POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra veřejného práva

Ochrana osobních údajů

Bakalářská práce

Personal data protection

Bachelor thesis

VEDOUCÍ PRÁCE

Mgr. Jiří Víšek, Ph. D.

AUTOR PRÁCE

Nikol Běželová

PRAHA

2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 28. 2. 2022

……..

Nikol Běželová

ANOTACE

Práce se zabývá aspekty ochrany osobních údajů v České republice i na mezinárodní úrovni. Vzhledem k častému úniku a zneužití dat je tato problematika stále aktuální. V práci je zohledněna historie, legislativní vývoj a současná právní úprava, která tuto problematiku upravuje. Práce obsahuje vysvětlení základních pojmů, které definuje nový zákon č. 110/2019 Sb., o zpracování osobních údajů. Jsou zde zmíněny i úkoly, pravomoci a činnost Úřadu pro ochranu osobních údajů. Závěrem se práce věnuje příkladům zneužití osobních údajů a způsobům, jak tyto osobní údaje ochránit.

KLÍČOVÁ SLOVA

Ochrana osobních údajů, Subjekt údajů, Osobní údaj, Nařízení Evropského parlamentu a Rady EU, Úřad pro ochranu osobních údajů, Zneužití osobních údajů

ANNOTATION

The thesis deals with aspects of personal data protection in the Czech Republic and internationally. Due to frequent data leakage and misuse, this issue is still very relevant. The thesis takes into account the history, legislative development and the current laws that regulates this issue. The thesis contains an explanation of the basic concepts defined by the new Act No. 110/2019 Coll., on the processing of personal data. There are also mentioned the tasks, powers and activities of the Office for Personal Data Protection. The conclusion is devoted to examples of misuse of personal data and how to protect this personal data.

KEYWORDS

Personal data protection, Data subject, Personal data, General Data Protection Regulation (GDPR), Office for Personal Data Protection, Misuse of personal data

OBSAH

ÚVOD

Ochrana osobních údajů je velmi diskutované téma, a proto je potřeba této problematice věnovat zvýšenou pozornost. Osobní údaje jsou součástí života každého člověka a doprovází ho od jeho narození až po smrt. Jedná se o jedinečné informace, které mohou jedince lehce identifikovat. Množství osobních údajů s přibývajícím věkem neúprosně narůstá, a s tím i potřeba osobní údaje chránit, aby nebyly zneužity. Osobní data jsou v dnešní době velmi cenné zboží, které může být lehko obchodovatelné po celém světě. Z tohoto důvodu vznikla legislativní úprava, která zaručí ochranu osobních dat před zneužitím nebo krádeží. V České republice se tato problematika začala více projednávat až na začátku 21. století.

Práce je systematicky členěna do šesti kapitol, které jsou dále uspořádány do jednotlivých podkapitol.

První kapitola práce je zaměřena na historický vývoj ochrany osobních údajů na mezinárodní úrovni a v České republice. Jsou zde například uvedeny zásadní rozdíly mezi starým zákonem č. 101/2000 Sb., o ochraně osobních údajů a novým zákonem, který jej nahradil, tedy zákonem č. 110/2019 Sb., o zpracování osobních údajů.

Druhá kapitola se věnuje implementaci 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. Zde je popsána věcná a místní působnost tohoto nařízení, dále jeho struktura, zásady a v neposlední řadě i cíle.

Další kapitola je zaměřená na legislativní úpravu ochrany osobních údajů v České republice. V této kapitole jsou blíže specifikovány předmět a působnost zákona č. 110/2019 Sb., o zpracování osobních údajů. Kapitola více obeznámí s nejzákladnějšími pojmy týkajícími se o ochrany osobních údajů a předá občanům informace o jejich určitých právech a povinnostech. Znalost zákona by se neměla podceňovat, jelikož za porušení povinností, které ukládá, hrozí významné sankce.

Čtvrtá kapitola se věnuje dozorovému úřadu, přesněji Úřadu pro ochranu osobních údajů, přičemž na začátku je vysvětleno, o jaký úřad se jedná, jaké má úkoly a pravomoci. V neposlední řadě jsou zde popsány sankce, které hrozí za případné porušení ochrany osobních údajů a výše jejich pokut.

Následně jsou popsány hlavní příčiny zneužití osobních údajů, jelikož tyto informace jsou zneužívány každý den. Jedná se především o lehkovážnost lidí, kteří si neuvědomují důsledky svého chování a nebezpečí zveřejňování osobních údajů. Lidé často souhlasí s použitím osobních údajů, aniž by věděli, jak s nimi bude dále naloženo. Proto jsou zde zmíněny zásady ochrany osobních údajů a případný postup, jak se zachovat při zneužití osobních údajů. V poslední kapitole jsou popsány soudní spory, které se týkaly porušení ochrany osobních údajů.

Cílem bakalářské práce je více objasnit problematiku ochrany osobních údajů v kontextu nového zákona č. 110/2019 Sb., o zpracování osobních údajů, a 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. Zároveň se v úvodních kapitolách bude snažit více přiblížit začátky legislativní úpravy ochrany osobních údajů, které tuto problematiku formulovaly. Jelikož aplikace zákona č. 110/2019 Sb., o zpracování osobních údajů, představuje zásah do každodenního zpracování osobních údajů, bude zde tato problematiku více vysvětlena i pro širší veřejnost.

1 HISTORIE OCHRANY OSOBNÍCH ÚDAJŮ

1.1 Vývoj ochrany osobních údajů na mezinárodní úrovni

Právo na soukromí původně vycházelo ze soukromoprávního pojetí „práva být nechán o samotě“. Toto pojetí popsal mezi prvními autor Thomas Cooley v roce 1888. Právo na soukromí, jako určitý jev, bylo poté souhrnně definováno v roce 1890 v článku S. D. Warrena a L. D. Brandeise „The Right of Privacy“. Autoři v něm vyvraceli myšlenku, že právo na soukromí vytvářejí jako zcela nové pojetí, ale tvrdili, že pouze více přibližují již existující právo, které bylo vytvořeno přirozeným vývojem základní zásady ochrany osoby v common law. Původně tato zásada ochraňovala jedince pouze před fyzickým poškozením, později se však natolik rozšířila, že chránila i pocity, povahu a intelekt jedince. Ochrana soukromí je tedy podle autorů pouze dalším bezprostředním a nezbytným krokem ve vývoji práva.[1]

Zanedlouho se toto teoretické pojetí začalo objevovat v právních řádech několika dalších států v Evropě i mimo ni. Do druhé světové války bylo ovšem toto právo chápáno stále v užším slova smyslu, a to jako již zmíněné „právo být nechán o samotě“. Chráněno bylo většinou dílčími právními předpisy a nepřikládala se mu taková váha jako dnes. První impulz změny vnímání práva na soukromí nastal v době praktik totalitních režimů, které přímo zasahovaly do lidského soukromí. Tyto zásahy vedly v době po druhé světové válce ke zdárnějšímu chápání role práva při ochraně soukromí. Počátek rozvoje byl pak zaznamenán v roce 1948 v podobě zakotvení práva na ochranu soukromí dle čl. 12 Všeobecné deklarace lidských práv. O dva roky později se stejné právo zakotvilo do článku 8 Úmluvy o ochraně lidských práv a základních svobod soudu pro lidská práva (dále jen „EÚLP“). Pro členské státy Rady Evropy je tato Úmluva zavazující a doposud formuje chápání soukromí a jeho ochranu národními úpravami v Evropě. [2]

Lidé se obecně začali více zajímat o ochranu osobních údajů s rozvojem výpočetní techniky. Mezi prvními se vzbouřila veřejnost v druhé polovině

[1] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str.56-57
[2] Tamtéž, str. 56-57

20. století v USA, poněvadž se zde zformuloval plán na vytvoření národního informačního centra, které bude obsahovat informace o občanech. Plán nakonec nebyl realizován kvůli odporu veřejnosti, ale toto téma vyvolalo zájem o otázky týkající se shromažďování osobních údajů. Tyto problémy nasměrovaly některé demokratické státy k tomu, aby akceptovaly zákony, které poskytovaly právní ochranu osobních údajů. Dalším důvodem pro zavedení legislativy byl masivní a rychlý rozvoj počítačové technologie.[3]

V roce 1968 se Evropská komise (dále jen „EK“) začala zabývat otázkami ochrany soukromí v kontextu s moderní technologií. Parlamentní zasedání Rady Evropy (dále jen „RE“) se rozhodlo provést šetření ochrany soukromí osob s ohledem na technologickou ochranu jednotlivců v členských státech.

Na začátku 70.let 20.století se začala výrazně měnit celá oblast lidských činností jako je získávání informací či uzavírání smluv. K těmto změnám došlo v důsledku vývoje nových technologií. Jelikož vývoj nových technologií představoval přírůstek nebezpečí zásahů do lidského soukromí, byla potřeba vytvořit regulaci, která by osoby před tímto nebezpečím přímo chránila. V roce 1980 byla vytvořena Směrnice Organizace pro hospodářskou spolupráci a rozvoj (dále jen „Směrnice OECD”), která sice měla chránit soukromí lidí, ale v tomto případě byla pouze doporučující. Prvoplánově měla Směrnice OECD sloužit jako návod pro vybudování legislativy na ochranu osobních údajů v zemích, které podobnou legislativou nedisponovaly. Tato směrnice jako první formulovala základní principy a mechanismy ochrany osobních údajů, jak jsou známy v dnešní době. Velké množství z nich lze také dohledat v 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 (dále jen „Nařízení GDPR“), kde jsou zapsány v neměnné podobě. Ve Směrnici OECD byly poprvé zformulovány zásadní pojmy týkající se ochrany osobních údajů, mezi které patří pojem osobní údaj, správce osobních údajů, nebo subjekt údajů. Dále zde byly určeny základní zásady ochrany osobních údajů, které jsou součástí čl. 5 Nařízení GDPR, a práva jedinců na jejich

[3] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str.57-58

zpracování osobních údajů, mezi která patří právo na informace o zpracování a právo podávat námitky proti zpracování. Tato směrnice měla celosvětový vliv na velké množství států, jelikož členy OECD nejsou jen evropské státy.[4]

1.1.1 Směrnice Evropského parlamentu a Rady 95/46/ES

Klíčový milník v ochraně osobních údajů přišel v roce 1995, kdy byla přijata 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 (dále jen „Směrnice Evropského parlamentu a Rady 95/46/ES“). Ta přináší regulaci ochrany osobních údajů na úrovni komunitárního práva. Tato směrnice logicky reagovala na vytvoření užších vztahů mezi unijními státy a utvoření vnitřního trhu pro volný pohyb zboží, který dále vede k volnému pohybu osobních údajů. Také odráží technologický posun v oblasti telekomunikačních sítí, které přenášení osobních údajů zjednodušily. Povýšením ochrany osobních údajů na závaznou úroveň v celé Evropské unii (dále jen ,,EU”) již existující překážky v toku osobních údajů, které byly vytvořeny jinou legislativou v každém členském státě, vymizely a dosavadní roztříštěnost statutu byla sjednocena, a to navzdory tomu, že tento statut má podobu směrnice, nikoli nařízení. Ochrana osobních údajů v legislativě jednotlivých členských států vychází zejména ze základních lidských práv. Tento krok vedoucí ke sjednocení, by měl vést ke zvýšené ochraně, stejně jako samotná směrnice, která vycházela z čl. 8 Listiny základních práv EU.[5]

Směrnice Evropského parlamentu a Rady 95/46/ES byla implementována do právního řádu České republiky (dále jen „ČR“) přijetím zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon o ochraně osobních údajů“). Tento zákon byl obecným zákonem na ochranu osobních údajů v ČR, jelikož z něj vycházející zvláštní pravidla pro zpracování osobních údajů lze

[4] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str.57-58
[5] Destination GDPR - how did we arrive here? . Object moved [online]. Copyright © [cit. 10.02.2022]. Dostupné z: https://sytorus.com/ie/Blog/Article/176?title=destination-gdpr-how-didwe-arrive-here

nalézt v několika konkrétních právních předpisech.[6] Začlenění této směrnice bylo jednou z podmínek pro vstup kandidátských zemí do EU. Nutno zmínit, že prvním právním předpisem o ochraně osobních údajů v ČR byla Vyhláška č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, která byla nahrazena výše uvedeným zákonem.

