EURÓPSKA
KOMISIA

V Bruseli 29. 5. 2019
COM(2019) 250 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

Usmernenie k nariadeniu o rámci pre voľný tok iných ako osobných údajov v Európskej únii

Obsah

1. Úvod ... 2

Účel tohto usmernenia ... 3

2. Vzájomné pôsobenie nariadenia o voľnom toku iných ako osobných údajov a všeobecného nariadenia o ochrane údajov – zmiešané súbory údajov ... 4

2.1 Pojem „iné ako osobné údaje“ v nariadení o voľnom toku iných ako osobných údajov 4

Osobné údaje ... 5

Iné ako osobné údaje ... 6

2.2 Zmiešané súbory údajov ... 8

3. Voľný tok údajov a odstránenie požiadaviek na lokalizáciu údajov ... 11

3.1 Voľný tok iných ako osobných údajov ... 11

3.2 Voľný tok osobných údajov ... 13

3.3 Rozsah pôsobnosti nariadenia o voľnom toku iných ako osobných údajov ... 14

3.4 Činnosti týkajúce sa vnútornej organizácie členských štátov ... 16

4. Samoregulačné prístupy podporujúce voľný tok údajov ... 17

4.1 Prenos údajov a zmena poskytovateľov cloudových služieb ... 17

Pojem prenosnosť a vzájomné pôsobenie so všeobecným nariadením o ochrane údajov ... 19

4.2 Kódexy správania a systémy certifikácie týkajúce sa ochrany osobných údajov ... 20

4.3 Posilnenie dôvery v cezhraničné spracúvanie údajov – certifikácia bezpečnosti ... 22

Záverečné poznámky ... 22

Európska komisia sprístupňuje tento dokument len na informačné účely. Neobsahuje žiadny striktný výklad nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii a nepredstavuje rozhodnutie ani stanovisko Európskej komisie. Nie sú ním dotknuté žiadne rozhodnutia ani stanoviská Európskej komisie a ani žiadne právomoci Súdneho dvora Európskej únie na výklad príslušného nariadenia v súlade so zmluvami EÚ.

1. Úvod

V rámci hospodárstva, ktoré je čoraz viac založené na údajoch, sú toky údajov základom obchodných procesov v spoločnostiach všetkých veľkostí a vo všetkých sektoroch. Nové digitálne technológie otvárajú nové príležitosti pre širokú verejnosť, podniky a orgány verejnej správy v Európskej únii (ďalej len „EÚ“).

Európsky parlament a Rada s cieľom zintenzívniť cezhraničnú výmenu údajov a posilniť dátové hospodárstvo prijali v novembri 2018 na základe návrhu Európskej komisie (ďalej len „Komisia“) nariadenie (EÚ) 2018/1807 o rámci pre voľný tok iných ako osobných údajov v Európskej únii[1] (ďalej len „nariadenie o voľnom toku iných ako osobných údajov“). Nariadenie sa uplatňuje od 28. mája 2019. Zásada voľného pohybu osobných údajov sa už stanovuje v nariadení (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)[2]. Vďaka tomu teraz existuje komplexný rámec pre spoločný európsky dátový priestor a voľný pohyb všetkých údajov v rámci Európskej únie[3].

Nariadením o voľnom toku iných ako osobných údajov sa vytvára právna istota pre podniky, vďaka ktorej môžu spracúvať svoje údaje kdekoľvek v EÚ, zvyšuje sa dôvera v služby spracúvania údajov a bojuje sa proti praktikám odkázanosti na určitého dodávateľa. Tým sa zväčší výber pre zákazníkov, zlepší sa efektívnosť a podporí sa zavádzanie cloudových technológií, čo povedie k významným úsporám pre podniky v EÚ. Z jednej štúdie vyplýva, že prechodom na cloud môžu podniky v EÚ ušetriť 20 – 50 % svojich nákladov na IT[4].

Vďaka uvedeným dvom nariadeniam môžu údaje voľne prúdiť medzi členskými štátmi, čo umožňuje používateľom služieb spracúvania údajov využívať údaje získané na rôznych trhoch EÚ na zlepšenie svojej produktivity a konkurencieschopnosti. Používatelia preto môžu naplno využívať úspory z rozsahu, ktoré poskytuje rozsiahly trh EÚ, a zároveň pritom zlepšovať svoju celosvetovú konkurencieschopnosť a zvyšovať prepojenosť európskeho dátového hospodárstva.

Nariadenie o voľnom toku iných ako osobných údajov má tri významné prvky:

- Ako pravidlo sa v ňom členským štátom zakazuje ukladať požiadavky týkajúce sa toho, kde majú byť údaje lokalizované. Výnimky z tohto pravidla môžu byť odôvodnené len verejnou bezpečnosťou v súlade so zásadou proporcionality.

---

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii, Ú. v. EÚ L 303, 28.11.2018, s. 59.

[2] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), Ú. v. EÚ L 119, 4.5.2016, s. 1.

[3] Všeobecné nariadenie o ochrane údajov sa vzťahuje aj na Európsky hospodársky priestor (EHP), ktorý zahŕňa Island, Lichtenštajnsko a Nórsko. Okrem toho sa nariadenie o voľnom toku iných ako osobných údajov označuje ako text s významom pre EHP.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe (Meranie ekonomického vplyvu cloud computingu v Európe)*, SMART 2014/0031, 2016. K dispozícii online na adrese: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- Zavádza sa ním mechanizmus spolupráce na zabezpečenie toho, aby príslušné orgány mohli naďalej uplatňovať svoje práva na prístup k údajom, ktoré sa spracúvajú v inom členskom štáte.
- Odvetvie sa ním motivuje, aby s podporou Komisie vytvorilo samoregulačné kódexy správania pri zmene poskytovateľa služieb a prenose údajov.

