EVROPSKÁ
KOMISE

V Bruselu dne 29.5.2019
COM(2019) 250 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

Pokyny k nařízení o rámci pro volný tok neosobních údajů v Evropské unii

Obsah

1 Úvod ... 2

Účel těchto pokynů ... 3

2 Vzájemné působení mezi nařízením o volném toku neosobních údajů a obecným nařízením o ochraně osobních údajů – smíšené soubory údajů ... 4

2.1 Pojem neosobních údajů v nařízení o volném toku neosobních údajů ... 4

Osobní údaje ... 4

Neosobní údaje ... 5

2.2 Smíšené soubory údajů ... 7

3 Volný tok údajů a odstranění požadavků na lokalizaci údajů ... 11

3.1 Volný pohyb neosobních údajů ... 11

3.2 Volný pohyb osobních údajů ... 13

3.3 Oblast působnosti nařízení o volném toku neosobních údajů ... 14

3.4 Činnosti související s vnitřní organizací členských států ... 16

4 Přístupy založené na samoregulaci k podpoře volného toku údajů ... 17

4.1 Přenesení údajů a změna poskytovatele cloudových služeb ... 17

Pojem přenositelnosti a vzájemné působení s obecným nařízením o ochraně osobních údajů ... 18

4.2 Kodexy chování a systémy pro vydávání osvědčení o ochraně osobních údajů ... 20

4.3 Posílení důvěry v přeshraniční zpracování údajů – osvědčení zabezpečení ... 21

Závěrečné poznámky ... 21

Tento dokument poskytla Evropská komise pouze pro informační účely. Neobsahuje žádný závazný výklad nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii a nezakládá rozhodnutí ani stanovisko Evropské komise. Není jím dotčeno žádné takovéto rozhodnutí či stanovisko Evropské komise ani pravomoc Soudního dvora Evropské unie vykládat uvedené nařízení v souladu se Smlouvami o EU.

1 Úvod

V ekonomice, která je stále více založená na datech, představují toky údajů základ obchodních procesů v podnicích všech velikostí a napříč odvětvími. Nové digitální technologie otevírají široké veřejnosti, podnikům a orgánům veřejné správy v Evropské unii (dále jen „EU“) nové příležitosti.

V zájmu dalšího zvýšení objemu přeshraniční výměny údajů a podpory ekonomiky založené na datech přijaly Evropský parlament a Rada v listopadu 2018 na základě návrhu Evropské komise (dále jen „Komise“) nařízení (EU) 2018/1807 o rámci pro volný tok neosobních údajů v Evropské unii[1] (dále jen „nařízení o volném toku neosobních údajů“). Nařízení je použitelné ode dne 28. května 2019. Zásada volného pohybu osobních údajů je už stanovena v nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů“)[2]. Díky tomu nyní existuje komplexní rámec pro společný evropský datový prostor a volný pohyb všech údajů v rámci Evropské unie[3].

Nařízení o volném toku neosobních údajů vytváří právní jistotu pro podniky, které tak mohou zpracovávat své údaje kdekoli v EU, zvyšuje důvěru ve služby zpracování údajů a potírá praxi obchodních proprietárních uzamčení (tzv. *vendor lock-in*). Tímto způsobem se pro zákazníky rozšíří možnost volby, zlepší účinnost a podpoří zavádění cloudových technologií, což povede k významným úsporám pro podniky v EU. Z jedné studie vyplývá, že přechodem na cloudové technologie by mohly podniky v EU ušetřit 20–50 % svých nákladů na IT[4].

Díky těmto dvěma nařízením mohou údaje mezi členskými státy proudit volně, což umožňuje uživatelům služeb zpracování údajů využívat údaje shromážděné na různých trzích EU ke zvýšení své produktivity a konkurenceschopnosti. Uživatelé tedy mohou plně využívat úspor z rozsahu, které velký trh EU nabízí, zlepšit svou celosvětovou konkurenceschopnost a zvýšit propojenost evropské ekonomiky založené na datech.

Nařízení o volném toku neosobních údajů má tři důležité prvky:

- V zásadě zakazuje členským státům ukládat požadavky týkající se lokalizace údajů. Výjimky z tohoto pravidla představují pouze případy, kdy je to odůvodněno veřejnou bezpečností v souladu se zásadou proporcionality.

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii, Úř. věst. L 303, 28.11.2018, s. 59.

[2] 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), Úř. věst. L 119, 4.5.2016, s. 1.

[3] Obecné nařízení o ochraně osobních údajů se vztahuje rovněž na Evropský hospodářský prostor (EHP), který zahrnuje Island, Lichtenštejnsko a Norsko. Kromě toho je nařízení o volném toku neosobních údajů označeno jako nařízení s významem pro EHP.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe* [Měření ekonomického dopadu cloud computingu v Evropě], SMART 2014/0031, 2016. K dispozici na webových stránkách na adrese: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- Nařízení zavádí mechanismus spolupráce, který má zajistit, aby příslušné orgány mohly i nadále vykonávat veškerá práva, která mají v oblasti přístupu k údajům zpracovávaným v jiném členském státě.
- Motivuje odvětví, aby s podporou Komise vypracovalo samoregulační kodexy chování týkající se změny poskytovatele služeb a přenosu údajů.

Účel těchto pokynů

Tyto pokyny představují naplnění čl. 8 odst. 3 nařízení o volném toku neosobních údajů, který ukládá Komisi, aby zveřejnila pokyny k vzájemnému působení tohoto nařízení a obecného nařízení o ochraně osobních údajů, „zejména pokud jde o soubory údajů obsahující jak osobní, tak neosobní údaje“.

Záměrem těchto pokynů je pomoci uživatelům – zejména malým a středním podnikům – porozumět vzájemnému působení mezi nařízením o volném toku neosobních údajů a obecným nařízením o ochraně osobních údajů[5]. Pokyny se proto zaměřují zejména na: i) pojmy neosobních údajů a osobních údajů; ii) zásady volného pohybu údajů a zákazu požadavků na lokalizaci údajů podle obou nařízení a iii) pojem přenositelnosti údajů podle nařízení o volném toku neosobních údajů. Věnuje se rovněž požadavkům v oblasti samoregulace stanoveným v obou nařízeních.

Nařízení o volném toku neosobních údajů se vztahuje pouze na „údaje jiné než osobní údaje“ ve smyslu definice stanovené v obecném nařízení o ochraně osobních údajů. Obecné nařízení o ochraně osobních údajů upravuje zpracování osobních údajů a tvoří nezbytnou součást rámce EU pro ochranu údajů[6]. Nařízení vstoupilo v členských státech v platnost dne 25. května 2018. V nařízení jsou stanovena harmonizovaná pravidla na ochranu osob v EU/EHP, pokud jde o zpracování jejich osobních údajů, a na volný pohyb těchto údajů. Obecné nařízení o ochraně osobních údajů kromě dalších ustanovení: i) upřesňuje, které informace představují osobní údaje; ii) stanoví právní základ pro jejich zpracování a iii) vymezuje práva a

[5] Ustanovení 37. bodu odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[6]
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), Úř. věst. L 119/1, 4.5.2016, s. 1.
- Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES, Úř. věst. L 295, 21.11.2018, s. 39.
- Směrnice (EU) 2016/680 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, Úř. věst. L 119, 4.5.2016, s. 89.
- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. L 201, 31.7.2002, s. 37 (v současné době se reviduje).

povinnosti, které je třeba při zpracování těchto údajů dodržovat[7]. Pokud jde o zásadu volného pohybu osobních údajů, v čl. 1 odst. 3 obecného nařízení o ochraně osobních údajů se stanoví, že „volný pohyb osobních údajů v Unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán“.

Ve většině reálných situací bude soubor údajů s velkou pravděpodobností tvořen údaji jak osobními, tak neosobními. Takový soubor se často nazývá „smíšeným souborem údajů“. V oddíle 2.2 níže je blíže vysvětleno vzájemné působení mezi nařízením o volném toku neosobních údajů a obecným nařízením o ochraně osobních údajů v souvislosti se smíšenými soubory údajů.