1.1.2 Směrnice 97/66/ES a 2002/58/ES

Po dvou letech vstoupila v platnost Směrnice 97/66/ES Evropského parlamentu a Rady z 15. prosince 1997 o zpracování osobních údajů a ochrany soukromí v sektoru telekomunikací, která nahradila po dvou letech účinnosti výše zmíněnou Směrnici Evropského parlamentu a Rady 95/46/ES. Nicméně, kvůli neustálému zrychlování obchodních a technologických inovací na přelomu milénia a prvních pár let 21. století, byla vyměněna za novou směrnici. Jedno z nejrychleji rostoucích odvětví bylo využívání elektronických médií k propagaci a prodeji produktů široké veřejnosti. Osobní e-mailové adresy a čísla mobilních telefonů se staly hlavní měnou při provádění marketingové a prodejní aktivity, kdy byla veřejnost pod neustálým tlakem spamu a nevyžádaných forem reklamy.[7]

Evropští zákonodárci zaznamenali tyto obtěžující aktivity jako impuls pro opětovnou regulaci úpravy ochrany soukromí a důvěrnosti osobních informací svých občanů. Tuto regulaci následně provedli v roce 2002 se zaměřením především na využívání osobních údajů pro cílené marketingové reklamy prostřednictvím elektronických médií. Byla tedy přijata Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.[8]

---

[6] MATES, Pavel a Karel NEUWIRT. Právní úprava ochrany osobních údajů v ČR: znění zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů: vybrané předpisy EUpoznámkové vydání se zapracovanou důvodovou zprávou. Praha: IFEC, 2000. AZ-IUS ISBN 80-86412-02-4. str. 113-116

[7] Destination GDPR - how did we arrive here? . Object moved [online]. Copyright © [cit. 10.02.2022]. Dostupné z: https://sytorus.com/ie/Blog/Article/176?title=destination-gdpr-how-didwe-arrive-here

[8] Tamtéž

1.2 Vývoj ochrany osobních údajů v České republice

Právo na ochranu osobních údajů vyplývá zejména z práva na soukromí, které bylo následně akceptováno jako samostatné právo. Potřeba ochrany osobních údajů se objevila v návaznosti na zneužívání osobních údajů během druhé světové války. Typickým příkladem bylo zneužití za účelem holocaustu, jelikož bylo možné v matričních knihách nalézt u narozených osob jejich náboženskou příslušnost. Navíc byly nalezeny záznamy ze sčítání obyvatel, které pocházely ze začátku 20. století a obsahovaly taktéž údaje o náboženství.[9]

Důležitějším milníkem v pokroku ochrany osobních údajů, který pochází z 60. let, je zlepšování a šíření technologií. Především proto, že výpočetní technika se dokáže zaměřit na nekonečné množství informací, které jsou poté uloženy a snadno zpřístupněny. Bylo tedy možné s informacemi rychle zacházet, sdružovat je s dalšími, a tím mohlo dojít k vytvoření ucelené představě o životě člověka nebo skupiny. Demonstrování těchto skutečností mohly zneužít například marketingové společnosti k cílenému prezentování svých produktů. Tyto informace by v rukou nesprávných osob či mocenských orgánů mohly výrazně ovlivnit i fungování systému v zemi.[10]

Z důvodu obav o ohrožení demokracie začaly západní státy v 70. letech přijímat zvláštní zákony o ochraně osobních údajů. Česká republika však tyto státy nenásledovala, jelikož zde byl vývoj ochrany osobních údajů od roku 1948 do roku 1989 zcela utiskován. Komunistický režim, který v té době vládl, nesouhlasil s tím, aby občané měli právo na ochranu soukromí. K ukotvení práva na soukromí a práva na ochranu před nekompetentním shromažďováním, zneužíváním nebo publikováním údajů o jednotlivci došlo až v čl. 10 Listiny základních práv a svobod (dále jen ,,LZPS") v roce 1991.[11]

V ČR se téma ochrany osobních údajů při jejich zpracování začalo řešit až se schválením zákona č. 56/1992 Sb., o ochraně osobních údajů v informačních

[9] MATES, Pavel, JANEČKOVÁ Eva, BARTÍK Václav. *Ochrana osobních údajů*. Praha: Leges, s.r.o., 2012, ISBN 978-80-87576-12-0. str. 71

[10] ŽŮREK, Jiří. *Praktický průvodce GDPR*: 2. aktualizované vydání. Olomouc: ANAG, 2018, ISBN 978-80-7554-152-9. str. 17

[11] NAVRÁTIL, Jiří a kol. *GDPR PRO PRAXI*. Plzeň: Aleš Čeněk, s.r.o., 2018, str.28 ISBN 978-80-7380-689-7. str. 29

systémech, který ovšem reguloval pouze na zpracování osobních údajů v informačních systémech (dále jen „zákon o ochraně osobních údajů v informačních systémech“). Zajímavostí je, že byl tento zákon přijat o pár měsíců dříve než LZSP, která v čl. 7 odst. 1 zaručuje integritu soukromí jedince a v čl. 10 odst. 3 všem právo na ochranu před neoprávněným sběrem informací. Bohužel se tento zákon nezabýval i zpracováním osobních údajů v papírové formě, kterých byla v 90. letech neustále většina. V zákoně o ochraně osobních údajů v informačních systémech také nikdy nebyly vybudovány dozorové orgány a chyběly účinné sankce za nedodržování stanovených povinností.[12] Neexistence takového orgánu patřila mezi zásadní důvody, proč se ČR nemohla do roku 2000 připojit k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. ledna 1981 (dále jen „Úmluva 108“), jelikož zákon o ochraně osobních údajů v informačních systémech nesplňoval její požadavky. Tento problém také postihl Ministerstvo zahraničí ČR a vybrané složky Ministerstva vnitra ČR, jelikož souhlas s Úmluvou 108 představovalo podmínku pro kooperaci v rámci Schengenského informačního systému.

Dne 4. dubna 2000 zákonodárce přinutily všechny tyto důvody ke schválení zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen zákon o ochraně osobních údajů“). Tímto zákonem byl současně i vybudován Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) jako dozorový úřad, který bude kontrolovat dodržování povinností, které vyplývají ze zákona při zpracování osobních údajů. „*Aby byly odstraněny pochybnosti, které vyvolávala stará úprava, stanovil nový zákon svou věcnou působnost na zpracování osobních údajů prováděné automatizovaně nebo jinak (např. manuálně)“*[13] Jelikož Česká republika musela splňovat určité podmínky v odvětví ochrany osobních údajů, aby mohla vstoupit do EU, byl v roce 2004 zásadněji upraven zákon o ochraně osobních údajů ve spojitosti s nutností transponovat Směrnici Evropského parlamentu a Rady 95/46/ES.

[12] MELOTÍKOVÁ, Petra. *Osobní údaje v kontextu GDPR*. Praha: Leges, s.r.o., 2020, ISBN 978-80-7502-507-4. str. 57
[13] Tamtéž, str. 58

Zákon o ochraně osobních údajů měl být se dnem účinnosti Nařízení GDPR zrušen, jelikož od 25. května 2018 upravuje náležitá práva a povinnosti Nařízení GDPR, na které přešlo hmotněprávní postavení zákona o ochraně osobních údajů.[14]

1.3 Nový zákon č. 110/2019 Sb., o zpracování osobních údajů a změny oproti dřívějšímu zákonu č. 101/2000 Sb., o ochraně osobních údajů

V České republice začal být dne 24. dubna 2019 platný a účinný nový zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „Adaptační zákon“), který více upřesňuje a dále reguluje podmínky zpracování osobních údajů v souladu s Nařízením GDPR. Nový zákon o ochraně osobních údajů zcela zrušil a nahradil dosavadní zákon o ochraně osobních údajů, který byl v určitých částech v rozporu s Nařízením GDPR. Adaptační zákon však nezpůsobil závratné změny, ale spíše upřesnil práva a povinnosti správců osobních údajů a upravil určité výjimky. Přijetím adaptačního zákona také došlo k upevnění pozice ÚOOÚ, který má nyní zřetelně určené pravomoci k vymáhání postihů za porušování pravidel, která stanovila legislativa v oblasti ochrany osobních údajů.[15]

Podle Nařízení GDPR je dítě kompetentní v souvislosti s nabídkou služeb informační společnosti udělit svůj souhlas, u kterého není zapotřebí udělení souhlasu zákonným zástupcem, dovršením 16 roku věku, každý členský stát tuto hranici však může snížit až na věk 13 let. Český zákonodárce určil věkovou hranici samostatného souhlasu dítěte v adaptačním zákoně v § 7 na 15 let. Tento souhlas zmocňuje správce zpracovávat osobní údaje v souvislosti s poskytováním a nabídkou služeb, které se týkají informačních technologií v nezbytném rozsahu. To vše však za použití podstatných ustanovení Nařízení GDPR.[16]

---

[14] ŽŮREK, Jiří. *Praktický průvodce GDPR*: 2. aktualizované vydání. Olomouc: ANAG, 2018, ISBN 978-80-7554-152-9. str. 18

[15] CHLEBUS, Tomáš. *Nový zákon o zpracování osobních údajů* [online]. [cit. 2.2.2022]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html

[16] JEŽEK, Mojmír. Nový český zákon o zpracování osobních údajů [online]. [cit. 2.2.2022]. Dostupné z: https://www.ecovislegal.cz/gdpr-a-ochrana-osobnich-udaju/novy-cesky-zakon-o-zpracovani-osobnich-udaju-2/

V čl. 37 odst. 1 písm. a) Nařízení GDPR je obecně stanovena povinnost veřejných subjektů, aby jmenovali pověřence pro ochranu osobních údajů, ale není zde zmíněna definice veřejného subjektu. *„Zákon o zpracování osobních údajů v § 14 stanoví, že veřejným subjektem je kromě orgánu veřejné moci také orgán zřízený zákonem, který plní zákonem stanovené úkoly ve veřejném zájmu.“*[17] V této oblasti tudíž došlo k vyjasnění pojmů diskutovaných už od přijetí Nařízení GDPR, a k upřesnění právní úpravy pro aplikaci Nařízení GDPR v české legislativě.

Adaptační zákon dále přináší nové skutkové podstaty přestupků, které spočívají v porušení povinností stanovených samotným Adaptačním zákonem, a vymezuje za ně rovněž sankce. Reaguje také na případy, ve kterých by došlo k porušení zákazu zveřejnění osobních údajů, které jsou stanoveny právním předpisem, který je součástí českého právního řádu. Při porušení tohoto zákazu lze podle adaptačního zákona udělit pokutu až do 1 000 000 Kč, nebo 5 000 000 Kč, bude-li se jednat o přestupek, který je spáchaný tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobným způsobem. Tuto odpovědnost nenesou orgány veřejné moci, u kterých ÚOOÚ upustí od udělení pokuty v případě, že takový přestupek vykoná.[18]

Dalším novým přínosem Adaptačního zákona je, že specifikuje zpracování osobních údajů na základě novinářské, akademické, umělecké nebo literární licence a posuzuje přiměřenosti takového zpracování. Při zpracování těchto osobních údajů je stanovena výjimka, týkající se poučovací a informační povinnosti správce, kdy postačí, aby subjekt údajů dostal informace o identitě správce pouze v grafické podobě, a to průkazem nebo označením, ústně, či jiným vhodným způsobem. Toto jednoduché ponaučení je však dostačující pouze v případě, kdy jsou zásady ochrany osobních údajů, které informují o právech subjektů údajů, uveřejněny na internetových stránkách správce.[19]

Ve spojitosti se zpracováním osobních údajů na základě výše vypsaných licencí došlo též k omezení práva subjektu údajů na podání námitky proti zpracování

[17] Zákon č. 110/2019 Sb., *o zpracování osobních údajů*, § 14
[18] Tamtéž, § 61
[19] JEŽEK, Mojmír. *Nový český zákon o zpracování osobních údajů* [online]. [cit. 2.2.2022]. Dostupné z: https://www.ecovislegal.cz/gdpr-a-ochrana-osobnich-udaju/novy-cesky-zakon-o-zpracovani-osobnich-udaju-2/

osobních údajů. V Nařízení GDPR je podání námitky a další zpracování podmíněno prokázáním jeho oprávněnosti ze strany správce, avšak Adaptační zákon stanovuje povinnost namítajícího subjektu údajů, aby uvedl konkrétní důvody neoprávněnosti zpracování. Správce pak pouze vyhodnotí, zda je vznesení námitky odůvodněné.[20]

[20] CHLEBUS, Tomáš. *Nový zákon o zpracování osobních údajů* [online]. [cit. 2.2.2022 Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html

2 GDPR

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze den 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) známé jako „GDPR" (General Data Protection Regulation) je v platnosti a účinnost nastává 25. května 2018 po dvouleté periodě určen k přípravě. Nahrazuje tak současný zákon č. 101/2000 Sb., o ochraně osobních údajů.[21] Nařízení GDPR bylo v roce 2016 publikováno ve Věstníku EU a jedná se o dosud nejucelenější soubor pravidel na ochranu osobních údajů na světě.

Vzhledem k masivnímu rozvoji nových technologií – internetové nabídky a služby, elektronické obchodování a používání sociálních sítí se mnohem více projevovalo, že EU musí na tento technologický rozvoj odpovídajícím způsobem reagovat. Lze tvrdit, že masivní digitální nárůst vystavuje vlastníky dat určitým rizikům, jelikož jeho používání s sebou nese obsáhlý sběr a zpracování osobních údajů. Současná globalizace způsobuje vyšší mobilitu a mezinárodní výměnu dat mezi institucemi a různými společnostmi. Zajištění bezpečnosti osobních údajů tak bude významnějším ukazatelem, především co se konkurence týče.

Nařízení GDPR je speciální v tom směru, že je závazné nejen pro všechny členské státy Evropské unie, ale také pro kohokoli, kdo má v úmyslu zpracovávat data jejich občanů. Je tedy nepodstatné, v jaké zemi se fyzicky zpracovávaná data nalézají, tedy kde jsou umístěny jednotlivé servery. Jelikož se jedná o nařízení EU, není potřeba jeho přímá implementace do právních řádů jednotlivých zemí Evropské unie. Z tohoto důvodů má GDPR formu unijního nařízení. Současně je tedy toto nařízení základem pro volný pohyb osobních údajů v rámci EU a určuje tak pravidla, za kterých k takovému pohybu osobních údajů může dojít.[22]

Účel vydání Nařízení GDPR je uveden v jeho čl. 1, který stanoví, že „*ustanovení čl. 8 odst. 1 Listiny základních práv Evropské unie a čl. 16 odst. 1 Smlouvy o fungování Evropské unie přiznávají každému právo na ochranu osobních údajů,*

[21] NEZMAR, Luděk. GDPR Praktický průvodce implementací Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 13
[22] NAVRÁTIL, Jiří a kol. *GDPR PRO PRAXI*. Plzeň: Aleš Čeněk, s.r.o., 2018, ISBN 978-80-7380-689-7. str. 29

které se jej týkají.“[23] Ačkoli bylo Nařízení GDPR vydáno právě formou nařízení, je třeba také zmínit, že je zde pro jednotlivé členské státy možnost se v určitých případech od něj odklonit a stanovit si speciální úpravu. Při splnění určitých podmínek, je možné dle čl. 23 Nařízení GDPR přijmout určité výjimky z některých jeho ustanovení. Mezi důvody přijetí Nařízení GDPR se řadila i snaha o odstranění nejednotnosti ochrany osobních údajů anebo redukce administrativní zátěže, kterou do té doby obstarávali správci osobních údajů a zpracovatelé. K redukci administrativní zátěže mělo dojít především prostřednictvím tzv. systému *One-Stop-Shop,* kdy se přeshraniční předávání osobních údajů mělo soustředit k jedinému dozorovému úřadu. Avšak během rozhodování o obsahu nařízení se rozhodlo ponechat tuto činnost i na ostatních vnitrostátních dozorových orgánech.[24]

2.1 Působnost Nařízení GDPR

Působnost Nařízení GDPR se dělí na dvě základní oblasti, a to na působnost věcnou a působnost místní.

