán, kterému nemohou být omezeny výslovně prohlášené pravomoci. V opačném případě by došlo k popření práv stanovených v čl. 8 odst. 1 a 3 LZPEU. ESD dále zdůraznil, že rozhodnutí Komise může zrušit pouze ESD, což také učinil a konstatoval, že právní předpisy a praxe ve Spojených státech nezajišťují odpovídající úroveň ochrany ve smyslu článku 25 směrnice 95/46 a dále, že rozhodnutí Komise neobsahuje žádné zjištění ohledně pravidel, které by omezily případné zásahy do základních práv osob. Kromě jiných důvodů dále soud argumentoval tím, že v rozhodnutí absentovalo ustanovení, které by stanovovalo, že USA „zajišťuje“ odpovídající úroveň ochrany osobních údajů, tak jak to vyžadoval čl. 25 odst. 6 směrnice 95/46.

V návaznosti na toto rozhodnutí vydala Komise dne 12. července 2016 prováděcí rozhodnutí[126], kterým zavedla program Privacy Shield. Ten je daleko obsáhlejší oproti Safe Harbour, přičemž zůstala možnost předávání osobních údajů bez potřeby povolení od dozorového úřadu či uzavření smluvní doložky se správcem dat v USA. Zůstává i možnost samostatné registrace jednotlivých společností do Privacy Shield, avšak byly zavedeny určité záruky, které by měly

[126] Official Journal of the European Union, COMMISSION IMPLEMENTING DECISION (EU) 2016/1250, L 207/1 C(2016) 4176). *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://publications.europa.eu/en/publication-detail/-/publication/c183d956-57a6-11e6-89bd-01aa75ed71a1/language-en/format-PDFA1A.

posilovat zajištění dodržování stanovených pravidel.[127] Jedná se zejména o kontroly společností americkými úřady, omezení přístupu veřejných orgánů k osobním údajům, řešení stížností subjektů údajů v rámci arbitrážního řízení a také zřízení ombudsmana pro ochranu osobních údajů. Kontrolní orgány by měly každoročně kontrolovat dodržování zásad pro zpracování osobních údajů ve spolupráci s Evropskou komisí, přičemž budou oprávněny ukládat sankce za jejich nedodržení či vymazat společnost z programu.[128] S ohledem na výše uvedené lze konstatovat, že předávání osobních údajů do třetích zemí a sociální sítě spolu velmi úzce souvisí. Lze tak shledat spolupráci mezi EU a USA jako velmi žádoucí, ačkoliv výsledky nejsou zcela dokonalé. Zejména bude důležité vést i v budoucnu dialog mezi zeměmi a pokračovat nadále v úzké spolupráci.

V rámci sociálních sítí také často zaměstnavatel sleduje profily svých současných či budoucích zaměstnanců, neboť uživatelé na sociálních sítích o sobě prozradí značné množství informací, o kterých se před zaměstnavatelem nezmiňují. Pokud uživatel nemá omezen přístup k těmto údajům, může je zaměstnavatel lehce shlédnout a to bez jakýchkoliv nákladů. Zaměstnavatel díky tomu má unikátní možnost kontroly svých zaměstnanců i mimo jejich pracovní dobu. Zároveň má také přístup k informacím o uchazečích o zaměstnání, na základě kterých si může zjistit, zda se nevyjadřuje nevhodně o bývalém zaměstnavateli, zda nepíše gramaticky chybně, či jaký vede život, což by se mohlo odrazit na jeho budoucím výkonu v zaměstnání. Zaměstnavatel zde naplňuje své oprávněné zájmy, které se však zároveň dostávají do rozporu s právem na soukromí a ochranu osobních údajů. Pro uchazeče o zaměstnání domnívajícího se, že mu nebylo poskytnuto zaměstnání na základě některé informace ze sociálních sítí, která vedla k diskriminaci, by bylo téměř nemožné dokázat, že tomu tak bylo. Uchazeč by na druhou stranu měl být s ohledem na zásadu transparentnosti informován, že o něm zaměstnavatel zpracovává osobní údaje, které mohou být využity při výběrovém řízení. Stejně tak pokud hodlá zaměstnavatel monitorovat chování svého zaměstnance na sociálních sítích, měl by ho o této skutečnosti dopředu informovat. Subjekt osobních údajů nemá

[127] Výčet společností, které jsou registrovány v programu Privacy Shield je dostupný na následující webové adrese: https://www.privacyshield.gov/list.
[128] SUCHÁ, Anna. „Ochranný štít“ namísto „bezpečného přístavu“. *Právní prostor* [online]. Ostrava: ATLAS consulting spol. s r.o. [cit. 2019-03-05]. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/ochranny-stit-na-misto-bezpecneho-pristavu.

možnost, aby bez tohoto upozornění zjistil, že ho někdo monitoruje, čímž je mu znemožněno využít svých práv (na informace, jejich opravu, výmaz apod.). Ve prospěch zaměstnavatele může být argumentováno zejména tím, že tyto informace o své osobě zveřejňuje subjekt dobrovolně. Osobní údaje však může také sdílet i jiná třetí osoba bez svolení subjektu údajů. Uživatelé také nemusí mít povědomí o tom, k jakému okruhu osob se data mohou dostat a předpokládají, že je uvidí pouze jejich přátelé. Přesto je však při zpracování zaměstnaneckých dat nutné dodržet zákonnost zpracování stanovenou čl. 6 GDPR. Souhlas v takovém případě může být problematický nejen z důvodů popsaných v kap. 2.6.1., ale také proto, že se jedná o poměr stran, které nemají rovnocenné postavení. Uzavřený souhlas o zpracování osobních údajů se zaměstnancem by byl shledán jako neplatný, neboť by na něho bylo pohlíženo jako na nesvobodný. Jako vhodný se zde jeví oprávněný zájem, při kterém však nesmí dojít k získání dat, které s ním evidentně nesouvisí. Například informace o tom, kde zaměstnanec trávil dovolenou je zcela irelevantní pro řádný výkon povolání. Mělo by tak dojít k vyvážení oprávněných zájmů zaměstnavatele a práva na ochranu osobních údajů zaměstnance. Zaměstnanec má zároveň právo podat námitky k zaměstnavateli, který je povinen se zpracovávání údajů zdržet. Opačně tomu však bude u profesních sociálních sítí, jako je např. LinkedIn, kde uživatelé poskytují své údaje zejména v souvislosti se zaměstnáním.

Lze shrnout, že pokud by se zaměstnavatel rozhodl získávat data o svých (budoucích) zaměstnancích, měl by důkladně zvážit, zda je takové monitorování ospravedlnitelné pro cíl, který tím chce dosáhnout. Dále by měl zvážit jaký právní titul využít pro získávání osobních údajů a zda nelze tyto informace získat jiným způsobem (např. pohovorem či motivační dopisem).[129] Nejvhodnějším postupem by mělo být stanovení si jasného cíle, za jakým je profil zaměstnance na sociální síti sledován (ochrana dobrého jména zaměstnavatele, ochrana značky apod.) a následně písemně vyrozumět zaměstnance o této skutečnosti, popřípadě mu zároveň poskytnout určitou dobu pro možnost promazání dat. Zaměstnavatel by neměl využívat data, které zjevně nesouvisí s cílem získávání dat a také by neměl přihlížet k evidentně starým příspěvkům. V momentě kdy bude jasné, že uchazeč

[129] LUKÁCS, Adrienn. To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection. Masaryk University Journal of Law and Technology [online]. 2017, 11(2), 185-214 [cit. 2019-03-08]. DOI: 10.5817/MUJLT2017-2-1. ISSN 18025943. Dostupné z: https://journals.muni.cz/mujlt/article/view/6437.

nebude přijat, by mělo dojít k odstranění údajů, pokud nebyl získán souhlas pro jejich uchování, neboť již pominul účel zpracování. Zaměstnavatel je oprávněn kontrolovat pouze veřejné příspěvky, není proto možné, aby požadoval po zaměstnanci přístupové údaje k účtu a kontroloval je tímto způsobem. Zaměstnavatel také nemá nárok na to, aby požadoval po zaměstnancích, aby si ho zařadil do okruhu přátel na sociálních sítích, aby se tak mohl dostat k neveřejným příspěvkům.[130]