Pro upřesnění – z obecného nařízení o ochraně osobních údajů a z nařízení o volném toku neosobních údajů nevyplývají žádné protichůdné závazky.

2 Vzájemné působení mezi nařízením o volném toku neosobních údajů a obecným nařízením o ochraně osobních údajů – smíšené soubory údajů

2.1 Pojem neosobních údajů v nařízení o volném toku neosobních údajů

Záměrem nařízení o volném toku neosobních údajů[8] je zajistit volný tok jiných než osobních údajů. Pojem „údaje“ se vyskytuje v celém znění nařízení a je třeba mu rozumět jako „údaje jiné než osobní údaje ve smyslu čl. 4 bodu 1 nařízení (EU) 2016/679“ [obecného nařízení o ochraně osobních údajů][9]. Tyto údaje – v tomto dokumentu jsou rovněž označovány jako „**neosobní údaje**“ – se vymezují v protikladu (*a contrario*) k osobním údajům, jak jsou stanoveny v obecném nařízení o ochraně osobních údajů.

Osobní údaje

V obecném nařízení o ochraně osobních údajů se uvádí: „ ‚osobními údaji‘ [se rozumí] veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen ‚subjekt údajů‘); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo

---

[7] Další pokyny k různým aspektům 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) a evropským právním předpisům v oblasti ochrany údajů naleznete na webových stránkách Evropského sboru pro ochranu osobních údajů, který vydal řadu pokynů v souladu s článkem 70 obecného nařízení o ochraně osobních údajů, které jsou k dispozici na adrese: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_cs. Příslušné webové stránky obsahují také odkazy na pokyny, doporučení a další dokumenty vydané předchůdcem Evropského sboru pro ochranu osobních údajů – pracovní skupinou zřízenou podle článku 29. V zájmu zvýšení informovanosti občanů a podniků 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 (obecném nařízení o ochraně osobních údajů) dále vydala Komise sdělení o ochraně údajů – pokyny týkající se přímé použitelnosti obecného nařízení o ochraně osobních údajů (COM/2018/043 final), které je k dispozici na adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

[8] Článek 1 nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[9] Viz čl. 3 bod 1 nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“.

Široká definice osobních údajů je záměrná a v obecném nařízení o ochraně osobních údajů zůstala v porovnání s předchozími právními předpisy v podstatě nezměněna[10]. Jednotlivými aspekty definice osobních údajů, jako např. složkami „veškeré informace“, „o“ (vztah mezi složkami a osobou), „identifikovaná nebo identifikovatelná“, se už zabývala pracovní skupina zřízená podle článku 29[11] ve svém stanovisku č. 4/2007 k pojmu osobních údajů přijatém dne 20. června 2007, WP 136.

V oblastech, jako je výzkum, je běžnou praxí pseudonymizace osobních údajů za účelem utajení totožnosti jednotlivce. **Pseudonymizace** je zpracování osobních údajů takovým způsobem, že bez použití dodatečných informací je nelze přiřadit konkrétní osobě. Tyto dodatečné informace se uchovávají odděleně a jsou chráněny pomocí organizačních nebo technických opatření (např. šifrováním)[12, 13]. Údaje, které byly pseudonymizovány, jsou však stále považovány za informace o identifikovatelné osobě, pokud je lze této osobě pomocí dodatečných informací přiřadit[14]. Tyto údaje **představují osobní údaje** ve smyslu obecného nařízení o ochraně osobních údajů.

Neosobní údaje

Pokud se nejedná o „osobní údaje“ ve smyslu definice obecného nařízení o ochraně osobních údajů, jedná se o údaje **neosobní**. Neosobní údaje mohou být zařazeny do kategorií podle původu:

---

[10] Viz čl. 2 písm. a) 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 (datum ukončení platnosti: 24. května 2018, zrušená obecným nařízením o ochraně osobních údajů). Viz též judikatura Soudního dvora týkající se definice osobních údajů, která uznává široký výklad tohoto pojmu, například rozsudek Soudního dvora ze dne 29. ledna 2009, *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; rozsudek Soudního dvora ze dne 24. listopadu 2011, *Scarlet Extended SA* v. *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771 či rozsudek Soudního dvora ze dne 19. října 2016, *Patrick Breyer* v. *Bundersrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

[11] Pracovní skupina zřízená podle článku 29 byla poradním orgánem, který Komisi poskytoval poradenství v záležitostech ochrany údajů a který pomáhal při přípravě harmonizovaných politik v oblasti ochrany údajů v EU. Poté, co dne 25. května 2018 vstoupilo v platnost obecné nařízení o ochraně osobních údajů, nahradil pracovní skupinu podle článku 29 Evropský sbor pro ochranu osobních údajů.

[12] Viz čl. 4 bod 5 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), který uvádí definici „pseudonymizace“.

[13] Například výzkumná studie o účincích nového léčivého přípravku by mohla být považována za pseudonymizaci, pokud by osobní údaje účastníků studie byly ve výzkumné dokumentaci nahrazeny jedinečnými atributy (např. číslem nebo kódem) a jejich osobní údaje s přiřazenými jedinečnými atributy by byly uchovávány odděleně v zabezpečeném dokumentu (např. v databázi chráněné heslem).

[14] Viz 26. bod odůvodnění 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).

- zaprvé: údaje, které se ani původně netýkaly identifikované nebo identifikovatelné fyzické osoby, jako jsou údaje o povětrnostních podmínkách vytvářené čidly instalovanými na větrných elektrárnách nebo údaje o potřebě údržby průmyslových strojů,

- zadruhé: údaje, které původně byly osobními údaji, ale později byly **anonymizovány**[15]. „Anonymizace“ osobních údajů se liší od pseudonymizace (viz výše), protože řádně anonymizované údaje nelze připsat konkrétní osobě, a to ani s použitím dodatečných údajů[16], a jedná se proto o údaje neosobní.

Posouzení, zda jsou údaje řádně anonymizovány, závisí na konkrétních a jedinečných okolnostech každého jednotlivého případu[17]. Několik příkladů opětovné identifikace souborů údajů, které byly údajně anonymizovány, je dokladem toho, že toto posouzení může být náročné[18]. Aby bylo možné určit, zda je jednotlivec identifikovatelný, je třeba posoudit všechny prostředky, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci jednotlivce[19].

Příklady neosobních údajů:

- Údaje agregované do té míry, že už nelze identifikovat jednotlivé události (např. jednotlivé cesty do zahraničí nebo vzorce cestování, které by mohly představovat osobní údaje), lze považovat za anonymní údaje[20]. Anonymní údaje se používají

[15] Viz 26. bod odůvodnění 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) v němž se stanoví, že „…zásady ochrany osobních údajů by se proto neměly vztahovat na anonymní informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným.“

[16] Viz rozsudek Soudního dvora ze dne 19. října 2016, *Patrick Breyer* v. *Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. Podle názoru Soudního dvora může adresa dynamického internetového protokolu (IP) představovat osobní údaje i v případě, že třetí strana (např. poskytovatel internetových služeb) má k dispozici dodatečné údaje, které by mohly umožnit identifikaci jednotlivce. Možnost identifikovat jednotlivce musí spočívat v prostředcích, o nichž lze rozumně předpokládat, že budou použity pro přímou či nepřímou identifikaci jednotlivce.

[17] Anonymizace údajů by měla být vždy prováděna za pomoci nejmodernějších technik anonymizace.

[18] Příklady opětovné identifikace údajně anonymizovaných údajů jsou uvedeny ve studii o budoucích tocích údajů, kterou pro Výbor Evropského parlamentu pro průmysl, výzkum a energetiku vypracoval Blackman, C. a Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee* [Toky údajů – budoucí scénáře: hloubková analýza pro Výbor pro průmysl, výzkum a energetiku], 2017, s. 22, 2. rámeček. K dispozici na webových stránkách na adrese: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf.

[19] Viz 26. bod odůvodnění nařízení (EU) 2016/679, obecného nařízení o ochraně osobních údajů, podle kterého „ke stanovení toho, zda lze rozumně předpokládat použití prostředků k identifikaci fyzické osoby, by měly být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji“.