Věcná působnost:

- automatizované zpracování osobních údajů,
- neautomatizované zpracování osobních údajů, které jsou zahrnuty v evidenci, nebo v ní mají být zahrnuty.

Věcná působnost se neaplikuje na zpracování osobních údajů uskutečňované:

- při výkonu činností, které nejsou zařazeny do oblasti působnosti práva Unie,
- členskými státy při výkonu činností, které se řadí do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU,
- fyzickou osobou během výhradně osobních či domácích činností,

[23] Nařízení GDPR, článek 1
[24] MELOTÍKOVÁ, Petra. *Osobní údaje v kontextu GDPR*. Praha: Leges, s.r.o., 2020, ISBN 978-80-7502-507-4. str. 60-61

- oprávněnými orgány za účelem prevence, šetření, odhalování, stíhání trestných činů či výkonu trestů, včetně obrany před hrozbami pro veřejnou bezpečnost.[25]

Místní působnost:

- zpracování osobních údajů ve vztahu s činnostmi provozovny správce nebo zpracovatele v EU, nehledě na to, zda zpracování osobních údajů se odehrává v EU nebo mimo ni,
- zpracování osobních údajů subjektů, nacházejících se v EU, správcem nebo zpracovatelem se sídlem mimo EU,
- zpracování osobních údajů správcem, který se nachází mimo EU ale na místě, kde je stále uplatňováno právo členského státu na základě mezinárodního práva veřejného.[26]

2.2 Struktura Nařízení GDPR

Nařízení GDPR se odlišuje od zákona zejména tím, že je složeno ze dvou částí. První část je nazvána Preambule a druhá část je normativní text, který určuje práva a povinnosti, jak je zvykem u formy zákona.

Preambule se skládá z tzv. recitálů, což jsou očíslované odstavce od 1 až 173, a jedná se o výklad normotvůrce. V Preambuli jsou vysvětleny důvody přijetí Nařízení GDPR a jsou zde popsány jednotlivé povinnosti, práva a nové instituty.

Ve druhé části Nařízení GDPR je formulován text, který určuje pravidla pro zpracování osobních údajů. Jedná se tedy o obdobný text jako v zákonu, s tím rozdílem, že je rozdělen na články (1 až 99), nikoli na paragrafy.

[25] NAVRÁTIL, Jiří a kol. *GDPR PRO PRAXI*. Plzeň: Aleš Čeněk, s.r.o., 2018, ISBN 978-80-7380-689-7. str. 32
[26] Tamtéž, str. 32

2.3 Právní předpisy

Ústavní základ ochrany osobních údajů

- Úmluva Rady Evropy č. 108 z roku 1981
- článek 8 Charty základních práv EU
- článek 16 Smlouvy o fungování Evropské unie
- článek 7, 10 odst. 3 a 13 Listiny základních práv a svobod

Obecné předpisy ochrany osobních údajů

- zákon č. 89/2012 Sb., občanský zákoník
- nařízení Evropského parlamentu a Rady 2016/679 (GDPR)
- zákon č. 110/2019 Sb., o zpracování osobních údajů

Dozor a správní trestání

- § 80b odst. 3 věta druhá a § 80c odst. 4 věta první zákona č. 273/2008 Sb., o Policii České republiky
- § 87 odst. 4 zákona č. 127/2005 Sb., o elektronických komunikacích
- § 16b a § 20 odst. 5 zákona č. 106/1999 Sb., o svobodném přístupu k informacím
- § 11 zákona č. 111/2009 Sb., o základních registrech
- §§ 16a – 16c zákona č. 328/1999 Sb., o občanských průkazech
- § 7 písm. f) zákona č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)
- § 34a odst. 4 a § 34c odst. 4 zákona č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o cestovních dokladech)
- § 17e odst. 6 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)
- § 25 odst. 2 zákona č. 159/2006 Sb., o střetu zájmů

- § 71a zákona č. 325/1999 Sb., o azylu

Procesní předpisy

- zákon č. 500/2004 Sb., správní řád
- zákon č. 150/2002 Sb., soudní řád správní
- zákon č. 141/1961 Sb., trestní řád
- zákon č. 255/2012 Sb., kontrolní řád
- zákon č. 99/1963 Sb., občanský soudní řád[27]

2.4 Cíle Nařízení GDPR

Mezi cíle Nařízení GDPR se řadí:

- adaptace právní regulace ochrany osobních údajů poměrům dnešní doby,
- unifikace práva ochrany osobních údajů v jednotlivých zemích Evropské unie a ostatních zemích, na které dopadá,
- upevnění práv v oblasti ochrany osobních údajů každé osoby, která je subjektem údajů, a docílit sjednoceného výkladu Nařízení GDPR dozorovými úřady jednotlivých zemí EU,
- upevnit důvěryhodnost EU a jejích členských zemí (to se vztahuje i na ostatní země, které pod Nařízení GDPR spadají) pro jiné země, které usilují o rozvoj obchodu s Evropskou unií a tím souvisejícím předáváním osobních údajů mezi zeměmi.[28]

[27] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Právní předpisy* [online]. [cit. 2.12.2021]. Dostupné z: https://www.uoou.cz/pravni-predpisy/ds-1257/p1=1257

[28] NAVRÁTIL, Jiří a kol. *GDPR PRO PRAXI*. Plzeň: Aleš Čeněk, s.r.o., 2018, ISBN 978-80-7380-689-7. str. 30

3 LEGISLATIVNÍ ÚPRAVA OCHRANY OSOBNÍCH ÚDAJŮ V ČESKÉ REPUBLICE

Legislativní ustanovení na ochranu osobních údajů v ČR dříve řešil především zákon o ochraně osobních údajů, který nahradil starší zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Spolu s novým občanským zákoníkem č. 89/2012 Sb., a jeho částí o soukromém právu. Občanský zákoník musí být vykládán konzistentním způsobem s LZSP, která říká, že každý má právo na integritu své osoby, právo chránit své soukromí, chránit soukromý a rodinný život, na ochranu před nekompetentním sbíráním, zveřejňováním nebo jiným zneužitím dat o své osobě a také právo na informace. Výše zmíněný zákon o ochraně osobních údajů byl zrušen ke dni 24. září 2019 a byl nahrazen Adaptačním zákonem. V důsledku těchto ustanovení se jeví legislativa ochrany osobních údajů jako velice komplikovaná. V této kapitole bude tedy přiblížen Adaptační zákon.

3.1 Předmět a působnost zákona

Zákon č. 110/2019 Sb., o zpracování osobních údajů, zapracovává náležité předpisy Evropské unie, kterými jsou *Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV*[29], a současně navazuje na přímo aplikovatelný předpis Evropské unie, zde se jedná o *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)*[30]. Není opomenuta ani úprava práv a povinností při zpracování osobních údajů, k uskutečnění práva každého na ochranu soukromí.

Zákon pracuje na realizaci práva každého na ochranu před neoprávněnými zásahy do ochrany osobních údajů, dále reguluje práva a povinnosti při

[29] Zákon č. 110/2019 Sb., *o zpracování osobních údajů*, § 2
[30] Tamtéž, § 4

zpracování osobních údajů a určuje podmínky, za kterých mohou být osobní údaje předány do jiných zemí. Vše je v souladu s předpisy Evropské unie a dalšími mezinárodními dohodami. Pro zajištění ochrany osobních údajů byl v neposlední řadě zřízen ÚOOÚ.

Do působnosti Adaptačního zákona spadá především zpracování osobních údajů dle Nařízení GDPR. Dále se jedná o zpracování osobních údajů odpovídajícími orgány za záměrem zamezování, vyhledávání nebo odkrývání trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, obstarávání bezpečnosti ČR nebo zabezpečování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Zákon působí také v oblasti zpracování osobních údajů při zabezpečování obranných a bezpečnostních zájmů České republiky a při zpracování osobních údajů, které se mají uchovat do evidence. Postavení a pravomoci Úřadu pro ochranu osobních údajů jsou upraveny taktéž v Adaptačním zákoně.[31]

3.2 Vymezení základních pojmů

3.2.1 Osobní údaj

Základní definice pojmu osobní údaj zmiňuje ustanovení Úmluvy Rady Evropy č. 108, která byla přijata dne 28. ledna 1981, které ho definuje takto: *„osobní údaje znamenají každou informaci týkající se identifikované nebo identifikovatelné fyzické osoby“*[32]*.* V českém právu je poté tento pojem vymezen v zákoně o ochraně osobních údajů, kdy osobním údajem se rozumí kterákoliv informace, pomocí které lze osobu přímo či nepřímo identifikovat, především na základě čísla, kódu nebo jednoho či více prvků, které jsou specifické pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.[33]

[31] Zákon č. 110/2019 Sb., *o zpracování osobních údajů*, § 51
[32] Úmluva 108, čl. 2
[33] Zákona č. 101/2000 Sb., *zákon o ochraně osobních údajů a o změně některých zákonů*, § 4

3.2.2 Anonymní údaj

Jedná se o informaci, kterou již ve svém původním tvaru, anebo po jejím zpracování nelze přiřadit k subjektu údajů. Již od počátku tento údaj nelze spojit s určitou osobou, a to ani při vynaložení rozumného úsilí (např. finančních prostředků). S pojmem anonymní údaj je spojený i další pojem, a to anonymizace. Jedná se o určité údaje, které se dříve daly přiřadit k identifikovatelné osobě, ale tuto identifikaci u nich již nelze uskutečnit.[34]

3.2.3 Zvláštní kategorie osobních údajů

Pro kategorii zvláštních osobních údajů se používá též označení citlivé údaje. Některé tyto osobní údaje by tak mohly svou povahou subjekt údajů samy o sobě poškodit v zaměstnání, ve škole či mohou způsobit jeho diskriminaci. Kvůli těmto příčinám je definována skupina údajů, které jsou označeny za citlivé, a při nakládání s nimi je brán zvýšený ohled na jejich ochranu. Větší opatrnost a ochrana se dávají najevo ve stanovených zvláštních právních předpisech, jejichž zásluhou je lze zpracovat.[35]

Dle zákona o ochraně osobních údajů se jedná o osobní údaje, které *"jsou vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů."*[36]

Citlivé osobní údaje lze zpracovávat jen z určitých titulů. Mezi tyto tituly se řadí zpracování, které je nezbytné pro ochranu životně důležitých zájmů subjektu údajů, v případě, že subjekt údajů je momentálně nezpůsobilý tento souhlas udělit,

[34] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, a.s., 2019, ISBN 978-80-7598-587-3. str. 137

[35] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Základní pojmy v GDPR [online]. [cit. 1.12.2021]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

[36] Zákon č. 101/2000 Sb., zákon o ochraně osobních údajů a o změně některých zákonů, § 4

zpracování údajů je přímo spojeno s osobními údaji, které již byly subjektem údajů zveřejněny, nebo udělení výslovného souhlasu subjektu údajů.[37]

3.2.4 Subjekt údajů

Hovoříme-li o subjektu údajů, jedná se o fyzickou osobu, které se osobní údaje přímo týkají. Subjektem údajů je míněna pouze již zmíněná fyzická osoba, nikoli právnická osoba, jelikož údaje spojované s právnickými osobami nejsou osobní údaje. Osobní údaje mohou být vztahovány pouze na fyzickou žijící osobu, poněvadž dle Nařízení GDPR je vyloučena působnost na údaje o zesnulých osobách. Člověk, který je subjektem údajů, má právo na vymáhání ochrany osobních údajů, zákon to však neukládá jako jeho povinnost [38]

3.2.5 Práva subjektu údajů

Nařízení GDPR přisuzuje subjektům údajů určitá práva. Jejich cílem je vyrovnat vztah mezi správcem a subjektem údajů. Práva subjektu údajů jsou stěžejním pilířem modelu ochrany osobních údajů v evropském prostředí. Důležité je zmínit, že Nařízení GDPR dává větší sílu právům subjektů, oproti zákonu o ochraně osobních údajů. Jedná se jak o aktualizaci současných práv, tak o vytvoření práv nových, jako je např. právo na přenositelnost. Právo na přenositelnost je právo subjektu údajů získat od správce své osobní údaje, které mu poskytl a předat je jinému správci.[39]

Subjekt údajů má především právo na informování o zpracování svých osobních údajů při shromažďování osobních informací. Jedná se tedy o právo na konkrétní informace o zprocesování jeho osobních údajů tak, aby byla naplněna zásada srozumitelnosti zpracování. Musí být poskytnuty informace záměru zpracování, totožnosti správce, o jeho příslušných zájmech, o příjemcích osobních informací. Zde se jedná o pasivní právo, jelikož subjekt údajů musí vůči správci vyvinout

[37] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, a.s., 2019, ISBN 978-80-7598-587-3. str. 124

[38] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Základní pojmy v GDPR* [online]. [cit. 1.12.2021]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

[39] Nařízení GDPR, článek 20 odstavec 1

vlastní iniciativu, aby mu požadované informace zpřístupnil. Nařízení GDPR formálně rozděluje poskytování informací na dvě skupiny, a to na informace o osobních údajích, které byly poskytnuty přímo subjektem údajů a ty, které nebyly získány od subjektu údajů.[40]

Pokud byly osobní údaje získány od subjektu údajů, musí správce poskytnout určité informace, mezi které spadá např.:

- identita a kontaktní údaje správce, případně jeho pověřeného zástupce,
- účely zpracování, pro které jsou osobní údaje shromažďovány,
- eventuální záměr správce předat osobní informace do třetí země,
- období, po které budou osobní údaje uchovány,
- existence práva podat stížnost u dozorového úřadu,
- eventualita odvolat souhlas.