Pokud by zaměstnavatel hodlal sledovat činnost zaměstnance na sociálních sítích, měl by s přihlédnutím k čl. 25 GDPR použít co možná nejšetrnější způsob. Zároveň by mělo dojít ke zpracování posouzení vlivu na ochranu osobních údajů, v rámci kterého by došlo k uvážení jednotlivých rizik se sledováním spojených. Vždy je však třeba sledovat proporcionalitu zpracování osobních údajů a poměřit ji s oprávněnými zájmy zaměstnavatele. Zjevně by tak nebylo v souladu s principem proporcionality, pokud by měla být sledována činnost zaměstnance na sociálních sítích ke zvýšení efektivity práce, neboť se tomu dá zabránit jinými způsoby, které méně zasahují do práv a svobod zaměstnanců (např. zákaz využívání sociálních sítí v pracovní době, stanovení časového limitu pro návštěvu sociálních sítí, nebo jejich zablokování na zařízeních zaměstnavatele).[131]

Členské státy mají možnost stanovit podrobnější pravidla k zajištění práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, náboru zaměstnanců, plánování apod.[132] Nakonec lze zdůraznit, že je to zejména uživatel, který dobrovolně předává osobní údaje na sociální sítě a měl by si vždy důkladně promyslet, jaké mohou mít dosah jeho příspěvky a komu mohou být zobrazeny. V tomto ohledu sociální sítě nabízí řadu možností nastavení soukromí, díky nimž je možné veškeré příspěvky zobrazovat pouze určitému okruhu uživatelů.

Se sociálními sítěmi úzce souvisí tzv. právo na výmaz, což původně nebyl legální pojem, neboť se toto právo vyvinulo teprve soudním výkladem. Právo být zapomenut vzniklo v rámci významného rozhodnutí ESD ze dne 13. května

[130] Stanovisko pracovní skupiny WP29 ze dne 8. června 2017, 02/2017.
[131] Op. cit.
[132] Čl. 88 GDPR.

2014[133], v rámci kterého se M. C. González domáhal, aby společnost Google Inc. smazala veškeré osobní údaje o jeho osobě a aby tyto údaje nebylo možné v budoucnu vyhledat, neboť při zadání jeho jména do internetového vyhledávače Google se objevovaly odkazy na španělský deník, který informoval o dražbě nemovitosti ve vlastnictví pana Gonzáleze v souvislosti s nedoplatkem na sociálním zabezpečení. González argumentoval tím, že nedoplatek byl již dávno uhrazen, přičemž předešel dražbě nemovitosti a tudíž je zmínka o nich irelevantní. V rámci sporu se na Soudní dvůr obrátil španělský nejvyšší soud s předběžnými otázkami, které se mimo jiné zaměřovaly i na výklad práva být zapomenut. Je třeba podotknout, že uvedené údaje nebyly neúplné či nepřesné povahy, proto nebylo možné požadovat smazání údajů z těchto důvodů dle původní Směrnice 95/46. ESD však dovodil, že neslučitelnost zpracování osobních údajů se Směrnicí 95/46 *„může plynout nejen ze skutečnosti, že uvedené údaje jsou nepřesné, ale konkrétně také ze skutečnosti, že jsou nepřiměřené, nepodstatné a přesahují míru s ohledem na účely, pro které jsou zpracovávány, že nejsou aktualizovány nebo že jsou uchovávány po dobu delší, než je nezbytně nutné, pokud nejsou uchovávány pro historické, statistické nebo vědecké účely.“*[134] ESD následně uvedl, že zpracování osobních údajů musí být odůvodněno po celou dobu jejich zpracování. Údaje by neměly být zpracovávány déle, než je doba nezbytně nutná pro uskutečnění cílů, ke kterým jsou shromažďovány. Od zveřejnění informací o dluzích Gonzáleze uplynulo v době rozhodování ESD již 16 let, přesto soud vyslovil, že mohou existovat konkrétní důvody veřejného zájmu k přístupu k těmto informacím. ESD tedy přenechal na posouzení španělského soudu, zda takovéto důvody existují. Je tedy třeba konstatovat, že všeobecné právo být zapomenut neexistuje a není tak možné požadovat po správci osobních údajů jejich výmaz bez přesvědčivých důvodů, kterými může být značné plynutí času, protiprávnost zpracovávání, nebo že jsou údaje nesprávné.[135]

Po zveřejnění tohoto rozhodnutí vytvořil Google na svých stránkách formulář, kde má každý možnost zažádat o odstranění konkrétních výsledků

[133] Rozsudek ESD ze dne 13. května 2014, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, EU:C:2014:317.
[134] Rozsudek ESD ze dne 13. května 2014, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, EU:C:2014:317, odst. 92.
[135] SLANINA, Jan. *Právo být zapomenut a další dopady rozsudku ESD C-131/12 Google Spain.* Epravo.cz [online]. Praha: epravo.cz [cit. 2019-02-18]. Dostupné z: https://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-ESD-c-13112-google-spain-94498.html.

zobrazených vyhledávačem Google. V příloze č. 4 je vidět jak takový formulář vypadá, Google v něm vyžaduje identifikaci žadatele, připojení dokladu totožnosti, URL adresy kde se osobní údaje nachází, čestné prohlášení a podpis. Po odeslání formuláře by měl Google posoudit, zda takové výsledky vyhledávání smaže či nikoliv. Svá rozhodnutí posuzuje s ohledem na neaktuálnost informací a také posuzuje, zda neexistuje veřejný zájem na zachování těchto informací. Posuzování je tedy plně v souladu s rozhodnutím ESD.

V současné době je právo být zapomenut výslovně zakotveno v článku 17 GDPR, poskytující subjektu údajů právo žádat o výmaz v případě, že je splněna jedna z podmínek stanovených v odst. 1, tedy pokud:

- osobní údaje již nejsou potřebné pro účely, pro které byly získány
- subjekt údajů odvolá svůj souhlas se zpracováním a neexistuje žádný další právní titul pro zpracování
- subjekt údajů vznese námitku dle čl. 21 odst. 1 a 2
- údaje byly zpracovávány protiprávně
- je dána povinnost v právu členského státu či EU ke smazání osobních údajů
- došlo ke shromáždění osobních údajů v souvislosti s nabídkou služeb informační společnosti dítěti podle čl. 8 odst. 1.

Zároveň se však tato pravidla neuplatní, pokud je zpracování nezbytné pro výkon práva na svobodu projevu a informace, plnění právní povinnosti, z důvodu veřejného zájmu v oblasti veřejného zdraví, pro účely archivace, vědy, výzkumu či statisticky a také pro určení, výkon nebo obhajobu právních nároku.[136] Další omezení spočívá ve zpracování osobních údajů pro účely vedení veřejného rejstříku. Na toto zpracování se neuplatní právo být zapomenut a to s ohledem na rozhodnutí ESD ve věcech C-138/11[137] a C-398/15[138], ve kterých ESD rozhodl, že se jedná o zpracování osobních údajů ve veřejném zájmu, které nepodléhá právu být zapomenut. Přesto by tyto údaje měly být zpracovávány pouze po dobu, po

[136] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 230.
[137] Rozsudek ESD ze dne 12. července 2012, Compass-Datenbank GmbH proti Rakouské republice, C-138/11, EU:C:2012:449.
[138] Rozsudek ESD ze dne 9. března 2017, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatore Mannimu, C-398/15, EU:C:2017:197.

kterou to vyžaduje jejich účel, přičemž v případě členů obchodních společností to může být i po jejich likvidaci, neboť mohou přetrvávat určitá práva či povinnosti.

3.7. Blockchain

Blockhain je finanční nástroj, který představuje databázi, která se neustále zvětšuje o záznamy o uskutečněných transakcích. V současnosti jsou na této technologii postavena většina kryptoměn. Výhodou blockchainu je bezpečnost transakcí a uchování dat, naopak nevýhodou je náročnost na spotřebu energie a nutnost připojení k internetu. Jednotlivé transakce probíhají za poplatek, který přísluší osobám poskytujícím výpočetní výkon, který slouží k provedení jednotlivých transakcí. Jako problematické se v rámci využívání blockchainu jeví nemožnost vyhovění práva být zapomenut, neboť z blockchainu není prakticky možné žádná data vymazat.