[20] Viz pracovní skupina zřízená podle článku 29: *Stanovisko č. 5/2014 k technikám anonymizace*, přijaté dne 10. dubna 2014, WP216, s. 9: „Výsledný soubor údajů lze kvalifikovat jako anonymní pouze v případě, že správce údajů sloučí údaje na úrovni, kde již nelze identifikovat jednotlivé operace. Například: jestliže organizace shromažďuje údaje o pohybech cestujících, budou jednotlivé vzorce cestování na úrovni operace u kteréhokoli účastníka stále představovat osobní údaje, neboť správce údajů (či jakákoli jiná osoba) má stále přístup k původním nezpracovaným údajům, i když byly ze souboru poskytovaného třetím stranám odstraněny přímé identifikátory. Pokud by však správce údajů vymazal nezpracované údaje a třetím stranám poskytoval

například pro účely statistik nebo v hlášeních o odbytu (například pro hodnocení oblíbenosti určitého výrobku a jeho vlastností).

- Údaje o vysokofrekvenčním obchodování ve finančním sektoru nebo údaje o přesném zemědělství, které pomáhají monitorovat a optimalizovat používání pesticidů, živin a vody.

Pokud však mohou být neosobní údaje jakýmkoli způsobem vztahovány k určitému jednotlivci, v důsledku čehož jej lze přímo či nepřímo identifikovat, musí být údaje považovány za osobní údaje.

Pokud například zpráva o kontrole kvality na výrobní lince umožňuje vztahovat údaje ke konkrétním pracovníkům ve výrobě (např. k těm, kteří nastavují výrobní parametry), pak jsou údaje považovány za osobní údaje a vztahuje se na ně obecné nařízení o ochraně osobních údajů. Stejná pravidla platí i v případě, že technologický vývoj a analýza údajů umožňuje konvertovat anonymizované údaje na osobní údaje. [21]

Vzhledem k tomu, že pojem osobních údajů se vztahuje na „fyzické osoby“, soubory údajů obsahující jména a kontaktní údaje právnických osob se v zásadě považují za údaje neosobní[22]. V určitých situacích však mohou představovat i údaje osobní[23]. Tak tomu bude například v případě, že jméno právnické osoby je totožné se jménem fyzické osoby, která ji vlastní, nebo pokud se informace vztahují k identifikované nebo identifikovatelné osobě[24].

2.2 Smíšené soubory údajů

Nařízení o volném toku neosobních údajů a obecné nařízení o ochraně osobních údajů přistupují k volnému pohybu údajů v EU ze dvou různých úhlů pohledu.

Nařízení o volném toku neosobních údajů stanoví obecný zákaz požadavků na lokalizaci údajů u neosobních údajů. Ustanovení čl. 4 odst. 1 tohoto nařízení zakazuje požadavky na

---

pouze agregované statistiky na vyšší úrovni, například ‚v pondělí bývá na trase X o 160 % více cestujících než v úterý‘, šlo by o anonymní údaje.“

[21] Pokud jsou osobní údaje zpracovávány protiprávně nebo způsobem, který jinak porušuje obecné nařízení o ochraně osobních údajů, jsou subjekty údajů (fyzické osoby) oprávněny podle obecného nařízení o ochraně osobních údajů podat stížnost u vnitrostátního dozorového úřadu (orgánu pro ochranu údajů) v EU nebo mají právo na účinnou soudní ochranu u vnitrostátního soudu. Příslušnost, úkoly a pravomoci vnitrostátních dozorových úřadů jsou upraveny v kapitole VI oddílu 2 obecného nařízení o ochraně osobních údajů.

[22] Ustanovení 14. bodu odůvodnění 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) stanoví, že „toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby“. Uvedené ustanovení je však třeba vykládat s ohledem na definici osobních údajů podle čl. 4 bodu 1 obecného nařízení o ochraně osobních údajů.

[23] Viz rozsudek Soudního dvora ze dne 9. listopadu 2010 ve spojených věcech *Volker und Markus Schecke GbR*, C-92/09 a *Hartmut Eifert*, C-93/09 v. *Land Hessen*, ECLI:EU:C:2010:662, bod 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_cs

lokalizaci údajů, ledaže jsou odůvodněny veřejnou bezpečností v souladu se zásadou proporcionality.

Obecné nařízení o ochraně osobních údajů kromě zajištění vysoké úrovně ochrany osobních údajů zajišťuje volný tok osobních údajů. Podle čl. 1 odst. 3 uvedeného nařízení není volný pohyb osobních údajů v Unii „z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán“. Obě nařízení společně stanoví volný pohyb „veškerých“ údajů v rámci EU. Zvláštním ustanovením jsou podrobněji věnovány oddíly 3.1 a 3.2.

Smíšené soubory údajů jsou tvořeny údaji osobními i neosobními. Smíšené soubory údajů představují v rámci ekonomiky založené na datech většinu souborů údajů a díky technologickému vývoji, jako je internet věcí (tj. digitální propojení objektů), umělá inteligence či technologie umožňující analýzu dat velkého objemu, jsou její běžnou součástí.

Příklady smíšených souborů údajů:

- daňové záznamy společnosti s uvedením jména a telefonního čísla výkonného ředitele společnosti,
- soubory údajů v bance, zejména soubory obsahující informace o klientech a podrobné údaje o transakcích, jako jsou platební služby (kreditní a debetní karty), aplikace pro řízení vztahů s partnery a úvěrové smlouvy, dokumenty obsahující směs údajů o fyzických i právnických osobách,
- anonymizované statistické údaje výzkumných institucí a shromážděné nezpracované údaje v původní podobě, jako např. odpovědi jednotlivých dotázaných na otázky v rámci statistického zjišťování,
- podniková znalostní databáze problémů v oblasti IT a jejich řešení tvořená jednotlivými hlášeními o mimořádných událostech v oblasti IT,
- údaje týkající se internetu věcí, pokud některé z nich umožňují dovozovat předpoklady o identifikovatelných osobách (např. o přítomnosti na určité adrese a uživatelských návycích), a
- analýza souboru operačních logovacích údajů výrobního zařízení ve výrobním průmyslu.

Příklad: služby řízení vztahů s klienty

Některé banky využívají služeb řízení vztahů s klienty poskytovaných třetími stranami, které v prostředí řízení vztahů s klienty vyžadují zpřístupnění údajů klienta. Údaje, které má k dispozici služba řízení vztahů s klienty, budou obsahovat veškeré informace potřebné k účinnému řízení interakce se zákazníky, jako např. poštovní a e-mailové adresy, telefonní čísla, produkty a služby, které zákazníci nakupují, či hlášení o odbytu, včetně souhrnných údajů. Tyto údaje proto mohou zahrnovat osobní i neosobní údaje o zákaznících.

V souvislosti se smíšenými soubory údajů nařízení o volném toku neosobních údajů[25] stanoví, že:

„V případě souborů údajů obsahujících jak osobní, tak neosobní údaje se toto nařízení vztahuje na část souboru údajů s neosobními údaji. Pokud jsou osobní a neosobní údaje v souboru údajů neoddělitelně propojeny, není tímto nařízením dotčeno použití nařízení (EU) 2016/679."

To znamená, že v případě souboru údajů obsahujících jak osobní, tak neosobní údaje:

- na část souboru údajů s neosobními údaji se vztahuje nařízení o volném toku neosobních údajů,
- na část souboru údajů s osobními údaji se vztahují ustanovení obecného nařízení o ochraně osobních údajů[26], a
- pokud jsou osobní a neosobní údaje v souboru údajů „neoddělitelně propojeny", na celý smíšený soubor údajů se v plném rozsahu vztahují práva a povinnosti týkající se ochrany údajů vyplývající z obecného nařízení o ochraně osobních údajů, a to i v případě, že osobní údaje tvoří jen malou část souboru údajů[27].

Tento výklad je v souladu s právem na ochranu osobních údajů, které zaručuje Listina základních práv Evropské unie[28], a 8. bodem odůvodnění nařízení o volném toku neosobních údajů[29]. V 8. bodě odůvodnění uvedeného nařízení se stanoví, že „tímto nařízením není dotčen právní rámec o ochraně fyzických osob v souvislosti se zpracováním osobních údajů…, a zejména [obecné nařízení o ochraně osobních údajů] a směrnice … (EU) 2016/680 a směrnice … 2002/58/ES".