Účel tohto usmernenia

Toto usmernenie je v súlade s článkom 8 ods. 3 nariadenia o voľnom toku iných ako osobných údajov, podľa ktorého sa vyžaduje, aby Komisia uverejnila usmernenie o vzájomnom pôsobení tohto nariadenia a všeobecného nariadenia o ochrane údajov, „najmä pokiaľ ide o súbory údajov zložené z osobných údajov a iných ako osobných údajov“.

Cieľom tohto usmernenia je pomôcť používateľom – najmä malým a stredným podnikom – pochopiť vzájomné pôsobenie nariadenia o voľnom toku iných ako osobných údajov a všeobecného nariadenia o ochrane údajov[5]. Usmernenie sa preto zameriava predovšetkým na: i) pojmy „iné ako osobné údaje“ a „osobné údaje“; ii) zásady voľného pohybu údajov a zákazu požiadaviek na lokalizáciu údajov podľa oboch nariadení a iii) pojem „prenosnosť údajov“ podľa nariadenia o voľnom toku iných ako osobných údajov. Vzťahuje sa aj na samoregulačné požiadavky stanovené v oboch nariadeniach.

Nariadenie o voľnom toku iných ako osobných údajov sa vzťahuje len na „iné ako osobné údaje“, ako sa vymedzujú vo všeobecnom nariadení o ochrane údajov. Všeobecným nariadením o ochrane údajov sa upravuje spracúvanie osobných údajov, ktoré je základnou súčasťou rámca EÚ na ochranu údajov[6]. V členských štátoch nadobudlo účinnosť 25. mája 2018. V nariadení sa stanovujú harmonizované pravidlá na ochranu osôb v EÚ/EHP v súvislosti so spracúvaním ich osobných údajov a s voľným pohybom týchto údajov. Vo všeobecnom nariadení o ochrane údajov: i) sa spresňuje, aké informácie predstavujú osobné údaje; ii) sa stanovujú právne dôvody ich spracúvania a iii) okrem iných ustanovení sa tu

[5] Odôvodnenie 37 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

[6]
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), Ú. v. EÚ L 119/1, 4.5.2016, s. 1.
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES, Ú. v. EÚ L 295, 21.11.2018, s. 39.
- Smernica (EÚ) 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, Ú. v. EÚ L 119, 4.5.2016, s. 89.
- Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. ES L 201, 31.7.2002, s. 37 (v súčasnosti sa reviduje).

vymedzujú práva a povinnosti, ktoré sa majú dodržiavať pri spracúvaní týchto údajov[7]. Pokiaľ ide o zásadu voľného pohybu osobných údajov, v článku 1 ods. 3 všeobecného nariadenia o ochrane údajov sa stanovuje, že „voľný pohyb osobných údajov v rámci Únie sa nesmie obmedziť ani zakázať z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov“.

Vo väčšine reálnych životných situácií je veľmi pravdepodobné, že súbor údajov bude pozostávať z osobných údajov aj iných ako osobných údajov. Takýto súbor sa často nazýva „zmiešaný súbor údajov“. V oddiele 2.2 sa vysvetľuje vzájomné pôsobenie nariadenia o voľnom toku iných ako osobných údajov a všeobecného nariadenia o ochrane údajov, pokiaľ ide o zmiešané súbory údajov.

V záujme jasnosti treba uviesť, že sa nevyskytujú žiadne protichodné povinnosti vyplývajúce zo všeobecného nariadenia o ochrane údajov a z nariadenia o voľnom toku iných ako osobných údajov.

2. Vzájomné pôsobenie nariadenia o voľnom toku iných ako osobných údajov a všeobecného nariadenia o ochrane údajov – zmiešané súbory údajov

2.1 Pojem „iné ako osobné údaje“ v nariadení o voľnom toku iných ako osobných údajov

Cieľom nariadenia o voľnom toku iných ako osobných údajov[8] je zabezpečiť voľný tok iných ako osobných údajov. V celom texte nariadenia sa používa pojem „údaje“, ktorý by sa mal chápať ako „iné údaje ako osobné údaje vymedzené v článku 4 bode 1 nariadenia (EÚ) 2016/679 [všeobecné nariadenie o ochrane údajov]“ [9]. Takéto údaje, ktoré sa v tomto dokumente označujú ako „**iné ako osobné údaje**“, sa vymedzujú v protiklade (*a contrario*) k osobným údajom, ako sa stanovujú vo všeobecnom nariadení o ochrane údajov.

---

[7] Ďalšie usmernenia o rôznych aspektoch nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), a európskych právnych predpisov o ochrane údajov sa uvádzajú na webovej stránke Európskeho výboru pre ochranu údajov, ktorý v súlade s článkom 70 všeobecného nariadenia o ochrane údajov vydal niekoľko usmernení dostupných na: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_sk. Príslušná webová stránka obsahuje aj odkazy na usmernenia, odporúčania a iné dokumenty, ktoré vydal predchodca Európskeho výboru pre ochranu údajov – pracovná skupina zriadená podľa článku 29. Okrem toho na zvýšenie informovanosti občanov a podnikov o nariadení Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), Komisia vydala oznámenie o ochrane údajov – usmernenie o priamom uplatňovaní všeobecného nariadenia o ochrane údajov (COM/2018/043 final) dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

[8] Článok 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

[9] Pozri článok 3 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

Osobné údaje

Vo všeobecnom nariadení o ochrane údajov sa uvádza: „‚osobné údaje' sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba"); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby."

Široké vymedzenie osobných údajov je zámerné a vo všeobecnom nariadení o ochrane údajov sa v porovnaní s predchádzajúcimi právnymi predpismi v zásade nezmenilo[10]. Rôzne aspekty vymedzenia pojmu osobné údaje, napríklad „akékoľvek informácie", „týkajúce sa", „identifikovanej alebo identifikovateľnej", už riešila pracovná skupina zriadená podľa článku 29[11] vo svojom stanovisku 4/2007 z 20. júna 2007 o pojme osobné údaje, WP 136.