Jedním z řešení by byl výmaz šifrovacího klíče, který zajišťuje přístup k informacím. V případě výmazu by tak sice nedošlo k odstranění informace jako takové, ale přístup k této informaci by byl navždy ztracen. Informace by zůstala ztracena v samotném blockchainu. Další možností by bylo uchovávat data mimo řetězec, což již v současnosti některé architektury blockchainu umožňují. Skladování osobních údajů mimo samotnou databázi blockchainu by však bylo proti smyslu této technologie.[139] Další možností by byla anonymizace dat, neboť na ně nedopadají právní předpisy v oblasti ochrany osobní údajů. Každopádně je to subjekt údajů, který má kontrolu nad protokoly a tedy i svými daty, přičemž kontrola dat, které uživatel blockchainu poskytne, nemusí být pro subjekt údajů snadná.[140] Pro blockchain je zároveň typické, že se jedná o zpracování osobních údajů, které je decentralizované, neboť provedení transakcí je uskutečňováno poskytováním hardwarového výkonu řadou uživatelů, kterým jsou za to vypláceny poplatky. Bylo by tedy zároveň nemožné obdržet od subjektu údajů souhlas se zpracováním osobních údajů. Zároveň také není prakticky zjistitelné, zda jsou data zpracovávána v rámci EU či v rámci třetích zemí. Bude tedy

[139] DONAGHUE, James. *Solutions Suggest Blockchain can Conform to GDPR's "Right to be Forgotten". BlockchainLand* [online]. Paříž [cit. 2019-02-19]. Dostupné z: https://theblockchainland.com/2018/08/08/solutions-suggest-blockchain-can-conform-to-gdprs-right-to-be-forgotten/.
[140] POSADAS, JR, Dalmacio V. The internet of Things: The GDPR and the Blockchain May Be Incompatible. *INTERNET LAW.* 2018, 21(11), 19-26.

zajímavé v budoucnu sledovat, jak se technologie vyvine s ohledem na právo být zapomenut.

3.8. Zvláštní ochrana osobních údajů u dětí

Děti využívají informační a komunikační technologie již od svého útlého věku a často je dokáží využívat na pokročilejší úrovni než jejich rodiče. Přesto si děti ve svém věku nemusí zcela uvědomovat konsekvence svého počínání, čímž se stávají velmi zranitelnými. S ohledem na jejich budoucí vývoj je nezbytné, aby jim byla poskytována zvláštní míra ochrany proti zásahům do jejich osobnosti. Dítě je na internetu vystaveno řadě hrozeb, jako je kyberšikana, zneužívání dětí, nebo také tzv. kybergroomingu, tedy zneužití cizí identity k vylákání dítěte na schůzku.[141] Zvláštní ochrana by měla být poskytována zejména při shromažďování údajů pro marketingové účely, vytváření osobnostních profilů a také při shromažďování údajů pro účely nabízení služeb přímo dětem.[142]

Pokud správce hodlá shromažďovat osobní údaje dětí, je vhodné provést posouzení dopadů ochrany osobních údajů na práva a svobody dětí, zejména pokud hrozí vysoké riziko omezování práv. U dětí je obzvláště nutné vzít v potaz jejich svobodu učit se a rozvíjet, přičemž k omezení těchto práv by mělo docházet jen v přiměřeném rozsahu. Zdůrazněna by měla být zejména zásada transparentnosti, kdy by dítě mělo vědět, jak bude s jeho údaji nakládáno a jaká rizika mohou plynout z předání údajů. Ačkoliv na to právní předpisy neodkazují, měl by správce vzít v potaz Úmluvu OSN o právech dítěte, konkrétně článek 3, který stanoví zájem dítěte jako předním hlediskem při jakékoliv činnosti týkající se dětí. Při zvažování procesu získávání osobních údajů od dětí může být vhodnou volbou přizvat si na spolupráci dítě a zjistit jak danému zpracování rozumí. Získání zpětné vazby dítěte může přispět k optimalizaci získávání dat a správce díky tomu bude schopen upravit proces získávání dat, tak aby mu děti skutečně rozuměly. Dětský fond Organizace spojených národů (UNICEF) doporučuje, aby společnosti braly v úvahu pohled dětí, a to přizváním konzultantů či zástupců dětí, jejichž pomocí by mělo během konzultace dojít k přesnému zachycení zkušeností

[141] POLČÁK, Radim. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8, s. 411.
[142] Bod č. 38 recitálu GDPR.

a názorů dětí.[143] Tohoto je třeba dbát zejména v případě, kdy správce hodlá využít právního titulu opravného zájmu správce.

Při zvažování právního důvodu pro zpracování osobních údajů dětí je potřeba se zaměřit zejména na souhlas. Čl. 8 GDPR stanoví, že zpracování osobních údajů dítěte na základě souhlasu, který je získán v souvislosti s nabídkou služeb informační společnosti přímo dítěti je zákonné, je-li uděleno dítětem starším 16 let. Členské státy mají možnost tuto spodní hranici snížit až na 13 let, přičemž v ČR by mělo dojít ke snížení spodní hranice na 15 let. Pokud by chtěl správce získat souhlasy osoby mladší, musel by být tento souhlas schválen osobou vykonávající rodičovskou povinnost, případně být udělen přímo touto osobou. Pokud udělí zákonný zástupce souhlas se zpracováním osobních údajů dítěte, pak zůstává v platnosti i po dosažení věku dítěte, který jej opravňuje udělovat souhlas samostatně. Dítě má však možnost vzít tento rodičovský souhlas zcela zpět či jej upravit. Správce by měl zavést určité mechanismy, které by měly ověřit věk dítěte, což může být problematické, neboť děti nemusí disponovat žádným dokladem a zároveň neexistuje žádný registr, kde by bylo možné věk dítěte ověřit. Vždy tak bude záležet na riziku, které může zpracováním vznikat, povětšinou by však měla postačit určitá forma čestného prohlášení, kde dítě potvrdí svůj věk.[144] Nabídka dále musí směřovat přímo vůči dítěti, neuplatní se tak rodičovský souhlas, pokud je služba nabízena např. skrze školní zařízení. Pokud správce nechce poskytovat své služby dětem, pak by měl stanovit omezení použití nad věk osmnácti let. Zároveň by měly být využity určité prostředky, aby děti k této službě neměly přístup, např. čestné prohlášení, doklad totožnosti apod. Restrikce v podobě věkového omezení a ověření totožnosti by měla dostatečně zaručit, že by se správce nemusel zabývat rodičovským souhlasem. V opačném případě, pokud není dána restrikce, je třeba uvažovat, že uživateli budou i děti a to i přesto, pokud jim služba není přímo určena. S ohledem na skutečnost, že internet nelze teritoriálně omezit, je také potřeba zvažovat z jakého členského státu dítě pochází, neboť každý členský stát má stanoven různý věkový limit. Správce kromě věku

[143] What should our general approach to processing children's personal data be?. *Information Commissioner's Office* [online]. Information Commissioner's Office, 2019 [cit. 2019-03-17]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be.

[144] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 166-167.

musí také ověřit státní příslušnost. Domnívám se, že možnost ponechaná členským státům ke zpřesnění právní úpravy je na tomto místě velmi nešťastná, neboť z výše uvedeného důvodu je patrné, že správce je nucen zpracovávat další osobní údaj. Takovéto ustanovení je pak v rozporu se zásadou minimalizace dat.

V případě souhlasů je třeba zároveň dbát občanského zákoníku[145], který stanoví, že nezletilý je způsobilý k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti úměrně k jeho věku. V případě, kdy by dítě dosahovalo věkové hranice, v rámci které může samostatně udělit souhlas, pak je potřeba přihlížet ještě k tomuto ustanovení. Pokud by tak měl být udělen souhlas k velmi komplikovanému zpracování, které by dítě nebylo s ohledem na svoji rozumovou a mravní vyspělost schopno posoudit, byl by i takovýto souhlas shledán neplatným. Konkrétně by se mohlo například jednat o dlouhodobé osobnostní profilování dítěte, které by mohlo mít v budoucnu negativní následky.[146]

[145] § 31 zákona č. 89/2012 Sb.
[146] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 168.