Praktický příklad:

Společnost provozující činnost v rámci EU nabízí služby prostřednictvím určité platformy. Podniky (zákazníci) nahrávají na platformu své dokumenty, které obsahují smíšené datové soubory. Jako „správce" je podnik nahrávající dokumenty povinen zajistit, aby zpracování bylo v souladu s obecným nařízením o ochraně osobních údajů. Společnost, která nabízí služby („zpracovatel"), a tedy soubory údajů jménem správce zpracovává, je povinna tyto údaje uchovávat a zpracovávat v souladu s obecným nařízením o ochraně osobních údajů a

[25] Ustanovení čl. 2 odst. 2 uvedeného nařízení.

[26] Ustanovení čl. 1 odst. 3 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). Viz též oddíl 3.2 uvedeného nařízení.

[27] Jak se uvádí *v pracovním dokumentu útvarů Komise* Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union *[Posouzení dopadů doprovázející návrh nařízení Evropského parlamentu a Rady o rámci pro volný tok neosobních údajů v Evropské unii]* (SWD(2017) 304 final), část 1/2, s. 3, „bez ohledu na to, kolik osobních údajů je ve smíšených souborech údajů obsaženo, ve vztahu k části souboru tvořené osobními údaji je třeba plně dodržovat obecné nařízení o ochraně osobních údajů."

[28] Listina základních práv Evropské unie, Úř. věst. C 362, 26.10.2012, s. 391.

[29] Ustanovení 8. bodu odůvodnění uvedeného nařízení.

například zajistit, aby byla zaručena odpovídající úroveň zabezpečení údajů, včetně použití šifrování.

Pojem „neoddělitelně propojeny“ není vymezen ani v jednom z obou nařízení[30]. Pro praktické účely se může jednat o situaci, kdy soubor údajů obsahuje osobní i neosobní údaje, přičemž jejich oddělení by bylo buď nemožné, nebo je správce nepovažuje z hospodářského hlediska za efektivní či technicky proveditelné. Například při nákupu systémů pro řízení vztahů s klienty a hlášení o odbytu by společnost musela zdvojnásobit své náklady na software tím, že by nakoupila samostatný software pro systém řízení vztahů s klienty (osobní údaje) a systém hlášení o odbytu (souhrnné/neosobní údaje) vycházející z údajů o řízení vztahů s klienty.

Oddělení souboru údajů rovněž pravděpodobně významně sníží jeho hodnotu. Kromě toho změna povahy údajů (viz oddíl 2.1) znesnadňuje jednoznačné rozlišování mezi jednotlivými kategoriemi údajů, a tím i jejich oddělení.

Důležité je, že ani jedno z obou nařízení neukládá podnikům povinnost oddělovat soubory údajů, které spravují nebo zpracovávají.

Na smíšený soubor údajů se proto budou obecně vztahovat povinnosti správců a zpracovatelů údajů a musí respektovat práva subjektů údajů stanovená v obecném nařízení o ochraně osobních údajů.

Zpracování údajů o zdravotním stavu

Údaje o zdravotním stavu mohou tvořit součást smíšeného souboru údajů. Příklady zahrnují elektronické zdravotní záznamy, klinická hodnocení nebo soubory údajů shromážděných různými mobilními aplikacemi na podporu tělesné a duševní pohody (např. aplikacemi pro sledování hodnot týkajících se našeho zdravotního stavu, aplikacemi, které nám připomínají, kdy máme užívat léky, nebo aplikacemi pro sledování pokroku při zlepšování fyzické kondice)[31]. Přesné rozlišení mezi osobními a neosobními údaji v těchto souborech údajů se s ohledem na technologický vývoj stále více stírá. Zpracování těchto údajů proto musí být v souladu s obecným nařízením o ochraně osobních údajů, zejména (vzhledem k tomu, že údaje o zdravotním stavu tvoří podle nařízení zvláštní kategorii údajů) s článkem 9, který stanoví obecný zákaz zpracování zvláštních kategorií osobních údajů a výjimky z tohoto zákazu.

Údaje ve smíšených souborech údajů obsahující údaje o zdravotním stavu mohou být cenným zdrojem informací, např. pro další lékařský výzkum, pro stanovení vedlejších účinků předepsaného léčivého přípravku, pro statistické účely, co se určitého onemocnění týče, nebo pro vývoj nových zdravotnických služeb nebo léčebných postupů. Požadavky obecného

[30] Nařízení o volném toku neosobních údajů a obecné nařízení o ochraně osobních údajů.

[31] Vývoj a provozování mobilních zdravotnických aplikací vyžaduje důsledné dodržování obecného nařízení o ochraně osobních údajů. Tyto požadavky budou dále zpřesněny v kodexu chování pro ochranu soukromí v souvislosti s mobilními zdravotnickými aplikacemi, který se v současné době připravuje. Bližší informace o stavu přípravy kodexu naleznete na adrese: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

nařízení o ochraně osobních údajů musí být splněny už při provádění prvotních operací zpracování, jakož i při provádění dalších operací zpracování údajů. Každé takové zpracování údajů o zdravotním stavu musí mít proto platný právní základ[32] a náležité odůvodnění a musí být zabezpečené a poskytovat dostatečné záruky.

Je současně nezbytné, aby jednotlivci a společnosti měli právní jistotu a důvěru ve zpracování údajů. To má zásadní význam i pro ekonomiku založenou na datech. Tato dvě nařízení tuto jistotu a důvěru zajišťují a obě sledují stejný cíl, tj. nenarušit volný pohyb údajů.

3 Volný tok údajů a odstranění požadavků na lokalizaci údajů

Tento oddíl podrobněji vysvětluje pojmy požadavků na lokalizaci údajů v nařízení o volném toku neosobních údajů a zásadu volného pohybu v obecném nařízení o ochraně osobních údajů. I když jsou tato ustanovení určena členským státům, může být pro podniky poučné, získají-li přesnější představu o tom, jak obě nařízení přispívají k volnému pohybu všech údajů v rámci EU.

3.1 Volný pohyb neosobních údajů

V nařízení o volném toku neosobních údajů[33] se stanoví, že „požadavky na lokalizaci údajů jsou zakázány, ledaže jsou odůvodněny veřejnou bezpečností v souladu se zásadou proporcionality“.

Požadavky na lokalizaci údajů se definuje[34] jako „jakákoli povinnost, zákaz, podmínka, omezení nebo jiný požadavek stanovený právními nebo správními předpisy členských států nebo vyplývající z obecných a stálých správních postupů členských států a veřejnoprávních subjektů, mimo jiné v oblasti zadávání veřejných zakázek, aniž by byla dotčena směrnice 2014/24/EU, který vyžaduje, aby zpracování údajů probíhalo na území určitého členského státu, nebo znesnadňuje zpracování údajů v kterémkoli jiném členském státě“[35].

Z definice vyplývá, že opatření omezující volný pohyb údajů v rámci EU mohou mít různé podoby. Mohou být stanovena formou zákonů, právních a správních předpisů nebo dokonce vyplývat z obecných a stálých správních postupů. Zákaz požadavků na lokalizaci údajů navíc zahrnuje přímá i nepřímá opatření, která by omezovala volný pohyb neosobních údajů.

Přímé požadavky na lokalizaci údajů mohou spočívat například v povinnosti uchovávat údaje na určitém zeměpisném místě (např. servery musí být umístěny v určitém členském

[32] Viz čl. 6 odst. 1 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).

[33] Ustanovení čl. 4 odst. 1 uvedeného nařízení.

[34] Ustanovení čl. 3 bodu 5 nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[35] Připomínáme, že možnosti výběru, které jsou účastníkům trhu a veřejnému sektoru k dispozici, pokud jde o místo zpracování údajů, jsou dále omezeny právní nejistotou ohledně rozsahu legitimních a nelegitimních požadavků na lokalizaci údajů (viz 4. bod odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii).

státě) nebo povinnosti dodržovat jedinečné vnitrostátní technické požadavky (např. údaje musí používat konkrétní vnitrostátní formáty).