Do druhé kategorie spadají osobní údaje, které nebyly poskytnuty od subjektu údajů. V případě, že osobní informace nejsou získány od subjektu údajů, musí správce na žádost poskytnout tyto informace:

- identita a kontaktní údaje správce, případně jeho pověřeného zástupce,
- účely zpracování, pro které jsou osobní údaje shromažďovány,
- původ, odkud osobní údaje pochází, eventuálně informace, zda pramení z veřejných zdrojů,
- druh dotčených osobních údajů.[41]

Převážné množství informací musí správce poskytnout, ať už se jedná o získání osobních údajů od subjektu údajů, či nikoli.

3.2.6 Správce osobních údajů

Další významnou osobou figurující v rámci ochrany osobních údajů je tzv. správce. Dle definice Nařízení GDPR, je správcem "*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně*

[40] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Základní pojmy v GDPR [online]. [cit. 1.12.2021]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx
[41] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Práva subjektu údajů* [online]. [cit. 9.1.2022]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

s jinými určuje účely a prostředky zpracování osobních 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"[42]

Správce je zodpovědný za dodržování zásad, zpracování, zachování povinností upravených nařízením a za zabezpečení osobních údajů. Správce musí plnit určité množství povinností, ke kterým musí být způsobilý. Mezi důležité povinnosti správce patří:

- aplikace cílené a standartní ochrany osobních údajů,
- jmenování pověřených osob pro ochranu osobních údajů,
- recenzování vlivu na ochranu osobních údajů a vykonávání předchozí konzultace,
- oznamovat ÚOOÚ případy porušení zabezpečení osobních údajů a informovat fyzické osoby o případech porušení zabezpečení osobních údajů subjektu osobních údajů,
- v neposlední řadě vést záznamy. [43]

3.2.7 Zpracovatel osobních údajů

V neposlední řadě je klíčovou osobou v oblasti ochrany osobních údajů tzv. zpracovatel osobních údajů. Zpracovatel, stejně jako správce, může být zastoupen jak fyzickou, tak právnickou osobou. Zpracovatel je subjekt, který je najímán správcem, aby pro něj vykonával zpracovatelské operace, týkající se osobních údajů. To znamená, že zpracovatel zpracovává osobní údaje pro správce. Zpracovatel se liší od správce především tím, že zpracovatel může vykonávat pouze zpracovatelské činnosti, kterými byl od správce pověřen, nebo vyplývají z jeho pověřené činnosti. Důležité je zmínit, že zpracovatel má přístup pouze k těm osobním údajům, které mu správce poskytl.[44]

[42] Nařízení GDPR, článek 4 odstavec 7
[43] ŠKORNIČKOVÁ, Eva. *Správce osobních údajů* [online]. [cit. 1.12.2021]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/spravce-osobnich-udaju/
[44] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 32

3.2.8 Příjemce osobních údajů

Příjemcem osobních údajů se rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoliv.“*[45] Za příjemce se ovšem nepovažují orgány veřejné moci, které mohou nabývat osobní údaje v rámci zvláštního šetření, které je v souladu s právem členského státu. Tyto orgány mohou zpracovávat určité osobní údaje pouze v souladu s použitelnými pravidly ochrany údajů pro vybrané zpracovatelské účely. Jako příjemce může také figurovat i tzv. třetí strana.

3.2.9 Třetí strana

Třetí strana je definována v čl. 4 odstavce 9 Nařízení GDPR jako *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jenž je oprávněna ke zpracování osobních údajů.“*[46]

3.2.10 Pověřenec

Funkce pověřence je definována v Nařízení GDPR a je důležité jí věnovat dostatečnou pozornost. Všichni správci osobních údajů si nemusí určit pověřence, ale Nařízení GDPR přímo vymezuje, v jakých případech musí být tato pozice obsazena. V právních řádech několika členských zemí EU se funkce pověřence vyskytla již před pár lety (např. Maďarsko, Francie, Polsko). Funkce pověřence spadá mezi řadové zaměstnance subjektu, to znamená, že pověřence musí jmenovat buďto správce, nebo zpracovatel. Pověřenec musí v mezích organizace zpracovatele osobních údajů vystupovat jako nezávislý subjekt a současně nesmí být ve střetu zájmů. Zároveň by mu správce neměl zadávat žádné pokyny. Dle Nešpůrka, Šuchmana a Jaroše: *„V praxi je již nyní běžné, že organizace mají v rámci své vnitřní struktury určené osoby, které dohlíží na zákonnost zpracování osobních údajů a poskytují rady a pokyny ostatním subjektům v rámci této*

[45] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR, a.s., 2019, ISBN 978-80-7598-587-3. str. 144

[46] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 32

organizace. Pověřenec má však zcela specifické postavení, jelikož není vázán pokyny správce či zpracovatele, ani nehledí na zájem organizace. V určitých případech dokonce proti zájmu správce či zpracovatele upozorňuje na porušování nařízení".[47]

3.2.10.1 Jmenování pověřence

Pověřenec pro ochranu osobních údajů musí být ustanoven do funkce podle svých profesních kvalit, především na základě svých odborných znalostí práva a praxe v oboru ochrany osobních údajů a svých schopností plnit úkoly vymezené v čl. 39 Nařízení GDPR. Správce nebo zpracovatel musí zpřístupnit kontaktní údaje pověřence pro ochranu osobních údajů a předat je dozorovému úřadu.

Správce nebo zpracovatel musí jmenovat pověřence v případech kdy:

- zpracování osobních údajů realizuje orgán veřejné moci či veřejný subjekt, kromě soudů, které jednají v rámci svých soudních jurisdikcí,
- nejvýznamnější činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli svému charakteru, svému rozsahu nebo svým záměrům vyžadují obsáhlé pravidelné a systematické monitorování subjektů údajů,
- nejvýznamnější činnosti správce nebo zpracovatele spočívají v objemném zpracování zvláštních kategorií údajů, které jsou uvedené v čl. 9 Nařízení GDPR nebo osobních údajů, které se vztahují k rozsudkům v trestních věcech dle čl. 10 Nařízení GDPR. [48]

Povinnost jmenovat pověřence pro ochranu osobních údajů dle čl. 37 odst. 1 písm. a) Nařízení GDPR nemusí splňovat příspěvkové organizace nebo jiné pomocné instituty (školní knihovny, správní služby nebo muzea), fakticky se jedná např. o Národní knihovnu zřizovanou Ministerstvem kultury, rovněž i o obchodní společnosti, které jsou ve vlastnictví státu, jelikož se jedná ze zákona o povinné subjekty o svobodném přístupu k informací. Orgány veřejné moci nebo veřejné subjekty jsou ty orgány, o kterých to určí vnitřní právní předpis konkrétního

[47] NEŠPŮREK, Robert, ŠUCHMAN, Jaroslav, JAROŠ, Ján. GDPR: nastane s nástupem nové regulace nedostatek pověřenců? *EU právní noviny,* 1/2018, str. 4
[48] Nařízení GDPR, článek 37 odstaven 1

členského státu. Mezi orgány veřejné moci se tak řadí např. i obec, a z tohoto důvodu musí všechny obce v České republice určit své pověřence. Další, kdo musí mít určeného pověřence, jsou tzv. instituce rozhodující o právech a povinnostech osob, což jsou např. školy.[49]

Správce nebo zpracovatel mají samozřejmě možnost, jmenovat svého pověřence i v případě, že jim to Nařízení GDPR přímo nenařizuje. V takovém případě platí stejné podmínky jako při povinném určování pověřence, a to především, že pověřenec musí být nezávislý, nesmí být ve střetu zájmů a musí mít přístup k nejvyššímu vedení. Výhoda dobrovolného jmenování svěřence tedy spočívá v tom, že v organizaci figuruje osoba, která pozoruje zpracování osobních údajů a kontroluje případný nesoulad. Pokud se jedná o organizaci, které není ze zákona uloženo určení pověřence a ani si nepřeje ho jmenovat, může namísto pověřence zaměstnat pracovníka nebo externího poradce, který bude vykonávat úkoly spojené s ochranou osobních údajů. V tomto případě je nutné vyřešit všechny nejasnosti ohledně jejich funkce, úkolů a postavení. Je nezbytné jasně uvést, že funkce této fyzické osoby nezastává pozici pověřence pro ochranu osobních údajů.[50]

Více správců a zpracovatelů může jmenovat jednoho společného pověřence, to vše za předpokladů, že organizace, ve kterých bude pověřenec svou funkci vykonávat spolu konkrétním způsobem souvisí. Tato možnost je uvedena v čl. 37 odst. 2 Nařízení GDPR, kde je stanoveno, že společný pověřenec musí být lehce dosažitelný z každého podniku. Při jmenování jednoho pověřence pro více subjektů, je potřeba brát na vědomí, aby pověřenec mohl vykonávat jednotlivé úkoly pro tyto subjekty.[51]

[49] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Základní příručka k ochraně údajů [online]. [cit. 18.2.2022]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-ochrane-udaju/ds-4744/p1=4744

[50] NEŠPŮREK, Robert, ŠUCHMAN, Jaroslav, JAROŠ, Ján. GDPR: nastane s nástupem nové regulace nedostatek pověřenců? *EU právní noviny,* 1/2018, str. 5

[51] Tamtéž, str. 5

3.2.10.2 Postavení pověřence

Správce a zpracovatel jsou povinni, dle čl. 38 Nařízení GDPR, pověřence patřičně a včas zapojit do všech záležitostí, které souvisí s ochranou osobních údajů. Pověřenec musí být přítomen na schůzkách vedoucích pracovníků a středního managementu, které se týkají přijímání rozhodnutí o osobních údajích. Správce a zpracovatel napomáhají pověřenci s poskytnutím zdrojů, které jsou nezbytné pro jeho práci a plnění úkolů dle čl. 39 Nařízení GDPR. Subjekty údajů mohou své dotazy, které souvisí se zpracováním jejich osobních údajů, směřovat na pověřence. Správce a zpracovatel garantují, aby pověřenec pro ochranu osobních údajů neobdržel žádné instrukce, které se týkají výkonu jeho úkolů.[52]

3.2.10.3 Úkoly pověřence

Pověřenec má několik stanovených úkolů, které musí vykonávat, a není možné, aby mu správce nebo zpracovatel určité úkoly nařizovali. Práva a povinnosti, které plynou z Nařízení GDPR, ovšem musí plnit správce a zpracovatel, nikoli pověřenec, ten má pouze kontrolní funkci. Pověřenec nesmí být ve spojitosti se svojí kontrolou nijak sankcionován nebo mu nesmí být dána výpověď. Avšak i pověřence se týká zákoník práce, a proto může být sankcionován nebo propuštěn z důvodů, které se netýkají jeho kontrolní činnosti.

Pověřenec má povinnost dodržovat mlčenlivost o veškerých informacích, které zjistil při výkonu své funkce. Jelikož při výkonu své práce má pověřenec poskytovat informace a rady správci nebo zpracovateli, musí znát evropské i národní právní předpisy a musí znát jejich aplikaci.[53]

Mezi hlavní úkoly pověřence pro ochranu osobních údajů patří:

- poskytovat informace a rady správcům nebo zpracovatelům, kteří realizují zpracování, pokud se jedná o jejich povinnosti podle tohoto nařízení a dalších předpisů EU nebo členských států ve sféře ochrany údajů,

[52] MELOTÍKOVÁ, Petra. *Osobní údaje v kontextu GDPR*. Praha: Leges, s.r.o., 2020, ISBN 978-80-7502-507-4. str. 76
[53] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Základní příručka k ochraně údajů [online]. [cit. 18.2.2022]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-ochrane-udaju/ds-4744/p1=4744

- sledovat dodržování Nařízení GDPR, dalších předpisů EU nebo členských států ve sféře ochrany údajů a konceptu správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozvržení povinností, zvyšování povědomí a školení zaměstnanců zapojených do operací zpracování a souvisejících auditů,
- poskytovat na vyžádání poradenství ohledně posouzení dopadu na ochranu osobních údajů a sledovat jejich uplatňování v souladu s čl. 35 Nařízení GDPR,
- spolupráce s dozorovým úřadem,
- působit jako kontaktní místo dozorového úřadu v záležitostech týkajících se zpracování, včetně předchozích konzultací podle čl. 36 Nařízení GDPR a případně vést konzultace o jakýchkoli jiných záležitostech.[54]

3.3 Zpracování osobních údajů

Mezi klíčové pojmy v oblasti ochrany osobních údajů patří i jejich zpracování, které je definováno jako *„operace nebo soubor operací osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“*[55] Nutno zmínit, že pojem zpracování osobních údajů má stále stejný význam a nebyl dřívějšími úpravami dle Nařízení GDPR nijak pozměněn.