V oblastiach, ako je výskum, je bežnou praxou pseudonymizovať osobné údaje s cieľom zamaskovať totožnosť jednotlivca. **Pseudonymizácia** je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť ku konkrétnej osobe bez použitia dodatočných informácií. Tieto dodatočné informácie sa uchovávajú oddelene a sú zabezpečené organizačnými alebo technickými opatreniami (napr. šifrovaním)[12,13]. Údaje, ktoré boli pseudonymizované, sa však stále považujú za informácie o identifikovateľnej osobe, ak ich možno priradiť k tejto osobe pomocou dodatočných informácií[14]. Takéto údaje **predstavujú osobné údaje** v súlade so všeobecným nariadením o ochrane údajov.

---

10 Pozri článok 2 písm. a) smernice Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (dátum ukončenia platnosti: 24. mája 2018, zrušená všeobecným nariadením o ochrane údajov). Pozri aj judikatúru Súdneho dvora týkajúcu sa vymedzenia pojmu osobné údaje, v ktorej sa uznáva široký výklad tohto pojmu, napríklad rozsudok Súdneho dvora z 29. januára 2009, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; rozsudok Súdneho dvora z 24. novembra 2011, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; rozsudok Súdneho dvora z 19. októbra 2016, *Patrick Breyer*/*Bundersrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

11 Pracovná skupina zriadená podľa článku 29 bola poradným orgánom, ktorý poskytoval Komisii poradenstvo týkajúce sa otázok ochrany údajov a ktorý pomáhal pri tvorbe harmonizovaných politík na ochranu údajov v EÚ. Po nadobudnutí účinnosti všeobecného nariadenia o ochrane údajov 25. mája 2018 bola pracovná skupina zriadená podľa článku 29 nahradená Európskym výborom pre ochranu údajov.

12 Pozri článok 4 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), v ktorom sa vymedzuje „pseudonymizácia".

13 Napríklad výskumná štúdia o účinkoch nového lieku by sa kvalifikovala ako pseudonymizácia, ak by sa osobné údaje účastníkov štúdie nahradili vo výskumnej dokumentácii jedinečnými atribútmi (napr. číslom alebo kódom) a ich osobné údaje by sa uchovávali oddelene s pridelenými jedinečnými atribútmi v zabezpečenom dokumente (napr. v databáze chránenej heslom).

14 Pozri odôvodnenie 26 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

Iné ako osobné údaje

Ak údaje nie sú „osobnými údajmi“, ako sa vymedzujú vo všeobecnom nariadení o ochrane údajov, ide o **iné ako osobné údaje**. Iné ako osobné údaje možno kategorizovať podľa pôvodu takto:

- Po prvé, údaje, ktoré sa pôvodne netýkali identifikovanej alebo identifikovateľnej fyzickej osoby, ako sú napríklad údaje o poveternostných podmienkach generované senzormi nainštalovanými na veterných turbínach alebo údaje o potrebách údržby priemyselných strojov.

- Po druhé, údaje, ktoré boli pôvodne osobnými údajmi, ale neskôr sa stali **anonymnými**[15]. „Anonymizácia“ osobných údajov sa líši od pseudonymizácie (pozri vyššie), keďže náležite anonymizované údaje nemožno priradiť ku konkrétnej osobe, a to ani s použitím dodatočných údajov[16], a preto ide o iné ako osobné údaje.

Posúdenie, či sú údaje riadne anonymizované, závisí od konkrétnych a jedinečných okolností každého jednotlivého prípadu[17]. Na základe viacerých príkladov opätovnej identifikácie súborov údajov, ktoré boli údajne anonymizované, sa ukázalo, že takéto zhodnotenie môže byť náročné[18]. Na stanovenie toho, či je jednotlivec identifikovateľný, sa treba pozerať na všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo iná osoba použije na identifikáciu jednotlivca, a to buď priamo alebo nepriamo[19].

Príklady iných ako osobných údajov:

- Údaje, ktoré sú agregované tak, že jednotlivé udalosti (napríklad individuálne cesty danej osoby alebo jej cestovné návyky, ktoré by mohli predstavovať osobné údaje) už

[15] Pozri odôvodnenie 26 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), v ktorom sa stanovuje, že „...zásady ochrany údajov by sa preto nemali uplatňovať na anonymné informácie, konkrétne na informácie, ktoré sa nevzťahujú na identifikovanú alebo identifikovateľnú fyzickú osobu, ani na osobné údaje, ktoré sa stali anonymnými takým spôsobom, že dotknutá osoba nie je alebo už nie je identifikovateľná“.

[16] Pozri rozsudok Súdneho dvora z 19. októbra 2016, *Patrick Breyer/Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. Súdny dvor rozhodol, že dynamická adresa internetového protokolu (IP adresa) môže predstavovať osobný údaj aj vtedy, ak tretia strana (napr. poskytovateľ internetových služieb) vlastní dodatočné údaje, ktoré by umožnili identifikáciu jednotlivca. Možnosť identifikácie jednotlivca musí predstavovať prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že sa použijú na identifikáciu jednotlivca, či už priamo alebo nepriamo.

[17] Anonymizácia údajov by sa mala vždy vykonávať s použitím najnovších anonymizačných techník.

[18] Príklady opätovnej identifikácie údajne anonymizovaných údajov sa uvádzajú v štúdii o budúcich tokoch údajov, ktorú pre výbor Európskeho parlamentu ITRE vypracovali Blackman, C., Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee (Toky údajov – Budúce scenáre: hĺbková analýza pre výbor ITRE),* 2017, s. 22, Rámček 2. K dispozícii online na adrese: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf.

[19] Pozri odôvodnenie 26 nariadenia (EÚ) 2016/679 (všeobecné nariadenie o ochrane údajov), podľa ktorého „na zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj“.

nie sú identifikovateľné, možno kvalifikovať ako anonymné údaje[20]. Anonymné údaje sa používajú napríklad v štatistikách alebo v správach o predaji (napríklad na posúdenie obľúbenosti produktu a jeho vlastností).