Závěr

Rozvoj informačních a komunikačních technologií představuje nejen pro ochranu osobních údajů, ale i pro právo obecně zcela nové výzvy. Na ochranu soukromí jakožto základní lidské právo se snaží reagovat EU skrze sekundární právní předpisy, jež byly v rámci této práce analyzovány s ohledem na internetové prostředí. Cílem této práce je uvést čtenáře do problematiky ochrany osobních údajů na internetu a představit, jakým způsobem by měl správce postupovat, pokud hodlá zpracovávat osobní údaje na internetu. V první části práce jsem definoval co jsou to osobní údaje a proč je důležité, aby byly chráněny. Podrobněji jsem analyzoval co vše lze považovat za osobní údaj v prostředí internetu. Popsány byly síťové identifikátory, soubory cookies či lokalizační údaje. Zároveň jsem rozebral kategorii citlivých osobních údajů, jejichž zpracování podléhá přísnějším pravidlům.

V druhé kapitole bylo představeno právo na ochranu soukromí a jeho ukotvení mezi základními lidskými právy, ze kterého je ochrana osobních údajů odvozena. Analyzován byl vývoj legislativy v oblasti ochrany osobních údajů v právu EU, v rámci které postupně dochází ke zpřísňování podmínek pro možnost zpracovávání osobních údajů. Popsány byly základní zásady jako je např. zásada zákonnosti, účelového omezení či minimalizace osobních údajů, na kterých je legislativa postavena, a které slouží jako vodítko pro výklad jednotlivých ustanovení.

Uvedl jsem právní tituly, na základě kterých je možné zpracovávat osobní údaje, přičemž jsem se podrobněji věnoval souhlasu se zpracováním osobních údajů a oprávněnému zájmu správce. Zaměřil jsem se zejména na GDPR, jakožto doposud poslední platný právní předpis v EU, mající významný dopad na internetové prostředí. Výklad jsem věnoval také návrhu nařízení ePrivacy a popsal jsem jaké by mohlo mít dopady na komunikační služby poskytované skrze internet, ať už se jedná o komunikaci interpersonální, nebo mezi stroji v rámci IoT. U návrhu nařízení ePrivacy se domnívám, že by ještě mělo dojít ke zvážení určitých změn, zejména k odstranění významově duplicitních ustanovení, která jsou již obsažená v GDPR. Zvážena by měla být i změna v rámci využívání přímého marketingu srkze internet, kdy by v rámci ePrivacy mělo dojít k omezení

využívání právního titulu oprávněného zájmu správce na základě předchozího obchodního vztahu.

Poslední část práce je věnována způsobu, jakým jsou právní předpisy na ochranu osobních údajů aplikovány v praxi a jak konkrétně by měl správce postupovat, pokud hodlá zpracovávat osobní údaje na internetu. V rámci výkladu byla zdůrazněna důležitost jednotlivých zásad, které by měly pomoci správci při praktické aplikaci jednotlivých ustanovení. Správci poskytující své služby skrze internet by měli věnovat ochraně osobních údajů značnou pozornost a zvážit, které kroky podniknou, aby zajistili soulad zpracování osobních údajů s právními předpisy. Měli by zejména posoudit, zda mají povinnost jmenovat pověřence pro ochranu osobních údajů, a v případě využívání nových technologií zpracovat důkladné posouzení vlivu na ochranu osobních údajů. Dále jsem nastínil, jak by si měl správce počínat v případě, kdy hodlá využívat cloud computingových služeb.

Rozebral jsem sociální sítě v souvislosti s právem být zapomenut a v jakých případech má zaměstnavatel právo sledovat chování svých současných či budoucích zaměstnanců na sociálních sítích. Poslední podkapitolu jsem věnoval specifikům ochrany osobních údajů dětí na internetu, zejména jsem uvedl podmínky, za nichž má správce možnost od dítěte získat souhlas se zpracováním osobních údajů.

Diplomová práce nepoukazuje pouze na jediná možná řešení, která by správce měl podniknout. Nabízí pouze určitá konkrétní řešení při zpracovávání osobních údajů, která by správce měl zvážit, pokud plánuje využívat informačních a komunikačních technologií pro svou činnost. Pokud by si správce nebyl jistý zda splňuje požadavky ochrany osobních údajů, měl by využít zejména stanoviska pracovní skupiny WP29, případně svou činnost konzultovat s dozorovým orgánem.

Resumé

This diploma thesis is focused on personal data protection within the scope of EU legislation. It focuses on the impact of legislation within the online environment. The thesis presents the practical application of the various legal regulations. Specifically, several decisions of the European Court of Justice are cited to illustrate some of the difficulties in the practical application of the data protection legislation.

The first part of the thesis defines the term ‘personal data’ and highlights various types of personal data commonly present on the Internet. Further, it explains which information this data could provide to anyone who scrutinizes it and why it is important to protect this data.

The next section describes the anchoring of the right to privacy within fundamental rights and freedoms and chronologically lists the most important EU regulations. An important part of the thesis is dedicated to the GDPR and ePrivacy proposals and the basic principles that are important for the interpretation of some of their provisions.

The last part is focused on the practical application of legal provisions. It describes the possible implications of the ePrivacy proposal on communication services. This thesis describes how personal data controllers should proceed to meet requirements imposed on them, especially when they are using services like cloud computing, social networks and blockchain. Furthermore, the issue of personal data protection of children is described, especially in cases where it is possible to use the consent to process the child's personal data as legal title. Finally, the personal data controllers must always consider context and think about the steps they will need to take in order to meet the privacy policy.

Seznam použitých pramenů

1. Odborná literatura

DONÁT, Josef a Jan TOMÍŠEK. *Právo v síti: průvodce právem na internetu.* V Praze: C.H. Beck, 2016. ISBN 978-80-7400-610-4.

JANSA, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALIŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. *internetové právo.* Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.

KLEMENT, Milan. *IP adresace a směrování v počítačových sítích.* Olomouc: Univerzita Palackého v Olomouci, 2015. ISBN 978-80-244-4571-7.

MAŠTALKA, Jiří. *Osobní údaje, právo a my.* V Praze: C.H. Beck, 2008. Beckova edice ABC. ISBN 978-80-7400-033-1.

MATEJKA, Ján. *internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, c2013. CZ.NIC. ISBN 978-80-904248-7-6.

NAVRÁTIL, Jiří. *GDPR pro praxi.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.

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

NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5.

NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů.* Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání.* Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář.* Praha: Leges, 2018. Komentátor. ISBN 978-80-7502-288-2

POLČÁK, Radim. *internet a proměny práva.* Praha: Auditorium, 2012. Téma (Auditorium). ISBN 978-80-87284-22-3.

POLČÁK, Radim. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8.

ŠIMÍČEK, Vojtěch, ed. *Právo na soukromí.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011. ISBN 978-80-210-5449-3.

TICHÝ, Luboš. *Evropské právo. 5., přeprac. vyd.* V Praze: C.H. Beck, 2014. Academia iuris (C.H. Beck). ISBN 978-80-7400-546-6.

VELTE, Anthony T., Toby J. VELTE a Robert C. ELSENPETER. *Cloud Computing: praktický průvodce.* Brno: Computer Press, 2011. ISBN 978-80-251-3333-0.

WALDO, James, Herbert LIN a Lynette I MILLETT. *Engaging privacy and information technology in a digital age.* Washington, D.C.: National Academies Press, c2007. ISBN 978-0-309-10392-3.

2. Odborné články

FAL, O. M. a V. F. KOZAK. *PERSONAL DATA PROTECTION PROBLEMS ASSOCIATED WITH CLOUD COMPUTING* [online]. USA: Springer US, 2014 [cit. 2019-03-04]. ISSN 1573-8337. Dostupné z: https://link.springer.com/article/10.1007/s10559-014-9667-8.

GRIMMELMANN, James. *Saving Facebook.* New York, 2008. Cornell Law School.

LUKÁCS, Adrienn. To Post, or Not to Post – That Is the Question: Employee Monitoring and Employees' Right to Data Protection. Masaryk University Journal of Law and Technology [online]. 2017, 11(2), 185-214 [cit. 2019-03-08]. DOI: 10.5817/MUJLT2017-2-1. ISSN 18025943. Dostupné z: https://journals.muni.cz/mujlt/article/view/6437.