3.3.1 Souhlas se zpracováním osobních údajů

Jedním z právních titulů pro zpracování osobních údajů je souhlas subjektu. Tento souhlas je definován v čl. 4 odst. 11 Nařízení GDPR jako „*projev vůle, který je svobodný, konkrétní, informovaný a jednoznačný a subjekt jím musí dát prohlášením nebo zjevným potvrzením najevo svolení ke zpracování svých*

[54] MELOTÍKOVÁ, Petra. *Osobní údaje v kontextu GDPR*. Praha: Leges, s.r.o., 2020, ISBN 978-80-7502-507-4. str. 77
[55] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 31

osobních údajů.“ [56] V Nařízení GDPR je však uváděno, že aby byl souhlas platný, musí být udělen prohlášením či evidentním potvrzením. Musí se tedy jednat o aktivní učinění souhlasu, to znamená, že za udělení souhlasu se již nebude brát zřetel na nečinnost subjektu jakožto udělení souhlasu, případně předvyplněné zaškrtávací pole, které subjekt údajů svépomoci nevymaže. Také v oblasti získávání a zpracování cookies bylo nutné provést změny, pokud jsou zprostředkovateli zpracovány osobní údaje. Zde je potřeba udělení aktivního souhlasu při používání webových stránek.

[56] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str. 93

4 DOZOROVÝ ÚŘAD A JEHO ČINNOST

Zřízení neboli existence dozorových úřadů, které dohlížejí a vymáhají zachování právních podmínek pro zpracování osobních údajů a ochranu práv vybraných osob, patří mezi jeden ze zásadních pilířů ochrany osobních údajů. Zřízení dozorových úřadů byl také jeden z požadavků Směrnice Evropského parlamentu a Rady 95/46/ES, jelikož dřívější zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech tuto podmínku neukládal. V dodatkovém protokolu k Úmluvě 108 byl proto přijat závazek, jenž ukládal povinnost při tvorbě nového zákona o ochraně osobních údajů, aby byl zřízen i dozorový orgán, který by zastával funkce, jež vyžadují výše zmíněné normy.[57]

Primární úkol pro každý dozorový úřad je sledování uplatňování Nařízení GDPR se záměrem chránit základní práva a svobody fyzických osob ve spojitosti se zpracováním jejich osobních údajů. Jednotlivý dozorový úřad je obecně příslušný k vykonávání úkolů dle Nařízení GDPR na vymezeném území svého státu.[58]

4.1 Úřad pro ochranu osobních údajů

V České republice se stal dozorovým orgánem Úřad pro ochranu osobních údajů, a to v podstatě pro veškeré zpracování osobních údajů. ÚOOÚ vznikl v roce 2000 na základě zákona č.101/2000 Sb., o ochraně osobních údajů, a jeho činnost je vymezena dle zákona č. 110/2019 Sb., o zpracování osobních údajů. Sídlo úřadu bylo vybudováno v Praze. ÚOOÚ je ústřední správní úřad, který je nezávislý a není podřízený vládě ani jejím nařízením či závazným pokynům. Při výkonu svého působení se ÚOOÚ řídí pouze právními předpisy a určitými předpisy Evropské unie, z toho vyplývá, že do jeho činnosti lze zasahovat pouze na základě zákona. Nezávislost ÚOOU je také zaručena tím, že jeho činnost je hrazena ze státního rozpočtu České republiky.[59]

---

[57] ŽŮREK, Jiří. *Praktický průvodce GDPR*: 2. aktualizované vydání. Olomouc: ANAG, 2018, ISBN 978-80-7554-152-9. str. 173

[58] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str. 405

[59] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 43

Z hlediska Evropy se jedná o relativně silný dozorový úřad s odpovídajícími pravomocemi. Hlavní obavy jsou převážně o jeho nezávislém postavení, jelikož nezávislost dozorového úřadu je jeho hlavním předpokladem, především při realizaci úkolů a výkonů kompetencí dle Nařízení GDPR.[60]

Požadavek nezávislosti postavení dozorových úřadu je přímo stanoven v čl. 51 Nařízení GDPR.

„1. Každý členský stát stanoví, že jeden nebo více nezávislých orgánů veřejné moci jsou pověřeny monitorováním uplatňování tohoto nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie (dále jen „dozorový úřad“).

2. Každý dozorový úřad přispívá k jednotnému uplatňování tohoto nařízení v celé Unii. Dozorové úřady za tímto účelem spolupracují mezi sebou a s Komisí v souladu s kapitolou VII.

3. Pokud je v některém členském státě zřízen více než jeden dozorový úřad, určí tento členský stát dozorový úřad, jenž má tyto úřady zastupovat ve sboru, a stanoví mechanismus, který zajistí, že budou ostatní dozorové úřady dodržovat pravidla týkající se mechanismu jednotnosti uvedeného v článku 63.“[61]

4.1.1 Úkoly dozorového úřadu

Každý dozorový úřad na svém území musí plnit určité úkoly, které jsou specifikovány v čl. 57 odst. 1 Nařízení GDPR. Vykonávání úkolů dozorového úřadu je pro osoby, jíž se osobní údaje týkají, a pověřence bezplatné. Jedná se spíše o obecné prohlášení, jelikož při zpoplatnění těchto úkolů by se jednalo o velmi mimořádnou situaci. Pokud by se však jednalo vůči dozorovému úřadu o očividně bezdůvodné a neadekvátní požadavky, z důvodu opakování se, je zde

[60] ŽŮREK, Jiří. *Praktický průvodce GDPR*: 2. aktualizované vydání. Olomouc: ANAG, 2018, ISBN 978-80-7554-152-9. str. 173
[61] Nařízení GDPR, článek 51

možnost uložení patřičného poplatku nebo odmítnutí žádosti vyhovět. Dozorový úřad však musí prokázat nedůvodnost nebo neadekvátnost odmítnuté žádosti.[62]

Jednotlivý úřad na svém území:

- *„monitoruje a vymáhá uplatňování Nařízení GDPR,*
- *zvyšuje povědomí veřejnosti o zpracování osobních údajů, jeho rizicích a podmínkách a podporuje porozumění těmto otázkám (zvláštní pozornost se má navíc věnovat dětem),*
- *poskytuje poradenství státním orgánům a institucím ohledně legislativních a správních opatření týkajících se ochrany práv a svobod fyzických osob v souvislosti se zpracováním,*
- *podporuje povědomí správců a zpracovatelů o jejich povinnostech,*
- *poskytuje na požádání subjektu údajů informace ohledně výkonu jeho práv,*
- *zabývá se stížnostmi a vhodným způsobem je prošetřuje a informuje stěžovatele o vývoji a následku,*
- *spolupracuje s ostatními dozorovými úřady za účelem oblasti informačních a komunikačních technologií a obchodních praktik,*
- *přijímá standartní smluvní doložky pro úpravu vztahu mezi správcem a zpracovatelem (čl. 28 odst. 8* Nařízení GDPR*) a standartní smluvní doložky pro předávání osobních údajů do třetích zemí (čl. 46 odst. 2 písm. d) Nařízení GDPR,*
- *připravuje a uchovává seznam zpracování, u nichž je požadavek provádět posouzení vlivu na ochranu osobních údajů,*
- *poskytuje poradenství v rámci předchozích konzultací,*
- *podporuje vydávání kodexů chování, vydává stanoviska a schvaluje kodexy chování,*
- *vybízí k zavedení mechanismů pro vydávání osvědčení o ochraně údajů, pečetí a známek a schvaluje kritéria pro vydávání osvědčení,*
- *navrhuje a zveřejňuje kritéria pro schvalování subjektu pro monitorování kodexů chování a subjektu pro vydávání osvědčení,*

[62] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str. 406

- *schvaluje subjekty pro monitorování kodexů chování a subjekty pro vydávání osvědčení,*
- *schvaluje smluvní doložky podle čl. 46 odst. 3 Nařízení GDPR, které jsou využity jako vhodná záruka pro předávání osobních údajů do třetí země,*
- *schvaluje závazná vnitropodniková pravidla podle čl. 47 Nařízení GDPR,*
- *přispívá k činnostem Sboru,*
- *vede interní záznamy o porušení Nařízení GDPR a o přijatých nápravných pravomocích,*
- *plní veškeré další úkoly související s ochranou osobních údajů.“*[63]

4.2 Pravomoci dozorového úřadu

K realizaci stanovených úkolů mají všechny dozorové úřady kompetence, které lze rozřadit do tří skupin: vyšetřovací, nápravná, povolovací a poradní. Dozorové úřady však nemají příslušnost k dozoru nad operacemi zpracování, které vykonávají soudy jednající v rámci svých soudních kompetencí.[64]

4.2.1 Vyšetřovací pravomoci

ÚOOÚ se při vyšetřovacích pravomocích, z hlediska procesního práva, řídí především zákonem č. 255/2012 Sb., o kontrole (kontrolní řád), a zákonem č. 500/2004 Sb., správní řád. Výchozími pravomocemi každého dozorového úřadu jsou vyšetřovací pravomoce, které se zakládají na možnostech:

- přikázat správci a zpracovateli, aby doložili veškeré informace, které jsou zapotřebí k vykonání jeho úkolů,
- vykonávat vyšetřování formou auditů ochrany údajů,
- realizovat přezkum vyhotovených osvědčení,
- oznámit správci nebo zpracovateli údajné nedodržení Nařízení GDPR,
- obdržet od správce a zpracovatele přístup k veškerým osobním informacím, které jsou zapotřebí k uskutečnění svých úkolů,

[63] ŽŮREK, Jiří. *Praktický průvodce GDPR*: 2. aktualizované vydání. Olomouc: ANAG, 2018, ISBN 978-80-7554-152-9. str. 174
[64] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 44

- obdržet přístup do veškerých prostorů, v nichž správce a zpracovatel pobývají, včetně veškerého vybavení, se kterým se zachází při zpracování osobních údajů.[65]

Podstatnou vyšetřovacích pravomocí je možnost uskutečňovat vyšetřování pomocí již zmíněných auditů, což znamená vyšetřování pomocí kontroly. Tato kontrola je také procesně regulována v kontrolním řádu a kontrolující orgán stanovuje, jak sledovaná osoba provádí povinnosti, které jí plynou z dalších právních předpisů nebo jí byly na základě těchto předpisů nařízeny.[66]

4.2.2 Nápravné pravomoci

ÚOOÚ se při nápravných pravomocích, z hlediska procesního práva, řídí především správním řádem, především postupem vydávání správních rozhodnutí, a dále také zákonem č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. Pro zajímavost lze zmínit, že pokuta se řadí mezi jedno z nápravných opatření. Nápravné pravomoci slouží jako prevence, ale i jako náprava.

Jednotlivé dozorové úřady mají všechny tyto nápravné kompetence:

- varovat správce či zpracovatele, že plánované operace zpracování nejspíše porušují Nařízení GDPR,
- udělit výtku správci či zpracovateli, jehož operace zpracování nedodržely zásady Nařízení GDPR,
- přikázat správci nebo zpracovateli, aby vyřídili žádost subjektu údajů o výkonu jeho práv,
- uložit správci či zpracovateli, aby uvedl operace zpracování do souladu s Nařízením GDPR, a to předem stanoveným způsobem a v dané lhůtě,
- přikázat správci, aby subjektu údajů sdělil případy porušení zabezpečení osobních údajů,
- nařídit prozatímní nebo trvalé omezení zpracování, včetně jeho zákazu,

[65] Nařízení GDPR, článek 58
[66] ŽŮREK, Jiří. *Praktický průvodce GDPR*: 2. aktualizované vydání. Olomouc: ANAG, 2018, ISBN 978-80-7554-152-9. str. 175-176

- přikázat opravu či výmaz osobních údajů nebo omezení zpracování a ohlašování takových opatření příjemcům, jimž byly osobní údaje odtajněny,
- odejmout osvědčení nebo přikázat, aby jej subjekt pro vydávání osvědčení odebral nebo aby jej nevydal, pokud nejsou požadavky na osvědčení plněny, nebo již přestaly být plněny,
- udělit správní pokutu podle čl. 83 Nařízení GDPR vedle či namísto nápravných opatření, podle faktorů každého jednotlivého případu. [67]

4.2.3 Povolovací a poradní pravomoci

Povolovací a poradní pravomoci lze členit do dvou skupin.

První skupinu vytvářejí kompetence, jež se vztahují k novým institutům, které Nařízení GDPR uplatňují. Jedná se o kompetenci umožnit poradenství správci, ve vztahu k předešlé konzultaci podle čl. 36 Nařízení GDPR, a schvalovat zpracování uskutečňované za účelem splnění úkolu ve veřejném zájmu.