- Údaje o vysokofrekvenčnom obchodovaní vo finančnom sektore alebo údaje o presnom poľnohospodárstve, ktoré pomáhajú monitorovať a optimalizovať používanie pesticídov, živín a vody.

Ak však iné ako osobné údaje možno akýmkoľvek spôsobom spojiť s jednotlivcom a ak môžu viesť k tomu, že tento jednotlivec bude priamo alebo nepriamo identifikovateľný, musia sa považovať za osobné údaje.

Napríklad, ak je vďaka správe o kontrole kvality na výrobnej linke možné spojiť údaje s konkrétnymi pracovníkmi v závode (napr. s tými, ktorí nastavujú výrobné parametre), údaje by sa mohli kvalifikovať ako osobné údaje a v tom prípade sa musí uplatniť všeobecné nariadenie o ochrane údajov. Rovnaké pravidlá platia vtedy, keď vývoj v oblasti technológií a analýza údajov umožňujú konvertovať anonymizované údaje na osobné údaje. [21]

Keďže vymedzenie pojmu osobné údaje sa vzťahuje na „fyzické osoby“, súbory údajov, ktoré obsahujú mená a kontaktné údaje právnických osôb, v zásade predstavujú iné ako osobné údaje[22]. V určitých situáciách však môže ísť o osobné údaje[23]. Takýto prípad nastane, ak je napríklad meno právnickej osoby rovnaké ako meno fyzickej osoby, ktorá ju vlastní, alebo ak sa informácie týkajú identifikovanej alebo identifikovateľnej fyzickej osoby[24].

---

20 Pozri: Pracovná skupina zriadená podľa článku 29: *Stanovisko č. 05/2014 o anonymizačných technikách*, prijaté 10. apríla 2014, WP216, s. 9: „Výsledný súbor údajov možno kvalifikovať ako anonymný len v prípade, že prevádzkovateľ agregoval údaje na úrovni, kde jednotlivé udalosti už nie sú identifikovateľné. Napríklad: ak organizácia zhromažďuje údaje o jednotlivých cestách, jednotlivé cestovné návyky na úrovni udalosti by sa stále kvalifikovali ako osobné údaje pre ktorúkoľvek stranu, pokiaľ prevádzkovateľ (alebo akákoľvek iná strana) má stále prístup k pôvodným nespracovaným údajom, dokonca aj v prípade, že priame identifikátory boli zo súboru poskytnutého tretím stranám odstránené. Ak by však prevádzkovateľ vymazal nespracované údaje a poskytol tretím stranám na vysokej úrovni len súhrnné štatistiky, napríklad ‚v pondelok býva na trase X o 160 % viac cestujúcich ako v utorok‘, to by sa kvalifikovalo ako anonymné údaje.“

21 Ak sa osobné údaje spracúvajú protizákonne alebo ak je spracúvanie inak v rozpore so všeobecným nariadením o ochrane údajov, dotknuté osoby (fyzické osoby) majú podľa všeobecného nariadenia o ochrane údajov právo podať sťažnosť vnútroštátnemu orgánu dohľadu (orgánu pre ochranu údajov) v EÚ alebo požiadať o účinný opravný prostriedok na vnútroštátnom súde. Úlohy, kompetencie a právomoci vnútroštátnych orgánov dohľadu sú upravené v kapitole VI oddiele 2 všeobecného nariadenia o ochrane údajov.

22 V odôvodnení 14 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), sa uvádza: „Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov, ktoré sa týka právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy a kontaktných údajov právnickej osoby.“ Toto však treba vykladať s ohľadom na vymedzenie pojmu osobné údaje v článku 4 ods. 1 všeobecného nariadenia o ochrane údajov.

23 Pozri rozsudok Súdneho dvora z 9. novembra 2010 v spojených veciach *Volker und Markus Schecke GbR* (C-92/09) a *Hartmut Eifert* (C-93/09)/*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_sk

2.2 Zmiešané súbory údajov

Nariadenie o voľnom toku iných ako osobných údajov a všeobecné nariadenie o ochrane údajov pristupujú k voľnému pohybu údajov v EÚ z dvoch rôznych uhlov.

V nariadení o voľnom toku iných ako osobných údajov sa stanovuje všeobecný zákaz požiadaviek na lokalizáciu údajov v prípade iných ako osobných údajov. Podľa článku 4 ods. 1 nariadenia sa zakazujú požiadavky na lokalizáciu údajov, pokiaľ nie sú odôvodnené verejnou bezpečnosťou v súlade so zásadou proporcionality.

Všeobecné nariadenie o ochrane údajov okrem zabezpečenia vysokej úrovne ochrany osobných údajov zabezpečuje aj voľný tok osobných údajov. V súlade s článkom 1 ods. 3 nariadenia voľný pohyb osobných údajov „sa nesmie obmedziť ani zakázať z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov“. Tieto dve nariadenia spolu zabezpečujú voľný pohyb „všetkých“ údajov v rámci EÚ. Osobitné ustanovenia sa bližšie rozvádzajú v oddieloch 3.1 a 3.2.

Zmiešaný súbor údajov pozostáva z osobných údajov aj iných ako osobných údajov. Zmiešané súbory údajov predstavujú väčšinu súborov údajov, ktoré sa používajú v dátovom hospodárstve, a vzhľadom na technologický vývoj, ako je internet vecí (t. j. digitálne prepájanie objektov), umelá inteligencia a technológie umožňujúce analýzu veľkých údajov, sú pomerne bežné.

Príklady zmiešaných súborov údajov:

- daňový záznam spoločnosti, v ktorom sa uvádza meno a telefónne číslo výkonného riaditeľa spoločnosti;
- súbory údajov v banke, najmä tie, v ktorých sa uvádzajú informácie o klientoch a podrobnosti o transakciách, ako sú platobné služby (kreditné a debetné karty), aplikácie riadenia partnerských vzťahov a zmluvy o úvere a dokumenty, v ktorých sa miešajú údaje týkajúce sa fyzických a právnických osôb;
- anonymizované štatistické údaje výskumnej inštitúcie a pôvodne získané nespracované údaje, ako sú napríklad odpovede jednotlivých respondentov na otázky štatistického zisťovania;
- znalostná databáza spoločnosti zahŕňajúca IT problémy a ich riešenia založená na individuálnych hláseniach incidentov v oblasti IT;
- údaje týkajúce sa internetu vecí, kde je na základe niektorých údajov možné vyvodiť predpoklady o identifikovateľných jednotlivcoch (napr. prítomnosť na konkrétnej adrese a užívateľské vzorce) a
- analýza údajov prevádzkových denníkov výrobných zariadení vo výrobnom priemysle.