Nepřímé požadavky na lokalizaci údajů, které by bránily zpracování neosobních údajů v kterémkoli jiném členském státě, mohou mít různé podoby. Mohou zahrnovat požadavky na používání technologických zařízení, jimž byla vydána osvědčení nebo jež jsou schválena v rámci určitého členského státu, nebo jiné požadavky, jejichž účinkem je, že znesnadňují zpracování údajů mimo určitou zeměpisnou oblast nebo území v rámci Evropské unie[36, 37].

Posouzení, zda konkrétní opatření představuje nepřímý požadavek na lokalizaci údajů, musí zohledňovat konkrétní okolnosti každého případu.

V nařízení o volném toku neosobních údajů[38] se používá pojem **veřejná bezpečnost**, jak jej vysvětluje judikatura Soudního dvora Evropské unie. Pojem veřejná bezpečnost „zahrnuje jak vnitřní, tak vnější bezpečnost členského státu[39], jakož i otázky ochrany obyvatelstva, zejména pokud jde o usnadnění vyšetřování, odhalení a stíhání trestné činnosti. Předpokládá existenci skutečné a dostatečně vážné hrozby pro některý ze základních zájmů společnosti[40], jako je např. ohrožení chodu veřejných institucí a základních veřejných služeb a přežití obyvatelstva, a dále rizik vážného narušení zahraničních vztahů, mírového soužití národů nebo vojenských zájmů.“

Kromě toho musí být veškeré požadavky na lokalizaci údajů zdůvodňované veřejnou bezpečností přiměřené. V souladu s judikaturou Soudního dvora Evropské unie zásada proporcionality vyžaduje, aby byla přijatá opatření vhodná k zajištění splnění sledovaného cíle a nepřekračovala meze toho, co je pro tento účel nezbytné[41].

---

[36] Ustanovení 4. bodu odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[37] Viz dvě studie o požadavcích na lokalizaci údajů, které byly provedeny před přijetím nařízení o volném toku neosobních údajů: 1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market* [Usnadnění přeshraničních toků údajů v rámci jednotného digitálního trhu], SMART č. 2015/2016. K dispozici na webových stránkách na adrese: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185; a 2) Time.lex, Spark Legal Network a Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions* [Přeshraniční tok údajů v rámci jednotného digitálního trhu: studie o omezeních vztahujících se na lokalizaci údajů]. SMART č. 2015/0054. K dispozici na webových stránkách na adrese: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695.

[38] Ustanovení 19. bodu odůvodnění uvedeného nařízení.

[39] Viz například rozsudek Soudního dvora ze dne 23. listopadu 2010, *Land Baden-Württemberg* v. *Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, bod 43, a rozsudek ze dne 4. dubna 2017, *Sahar Fahimian* v. *Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, bod 39.

[40] Viz například rozsudek Soudního dvora ze dne 22. prosince 2008, *Komise Evropských společenství* v. *Rakouská republika*, C-161/07, ECLI:EU:C:2008:759, bod 35 a judikatura uvedená v tomto rozsudku a rozsudek ze dne 26. března 2009, *Komise Evropských společenství* v. *Italská republika*, C-326/07, ECLI:EC:C:2009:193, bod 70 a judikatura uvedená v tomto rozsudku.

[41] Viz například rozsudek Soudního dvora ze dne 8. července 2010, *Afton Chemical Limited* v. *Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, bod 45 a judikatura uvedená v tomto rozsudku.

V zájmu jasnosti nejsou zákazem požadavků na lokalizaci údajů dotčena už existující omezení stanovená v právu EU[42].

Nařízení o volném toku neosobních údajů navíc neukládá podnikům žádné povinnosti ani neomezuje jejich smluvní svobodu rozhodovat o tom, kde mají být jejich údaje zpracovávány.

Členské státy mají povinnost zveřejnit podrobnosti o veškerých požadavcích na lokalizaci údajů platných na jejich území prostřednictvím **jednotného vnitrostátního online informačního místa** (vnitrostátních webových stránek). Průběžně tyto údaje aktualizují nebo poskytují aktualizované podrobné informace ústřednímu informačnímu místu zřízenému jiným aktem EU[43]. Pro potřeby podniků a za účelem zajištění jejich snadného přístupu k příslušným informacím v celé EU zveřejní Komise odkazy na tato informační místa na portálu Vaše Evropa[44].

3.2 Volný pohyb osobních údajů

V obecném nařízení o ochraně osobních údajů[45] se stanoví, že „volný pohyb osobních údajů v Unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán“.

Pokud některý členský stát uloží požadavky na lokalizaci osobních údajů z jiného důvodu než z důvodu ochrany osobních údajů, bude třeba tyto požadavky posuzovat s ohledem na ustanovení týkající se základních svobod a oprávněných důvodů pro odchylky od těchto svobod stanovených ve Smlouvě o fungování Evropské unie[46, 47] a v příslušných právních předpisech EU, jako je směrnice o službách[48] a směrnice o elektronickém obchodu[49].

---

42 Viz například čl. 245 odst. 2 směrnice 2006/112/ES ze dne 28. listopadu 2006 o společném systému daně z přidané hodnoty, v němž se stanoví, že „členské státy mohou požadovat, aby jim osoby povinné k dani usazené na jejich území oznámily místo uchovávání faktur, pokud je mimo jejich území“. Tento požadavek však musí být vykládán v souladu s článkem 249, v němž se stanoví, že: „Uchovává-li osoba povinná k dani faktury, které vystavuje nebo přijímá, elektronickými prostředky zajišťujícími přístup on-line k údajům a nachází-li se místo uchovávání v jiném členském státě, než kde je usazena, jsou příslušné orgány členského státu, v němž je usazena, pro účely této směrnice oprávněny mít přístup k těmto fakturám pomocí elektronických prostředků, stahovat je a používat je v mezích stanovených předpisy členského státu, ve kterém je osoba povinná k dani usazena, a v rozsahu, ve kterém je tento stát potřebuje pro účely kontroly.“

43 Ustanovení čl. 4 odst. 4 nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

44 https://europa.eu/youreurope/index.htm

45 Ustanovení čl. 1 odst. 3 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).

46 Konsolidované znění Smlouvy o fungování Evropské unie, Úř. věst. C 326, 26.10.2012, s. 47.

47 Viz též rozsudek Soudního dvora ze dne 19. června 2008, *Komise Evropských společenství* v. *Lucemburské velkovévodství*, C-319/06, ECLI:EU:C:2008:350, body 90–91: Soudní dvůr dospěl k závěru, že povinnost poskytnout a uchovávat určité dokumenty v konkrétním členském státě představuje omezení volného pohybu služeb; skutečnost, že by přítomnost těchto dokumentů „mohla obecně usnadňovat výkon kontrolní úlohy orgány tohoto státu“ k odůvodnění nestačí.

48 Směrnice Evropského parlamentu a Rady 2006/123/ES ze dne 12. prosince 2006 o službách na vnitřním trhu, Úř. věst. L 376, 27.12.2006, s. 36.

Příklad:

Určité vnitrostátní právo ukládá, aby byly mzdové účty umístěny v určitém členském státě z důvodů souvisejících s regulačním dohledem, např. ze strany vnitrostátního správce daně. Takové vnitrostátní ustanovení by do oblasti působnosti čl. 1 odst. 3 obecného nařízení o ochraně osobních údajů nespadalo, jelikož důvody by byly jiné než ochrana osobních údajů. Tento požadavek by musel být namísto toho posuzován s ohledem na ustanovení týkající se základních svobod a oprávněných důvodů pro odchylky od těchto svobod stanovených ve Smlouvě o fungování Evropské unie.

Obecné nařízení o ochraně osobních údajů[50] uznává, že členské státy mohou zavádět podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu. Tím by však, jak se uvádí v 53. bodě odůvodnění, neměl být omezen volný pohyb osobních údajů v rámci Unie, pokud se tyto podmínky uplatní na přeshraniční zpracování takových údajů. To je v souladu s článkem 16 Smlouvy o fungování Evropské unie, který poskytuje právní základ pro přijetí pravidel týkajících se práva na ochranu osobních údajů a pravidel týkajících se volného pohybu těchto údajů.