Do druhé skupiny spadají kompetence vztahující se ke svěřování osobních údajů do tzv. třetích zemí, tedy do zemí mimo EU. Mezi kompetence dozorového úřadu se řadí přijímání standartních doložek o ochraně osobních údajů, povolování smluvních doložek, schvalování správních úmluv, které se týkají předávání osobních údajů mezi orgány veřejné moci nebo veřejnými subjekty a ratifikování obligatorních podnikových pravidel.[68]

Do jednotlivých povolovacích a poradních pravomocí se řadí:

- umožňovat poradenství správci při předchozí poradě dle čl. 36 Nařízení GDPR,
- z vlastní iniciativy nebo na požádání vyhlašovat stanoviska určená vnitrostátnímu parlamentu, vládě členského státu nebo i veřejnosti, ohledně veškerých otázek týkajících se ochrany osobních údajů,

[67] Nařízení GDPR, článek 58
[68] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str. 426

- schvalovat zpracování uvedené v čl. 36 odst. 5 Nařízení GDPR, jestliže právo členského státu takové předešlé povolení vyžaduje,
- uveřejňovat stanoviska a ratifikovat kodexy chování,
- pověřovat subjekty pro vyhotovování osvědčení,
- vydávat osvědčení a povolovat kritéria pro vydávání osvědčení (ÚOOÚ bude pouze schvalovat kritéria pro vydávání osvědčení ale osvědčení jako takové budou vydávat k tomu příslušné subjekty),
- akceptovat běžné smluvní doložky pro úpravu vztahu mezi správcem a zpracovatelem a běžné doložky pro předávání do zemí mimo EU,
- schvalovat smluvní doložky podle čl. 46 odst. 3 písm. a) Nařízení GDPR,
- schvalovat správní dohody podle čl. 46 odst. 3 písm. b) Nařízení GDPR,
- povolovat obligatorní vnitropodniková pravidla dle čl. 47 Nařízení GDPR.[69]

Pokud se bude poskytovat poradenství či konzultace v mezích institutu předešlé konzultace podle čl. 36 Nařízení GDPR, bude se jednat o nezávazné poradenství a nepůjde o formu zvláštního procesního úkonu (správního rozhodnutí).[70]

4.3 Sankce

V každé právní normě bývá zpravidla zakotvena i sankční část, která funguje jako preventivní a donucující účinek na příjemce právní normy. To znamená, že cílem hrozby postihu je přimět adresáty chovat se podle normou určených pravidel. V čl. 83 Nařízení GDPR jsou stanoveny podmínky pro ukládání pokut i s jejich možnou výší. Ukládání správních pokut musí být efektivní, adekvátní, ale současně i odstrašující. Správní pokuty jsou ukládány dle individuálního jednotlivého případu, a to vyjma určitých opatření vydaných v čl. 58 odst. 2 Nařízení GDPR. Důležité tedy je, že za každé porušení Nařízení GDPR není nutno, aby byla uložena pokuta. Správce může nejdříve obdržet upozornění, že plánované operace zpracování patrně porušují Nařízení GDPR, nebo může být správce, jehož operace zpracování porušily Nařízení GDPR, napomenut nebo mu může být přikázáno, aby splnil žádost subjektu údajů. Jako další nápravné

[69] Nařízení GDPR, článek 58
[70] ŽŮREK, Jiří. *Praktický průvodce GDPR*: 2. aktualizované vydání. Olomouc: ANAG, 2018, ISBN 978-80-7554-152-9. str. 178

opatření, které lze udělit místo či současně s pokutou, je např. odebrání osvědčení, uložení dočasného nebo permanentního omezení zpracování, včetně jeho zakázání nebo přikázání přerušení toků údajů adresátovi v zemi mimo EU. V neposlední řadě může být správci přikázáno, aby se zpracování shodovalo s Nařízením GDPR.[71]

Mezi funkce ÚOOÚ spadají i povinnosti a oprávnění udělovat sankce. Výše sankcí je upravena v hlavě VI Adaptačního zákona, zde jsou definovány skutkové podstaty přestupků. Přestupek je přímo definován takto: *„Přestupkem je společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.“*[72] ÚOOÚ projednává všechna porušení povinností a zároveň ukládá pokuty. Pokud se jedná o sankční řízení, vychází ÚOOÚ z charakteru, vážnosti, způsobu jednání, míře zavinění, doby trvání a následků ilegálního jednání. Při projednávání přestupků postupuje ÚOOÚ především podle Adaptačního zákona. Promlčecí lhůta je určena v § 30 zákona o odpovědnosti za přestupky a řízení o nich. Při nedodržení Nařízení GDPR se jedná o 3letou promlčecí lhůtu, poněvadž se projednává čin, u kterého je ze zákona stanovena sazba pokuty ve výši minimálně 100 000 Kč. Zisk z uložených pokut putuje do státního rozpočtu a jedná se o jeho příjem. V případě, že nastanou při vybírání pokut určité problémy, může je začít vymáhat Celní úřad.[73]

Dle Nařízení GDPR lze rozdělit druhy porušování do dvou skupin, které se liší dle výše možné sankce. Rozlišují se dle případného dopadu nedodržení zájmu Nařízení GDPR, kterým je ochrana práv a svobod osob, kterých se týkají osobní údaje, při jejich zpracování. To znamená, že porušení povinností, které se týkají ohrožení zájmů chráněných Nařízení GDPR, je možné sankcionovat více než porušení povinností, které chráněný zájem ohrožují méně.[74]

---

[71] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 43
[72] zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, § 5
[73] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str. 428-429
[74] Nařízení GDPR, článek 84

Jako první je v Adaptačním zákoně uvedený přestupek, kdy fyzická osoba, právnická osoba nebo podnikající fyzická osoba spáchá přestupek porušením zákazu uveřejňování osobních informací, které jsou stanoveny určitým právním předpisem. Při porušení tohoto přestupku hrozí pokuta do výše 1 000 000 Kč, nebo až 5 000 000 Kč, dopustí-li se osoba přestupku zveřejňování údajů v tisku, v televizi, v rozhlasu, na veřejně přístupné počítačové síti nebo jiným srovnatelně účinným způsobem.[75]

Pokud se jedná o orgány veřejné moci a veřejné subjekty, které se dopustí při zpracování osobních údajů přestupku, lze jim uložit pokutu do maximální výše 10 000 000 Kč. Pokuty uložené těmto orgánům plynou především z veřejných rozpočtů a bylo by neúčelné uchovat pro tyto subjekty nejvyšší možnou výši pokuty, tj. 20 000 000 EUR. Někteří politici se snažili prosadit úplné ustoupení od pokutování těchto subjektů, avšak tento návrh nebyl schválen. Pokud se jedná o udělování pokut ostatním subjektům, postupuje se podle níže uvedeného.[76]

První kategorie porušení Nařízení GDPR, za které lze uložit pokutu do výše 10 000 000 EUR, resp. jedná-li se o podnik, tak do výše 2 % souhrnného ročního obratu celosvětově, dle toho, která hodnota je vyšší. Jedná se o porušení ustanovení o povinnostech správce a zpracovatele, které se týkají např. povinností při zabezpečení ochrany osobních údajů, povinností spolupráce s dozorovým úřadem, povinností, které se týkají jmenování pověřence nebo povinností vztahujících se na činnost při získávání osvědčení.[77]

Ve druhé kategorii je výčet závažnějších porušení Nařízení GDPR, které lze pokutovat až do výše 20 000 000 EUR, resp. jedná-li se o podnik, tak do výše 4 % souhrnného ročního obratu celosvětově, dle toho, která hodnota je vyšší. Jedná se zejména o nesplnění základních zásad pro zpracování, včetně podmínek týkajících se jeho souhlasu, porušení práv subjektu údajů, porušení povinnosti splnit příkaz, nebo dočasné omezení zpracování nebo pozastavení toků údajů

[75] zákon č. 110/2019 Sb., o zpracování osobních údajů, § 61
[76] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 44
[77] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7. str. 428-429

dozorovým úřadem nebo nesplnění nařízení dozorového úřadu dle čl. 58 odst. 2 Nařízení GDPR.[78]

[78] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: GRADA Publishing a.s., 2017, ISBN 978-80-271-0668-4. str. 44

5 HLAVNÍ PŘÍČINY ZNEUŽITÍ OSOBNÍCH ÚDAJŮ

Osobní údaje jsou zneužívány každý den. Zneužití dat usnadňuje zejména existence sociálních sítí, kam uživatelé zadávají osobní údaje bez předešlého uvážení. Hlavním důvodem zneužití osobních údajů je lehkovážnost lidí, neuvědomujících si důsledky svého jednání a nebezpečí zveřejnění osobních údajů. Sociální sítě jsou samozřejmě velmi populární, zejména kvůli jejich výhodám. Lidé se pomocí nich mohou zdarma spojit s přáteli, rodinou a s dalšími osobami z jiných zemí. Na svých profilech lidé píší o věcech, které dělali, o místech, která navštívili, nebo si předávají různé rady. Mnoho sociálních sítí, jako je např. Facebook, může dokonce propojit přátele a navrhnout lidi, které možná znáte. Mnoho lidí se domnívá, že jsou tyto systémy bezpečné, ale opak je pravdou. Spousta uživatelů, kteří na profilu ustavičně sdílí své zážitky a zkušenosti ze života, poskytují rozsáhlé množství dat, které je poté veřejně přístupné nejen pro jejich přátelé. Uživatele mohou ohrozit různé věci, které se objevují na sociálních sítích. Např. při ucházení se o novou práci není pro zaměstnavatele nic jednoduššího, než se podívat na sociální sítě a zjistit si, určité informace o uchazeči. Tyto informace nemusí vytvořit dobrý první dojem. Ke zneužití osobních údajů nedochází pouze na sociálních sítích ale např. i na pracovištích, pomocí kamerových systémů. Na veřejném prostranství může dojít ke zneužití osobních údajů např. i pomocí létajících dronů. Uživatelé dronů narušují soukromí tím, že např. fotografují, nahrávají videa nebo pořizují audio záznamy osob bez jejich souhlasu.[79]

5.1 Zásady ochrany osobních údajů

Osobní údaje jsou v dnešní době velmi cenné informace, které ovšem mohou být lehce zneužity. Proto by každý občan měl vědět, jak nejlépe svoje osobní informace chránit a jak předcházet jejich zneužití, eventuálně odcizení. Případné doporučení a návod, jak předcházet zneužití osobních údajů, lze najít na webových stránkách ÚOOÚ.

[79] KINCL, Petr. *Sociální sítě a osobní údaje: Jak se bránit zneužití?* [online]. [cit. 23.1.2022]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/socialni-site-a-osobni-udaje

První zásadou při poskytování osobních údajů je si důkladně přečíst dokument, a zaměřit se na pravomoci, které souhlasem, případně podpisem získává zpracovatel osobních údajů. Udělení souhlasu s poskytnutím osobních údajů musí být vědomé, svobodné a informované. Důležitou zásadou je nepodepisovat nebo neudělovat souhlas s něčím, co je nejasné. Sdělovat osobní informace v soukromí a informovat se o jednotlivých údajích, které se budou shromažďovat. Při zjištění nekompletních či lživých údajů žádat okamžitou úpravu, doplnění nebo výmaz údajů. Bez souhlasu subjektu údajů nelze zhotovovat jakékoli kopie nebo skenovat osobní doklady. V neposlední řadě si člověk musí dávat pozor, zda o něm nejsou pořizovány kamerové záznamy a v případě, že tomu tak je, tak na to musí být upozorněn minimálně nástěnným obrázkem, že prostor je sledován.[80]

V dnešní době si subjekt údajů musí dávat největší pozor, komu sděluje své osobní informace, především na internetu. Ať už se jedná o vytváření nových účtů na různých internetových stránkách, nebo o vyplňování anket či dotazníků, je nutné s osobními údaji zacházet velmi opatrně. Obchod s osobními údaji se stává čím dál častějším tématem a existují ohromné databáze osobních údajů, které se prodávají v aukcích, a proto se vyplatí umět si svá data ochránit.

Při registraci na webovou stránku se musí věnovat dostatečná pozornost tomu, jaké osobní údaje se sdělují. Většina formulářů pro registraci má např. označena textová okna, která jsou nutná pro vytvoření registrace, tudíž stačí vyplnit pouze základní informace, které jsou dostačující. Často se také doporučuje si vytvořit speciální emailovou adresu právě na výše zmiňované registrace a na obdržování nevyžádaných reklam. Svolení se zasíláním reklamních emailů jde samozřejmě jak při registraci, tak i dodatečně odvolat. V neposlední řadě je důležité zvolit si tzv. „silné heslo“, které by nemělo být lehce odhadnutelné a mělo by se jednat o kombinaci velkých a malých písmen, číslic a speciálních znaků.

Při používání sociálních sítí je důležité, aby si každý člověk svůj profil dobře zabezpečil. A to především úpravou v nastavení, kde lze vybrat, kdo další na sociálních sítích může vidět vaše osobní informace, případně obsah, který

[80] CZ.NIC, Z. S. P. O.. *Ochrana osobních údajů* [online]. [cit. 23.1.2022]. Dostupné z: https://www.jaknainternet.cz/page/1183/ochrana-osobnich-udaju/

sdílíte. Jelikož právě na sociálních sítích může dojít ke krádeži soukromých dat a informací. V dnešní době však mají sociální sítě o této problematice přehled, a proto se snaží pomoci chránit data svých uživatelů.

5.2 Postup při zneužití osobních údajů

Každý subjekt údajů by měl znát kroky, které musí podstoupit v případě, že budou jeho osobní údaje zneužity. Jedná se o případ, kdy preventivní opatření nebyla dostatečná, nebo se i přes všechno úsilí podařilo osobní údaje odcizit a zneužít. V této kapitole bude popsán stručný návod, jak v takovém případě postupovat.

Pokud má člověk podezření, že s jeho osobními údaji není jednáno v souladu se zákonem, má několik možností, jak tuto situaci řešit. Jako první možnost se naskytuje obrátit se na Policii ČR, která by měla tuto skutečnost prověřit. Případně je možné zaslat stížnost na ÚOOÚ. Podání týkající se nesprávného zacházení s osobními údaji by mělo obsahovat konkrétní informace, aby byl zvolen efektivní a cílený postup. V podání by měl být označen podezřelý subjekt, který porušil zákon, popis jeho jednání, při kterém došlo k porušení zákona, uvedení, jakých osobních údajů se týká porušení a materiály které dokazují vztah oznamovatele a zpracovatele. Neměly by chybět ani podklady, ze kterých lze odvodit porušení zákona. V neposlední řadě musí ten, kdo podává stížnost uvést své identifikační a kontaktní údaje. Tato osoba není účastníkem správního řízení, ale může být vyslechnuta jako svědek.[81]

Pokud se subjekt údajů rozhodne podat stížnost na správce nebo zpracovatele prostřednictvím ÚOOÚ, lze na jejich stránkách přímo dohledat formulář k podání. Formulář lze vyplnit a zaslat elektronicky nebo vytisknout a zaslat na adresu ÚOOÚ.