NEŠPŮREK, Robert, Jaroslav ŠUCHMAN a Ján JAROŠ. Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?. *Epravo.cz magazine* [online]. 2018,

2018(1), 41-43 [cit. 2019-03-08]. Dostupné z: https://www.epravo.cz/_dataPublic/data/E-pravo_mag/2018_E1_web.pdf.

PATHAK, P.B. internet of Things: A Look at Paradigm Shifting Applications and Challenges. *International Journal of Advanced Research in Computer Science* [online]. 2016, 7(2), 50-51 [cit. 2019-03-10]. ISSN 0976-2697. Dostupné z: www.ijarcs.info.

POSADAS, JR, Dalmacio V. The internet of Things: The GDPR and the Blockchain May Be Incompatible. *INTERNET LAW.* 2018, 21(11).

Rolf H Weber and Romana Weber, *internet of Things: Legal Perspectives*, vol 49 (Springer Science & Business Media, 2010).

WACHTER, Sandra. The GDPR and the internet of Things: a three-step transparency model. *Law, Innovation and Technology* [online]. 2018, 10(2), 266-294 [cit. 2019-03-10]. DOI: 10.1080/17579961.2018.1527479. ISSN 1757-9961. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1527479.

3. Dokumenty a právní předpisy

Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, 17/EN WP 259. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849.

Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248 rev. 01. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

Article 29 Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 17/EN WP 247. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

Article 29 Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Article 29 Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN WP 196. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://www.pdpjournals.com/docs/88016.pdf.

Commission staff working document, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, SWD(2017) 5 final. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0005&from=GA.

Listina základních práv Evropské unie

Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů

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).

Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).

Official Journal of the European Union, COMMISSION IMPLEMENTING DECISION (EU) 2016/1250, L 207/1 C(2016) 4176. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://publications.europa.eu/en/publication-detail/-/publication/c183d956-57a6-11e6-89bd-01aa75ed71a1/language-en/format-PDFA1A.

Rozhodnutí Komise ze dne 26. července 2000, K(2000) 2441. *Evropská komise* [online]. [cit. 17. 3. 2019]. Dostupné z: https://www.uoou.cz/files/rk_26-07-00.pdf.

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Smlouva o Evropské unii

Smlouva o fungování Evropské unie

Úmluva Rady Evropy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních dat.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

4. Judikatura a soudní rozhodnutí

Rozsudek ESD ze dne 12. července 2012, Compass-Datenbank GmbH proti Rakouské republice, C-138/11, EU:C:2012:449.

Rozsudek ESD ze dne 13. května 2014, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, EU:C:2014:317.

Rozsudek ESD ze dne 19. října 2016, Patrick Breyer protiBundesrepublik Deutschland, C-582/14, EU:C:2016:779.

Rozsudek ESD ze dne 29. ledna 2008, Productores de Música de España (Promusicae) v. Telefónica de España SAU, EU:C:2008:54.

Rozsudek ESD ze dne 9. března 2017, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce proti Salvatore Mannimu, C-398/15, EU:C:2017:197.

Rozsudek Soudního dvora (velkého senátu) ze dne 6. října 2015, Maximillian Schrems proti Data Protection Commissioner, C-362/14, EU:C:2015:650.

Rozsudek ESD ze dne 17. října 2013, Michael Schwarz proti Stadt Bochum, C-291/12, EU:C:2013:670.

Rozsudek ESD ze dne 6. listopadu 2003, Bodil Lindqvist, C-101/01, EU:C:2003:596

Rozsudek ESD ze dne 9. listopadu 2010, Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) proti Land Hessen, za přítomnosti: Bundesanstalt für Landwirtschaft und Ernährung, ve spojených věcech C-92/09 a C-93/09, EU:C:2010:662.

5. Internetové zdroje

Cross-border issues under EU data protection law with regards to personal data protection. Taylor & Francis Online [online]. Londýn: Informa UK Limited, 2018, 24.05.2017 [cit. 2018-09-17]. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1330740.

DECEW, Judith. Privacy. *Stanford Encyclopedia of Philosophy* [online]. Kalifornie: The Metaphysics Research Lab, 2016, 14.5.2002 [cit. 2018-09-29]. Dostupné z: https://plato.stanford.edu/entries/privacy/#CriPri.

Digital economy and society statistics - households and individuals. Eurostat [online]. Luxembourg [cit. 2018-04-08]. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#internet_access.

Digital single market. European Commission [online]. 2018 [cit. 2019-02-10]. Dostupné z: https://ec.europa.eu/commission/priorities/digital-single-market_en.

DONAGHUE, James. *Solutions Suggest Blockchain can Conform to GDPR's "Right to be Forgotten". BlockchainLand* [online]. Paříž [cit. 2019-02-19]. Dostupné z: https://theblockchainland.com/2018/08/08/solutions-suggest-blockchain-can-conform-to-gdprs-right-to-be-forgotten/.

ePrivacy může ohrozit technologické inovace. Sdružení pro internetový rozvoj [online]. Praha [cit. 2019-03-16]. Dostupné z: http://www.spir.cz/eprivacy-muze-ohrozit-technologicke-inovace.

Eurobarometer průzkum z července 2016, č. 443 (SMART 2016/079), dostupný z: ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82290.

EUROPEAN DATA PROTECTION SUPERVISOR [online]. Brussels, 2019 [cit. 2019-03-17]. Dostupné z: https://edps.europa.eu/edps-homepage_en.

GOLD, Jon. *Lab makes data sharing easier so medical IoT devices can be smarter*. Network World [online]. Framingham: IDG Communications, 2018 [cit. 2018-10-09]. Dostupné z: https://www.networkworld.com/article/3295905/internet-of-things/lab-makes-data-sharing-easier-so-medical-iot-devices-can-be-smarter.html?utm_campaign=IoT%2BWeekly%2BNews&utm_medium=web&utm_source=IoT_Weekly_News_125.

HÄRTING, Niko. *STUDY ON THE IMPACT OF THE PROPOSED EPRIVACY REGULATION* [online]. Berlin, 2017 [cit. 2019-03-14]. Dostupné z: https://www.haerting.de/sites/default/files/downloads/study_on_the_impact_of_the_proposed_eprivacy_regulation.pdf. Studie. HÄRTING Rechtsanwälte.

HRADSKÝ, Jiří. *Přímý marketing ve světle nařízení eprivacy a GDPR.* Iurium [online]. iurium, [2018] [cit. 2019-02-20]. Dostupné z: https://www.iurium.cz/2018/12/15/primy-marketing-ve-svetle-narizeni-eprivacy-a-gdpr/.

China's data privacy standard came into effect this May - inspired by GDPR. Computerworld UK [online]. London, 2018 [cit. 2018-09-11]. Dostupné z: https://www.computerworlduk.com/data/how-chinas-data-privacy-law-was-inspired-by-gdpr-3678918/.

IoT regulation: IoT, GDPR, ePrivacy Regulation and more regulations. *I-SCOOP* [online]. Belgium: i-SCOOP, 2019 [cit. 2019-03-10]. Dostupné z: https://www.i-scoop.eu/internet-of-things-guide/iot-regulation/.

KELION, Leo. *Facebook seeks facial recognition consent in EU and Canada.* BBC [online]. London [cit. 2019-03-01]. Dostupné z: https://www.bbc.com/news/technology-43797128.

KUCHLER, Hannah. Facebook chief admits 'mistakes' over data leaks. *FINANCIAL TIMES* [online]. London: Nikkei, 2019 [cit. 2018-09-17]. Dostupné z: https://www.ft.com/content/3130c420-3c0c-11e8-b9f9-de94fa33a81e.

LARSON, Selena. *Every single Yahoo account was hacked - 3 billion in all*. In: CNN: tech [online]. 4.10.2017 [cit. 2018-04-08]. Dostupné z: http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

NESPUREK, Robert, Richard OTEVŘEL a Monika MATYSOVÁ. *Breyer Ruling, And Dynamic IP Addresses As Personal Data.* Mondaq [online]. Copyright © 1994-2018 Mondaq ®, 2019 [cit. 2019-01-22]. Dostupné z: http://www.mondaq.com/x/677894/data+protection/Breyer+Ruling+And+Dynamic+IP+Addresses+As+Personal+Data.