3.3 Oblast působnosti nařízení o volném toku neosobních údajů

Jak již bylo uvedeno, záměrem nařízení o volném toku neosobních údajů je zajistit volný pohyb neosobních údajů „v rámci Unie“[51]. Nevztahuje se proto na zpracování údajů, které probíhá mimo Unii, ani na požadavky na lokalizaci těchto údajů[52, 53].

Oblast působnosti nařízení se proto v souladu s čl. 2 odst. 1 omezuje na zpracování elektronických neosobních údajů v EU, které je:

(a) poskytováno jako služba uživatelům, kteří mají bydliště nebo jsou usazení v EU, bez ohledu na to, zda je v EU usazen poskytovatel služeb, či nikoli; nebo
(b) prováděno fyzickou nebo právnickou osobou, která má bydliště nebo je usazena v EU, pro její vlastní potřebu.

---

[49] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“), Úř. věst. L 178, 17.7.2000, s. 1.

[50] Ustanovení čl. 9 odst. 4 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).

[51] Viz článek 1 nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[52] Viz 15. bod odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[53] Pojem „zpracování“ je definován široce (čl. 3 bod 2 nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii), a jak je zdůrazněno v 17. bodě odůvodnění, nařízení by se mělo použít na zpracování údajů v nejširším slova smyslu a zahrnovat používání všech typů IT systémů.

Příklady:

Ustanovení čl. 2 odst. 1 písm. a) nařízení o volném toku neosobních údajů:

- Poskytovatel cloudových služeb usazený v USA poskytuje své služby zpracování údajů zákazníkům, kteří mají bydliště nebo jsou usazeni v EU. Poskytovatel cloudových služeb provádí svou činnost prostřednictvím serverů umístěných na území EU, kde jsou uloženy nebo jinak zpracovávány údaje jeho evropských zákazníků. Poskytovatel cloudových služeb nemusí vlastnit infrastrukturu umístěnou v EU, ale může si např. také pronajímat prostor na serveru v EU. Na toto zpracování se nařízení o volném toku neosobních údajů vztahuje.
- Poskytovatel cloudových služeb, který je usazen v Japonsku, poskytuje své služby evropským zákazníkům. Zpracovatelské kapacity poskytovatele se nacházejí v Japonsku a veškeré zpracovatelské činnosti probíhají zde. Na tento případ se nařízení o volném toku neosobních údajů nevztahuje, jestliže veškeré zpracovatelské činnosti probíhají mimo EU[54].

Ustanovení čl. 2 odst. 1 písm. b) nařízení o volném toku neosobních údajů:

- Malý evropský začínající podnik z členského státu A se rozhodne rozšířit své podnikání a otevře provozovnu v členském státě B. V zájmu minimalizace nákladů se rozhodne centralizovat ukládání a zpracování údajů nové provozovny na svém serveru, který se nachází v členském státě A. Členské státy nesmějí tuto snahu o centralizaci informačních technologií zakázat, ledaže je to odůvodněno veřejnou bezpečností v souladu se zásadou proporcionality.

Přestože se nařízení o volném toku neosobních údajů nevztahuje na případy, kdy je veškeré zpracování neosobních údajů prováděno mimo EU, pokud jsou součástí souboru údajů osobní údaje, je třeba dodržovat obecné nařízení o ochraně osobních údajů. Zejména musí být v každém případě dodržována pravidla pro předávání osobních údajů do třetích zemí nebo mezinárodním organizacím stanovená v obecném nařízení o ochraně osobních údajů[55].

[54] Připomínáme, že nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii se nevztahuje na požadavky na lokalizaci údajů uložené členskými státy, pokud jde o uchovávání neosobních údajů ve třetích zemích, které mohou být obsaženy ve vnitrostátních právních řádech. V zájmu jasnosti je třeba uvést, že se obecné nařízení o ochraně osobních údajů vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v EU, správcem nebo zpracovatelem, který není usazen v EU, pokud činnosti zpracování souvisejí: a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba, nebo b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie (viz čl. 3 odst. 2 obecného nařízení o ochraně osobních údajů).

[55] Informace související s předáváním osobních údajů do třetích zemí naleznete na webových stránkách Komise: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_cs a ve *sdělení Komise Evropskému parlamentu a Radě – Výměna a ochrana osobních údajů v globalizovaném světě*, COM(2017) 07 final, k dispozici na adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM%3A2017 %3A7 %3AFIN. Komise dne 23. ledna 2019 přijala ve vztahu k Japonsku tzv. rozhodnutí o odpovídající ochraně, jež umožní volný pohyb osobních údajů mezi oběma ekonomikami založený na silných zárukách ochrany těchto údajů.

3.4 Činnosti související s vnitřní organizací členských států

Nařízení o volném toku neosobních údajů neukládá členským státům povinnost prostřednictvím externích poskytovatelů zajišťovat služby související s neosobními údaji, které si přejí poskytovat samy nebo je organizovat jiným způsobem než prostřednictvím zadávání veřejných zakázek[56].

Ustanovení čl. 2 odst. 3 druhého pododstavce nařízení o volném toku neosobních údajů uvádí:

„Tímto nařízením nejsou dotčeny právní a správní předpisy týkající se **vnitřní organizace** členských států a kterými se veřejným orgánům a veřejnoprávním subjektům uvedeným v čl. 2 odst. 1 bodu 4 směrnice 2014/24/EU[57] přidělují pravomoci a povinnosti související se **zpracováním údajů, a to bez smluvní odměny soukromých stran**, ani právní a správní předpisy členských států, kterými se upravuje výkon těchto pravomocí a povinností.“[58]

Mohou existovat oprávněné zájmy, které by vyžadovaly, aby veřejné orgány služby zpracování údajů „zajišťovaly samy“, jako např. „interně“ nebo prostřednictvím vzájemných ujednání mezi orgány veřejné správy. Typické příklady zahrnují využívání „cloudu spravovaného vládními institucemi“ nebo situaci, kdy vládní instituce využívají centralizované IT agentury s cílem poskytovat služby zpracování údajů veřejným orgánům a veřejnoprávním subjektům.

Nařízení o volném toku neosobních údajů však členské státy vyzývá, aby hospodářské a jiné výhody zajištění služeb externími poskytovateli zvážily[59, 60]. Jakmile vnitrostátní orgány začnou zajišťovat služby zpracování údajů externími poskytovateli spojené se smluvní odměnou soukromých stran a probíhá-li toto zpracování v EU, vztahuje se na ně nařízení o volném toku neosobních údajů, což znamená, že se na obecné a správní postupy vnitrostátních orgánů vztahuje zásada volného toku neosobních údajů. Konkrétně to znamená, že nesmí nadále omezovat lokalizaci údajů, např. při zadávání veřejných zakázek[61].

---

[56] Ustanovení 14. bodu odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[57] Podle čl. 2 odst. 1 bodu 4 směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES, Úř. věst. L 94, 28.3.2014, s. 65, se „‚veřejnoprávními subjekty‘ rozumějí subjekty se všemi těmito vlastnostmi: a) jsou založeny za zvláštním účelem spočívajícím v uspokojování potřeb obecného zájmu, které nemají průmyslovou nebo obchodní povahu; b) mají právní subjektivitu a c) jsou financovány převážně státem, regionálními nebo místními orgány nebo jinými veřejnoprávními subjekty; nebo podléhají řídicímu dohledu těchto orgánů nebo subjektů; nebo je v jejich správním, řídícím nebo dozorčím orgánu více než polovina členů jmenována státem, regionálními nebo místními orgány nebo jinými veřejnoprávními subjekty.“

[58] Ustanovení 13. bodu odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii upozorňuje, že směrnice 2014/24/EU není nařízením dotčena.

[59] Ustanovení 14. bodu odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

[60] Externím poskytovatelem služeb je míněn jakýkoli subjekt, který není „veřejnoprávním subjektem“ ve smyslu čl. 2 odst. 1 bodu 4 směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES, Úř. věst. L 94, 28.3.2014, s. 65.