[81] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Chci podat stížnost na správce nebo zpracovatele* [online]. [cit. 29.1.2022]. Dostupné z: https://www.uoou.cz/chci-podat-stiznost-na-spravce-nebo-zpracovatele/ds-4454/p1=4454

6 PORUŠENÍ NAŘÍZENÍ GDPR

Schválení Nařízení GDPR jasně ukázalo, že Evropská unie bere soukromí spotřebitelů mimořádně vážně a že ochrana osobních údajů občanů EU je nejvyšší prioritou. Potenciál masivních pokut, které mohou významně poškodit provozní schopnosti a globální reputaci, postavil mnoho organizací do pozoru. Nařízení GDPR povoluje sankce ve výši až 20 milionů eur nebo až čtyř procent z celosvětových příjmů organizace. Nyní, když je nařízení účinné již více než čtyři roky, objevují se trendy vymáhání pokut a ukazují, že úřady pro ochranu osobních údajů v členských státech EU se nebojí udělovat vysoké pokuty, v případě, že dojde k jeho porušení. Organizace jako takové musí porozumět globálním dopadům, které tato činnost může způsobit, a přezkoumat své plány na dodržování zásad ochrany osobních údajů, aby již nedocházelo k porušování Nařízení GDPR.

Podle přehledu, který zpracoval tým firmy Atlas VPN na základě dat webu GDPR Enforcement Tracker, který vytvořila právnická firma CMS, bylo v roce 2021 uděleno celkem 412 sankcí. Nejvíce jich bylo uděleno ve Španělsku, dále v Itálii, Rumunsku a Maďarsku. V České republice bylo od roku 2018 uděleno celkem 25 pokut za porušení Nařízení GDPR.[82]

6.1 The right to be forgotten – Právo být zapomenut

The right to be fotgotten, neboli právo být zapomenut je rozšířeným právem na výmaz. Jedná se o provedení úměrných kroků, včetně technického opatření, k vymazání všech odkazů na osobní údaje a jejich kopií žadatele. V Nařízení GDPR je však uvedeno mnoho výjimek, tudíž bude toto právo složité uplatnit. Jedná se především o případy, kdy jsou osobní údaje zpracovávány státními institucemi.

[82] ROVNÝ, Tomáš. *Amazon, Google, WhatsApp a další hříšníci. Pokuty za porušení GDPR byly loni rekordní* [online]. [cit. 13.2.2022]. Dostupné z: https://ekonomickydenik.cz/amazon-google-whatsapp-a-dalsi-hrisnici-pokuty-za-poruseni-gdpr-byly-loni-rekordni/

Aby měl správce povinnost zlikvidovat osobní údaje, musí být splněna alespoň jedna z těchto podmínek:

- *„osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,*
- *subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,*
- *subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,*
- *osobní údaje byly zpracovány protiprávně,*
- *osobní údaje musí být vymazány ke splnění právní povinnosti,*
- *osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 Nařízení GDPR.“*[83]

Právo být zapomenut se uplatnilo například ve sporu Gonzáles vs. Google Inc.

6.2 Internetový prodejce Amazon

Americká internetový prodejce Amazon obdržel od Evropské unie pokutu 746 milionů eur, což je v přepočtu 19 miliard Kč. Tuto pokutu dostal za předávání osobních údajů, které bylo v rozporu s pravidly pro jejich ochranu, tedy v rozporu s Nařízením GDPR. Společnost Amazon tuto skutečnost sama potvrdila v její podrobné zprávě o hospodaření, kterou jsou všechny obchodované firmy ve Spojených státech nuceny veřejně předkládat Komisi pro cenné papíry (dále jen „SEC“).

Projednávání porušení Nařízení GDPR společností Amazon vzešlo od stížnosti, která byla podaná v roce 2018 francouzskou skupinou pro práva na ochranu soukromí. Jednalo se o skutečnost, že společnost Amazon údajně nezakládá své reklamní postupy na svobodném souhlasu, čímž porušuje požadavky Nařízení GDPR na zpracování osobních údajů. Problémy vyplývaly ze způsobu, jakým společnost Amazon využívala údaje spotřebitelů pro cílenou reklamu. Ačkoli stížnost vznikla ve Francii, Nařízení GDPR umožňuje, aby se vyšetřováním

[83] ŠKORNIČKOVÁ, Eva. *Právo být zapomenut* [online]. [cit. 18.2.2022]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravo-byt-zapomenut/

zabýval jeden vedoucí dozorový úřad, pokud organizace působí ve více zemích EU. Společnost Amazon určila lucemburský úřad, který se ujala vedení řešení této stížnosti ve spolupráci s Úřadem pro ochranu osobních údajů ve Francii.[84]

Společnost Amazon sdělila svůj záměr podat odvolání a tvrdila, že nedošlo k narušení bezpečnosti údajů ani k jejich vyzrazení třetí osobě. Dokud nebude tento proces ukončen, nebudou o obviněních zveřejněny žádné další podrobnosti, jelikož v Lucembursku platí zákon, který zakazuje zveřejňování informací až do ukončení odvolacího řízení.

Dne 16. července 2021 vyšlo rozhodnutí, kde lucemburský úřad pro ochranu osobních údajů CNPD uložil firmě Amazon Europe Core pokutu. Amazon je největší internetový obchod na světe. Společnost založil Jeff Bezos, který je v současné době jeden z nejbohatších lidí světa. Hodnota jeho majetku se podle informací agentury Bloomberg pohybuje kolem 190 miliard dolarů.

Dle prohlášení agentury *Bloomberg* po uložení sankce skončilo vyšetřování, které začalo v roce 2018 na popud francouzských aktivistů, kteří se zajímali o ochranu osobních dat.[85]

6.3 Provozovatel komunikační aplikace WhatsApp

Dne 2. září 2021 oznámila irská Komise pro ochranu osobních údajů (DPC) rozhodnutí udělit společnosti WhatsApp pokutu ve výši 225 milionů eur, což je čtyřiapůlkrát více, než pokuta za rok 2019 vůči společnosti Google.

Vyšetřování společnosti WhatsApp bylo zahájeno 10. prosince 2018 a zkoumalo se, zda společnost splnila své povinnosti transparentnosti, které se týkají Nařízení GDPR. Jedná se o poskytování informací a transparentnosti těchto informací jak uživatelům aplikace, tak i těm, kteří ji nepoužívají.

---

[84] JD SUPRA, LLC. *Recent GDPR Fines Against Amazon and WhatsApp Set New Records* [online]. [cit. 10.2.2022]. Dostupné z: https://www.jdsupra.com/legalnews/recent-gdpr-fines-against-amazon-and-6369820/

[85] SVOBODA, Jiří. *Amazon za údajné porušení GDPR čelí rekordní pokutě. V Lucembursku má zaplatit 19 miliard korun* [online]. [cit. 10.2.2022]. Dostupné z: https://cc.cz/amazon-za-udajne-poruseni-gdpr-celi-rekordni-pokute-v-lucembursku-ma-zaplatit-19-miliard-korun/

DPC dospěla k závěru, že společnost WhatsApp neposkytla požadované informace o ochraně osobních údajů uživatelům aplikace WhatsApp (jak požaduje čl. 13 Nařízení GDPR), dále neposkytla informace o ochraně osobních údajů relevantní pro kontakty uživatelů aplikace WhatsApp ("neuživatelů"), jejichž osobní údaje byly zpracovávány, aby uživatelé věděli, které z jejich kontaktů jsou rovněž uživateli aplikace WhatsApp (jak požaduje čl. 14 Nařízení GDPR). Společnost také nezpřístupnila informace o ochraně osobních údajů ve "snadno dostupné formě" (jak požaduje čl. 12 Nařízení GDPR) a v důsledku toho rovněž nedodržela zastřešující zásadu transparentnosti podle čl. 5 odst. 1 písm. a) Nařízení GDPR. Výbor DPC rovněž společnosti WhatsApp uložil povinnost poskytnout požadované informace o ochraně osobních údajů ve lhůtě 3 měsíců od data vydání rozhodnutí (což je 20. srpna 2020) a udělil jí výtku.[86]

Vzhledem k tomu, že zpracování osobních údajů společností WhatsApp se podstatně dotýká subjektů údajů ve více než jednom členském státě a že jediná provozovna společnosti WhatsApp v EU byla v Irsku, byla uplatněna ustanovení o spolupráci a jednotnosti podle čl. 60 Nařízení GDPR (Spolupráce mezi vedoucím dozorovým úřadem a dalšími dotčenými dozorovými úřady). Za účelem splnění tohoto požadavku předložil DPC návrh rozhodnutí všem ostatním dozorovým úřadům. Šest z nich se k rozhodnutí vyjádřilo, šest dalších předložilo relevantní a odůvodněné námitky. V řadě bodů nebylo možné dosáhnout konsensu – proto byly předloženy Evropskému výboru pro ochranu osobních údajů (dále jen „EDPB“), aby dospěl k rozhodnutí podle čl. 65 Nařízení GDPR.[87]

Rozhodnutí stanovilo, že oznámení o ochraně osobních údajů musí být podrobná, především s mnohem podrobnějšími údaji, než je v současnosti obvykle zvykem a musí být snadno dostupná, bez použití více propojených dokumentů, které může být obtížné najít a asimilovat. Podle irské Komise pro ochranu dat WhatsApp unijní

[86] JD SUPRA, LLC. *Recent GDPR Fines Against Amazon and WhatsApp Set New Records* [online]. [cit. 10.2.2022]. Dostupné z: https://www.jdsupra.com/legalnews/recent-gdpr-fines-against-amazon-and-6369820/

[87] BOARDMAN, Ruth. *Irish Data Protection Commission WhatsApp decision: what do you need to know?* [online]. [cit. 15.2.2022]. Dostupné z: https://www.twobirds.com/en/insights/2021/uk/irish-data-protection-commission-whatsapp-decision

pravidla porušuje nakládáním s daty uživatelů a jejich sdílením s ostatními aplikacemi, které vlastní Facebook.[88]

Toto rozhodnutí bylo výsledkem tříletého vyšetřování, zda WhatsApp poskytl spotřebitelům dostatek podrobností v jejich zásadách ochrany osobních údajů o jejich postupech zpracování dat. WhatsApp se také hodlá proti tomuto trestu odvolat.[89]

6.4 Gonzáles vs. Google Inc.

V roce 1998 zveřejnil španělský deník La Vanguardia ve svém tištěném vydání dvě oznámení o nuceném prodeji nemovitostí, které vznikly z dluhů na sociálním zabezpečení. Oznámení byla zveřejněna na příkaz španělského ministerstva práce a sociálních věcí a jejich účelem bylo přilákat co nejvíce zájemců. Verze vydání byla později zpřístupněna na internetu.

Jedna z nemovitostí popsaných v novinových oznámeních patřila Mariu Costeja Gonzálezovi, který byl v oznámeních jmenován. V listopadu 2009 se Costeja obrátil na noviny se stížností, že zadání jeho jména do vyhledávače Google vedlo k těmto oznámením. Požádal o odstranění údajů, které se ho týkaly, s odůvodněním, že nucený prodej byl uzavřen před několika lety a již není relevantní. Po společnosti Google byla v únoru 2010 vyžadována obdobná úprava výsledků vyhledání, aby jeho jméno nebylo spojováno s výše zmíněnými informacemi. Společnost Google Spain předala žádost společnosti Google Inc., se sídlem v Kalifornii ve Spojených státech, přičemž se domnívala, že toto je odpovědný orgán. Costeja následně podal stížnost španělskému úřadu pro ochranu údajů (dále jen „AEPD“) se žádostí, aby noviny byly povinny odstranit data a aby Google Spain nebo Google Inc. byly povinny odstranit odkazy na tato data. Dne 30. července 2010 ředitel AEPD zamítl stížnost na noviny, ale potvrdil

[88] ROVNÝ, Tomáš. *Amazon, Google, WhatsApp a další hříšníci. Pokuty za porušení GDPR byly loni rekordní* [online]. [cit. 13.2.2022]. Dostupné z: https://ekonomickydenik.cz/amazon-google-whatsapp-a-dalsi-hrisnici-pokuty-za-poruseni-gdpr-byly-loni-rekordni/
[89] JD SUPRA, LLC. *Recent GDPR Fines Against Amazon and WhatsApp Set New Records* [online]. [cit. 10.2.2022]. Dostupné z: https://www.jdsupra.com/legalnews/recent-gdpr-fines-against-amazon-and-6369820/

stížnost na Google Spain a Google Inc. a vyzval je, aby odstranili odkazy, týkající se Costeja a znemožnili přístup k informacím o něm.[90]

Regulátor odmítl stažení informací z tištěného deníku, jelikož informace byly publikovány právem a z veřejných zdrojů. Společnosti Google však bylo nařízeno, aby údaje o Costejovi byly smazány a aby se k nim v budoucnu nikdo nemohl znovu dostat. Společnosti Google Spain a Google Inc. následně podaly proti tomuto rozhodnutí samostatné žaloby u Národního soudu Španělska (Audiencia Nacional).