Príklad: služby správy vzťahov s klientmi

Niektoré banky využívajú služby správy vzťahov s klientmi poskytované tretími stranami, ktoré si vyžadujú sprístupnenie údajov klienta v prostredí správy vzťahov s klientmi. Údaje uchovávané v rámci služby správy vzťahov s klientmi budú zahŕňať všetky informácie potrebné na účinné riadenie interakcie s klientom, ako je jeho poštová a e-mailová adresa, telefónne číslo, produkty a služby, ktoré si kúpil, a správy o predaji vrátane agregovaných údajov. Tieto údaje preto môžu zahŕňať osobné údaje aj iné ako osobné údaje klienta.

Pokiaľ ide o zmiešané súbory údajov, v nariadení o voľnom toku iných ako osobných údajov[25] sa stanovuje, že:

„V prípade súboru údajov pozostávajúcich z osobných údajov a iných ako osobných údajov sa toto nariadenie uplatňuje na časť súboru údajov, ktorú tvoria iné ako osobné údaje. Ak sú osobné údaje a iné ako osobné údaje v súbore údajov neoddeliteľne prepojené, toto nariadenie nemá vplyv na uplatňovanie nariadenia (EÚ) 2016/679.“

To znamená, že v prípade súboru údajov pozostávajúceho z osobných údajov aj iných ako osobných údajov:

- nariadenie o voľnom toku iných ako osobných údajov sa uplatňuje na časť súboru údajov, ktorú tvoria iné ako osobné údaje;
- ustanovenie všeobecného nariadenia o ochrane údajov týkajúce sa voľného toku[26] sa vzťahuje na časť súboru údajov, ktorú tvoria osobné údaje; a
- ak sú časť, ktorú tvoria iné ako osobné údaje, a časť, ktorú tvoria osobné údaje, „neoddeliteľne prepojené“, práva a povinnosti týkajúce sa ochrany údajov vyplývajúce zo všeobecného nariadenia o ochrane údajov sa plne uplatňujú na celý zmiešaný súbor údajov, a to aj v prípade, že osobné údaje predstavujú len malú časť tohto súboru údajov[27].

Tento výklad je v súlade s právom na ochranu osobných údajov, ktoré sa zaručuje v Charte základných práv Európskej únie[28], a s odôvodnením 8 nariadenia o voľnom toku iných ako osobných údajov[29]. V odôvodnení 8 uvedeného nariadenia sa uvádza, že „právny rámec o ochrane fyzických osôb, pokiaľ ide o spracúvanie osobných údajov [...] a najmä [všeobecné nariadenie o ochrane údajov] [...] a smernice [...] (EÚ) 2016/680 a 2002/58/ES nie sú týmto nariadením dotknuté“.

Praktický príklad:

25 Článok 2 ods. 2 uvedeného nariadenia.

26 Článok 1 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). Pozri aj oddiel 3.2 tohto nariadenia.

27 Ako sa uvádza v *pracovnom dokumente útvarov Komisie s názvom Posúdenie vplyvu priložené k návrhu nariadenia Európskeho parlamentu a Rady o rámci pre voľný tok iných ako osobných údajov v Európskej únii* [SWD(2017) 304 final], časť 1/2, s. 3, „bez ohľadu na to, koľko osobných údajov je zahrnutých do zmiešaných súborov údajov, v súvislosti s časťou súboru, ktorú tvoria osobné údaje, treba v plnej miere dodržiavať GDPR [všeobecné nariadenie o ochrane údajov]“.

28 Charta základných práv Európskej únie, Ú. v. EÚ C 362, 26.10.2012, s. 391.

29 Odôvodnenie 8 uvedeného nariadenia.

Spoločnosť pôsobiaca v rámci EÚ ponúka svoje služby prostredníctvom platformy. Podniky (klienti) nahrávajú na platformu svoje dokumenty, ktoré obsahujú zmiešané súbory údajov. Ako „prevádzkovateľ“ musí podnik nahrávajúci dokumenty zabezpečiť, aby bolo spracúvanie v súlade so všeobecným nariadením o ochrane údajov. Spracovaním súboru údajov v mene prevádzkovateľa musí spoločnosť, ktorá ponúka služby (ďalej len „spracovateľ“), uchovávať a spracúvať údaje v súlade so všeobecným nariadením o ochrane údajov, aby sa napríklad zabezpečilo, že je zaručená primeraná úroveň bezpečnosti údajov, a to aj pomocou šifrovania.

Pojem „neoddeliteľne prepojené“ sa ani v jednom z uvedených dvoch nariadení[30] nevymedzuje. Z praktických dôvodov sa môže vzťahovať na situáciu, keď súbor údajov obsahuje osobné údaje, ako aj iné ako osobné údaje, pričom oddelenie týchto dvoch typov údajov by bolo buď nemožné, alebo by ho prevádzkovateľ považoval za ekonomicky neefektívne či technicky nerealizovateľné. Napríklad pri nákupe systému správy vzťahov s klientmi a systému vykazovania predaja by spoločnosť musela zdvojnásobiť svoje náklady na softvér kúpou samostatného softvéru pre systém správy vzťahov s klientmi (osobné údaje) a pre systém vykazovania predaja (agregované/iné ako osobné údaje) na základe údajov zo systému správy vzťahov s klientmi.