[61] Ustanovení 13. bodu odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

4 Přístupy založené na samoregulaci k podpoře volného toku údajů

Samoregulace přispívá k inovacím a důvěře mezi účastníky trhu a dokáže lépe reagovat na změny na trhu. Tento oddíl poskytuje přehled iniciativ v oblasti samoregulace ve vztahu ke zpracování osobních i neosobních údajů.

4.1 Přenesení údajů a změna poskytovatele cloudových služeb

Jedním z účelů nařízení o volném toku neosobních údajů je zabránit praxi obchodních proprietárních uzamčení (tzv. *vendor lock-in*). Jedná se o praxi, kdy uživatelé nemohou změnit poskytovatele služeb, protože jejich údaje jsou „uzamčeny“ v systému poskytovatele, například kvůli specifickému formátu údajů nebo smluvním ujednáním, a jejich přenos mimo systém IT poskytovatele není možný. Možnost přenést údaje bez obtíží je důležitá, aby uživatelé měli možnost svobodně si volit poskytovatele služeb zpracování údajů a byla tak zajištěna účinná hospodářská soutěž na trhu.

Přenositelnost údajů mezi podniky se stává čím dál tím důležitější v celé řadě digitálních odvětví, včetně cloudových služeb.

Podle článku 6 nařízení o volném toku neosobních údajů Komise s cílem přispět konkurenceschopné ekonomice založené na datech podporuje a usnadňuje tvorbu samoregulačních kodexů chování na úrovni Unie (dále jen „kodexy chování“). Vytváří základ, na němž může odvětví vypracovat samoregulační kodexy chování týkající se změny poskytovatele služeb a přenosu údajů mezi různými systémy IT.

Při tvorbě těchto kodexů chování týkajících se přenosu údajů je třeba zohlednit řadu hledisek, jako jsou:

- **osvědčené postupy** pro usnadnění změny poskytovatele služeb a přenosu údajů ve strukturovaném, běžně používaném a strojově čitelném formátu,
- **minimální požadavky na informace**, které zajistí, aby byly profesionálním uživatelům před uzavřením smlouvy poskytnuty dostatečně podrobné a jasné informace o postupech, technických požadavcích, časových rámcích a poplatcích, které se uplatní v případě, že si profesionální uživatel přeje změnit poskytovatele služeb nebo přenést údaje zpět do svých vlastních IT systémů,
- **přístupy k systémům certifikace** pro lepší srovnatelnost cloudových služeb a
- **plány v oblasti komunikace** s cílem zvýšit informovanost o kodexech chování.

V oblasti trhu s cloudovými službami začala Komise podporovat činnost pracovních skupin zúčastněných stran cloudových služeb v rámci jednotného digitálního trhu, které sdružují odborníky v oblasti cloudových služeb a jejich profesionální uživatele, včetně malých a středních podniků. V této fázi jde o jednu podskupinu, která připravuje samoregulační kodexy chování pro přenos údajů a změnu poskytovatele cloudových služeb (pracovní skupina

SWIPO)[62], a další podskupinu, která připravuje systém osvědčení zabezpečení cloudových služeb (pracovní skupina CSPCERT)[63].

Pracovní skupina SWIPO vypracovává kodexy chování pokrývající celé spektrum cloudových služeb; infrastruktura jako služba (IaaS), platforma jako služba (PaaS) a software jako služba (SaaS).

Komise očekává, že jednotlivé kodexy chování doplní **vzorové smluvní doložky**[64]. Ty umožní, aby provádění a uplatňování kodexů chování v praxi probíhalo s dostatečnou technickou a právní specifičností, což bude mít význam zejména pro malé a střední podniky. Vypracování návrhu vzorových smluvních doložek je plánováno po dokončení kodexů chování (které by měly být připraveny do 29. listopadu 2019).

V souladu s článkem 8 nařízení o volném toku neosobních údajů Komise vyhodnotí provádění nařízení, a to do 29. listopadu 2022. To umožní posoudit: i) dopad na volný tok údajů v Evropě; ii) uplatňování nařízení, zejména pokud jde o smíšené soubory údajů; iii) do jaké míry členské státy účinně zrušily stávající neodůvodněná omezení týkající se lokalizace údajů; a iv) účinnost, s níž se kodexy chování v oblasti přenosu údajů a změny poskytovatele cloudových služeb projeví na trhu.

Pojem přenositelnosti a vzájemné působení s obecným nařízením o ochraně osobních údajů

Pojem přenositelnosti údajů se vyskytuje v obou nařízeních[65] a záměrem obou nařízení je usnadnit přenos údajů z jednoho IT prostředí do jiného, tj. buď do systémů jiných poskytovatelů, nebo vlastních systémů. Zabraňuje se tak praxi obchodních proprietárních uzamčení a posiluje se hospodářská soutěž mezi poskytovateli služeb. Nařízení se však liší svým přístupem k přenositelnosti, pokud jde o vztah mezi cílovými zájmovými skupinami a právní povahou ustanovení.

Právo na přenositelnost osobních údajů podle článku 20 obecného nařízení o ochraně osobních údajů se zaměřuje na vztah mezi subjektem údajů a správcem. Týká se práva subjektu údajů obdržet osobní údaje, které poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a práva na jejich přenos k jinému správci nebo do vlastního úložiště, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil[66]. Subjekty údajů v tomto vztahu jsou obvykle spotřebiteli různých online služeb, kteří si přejí provést změnu poskytovatele služeb.

---

62 Pracovní skupina pro změnu poskytovatelů cloudových služeb a přenos údajů.

63 Evropská pracovní skupina pro systém osvědčení poskytovatelů cloudových služeb. Viz též oddíl 4.3.

64 Viz 30. bod odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

65 Článek 6 nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii a článek 20 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).

66 Viz pracovní skupina zřízená podle článku 29: *Pokyny k právu na přenositelnost údajů*. WP 242 rev.01, přijaté dne 13. prosince 2016 ve znění poslední revize ze dne 5. dubna 2017.

Článek 6 nařízení o volném toku neosobních údajů nestanoví právo profesionálních uživatelů na přenesení údajů, ale podporuje odvětví v uplatňování samoregulačního přístupu prostřednictvím dobrovolných kodexů chování. Zároveň se zaměřuje na situaci, kdy profesionální uživatel zadá zpracování svých údajů třetí straně, která zajišťuje služby zpracování údajů[67]. V souladu s čl. 3 bodem 8 nařízení o volném toku neosobních údajů může „profesionální uživatel" zahrnovat „fyzickou nebo právnickou osobu, včetně veřejného orgánu nebo veřejnoprávního subjektu, která využívá nebo požaduje službu zpracování údajů pro účely související s její obchodní činností, podnikáním, řemeslem, profesí či úlohou".

V praxi se přenositelnost podle článku 6 nařízení o volném toku neosobních údajů týká vzájemných kontaktů na úrovni podniků mezi profesionálním uživatelem (který může v případech zahrnujících zpracování osobních údajů představovat „správce" ve smyslu obecného nařízení o ochraně osobních údajů) a poskytovatelem služeb (který bude v některých případech analogicky „zpracovatelem").

Navzdory rozdílům se mohou vyskytnout situace, kdy by se na přenos údajů v souvislosti se smíšenými soubory údajů vztahovalo jak nařízení o volném toku neosobních údajů, tak obecné nařízení o ochraně osobních údajů.

Příklad:

Podnik, který využívá určitou cloudovou službu, se rozhodne změnit poskytovatele cloudových služeb a přenést veškeré údaje k novému poskytovateli. Změna poskytovatele služeb a přenos údajů je předmětem smlouvy mezi zákazníkem a poskytovatelem cloudových služeb. Pokud se původní poskytovatel cloudových služeb řídí kodexem chování vypracovaným na základě nařízení o volném toku neosobních údajů, přenos údajů musí probíhat v souladu s požadavky v něm uvedenými.

Pokud jsou součástí přenášených souborů údajů také osobní údaje, musí přenos probíhat v souladu se všemi příslušnými ustanoveními obecného nařízení o ochraně osobních údajů, a zejména musí zajišťovat, aby nový poskytovatel cloudových služeb splňoval příslušné požadavky, jako jsou např. požadavky na zabezpečení[68].