Proposal for an ePrivacy Regulation. European Commission [online]. 2018 [cit. 2019-02-10]. Dostupné z: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

Right environment for digital networks and services. European Commission [online]. 2018 [cit. 2019-02-10]. Dostupné z: https://ec.europa.eu/digital-single-market/en/right-environment-digital-networks-and-services.

SLANINA, Jan. *Právo být zapomenut a další dopady rozsudku ESD C-131/12 Google Spain.* Epravo.cz [online]. Praha: epravo.cz [cit. 2019-02-18]. Dostupné z: https://www.epravo.cz/top/clanky/pravo-byt-zapomenut-a-dalsi-dopady-rozsudku-ESD-c-13112-google-spain-94498.html.

SUCHÁ, Anna. „Ochranný štít" namísto „bezpečného přístavu". *Právní prostor* [online]. Ostrava: ATLAS consulting spol. s r.o. [cit. 2019-03-05]. Dostupné z:

https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/ochranny-stit-na-misto-bezpecneho-pristavu.

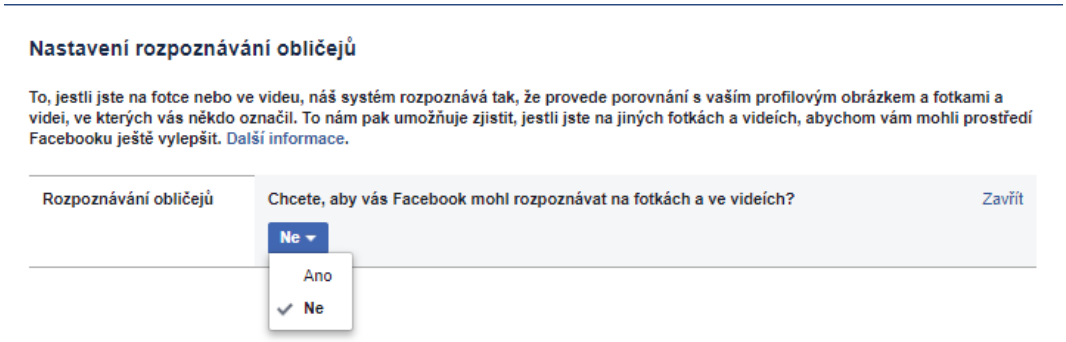
ŠVEJDOVÁ, Martina. *Marketing ve světle ustanovení GDPR.* Epravo.cz [online]. Praha: epravo.cz, [2018] [cit. 2019-02-20]. Dostupné z: https://www.epravo.cz/top/clanky/marketing-ve-svetle-ustanoveni-gdpr-106977.html.

What should our general approach to processing children's personal data be?. *Information Commissioner's Office* [online]. Information Commissioner's Office, 2019 [cit. 2019-03-17]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be.

YUN CHEE, Foo. *Exclusive: EU privacy chief expects first round of fines under new law by year-end.* Reuters [online]. New York: Thomson Reuters, 2019 [cit. 2019-02-11]. Dostupné z: https://uk.reuters.com/article/us-eu-gdpr-exclusive/exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end-idUKKCN1MJ2AY.

ZEVENBERGEN, Jaap. *European Privacy Law and its Effect on Location Information* [online]. Delft, the Netherlands, 2004 [cit. 2019-03-03]. Dostupné z: http://www.otb.tudelft.nl/fileadmin/Faculteit/Onderzoeksinstituut_OTB/Over_OTB/Medewerkers/alle_medewerkers/doc/jaapz.pdf. Delft University of Technology.

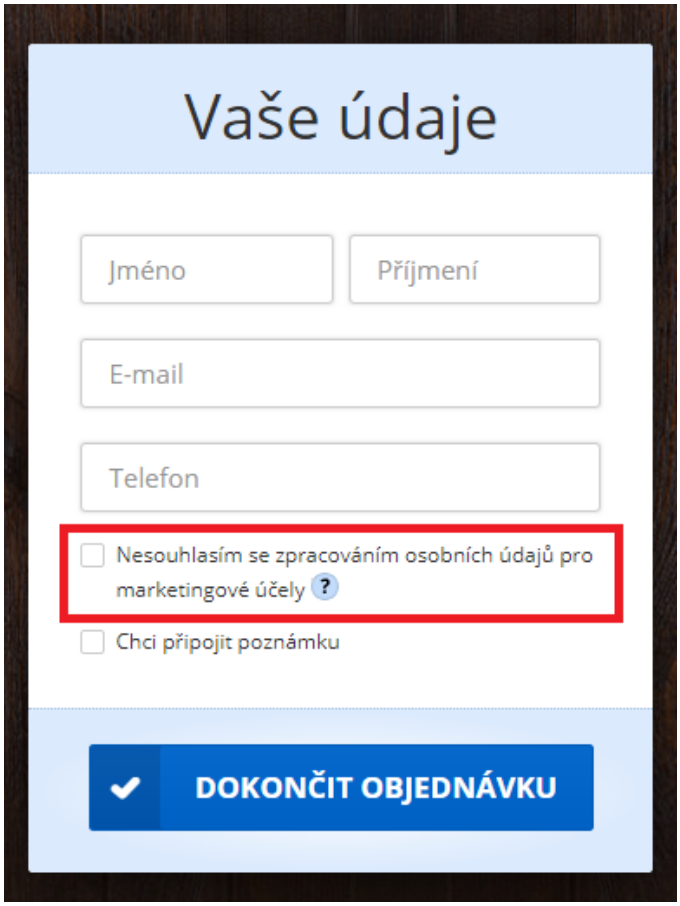
Příloha č. 1



Příloha č. 1 ukazuje, jak sociální síť Facebook pro přijetí nařízení GDPR začlenila povinnost získávání souhlasu pro automatické zpracovávání fotografií, které rozpoznávalo obličeje svých uživatelů.

Zdroj:
https://www.facebook.com/settings?tab=facerec&section=face_recognition&view

Příloha č. 2



Příloha č. 2 znázorňuje častou praxi internetových obchodů, které vyžadují po uživateli aktivní jednání, aby nebyl udělen souhlas pro zasílání marketingových sdělení, což odporuje požadavku na učinění projevu vůle.

Zdroj: https://www.knihydobrovsky.cz/

Příloha č. 3

Cloud Computing Risk Assessment Module

The following is intended as a sample risk assessment for health care organizations that utilize cloud services. It is intended to address the risks to confidentiality, integrity, and availability that the health care organization should consider addressing. It is not intended to address the risks to the cloud provider, who should separately perform its own risk assessment. The identified risks are examples, and should be modified based on the specific circumstances of the cloud provider, who likely will have a different set of existing controls, different risk levels, and may face additional categories of risks. Recommended Best Practice Controls are potential ways to address risks and are not intended to represent the only appropriate controls.