Rozdelením súboru údajov sa takisto pravdepodobne významne zníži hodnota súboru údajov. Navyše meniaca sa povaha údajov (pozri oddiel 2.1) sťažuje jasné rozlíšenie, a tým aj oddelenie rôznych kategórií údajov.

Dôležité je, že ani podľa jedného z týchto dvoch nariadení nie sú podniky povinné oddeľovať súbory údajov, ktoré prevádzkujú alebo spracúvajú.

Na zmiešaný súbor údajov sa preto vo všeobecnosti budú vzťahovať povinnosti prevádzkovateľov a spracovateľov, pričom tento súbor údajov bude v súlade s právami dotknutých osôb stanovenými vo všeobecnom nariadení o ochrane údajov.

Spracúvanie údajov týkajúcich sa zdravia

Údaje týkajúce sa zdravia môžu byť súčasťou zmiešaného súboru údajov. Medzi príklady patria elektronické zdravotné záznamy, klinické skúšanie alebo súbory údajov získané rôznymi mobilnými aplikáciami v oblasti zdravia a duševnej pohody (napríklad aplikácie na meranie nášho zdravotného stavu, na pripomenutie užitia liekov alebo na sledovanie pokroku našej kondície)[31]. S technologickým vývojom je presné rozdelenie na osobné a iné ako osobné údaje v týchto súboroch údajov čoraz nejasnejšie. Ich spracúvanie preto musí byť v súlade so všeobecným nariadením o ochrane údajov, najmä (vzhľadom na to, že údaje týkajúce sa zdravia sú podľa tohto nariadenia osobitnou kategóriou údajov) s článkom 9, v ktorom sa

[30] Nariadenie o voľnom toku iných ako osobných údajov a všeobecné nariadenie o ochrane údajov.

[31] Vývoj a prevádzka mobilných zdravotníckych aplikácií si vyžadujú prísne dodržiavanie pravidiel všeobecného nariadenia o ochrane údajov. Tieto požiadavky sa bližšie spresnia v kódexe správania pre mobilné zdravotnícke aplikácie z hľadiska súkromia, ktorý sa v súčasnosti pripravuje. Viac informácií o stave jeho prípravy sa uvádza na: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

stanovuje všeobecný zákaz spracúvania osobitných kategórií údajov a výnimky z tohto zákazu.

Údaje v zmiešaných súboroch údajov, ktoré obsahujú údaje týkajúce sa zdravia, môžu byť cenným zdrojom informácií, napr. pre ďalší lekársky výskum, na meranie vedľajších účinkov predpísaného lieku, na štatistické účely v súvislosti s chorobami alebo na vývoj nových zdravotníckych služieb alebo druhov liečby. Pri vykonávaní prvotných operácií spracúvania a pri vykonávaní ďalších operácií spracúvania údajov sa však musí dodržiavať všeobecné nariadenie o ochrane údajov. Každé takéto spracovanie údajov týkajúcich sa zdravia preto musí mať platný právny základ[32] a primerané odôvodnenie, musí byť bezpečné a musí poskytovať dostatočné záruky.

Je teda nevyhnutné, aby jednotlivci a spoločnosti mali právnu istotu a dôveru v spracúvanie údajov. Toto je zásadné aj pre dátové hospodárstvo. Tento cieľ zabezpečujú obe nariadenia a obe sa zameriavajú na to, aby nedošlo k narušeniu voľného pohybu údajov.

3. Voľný tok údajov a odstránenie požiadaviek na lokalizáciu údajov

V tomto oddiele sa podrobnejšie vysvetľujú požiadavky na lokalizáciu údajov podľa nariadenia o voľnom toku iných ako osobných údajov a zásada voľného pohybu podľa všeobecného nariadenia o ochrane údajov. Hoci sa tieto ustanovenia zameriavajú na členské štáty, môžu podnikom poskytnúť informácie na získanie presnejšej predstavy o tom, ako tieto dve nariadenia prispievajú k voľnému pohybu všetkých údajov v rámci EÚ.

3.1 Voľný tok iných ako osobných údajov

V nariadení o voľnom toku iných ako osobných údajov[33] sa stanovuje, že „požiadavky na lokalizáciu údajov sú zakázané okrem prípadov, keď sú odôvodnené dôvodmi verejnej bezpečnosti v súlade so zásadou proporcionality“.

Požiadavky na lokalizáciu údajov sa vymedzujú[34] ako „akákoľvek povinnosť, zákaz, podmienka, obmedzenie alebo iná požiadavka stanovená v zákonoch, iných právnych predpisoch alebo správnych opatreniach členského štátu alebo vyplývajúca zo všeobecných a konzistentných administratívnych postupov v členskom štáte a verejnoprávnych inštitúciách, a to aj v oblasti verejného obstarávania bez toho, aby bola dotknutá smernica 2014/24/EÚ, ktorá ukladá spracúvanie údajov na území konkrétneho členského štátu alebo obmedzuje spracúvanie údajov v ktoromkoľvek inom členskom štáte[35]“.

---

32 Článok 6 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

33 Článok 4 ods. 1 uvedeného nariadenia.

34 Článok 3 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

35 Upozorňujeme, že právna neistota týkajúca sa rozsahu oprávnených a neoprávnených požiadaviek na lokalizáciu údajov ešte viac obmedzuje možnosti, ktoré majú účastníci trhu a verejný sektor k dispozícii v súvislosti s lokalizáciou spracúvania údajov [pozri odôvodnenie 4 nariadenia Európskeho parlamentu

Vymedzenie ilustruje, že opatrenia obmedzujúce voľný pohyb údajov v rámci EÚ môžu mať rôzne formy. Môžu byť zakotvené v právnych predpisoch, správnych predpisoch a ustanoveniach alebo dokonca môžu vyplývať zo všeobecných a konzistentných administratívnych postupov. Navyše zákaz požiadaviek na lokalizáciu údajov zahŕňa priame aj nepriame opatrenia, ktoré by obmedzovali voľný pohyb iných ako osobných údajov.