Dne 26. února 2013 se konalo písemné jednání s následným ústním jednáním, na kterém se kromě stran vyjádřily také vlády Rakouska, Řecka, Itálie, Španělska a Polska a Evropská komise. Generální advokát Niilo Jääskinen vydal své stanovisko dne 25. června 2013, poté byl rozsudek vynesen dne 13. května 2014. Účelem stanoviska generálního advokáta je poradit soudu v nových právních otázkách. Pro soud to není závazné.[91]

Soudní dvůr EU (dále jen „SDEU“) konstatoval, *že „provozovatel vyhledávače musí za určitých podmínek ze zobrazeného seznamu výsledků vyhledávání provedeného na základě jména osoby vymazat odkazy na webové stránky zveřejněné třetími osobami a obsahující informace týkající se této osoby. Soudní dvůr upřesnil, že tuto povinnost může mít rovněž v případě, že toto jméno nebo tyto informace nebyly předtím nebo současně vymazány z uvedených webových stránek, a to případně i tehdy, jestliže je jejich zveřejnění na uvedených stránkách samo o sobě v souladu se zákonem.“*[92]

Soud svou argumentaci odůvodnil tím, že vyhledávač je z hlediska evropských předpisů zpracovatelem osobních údajů.

---

[90] SLÍŽEK, David. *Evropský soud ve sporu s Googlem: vyhledávače musí na požádání měnit minulost* [online]. [cit. 18.2.2022]. Dostupné z: https://www.lupa.cz/clanky/evropsky-soud-ve-sporu-s-googlem-vyhledavace-musi-na-pozadani-menit-minulost/

[91] GOLDEN DATA. *Google Spain v. AEPD: Remembering the “Right to be Forgotten”* [online]. [cit. 18.2.2022]. Dostupné z: https://medium.com/golden-data/google-v-spain-the-right-to-be-forgotten-aaee50dae43c

[92] SLÍŽEK, David. *Evropský soud ve sporu s Googlem: vyhledávače musí na požádání měnit minulost* [online]. [cit. 18.2.2022]. Dostupné z: https://www.lupa.cz/clanky/evropsky-soud-ve-sporu-s-googlem-vyhledavace-musi-na-pozadani-menit-minulost/

Soud dále uvedl, že prostřednictvím vyhledávání je k dispozici velké množství strukturovaných informací o lidech, které efektivně umožňují sestavit detailní profily. Dopad na uživatele může být tak rozsáhlý, že musí mít právo smazat informace související s jejich jménem. Provozovatelé vyhledávačů si však mohou nejprve ověřit, zda je jejich požadavek opodstatněný.[93]

Při hodnocení, zda by měl vyhledávač vymazat osobní údaje, je třeba zvážit nalezení rovnováhy mezi právy příslušného uživatele a právy všech uživatelů internetu, kteří mohou mít zájem o přístup k příslušným informacím. Uvedl však, že veřejně činné osobnosti, jako jsou politici, musí mít v tomto ohledu menší ochranu než „obyčejní" lidé.

Mazání dat však není vůbec závislé na tom, zda jsou údaje pravdivé či nikoli. Soud totiž tvrdí, že je zásadní dnešní významnost informací:

„Soudní dvůr v tomto ohledu poznamenal, že i zpracování přesných údajů, které bylo původně v souladu se zákonem, se časem může stát neslučitelným s touto směrnicí, pokud se s ohledem na veškeré okolnosti daného případu zdají tyto údaje nepřiměřené, nepodstatné nebo již nepodstatné, nebo přesahují míru s ohledem na účely, pro které byly zpracovány, a uplynulý čas."[94]

Rozhodnutí SDEU může mít velký dopad na nynější fungování vyhledávačů, i na to, co prostřednictvím jich vyhledáme.[95]

[93] GOLDEN DATA. *Google Spain v. AEPD: Remembering the "Right to be Forgotten"* [online]. [cit. 18.2.2022]. Dostupné z: https://medium.com/golden-data/google-v-spain-the-right-to-be-forgotten-aaee50dae43c

[94] SLÍŽEK, David. *Evropský soud ve sporu s Googlem: vyhledávače musí na požádání měnit minulost* [online]. [cit. 18.2.2022]. Dostupné z: https://www.lupa.cz/clanky/evropsky-soud-ve-sporu-s-googlem-vyhledavace-musi-na-pozadani-menit-minulost/

[95] BALL, James. *Costeja González and a memorable fight for the 'right to be forgotten'* [online]. [cit. 18.2.2022]. Dostupné z: https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten

ZÁVĚR

Práce je uceleným pohledem na ochranu osobních údajů na mezinárodní úrovni a v České republice. Cílem práce bylo více přiblížit a vysvětlit dění kolem ochrany osobních údajů. Jaké skutečnosti předcházely ochraně osobních údajů a jak se postupně formulovaly. Jsou zde také vymezeny veškeré základní pojmy, týkající se ochrany osobních údajů, jako jsou např. subjekt údajů, zpracování osobních údajů nebo správce osobních údajů.

Popsáno je zejména jak se svými osobními údaji nakládat, chránit je a co dělat v případě jejich zneužití. Zneužívání osobních údajů je každodenní záležitost, jedná se např. o reklamní účely, odcizení identity nebo poskytování údajů třetím stranám bez souhlasu subjektu údajů. Ke zneužívání dat pomáhají i sociální sítě, kde lidé bezmyšlenkovitě sdílí své osobní údaje. Je až neuvěřitelné, jak lehce se dají zneužít, či ukrást osobní údaje. Z tohoto důvodu ÚOOÚ zveřejnil na svých webových stránkách doporučení a návod, jak předejít možnému zneužití.

Z práce vyplývá, že ochrana osobních údajů je stále velice problematické téma. K formulaci ochrany osobních údajů v poslední době přispěl nový zákon č. 110/2019 Sb., o zpracování osobních údajů, který konkretizuje některá obecná ustanovení Nařízení GDPR.

Fyzické osoby se díky Adaptačnímu zákonu a Nařízení GDPR stávají rovnější velkým obchodním společnostem. V dnešní době mají práva, která jsou vymahatelná napříč celou Evropskou unií. Upřesnění a sjednocení Nařízení GDPR lze tedy považovat za cenný přínos.

V práci jsou uvedeny konkrétní případy porušení ochrany osobních údajů, jaký byl soudní proces a následné rozhodnutí. Ve světle těchto nedávných rozhodnutí by se organizace, na které se vztahuje GDPR nebo jakýkoli jiný zákon na ochranu soukromí, měly více zaměřit na své úsilí o dodržování ochrany osobních údajů. Tvrdé vymáhání proti velkým technologickým společnostem ukazuje, že úřady pro ochranu údajů se nebojí jít po prominentních organizacích. Zatímco vysoká pokuta pravděpodobně nezničí větší organizace, jakékoli požadavky na změnu postupů zpracování mohou mít zásadní dopad vyžadující velké úsilí. Také pro menší společnosti mohou být pokuty jako tato zničující. Všichni správci a zpracovatelé

by tudíž měli dbát na to, zda zpracovávají osobní údaje a data ve znění zákona č. 110/2019 Sb., o zpracování osobních informací, a Nařízení GDPR.

Adaptační zákon a Nařízení GDPR velkou mírou dopomáhají k ochraně osobních údajů. Právě jednoznačné popsání nakládání s osobními údaji je pro mnohé uživatele zásadní. Každý musí být informován o tom, jak s jeho osobními údaji bude naloženo. Ve výsledku je ale nutné, aby každý občan znal svá práva a povinnosti ohledně osobních údajů, chránil své osobní údaje, zabezpečoval je a v nutném případě i vymáhal svá práva na jejich ochranu.

SEZNAM POUŽITÝCH ZKRATEK

ÚOOÚ – Úřad pro ochranu osobních údajů

ČR – Česká republika

EU – Evropská unie

OECD – Organizace pro hospodářskou spolupráci a rozvoj

SDEU – Soudní dvůr Evropské unie

EK – Evropská komise

RE – Rada Evropy

AEPD – Španělský úřad pro ochranu údajů

DPC – Irská Komise pro ochranu osobních údajů

EDPB – Evropský sbor pro ochranu osobních údajů

CNPD – Lucemburský úřad pro ochranu osobních údajů

SEC – Komise pro cenné papíry

EÚLP – Evropská úmluva o ochraně lidských práv

LZPS – Listina základních práv a svobod

SEZNAM POUŽITÝCH ZDROJŮ

Monografie

GERLOCH, Aleš, Jiří HŘEBEJK a Vladimír Zoubek. Ústavní systém České republiky. 5. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-807-3804-237.

KLÍMA, Karel. Komentář k Ústavě a Listině. 2. rozšířené vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009. ISBN 978-80-271-0668-4.

MATES, Pavel, JANEČKOVÁ Eva, BARTÍK Václav. Ochrana osobních údajů. Praha: Leges, s.r.o., 2012, ISBN 978-80-87576-12-0.

MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer ČR, a.s., 2019, ISBN 978-80-7598-587-3.

NEŠPŮREK, Robert, ŠUCHMAN, Jaroslav, JAROŠ, Ján. GDPR: nastane s nástupem nové regulace nedostatek pověřenců? EU právní noviny, 1/2018,

NEZMAR, Luděk. GDPR Praktický průvodce implementací. Praha: GRADA Publishing a.s., 2017, 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. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

PAVLÍČEK, Václav a kol. Ústavní právo a státověda. I. díl. Obecná státověda. Praha: Linde, 2014. ISBN 978-80-7502-053-6.

PAVLÍČEK, Václav a kol. Ústavní právo a státověda. II. díl. Ústavní právo České republiky. 2. aktualizované vydání. Praha: Leges, 2015. 1152 s. ISBN 978-80-7502-084-0.

POKORNÁ, Andrea a Helena DVOŘÁKOVÁ. Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek: stěžejní

judikatura SDEU a vybraná judikatura ESLP: výkladové pokyny a stanoviska skupiny WP29 a EBDP: zákon o zpracování osobních údajů. Praha: Wolters Kluwer, 2020. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-309-1.

ŽŮREK, Jiří. Praktický průvodce GDPR: 2. aktualizované vydání. Olomouc: ANAG, 2018, ISBN 978-80-7554-152-9.

Legislativní zdroje

Zákon č. 110/2019 Sb., *o zpracování osobních údajů*

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

Zákon č. 250/2016 Sb., *o odpovědnosti za přestupky a řízení o nich*

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)

Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. ledna 1981

Internetové zdroje

AMAZON.COM. UNITED STATES SECURITIES AND EXCHANGE COMMISSION [online]. [cit. 26.2.2022]. Dostupné z: https://www.sec.gov/ix?doc=/Archives/edgar/data/1018724/000101872421000020/amzn-20210630.htm

BOARDMAN, Ruth. Irish Data Protection Commission WhatsApp decision: what do you need to know? [online]. [cit. 15.2.2022]. Dostupné z: https://www.twobirds.com/en/insights/2021/uk/irish-data-protection-commission-whatsapp-decision

CZ.NIC, Z. S. P. O.. Ochrana osobních údajů [online]. [cit. 23.1.2022]. Dostupné z: https://www.jaknainternet.cz/page/1183/ochrana-osobnich-udaju/

Destination GDPR - how did we arrive here? . Object moved [online]. Copyright © [cit. 10.02.2022]. Dostupné z: https://sytorus.com/ie/Blog/Article/176?title=destination-gdpr-how-didwe-arrive-here

GOLDEN DATA. Google Spain v. AEPD: Remembering the "Right to be Forgotten" [online]. [cit. 18.2.2022]. Dostupné z: https://medium.com/golden-data/google-v-spain-the-right-to-be-forgotten-aaee50dae43c

CHLEBUS, Tomáš. Nový zákon o zpracování osobních údajů [online]. [cit. 2.2.2022]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html

JEŽEK, Mojmír. Nový český zákon o zpracování osobních údajů [online]. [cit. 2.2.2022]. Dostupné z: https://www.ecovislegal.cz/gdpr-a-ochrana-osobnich-udaju/novy-cesky-zakon-o-zpracovani-osobnich-udaju-2/

KINCL, Petr. Sociální sítě a osobní údaje: Jak se bránit zneužití? [online]. [cit. 23.1.2022]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/socialni-site-a-osobni-udaje

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Základní pojmy v GDPR [online]. [cit. 1.12.2021]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

ROVNÝ, Tomáš. Amazon, Google, WhatsApp a další hříšníci. Pokuty za porušení GDPR byly loni rekordní [online]. [cit. 13.2.2022]. Dostupné z: https://ekonomickydenik.cz/amazon-google-whatsapp-a-dalsi-hrisnici-pokuty-za-poruseni-gdpr-byly-loni-rekordni/

SLÍŽEK, David. Evropský soud ve sporu s Googlem: vyhledávače musí na požádání měnit minulost [online]. [cit. 18.2.2022]. Dostupné z: https://www.lupa.cz/clanky/evropsky-soud-ve-sporu-s-googlem-vyhledavace-musi-na-pozadani-menit-minulost/

SVOBODA, Jiří. Amazon za údajné porušení GDPR čelí rekordní pokutě. V Lucembursku má zaplatit 19 miliard korun [online]. [cit. 10.2.2022]. Dostupné z: https://cc.cz/amazon-za-udajne-poruseni-gdpr-celi-rekordni-pokute-v-lucembursku-ma-zaplatit-19-miliard-korun/

ŠKORNIČKOVÁ, Eva. Právo být zapomenut [online]. [cit. 18.2.2022]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravo-byt-zapomenut/

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Chci podat stížnost na správce nebo zpracovatele [online]. [cit. 29.1.2022]. Dostupné z: https://www.uoou.cz/chci-podat-stiznost-na-spravce-nebo-zpracovatele/ds-4454/p1=4454

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Práva subjektu údajů [online]. [cit. 9.1.2022]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Právní předpisy [online]. [cit 2.12.2021]. Dostupné z: https://www.uoou.cz/pravni-predpisy/ds-1257/p1=1257

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Základní příručka k ochraně údajů [online]. [cit. 18.2.2022]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-ochrane-udaju/ds-4744/p1=4744