Příklad:

V případě, že se banka rozhodne změnit poskytovatele řízení vztahů s klienty, může se stát, že bude třeba přenést některé (osobní i neosobní) údaje od původního poskytovatele k novému. Na tyto údaje se pak budou vztahovat různé regulatorní požadavky, z nichž některé vyplývají

[67] Ustanovení 29. bodu odůvodnění nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii: „Zatímco individuální spotřebitelé požívají výhod zakotvených ve stávajícím právu Unie [tj. v obecném nařízení o ochraně osobních údajů], uživatelům jednajícím v rámci své podnikatelské nebo profesní činnosti není změna poskytovatele služeb usnadňována."

[68] Viz pracovní skupina zřízená podle článku 29: *Stanovisko č. 05/2012 ke cloud computingu* přijaté dne 1. července 2012, WP196, které blíže upřesňuje postavení a povinnosti uživatelů a poskytovatelů cloudových služeb v souvislosti se zpracováním osobních údajů.

z obecného nařízení o ochraně osobních údajů a další z nařízení o volném toku neosobních údajů.

4.2 Kodexy chování a systémy pro vydávání osvědčení o ochraně osobních údajů

K prokázání souladu s povinnostmi podle obecného nařízení o ochraně osobních údajů (viz čl. 24 odst. 3 a čl. 28 odst. 5) je možné použít kodexy chování a systémy pro vydávání osvědčení.

V souladu s čl. 40 odst. 1 a čl. 42 odst. 1 obecného nařízení o ochraně osobních údajů by členské státy, dozorové úřady, Evropský sbor pro ochranu osobních údajů a Komise měly odvětví povzbuzovat k vypracování kodexů chování a k zavedení mechanismů pro vydávání osvědčení o ochraně údajů.

Kodex chování pro konkrétní odvětví mohou připravit sdružení nebo jiné subjekty zastupující konkrétní kategorii správců nebo zpracovatelů. Návrh kodexu musí být předložen příslušnému dozorovému úřadu ke schválení[69]. Pokud se návrh kodexu chování týká činností zpracování údajů v několika členských státech, dozorový úřad musí kodex před schválením předložit Evropskému sboru pro ochranu osobních údajů. Sbor následně vydá stanovisko, zda je návrh kodexu v souladu s obecným nařízením o ochraně osobních údajů.

Evropský sbor pro ochranu osobních údajů zveřejnil své pokyny č. 1/2019 týkající se kodexů chování a subjektů pro monitorování souladu s kodexem chování podle obecného nařízení o ochraně osobních údajů[70]. Pokyny obsahují informace o vypracování kodexů chování, kritéria pro jejich schvalování a další užitečné informace. Podobně pokyny Evropského sboru pro ochranu osobních údajů č. 1/2018 o vydávání osvědčení a stanovení certifikačních kritérií podle článků 42 a 43 obecného nařízení o ochraně osobních údajů poskytují informace o vydávání osvědčení podle tohoto nařízení a o vývoji a schvalování certifikačních kritérií[71].

Příklady kodexů chování vytvořených odvětvím cloud computingu:

Kodex chování EU v oblasti cloud computingu, který vznikl za podpory Komise, byl vypracován ve spolupráci se skupinou pro spolupráci subjektů v oblasti cloud computingu *Cloud Select Industry Group* (C-SIG) na základě směrnice o ochraně údajů[72] a následně

[69] Viz čl. 40 odst. 5 a článek 55 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).

[70] Evropský sbor pro ochranu osobních údajů: *Pokyny č. 1/2019 týkající se kodexů chování a subjektů pro monitorování podle nařízení 2016/679*, přijaté dne 12. února 2019, verze pro veřejnou konzultaci, k dispozici na internetové adrese: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_cs.

[71] Evropský sbor pro ochranu osobních údajů: *Pokyny č. 1/2018 o vydávání osvědčení a určování kritérií pro vydávání osvědčení podle článků 42 a 43 nařízení 2016/679*, přijaté dne 23. ledna 2019, k dispozici na internetové adrese: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_cs.

[72] 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 (datum ukončení platnosti: 24. května 2018).

obecného nařízení o ochraně osobních údajů. Kodex chování EU v oblasti cloud computingu pokrývá celé spektrum cloudových služeb – software jako služba (SaaS), platforma jako služba (PaaS) a infrastruktura jako služba (IaaS)[73].

Kodex chování poskytovatelů služeb infrastruktury cloud computingu v Evropě (CISPE)[74] se zaměřuje na poskytovatele IaaS. Kodex chování CISPE se skládá z požadavků týkajících se poskytovatelů IaaS, kteří působí jako zpracovatelé údajů ve smyslu obecného nařízení o ochraně osobních údajů. Obsahuje rovněž ustanovení týkající se správní struktury provádění a uplatňování kodexu.

Kodex chování Aliance pro zabezpečení cloud computingu s ohledem na soulad s požadavky obecného nařízení o ochraně osobních údajů se zaměřuje na všechny zúčastněné subjekty v oblasti cloud computingu a evropských právních předpisů v oblasti osobních údajů, jako jsou poskytovatelé cloudových služeb, zákazníci využívající cloudových služeb a potenciální zákazníci, cloudoví auditoři a zprostředkovatelé cloudových služeb. Kodex chování pokrývá celé spektrum poskytovatelů cloudových služeb[75].

4.3 Posílení důvěry v přeshraniční zpracování údajů – osvědčení zabezpečení

Jak je uvedeno v 33. bodě odůvodnění nařízení o volném toku neosobních údajů, posílením důvěry v bezpečnost přeshraničního zpracování údajů by se měla omezit tendence účastníků trhu a veřejného sektoru používat lokalizaci údajů jako náhražku bezpečnosti údajů. Vedle balíčku týkajícího se kybernetické bezpečnosti, který navrhla Komise v roce 2017[76], připravuje pracovní skupina CSPCERT doporučení pro účely vytvoření evropského systému osvědčení cloud computingu, která budou předložena Komisi. Tento systém může usnadnit volný pohyb údajů, umožnit lepší srovnatelnost cloudových služeb a podpořit zavádění cloud computingu. Komise může uložit agentuře ENISA (Agentura Evropské unie pro kybernetickou bezpečnost), aby připravila konkrétní návrh systému v souladu s příslušnými ustanoveními aktu o kybernetické bezpečnosti[77]. Tento systém se může zaměřovat na osobní i neosobní údaje. Kromě aktu o kybernetické bezpečnosti – a jak je také zdůrazněno v oddíle 4.2 – lze k prokázání existence vhodných záruk o zabezpečení údajů použít rovněž obecné nařízení o ochraně osobních údajů[78].

Závěrečné poznámky

Právní jistota a důvěra ve zpracování údajů jsou nezbytným předpokladem pro to, aby byla EU schopna využívat veškerý potenciál svých údajů a vytvořit podmínky pro rozvoj

[73] Bližší informace o kodexu chování EU v oblasti cloud computingu naleznete na adrese: https://eucoc.cloud/en/home.html.

[74] Bližší informace o kodexu chování CISPE naleznete na adrese: https://cispe.cloud/code-of-conduct/.

[75] Bližší informace o kodexu chování Aliance pro zabezpečení cloud computingu naleznete na adrese: https://gdpr.cloudsecurityalliance.org/.

[76] Bližší informace viz: https://ec.europa.eu/digital-single-market/en/cyber-security.

[77] Nařízení Evropského parlamentu a Rady ze dne 17. dubna 2019 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 (akt o kybernetické bezpečnosti).

[78] Viz 74. bod odůvodnění aktu o kybernetické bezpečnosti.

hodnotových řetězců napříč odvětvími a hranicemi. Tato dvě nařízení tuto jistotu a důvěru zajišťují a obě sledují stejný cíl, kterým je volný pohyb údajů. Nařízení o volném toku neosobních údajů a obecné nařízení o ochraně osobních údajů společně vytvářejí základ pro volný tok všech údajů v rámci Evropské unie a vysoce konkurenceschopnou evropskou ekonomiku založenou na datech.