Priame požiadavky na lokalizáciu údajov môžu pozostávať napríklad z povinnosti uchovávať údaje na konkrétnom geografickom mieste (napr. servery sa musia nachádzať v konkrétnom členskom štáte) alebo povinnosti spĺňať jedinečné národné technické požiadavky (napr. údaje musia používať osobitné národné formáty).

Nepriame požiadavky na lokalizáciu údajov, ktoré by mohli brániť spracovaniu iných ako osobných údajov v ktoromkoľvek inom členskom štáte, môžu mať rôzne formy. Môžu zahŕňať požiadavky na používanie technologických zariadení, ktoré sú certifikované alebo schválené v konkrétnom členskom štáte, alebo iné požiadavky, ktoré majú za následok zložitejšie spracúvanie údajov mimo konkrétnej geografickej oblasti alebo územia v rámci Európskej únie[36,37].

V posúdení, či konkrétne opatrenie predstavuje nepriamu požiadavku na lokalizáciu údajov, sa musia zohľadňovať osobitné okolnosti každého prípadu.

V nariadení o voľnom toku iných ako osobných údajov[38] sa odkazuje na pojem **verejná bezpečnosť**, ako sa uvádza v judikatúre Súdneho dvora Európskej únie. Verejná bezpečnosť „zahŕňa tak vnútornú, ako aj vonkajšiu bezpečnosť členského štátu[39], ako aj otázky verejnej bezpečnosti, s cieľom predovšetkým uľahčiť vyšetrovanie, odhaľovanie a stíhanie trestných činov. Predpokladá existenciu skutočnej a dostatočne vážnej hrozby ovplyvňujúcej jeden zo základných záujmov spoločnosti[40], akou je ohrozenie fungovania inštitúcií a základných

---

a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii].

36 Odôvodnenie 4 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

37 Pozri dve štúdie o požiadavkách na lokalizáciu údajov, ktoré boli zrealizované pred prijatím nariadenia o voľnom toku iných ako osobných údajov: 1. Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market (Uľahčenie cezhraničných tokov údajov na digitálnom jednotnom trhu)*, SMART number 2015/2016. K dispozícii online 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 (Cezhraničný tok údajov na digitálnom jednotnom trhu: štúdia obmedzení týkajúcich sa lokalizácie údajov)*. SMART number 2015/0054. K dispozícii online na adrese: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695.

38 Odôvodnenie 19 uvedeného nariadenia.

39 Pozri napríklad rozsudok Súdneho dvora z 23. novembra 2010, *Land Baden-Württemberg/Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, bod 43 a rozsudok zo 4. apríla 2017, *Sahar Fahimian/Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, bod 39.

40 Pozri napríklad rozsudok Súdneho dvora z 22. decembra 2008, *Komisia Európskych spoločenstiev/Rakúska republika*, C-161/07, ECLI:EU:C:2008:759, bod 35 a judikatúru, na ktorú sa v ňom odkazuje, a rozsudok z 26. marca 2009, *Komisia Európskych spoločenstiev/Talianska republika*, C-326/07, ECLI:EC:C:2009:193, bod 70 a judikatúru, na ktorú sa v ňom odkazuje.

verejných služieb a prežitie obyvateľstva, ako aj riziko vážneho narušenia zahraničných vzťahov, mierového spolužitia národov alebo riziko vojenských záujmov“.

Navyše každá požiadavka na lokalizáciu údajov odôvodnená verejnou bezpečnosťou musí byť primeraná. V súlade s judikatúrou Súdneho dvora Európskej únie si zásada proporcionality vyžaduje, aby sa prijali opatrenia, ktoré budú primerané na zabezpečenie dosiahnutia sledovaného cieľa a ktoré nebudú prekračovať rámec toho, čo je na tento účel nevyhnutné[41].

V záujme jasnosti treba uviesť, že zákazom požiadaviek na lokalizáciu údajov nie sú dotknuté už existujúce obmedzenia stanovené v právnych predpisoch EÚ[42].

Navyše v nariadení o voľnom toku iných ako osobných údajov sa podnikom neukladajú žiadne povinnosti ani sa neobmedzuje ich zmluvná sloboda rozhodovať o tom, kde sa majú ich údaje spracúvať.

Od členských štátov sa vyžaduje, aby sa podrobnosti o všetkých požiadavkách na lokalizáciu údajov, ktoré platia na ich území, zverejňovali na **národnom online jednotnom informačnom mieste** (národné webové stránky). Členské štáty musia tieto informácie aktualizovať alebo poskytovať aktuálne informácie centrálnemu informačnému miestu zriadenému podľa iného aktu EÚ.[43] Komisia uverejní odkazy na tieto informačné miesta na portáli Vaša Európa pre potreby podnikov a na zabezpečenie ich ľahkého prístupu k príslušným informáciám v rámci celej EÚ[44].

3.2 Voľný tok osobných údajov

Vo všeobecnom nariadení o ochrane údajov[45] sa stanovuje, že „voľný pohyb osobných údajov v rámci Únie sa nesmie obmedziť ani zakázať z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov“.

Ak členský štát uloží požiadavky na lokalizáciu v súvislosti s osobnými údajmi z iných dôvodov, ako je ochrana osobných údajov, budú sa musieť posúdiť z hľadiska ustanovení

---

41 Pozri napríklad rozsudok Súdneho dvora z 8. júla 2010, *Afton Chemical Limited/Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, bod 45, ako aj judikatúru, na ktorú sa v ňom odkazuje.