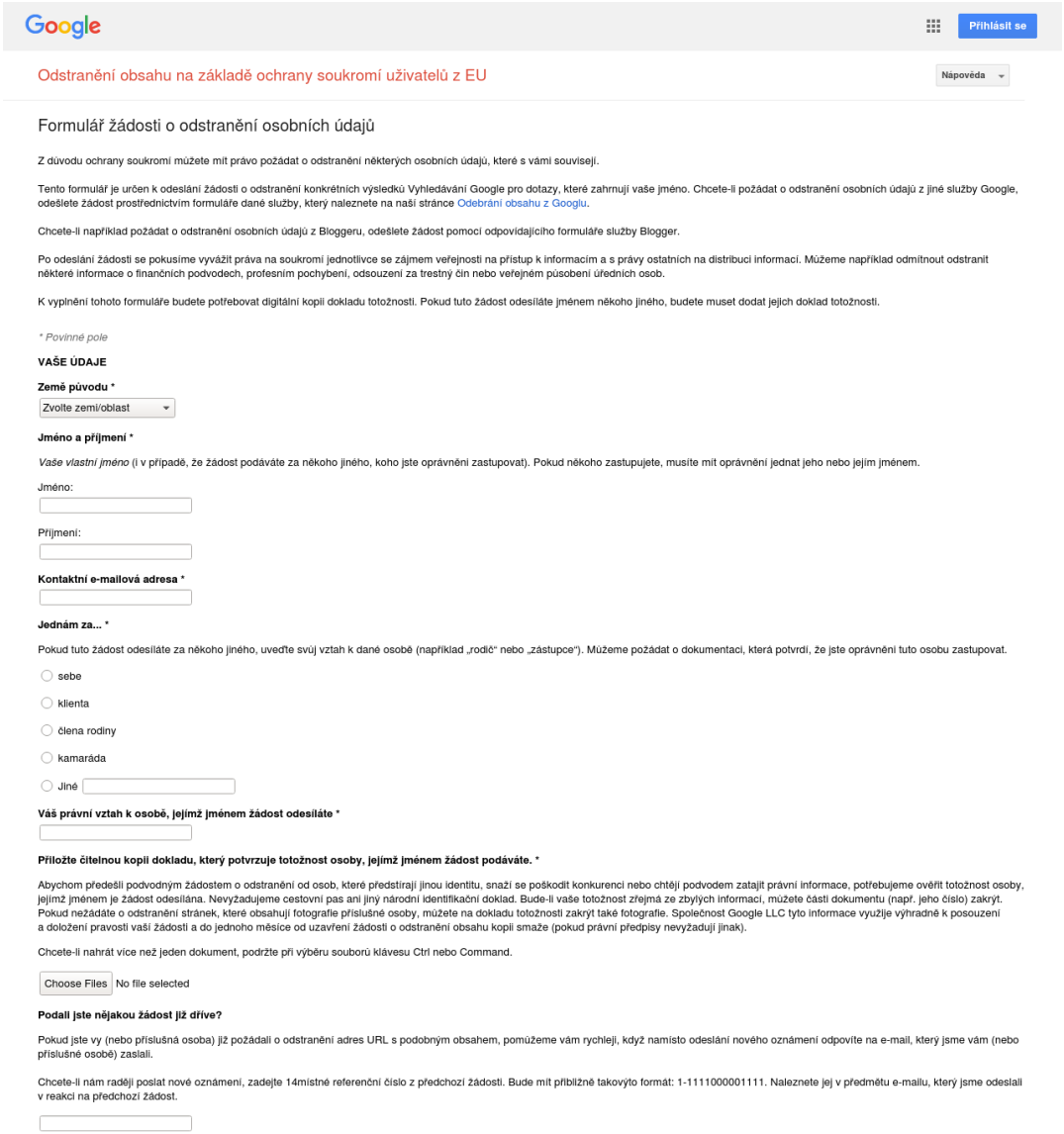
As vulnerabilities are discovered you can record them and evaluate the level of risk using this report.

Vulnerability Name	Risk Description	Threat Source	Existing Controls	Likelihood of Occurrence	Impact Severity	Risk Level	Potential Best Practice Control
Weak password protections for cloud services	Unauthorized person is able to obtain access to information by guessing a password	Adversarial insider or outsider	Vendor default password and no administrative password policy	Moderate	High	Moderate	Turn on vendor feature requiring strong passwords and implement policy prohibiting weak password practices
Unlimited password attempts for cloud services	Unauthorized person uses automated attack to obtain passwords	Adversarial outsider (e.g., hacker)	Vendor default does not limit password attempts	Moderate	High	Moderate	Turn on vendor feature limiting failed login attempts
Social engineering attempt to obtain password to cloud services	Unauthorized person obtains password by posing as insider (e.g., IT department)	Adversarial outsider (e.g., hacker)	None	Moderate	High	Moderate	Institute policy and provide training that users may not share passwords with others, including IT department
Password to cloud services is written down and available to unauthorized persons	Unauthorized person obtains copy of written password to cloud services	Adversarial insider or outsider	None	Moderate	High	Moderate	Institute policy and provide training that users may not write down passwords and leave unattended
Download of cloud information	Authorized user downloads local copy of information from cloud onto unsecure device, which is lost or stolen	Users	None	High	High	High	Determine appropriate download policy (e.g. information may only be downloaded in limited circumstances and only to properly secured devices)
Corruption during transit	Information is partial or incorrect (e.g. due to packet loss), resulting in patient safety concerns due to incomplete medical information	Accidental	Software application checks integrity of transmitted data	Very Low	High	Low	No additional control necessary
Service outage at cloud provider	Lack of access to information, potentially including electronic health	Accidental or environmental	None	Moderate	High	Moderate	Evaluate business continuity and disaster recovery options (e.g. from cloud provider or through

V příloze č. 3 je znázorněna část vzorové analýzy rizik určených pro zdravotní organizace využívající cloudových služeb. V rámci tabulky je vidět, jakým způsobem může správce analyzovat možná rizika, jejich zdroj a pravděpodobnost výskytu rizika. Poslední sloupec znázorňuje, jakým nejvhodnějším způsobem lze daná rizika kontrolovat.

Zdroj: https://www.himss.org/library/health-it-privacy-security/sample-cloud-risk-assessment

Příloha č. 4



Google

Přihlásit se

Odstranění obsahu na základě ochrany soukromí uživatelů z EU

Nápověda

Formulář žádosti o odstranění osobních údajů

Z důvodu ochrany soukromí můžete mít právo požádat o odstranění některých osobních údajů, které s vámi souvisejí.

Tento formulář je určen k odeslání žádosti o odstranění konkrétních výsledků Vyhledávání Google pro dotazy, které zahrnují vaše jméno. Chcete-li požádat o odstranění osobních údajů z jiné služby Google, odešlete žádost prostřednictvím formuláře dané služby, který naleznete na naší stránce Odebrání obsahu z Googlu.

Chcete-li například požádat o odstranění osobních údajů z Bloggeru, odešlete žádost pomocí odpovídajícího formuláře služby Blogger.

Po odeslání žádosti se pokusíme vyvážit práva na soukromí jednotlivce se zájmem veřejnosti na přístup k informacím a s právy ostatních na distribuci informací. Můžeme například odmítnout odstranit některé informace o finančních podvodech, profesním pochybení, odsouzení za trestný čin nebo veřejném působení úředních osob.

K vyplnění tohoto formuláře budete potřebovat digitální kopii dokladu totožnosti. Pokud tuto žádost odesíláte jménem někoho jiného, budete muset dodat jejich doklad totožnosti.

** Povinné pole*

VAŠE ÚDAJE

Země původu *

Zvolte zemi/oblast

Jméno a příjmení *

Vaše vlastní jméno (i v případě, že žádost podáváte za někoho jiného, koho jste oprávněni zastupovat). Pokud někoho zastupujete, musíte mít oprávnění jednat jeho nebo jejím jménem.

Jméno:

Příjmení:

Kontaktní e-mailová adresa *

Jednám za... *

Pokud tuto žádost odesíláte za někoho jiného, uveďte svůj vztah k dané osobě (například „rodič“ nebo „zástupce“). Můžeme požádat o dokumentaci, která potvrdí, že jste oprávněni tuto osobu zastupovat.

- sebe
- klienta
- člena rodiny
- kamaráda
- Jiné

Váš právní vztah k osobě, jejímž jménem žádost odesíláte *

Přiložte čitelnou kopii dokladu, který potvrzuje totožnost osoby, jejímž jménem žádost podáváte. *

Abychom předešli podvodným žádostem o odstranění od osob, které představují jinou identitu, snaží se poškodit konkurenci nebo chtějí podvodem zatajit právní informace, potřebujeme ověřit totožnost osoby, jejímž jménem je žádost odesílána. Nevyžadujeme cestovní pas ani jiný národní identifikační doklad. Bude-li vaše totožnost zřejmá ze zbylých informací, můžete části dokumentu (např. jeho číslo) zakrýt. Pokud nežádáte o odstranění stránek, které obsahují fotografie příslušné osoby, můžete na dokladu totožnosti zakrýt také fotografie. Společnost Google LLC tyto informace využije výhradně k posouzení a doložení pravosti vaší žádosti a do jednoho měsíce od uzavření žádosti o odstranění obsahu kopii smaže (pokud právní předpisy nevyžadují jinak).

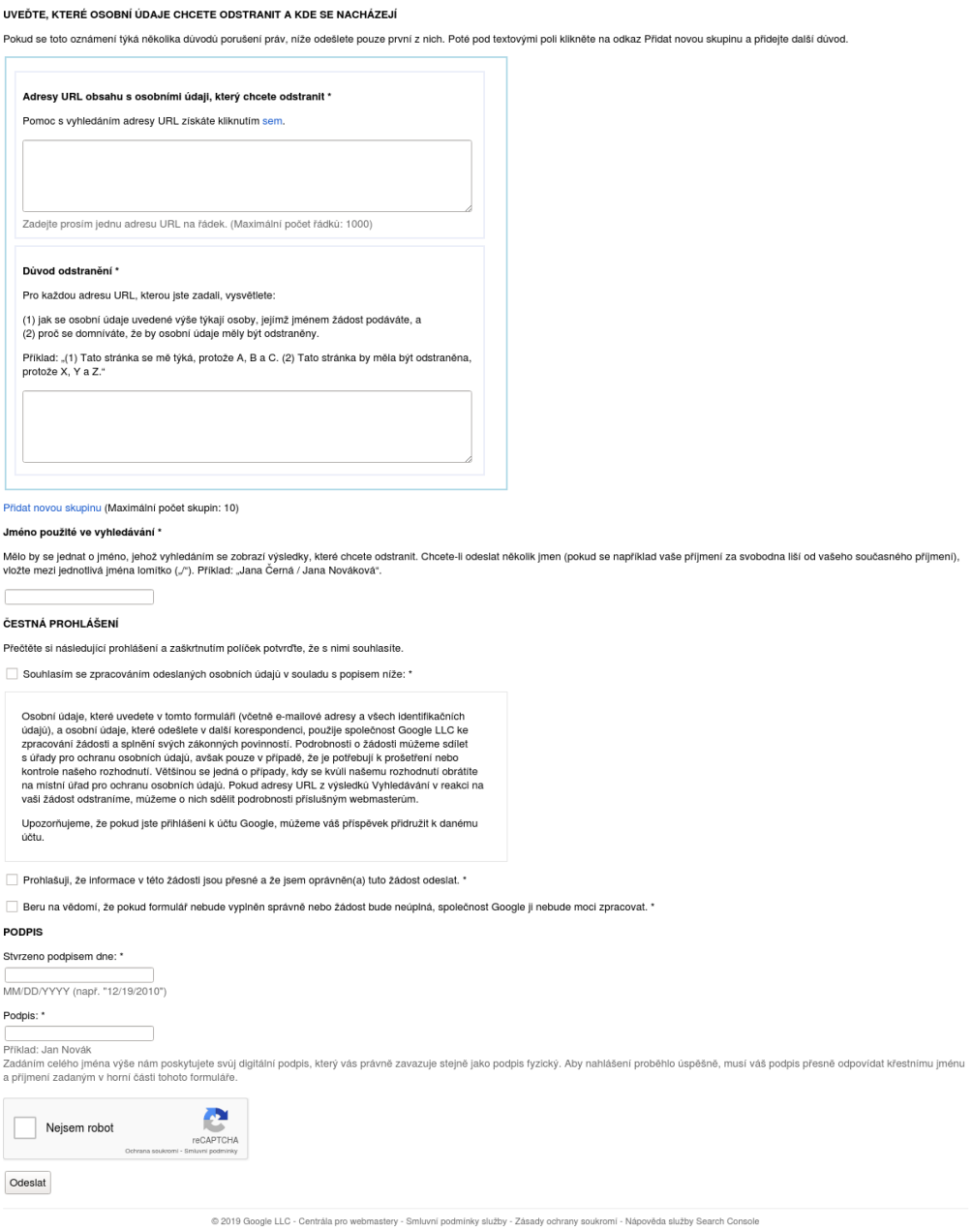
Chcete-li nahrát více než jeden dokument, podržte při výběru souborů klávesu Ctrl nebo Command.

Choose Files No file selected

Podali jste nějakou žádost již dříve?

Pokud jste vy (nebo příslušná osoba) již požádali o odstranění adres URL s podobným obsahem, pomůžeme vám rychleji, když namísto odeslání nového oznámení odpovíte na e-mail, který jsme vám (nebo příslušné osobě) zaslali.

Chcete-li nám raději poslat nové oznámení, zadejte 14místné referenční číslo z předchozí žádosti. Bude mít přibližně takovýto formát: 1-1111000001111. Naleznete jej v předmětu e-mailu, který jsme odeslali v reakci na předchozí žádost.



UVEĎTE, KTERÉ OSOBNÍ ÚDAJE CHCETE ODSTRANIT A KDE SE NACHÁZEJÍ

Pokud se toto oznámení týká několika důvodů porušení práv, níže odešlete pouze první z nich. Poté pod textovými poli klikněte na odkaz Přidat novou skupinu a přidejte další důvod.

Adresy URL obsahu s osobními údaji, který chcete odstranit *

Pomoc s vyhledáním adresy URL získáte kliknutím sem.

Zadejte prosím jednu adresu URL na řádek. (Maximální počet řádků: 1000)

Důvod odstranění *

Pro každou adresu URL, kterou jste zadali, vysvětlete:

(1) jak se osobní údaje uvedené výše týkají osoby, jejímž jménem žádost podáváte, a
(2) proč se domníváte, že by osobní údaje měly být odstraněny.

Příklad: „(1) Tato stránka se mě týká, protože A, B a C. (2) Tato stránka by měla být odstraněna, protože X, Y a Z."

Přidat novou skupinu (Maximální počet skupin: 10)

Jméno použité ve vyhledávání *

Mělo by se jednat o jméno, jehož vyhledáním se zobrazí výsledky, které chcete odstranit. Chcete-li odeslat několik jmen (pokud se například vaše příjmení za svobodna liší od vašeho současného příjmení), vložte mezi jednotlivá jména lomítko („/"). Příklad: „Jana Černá / Jana Nováková".

ČESTNÁ PROHLÁŠENÍ

Přečtěte si následující prohlášení a zaškrtnutím políček potvrďte, že s nimi souhlasíte.

Souhlasím se zpracováním odeslaných osobních údajů v souladu s popisem níže: *

Osobní údaje, které uvedete v tomto formuláři (včetně e-mailové adresy a všech identifikačních údajů), a osobní údaje, které odešlete v další korespondenci, použije společnost Google LLC ke zpracování žádosti a splnění svých zákonných povinností. Podrobnosti o žádosti můžeme sdílet s úřady pro ochranu osobních údajů, avšak pouze v případě, že je potřebují k prošetření nebo kontrole našeho rozhodnutí. Většinou se jedná o případy, kdy se kvůli našemu rozhodnutí obrátíte na místní úřad pro ochranu osobních údajů. Pokud adresy URL z výsledků Vyhledávání v reakci na vaši žádost odstraníme, můžeme o nich sdělit podrobnosti příslušným webmasterům.

Upozorňujeme, že pokud jste přihlášeni k účtu Google, můžeme váš příspěvek přidružit k danému účtu.

Prohlašuji, že informace v této žádosti jsou přesné a že jsem oprávněn(a) tuto žádost odeslat. *

Beru na vědomí, že pokud formulář nebude vyplněn správně nebo žádost bude neúplná, společnost Google ji nebude moci zpracovat. *

PODPIS

Stvrzeno podpisem dne: *

MM/DD/YYYY (např. "12/19/2010")

Podpis: *

Příklad: Jan Novák
Zadáním celého jména výše nám poskytujete svůj digitální podpis, který vás právně zavazuje stejně jako podpis fyzický. Aby nahlášení proběhlo úspěšně, musí váš podpis přesně odpovídat křestnímu jménu a příjmení zadaným v horní části tohoto formuláře.

Nejsem robot reCAPTCHA Ochrana soukromí - Smluvní podmínky

Odeslat

© 2019 Google LLC - Centrála pro webmastery - Smluvní podmínky služby - Zásady ochrany soukromí - Nápověda služby Search Console

Příloha č. 4 znázorňuje formulář pomocí kterého lze žádat po společnosti Google, aby se v jeho internetovém vyhledávači přestaly zobrazovat výsledky o osobě žadatele. Formulář představuje praktickou implementaci práva být zapomenut.

Zdroj: https://www.google.com/webmasters/tools/legal-removal-request?hl=cs&pid=0&complaint_type=14