42 Pozri napríklad článok 245 ods. 2 smernice 2006/112/ES z 28. novembra 2006 o spoločnom systéme dane z pridanej hodnoty, v ktorom sa uvádza, že „členské štáty môžu vyžadovať, aby im zdaniteľné osoby usadené na ich území oznámili miesto uchovávania, ak sa toto miesto nachádza mimo ich územia“. Táto požiadavka sa však musí vykladať v súlade s článkom 249, v ktorom sa uvádza, že: „ak zdaniteľná osoba uchováva faktúry, ktoré vyhotovuje alebo prijíma elektronicky, čím zaručuje prístup k údajom online a ak miesto uchovávania je v inom členskom štáte ako štáte, v ktorom je usadená, príslušné orgány v členskom štáte, v ktorom je usadená, majú na účely tejto smernice právo na elektronický prístup k týmto faktúram, právo sťahovať ich a používať ich v medziach stanovených pravidlami členského štátu, v ktorom je zdaniteľná osoba usadená, a pokiaľ je to potrebné na účely kontroly.“

43 Článok 4 ods. 4 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

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

45 Článok 1 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

o základných slobodách a povolených dôvodoch na odchýlenie sa od týchto slobôd uvedených v Zmluve o fungovaní Európskej únie[46,47] a príslušných právnych predpisoch EÚ, ako sú napríklad smernica o službách[48] a smernica o elektronickom obchode[49].

Príklad:

Podľa vnútroštátneho práva sa vyžaduje, aby sa mzdové účty nachádzali v konkrétnom členskom štáte z dôvodov súvisiacich s regulačnou kontrolou, ktorú vykonáva napríklad vnútroštátny daňový orgán. Takéto vnútroštátne ustanovenie by nepatrilo do pôsobnosti článku 1 ods. 3 všeobecného nariadenia o ochrane údajov, pretože príslušné dôvody sú iné ako ochrana osobných údajov. Namiesto toho by sa táto požiadavka musela posudzovať na základe ustanovení o základných slobodách a povolených dôvodoch na odchýlenie sa od týchto slobôd uvedených v Zmluve o fungovaní Európskej únie.

Vo všeobecnom nariadení o ochrane údajov[50] sa uznáva, že členské štáty môžu stanoviť podmienky vrátane obmedzení, pokiaľ ide o spracovanie genetických údajov, biometrických údajov alebo údajov týkajúcich sa zdravia. Ako sa však uvádza v odôvodnení 53, takéto vnútroštátne obmedzenia by nemali brániť voľnému toku osobných údajov v rámci EÚ, ak sa tieto podmienky vzťahujú na cezhraničné spracúvanie takýchto údajov. Takýto postup je v súlade s článkom 16 Zmluvy o fungovaní Európskej únie, v ktorom sa stanovuje právny základ pre prijatie pravidiel týkajúcich sa práva na ochranu osobných údajov a pravidiel týkajúcich sa voľného pohybu takýchto údajov.

3.3 Rozsah pôsobnosti nariadenia o voľnom toku iných ako osobných údajov

Ako už bolo uvedené, cieľom nariadenia o voľnom toku iných ako osobných údajov je zabezpečiť voľný tok iných ako osobných údajov „v rámci Únie“[51]. Nevzťahuje sa preto na operácie spracúvania, ktoré sa vykonávajú mimo EÚ, a na požiadavky na lokalizáciu údajov súvisiace s takýmto spracúvaním[52,53].

---

46 Konsolidované znenie Zmluvy o fungovaní Európskej únie, Ú. v. EÚ C 326, 26.10.2012, s. 47 – 390.

47 Pozri tiež rozsudok Súdneho dvora z 19. júna 2008, *Komisia Európskych spoločenstiev/Luxemburské* veľkovojvodstvo, C-319/06, ECLI:EU:C:2008:350, body 90 – 91: Súdny dvor usúdil, že povinnosť mať k dispozícii a uchovávať určité dokumenty v konkrétnom členskom štáte predstavuje obmedzenie slobodného poskytovania služieb. Zdôvodnenie, že prítomnosť uvedených dokumentov by „všeobecne uľahčovala vykonanie kontrolných úloh zo strany orgánov tohto štátu“, nie je dostatočné.

48 Smernica Európskeho parlamentu a Rady 2006/123/ES z 12. decembra 2006 o službách na vnútornom trhu, Ú. v. EÚ L 376, 27.12.2006, s. 36 – 68.

49 Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode), Ú. v. ES L 178, 17.7.2000, s. 1 – 16.

50 Článok 9 ods. 4 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

51 Pozri článok 3 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

52 Pozri odôvodnenie 15 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

Rozsah pôsobnosti nariadenia sa preto v súlade s článkom 2 ods. 1 obmedzuje na spracúvanie elektronických iných ako osobných údajov v EÚ, pričom toto spracúvanie:

a) sa poskytuje ako služba používateľom s pobytom alebo miestom usadenia v EÚ bez ohľadu na to, či poskytovateľ služieb je alebo nie je usadený v EÚ, alebo
b) vykonáva fyzická alebo právnická osoba s pobytom alebo miestom usadenia v EÚ pre svoje vlastné potreby.

Príklady:

Článok 2 ods. 1 písm. a) nariadenia o voľnom toku iných ako osobných údajov:

- Poskytovateľ cloudových služieb so sídlom v Spojených štátoch amerických poskytuje svoje služby spracúvania zákazníkom s pobytom v EÚ alebo usadeným v EÚ. Poskytovateľ cloudových služieb spravuje svoje činnosti prostredníctvom serverov nachádzajúcich sa na území EÚ, kde sa uchovávajú alebo inak spracúvajú údaje jeho európskych zákazníkov. Poskytovateľ cloudových služieb nemusí vlastniť infraštruktúru nachádzajúcu sa v EÚ, ale môže si napríklad prenajímať serverový priestor v EÚ. Na spracúvanie takýchto údajov sa vzťahuje nariadenie o voľnom toku iných ako osobných údajov.
- Poskytovateľ cloudových služieb so sídlom v Japonsku ponúka svoje služby európskym zákazníkom. Spracovateľské kapacity poskytovateľa sa nachádzajú v Japonsku, kde sa uskutočňujú aj všetky spracovateľské činnosti. Ak sa všetky činnosti spracúvania vykonávajú mimo EÚ, nariadenie o voľnom toku iných ako osobných údajov sa v takom prípade neuplatňuje[54].

Článok 2 ods. 1 písm. b) nariadenia o voľnom toku iných ako osobných údajov:

- Malý európsky startup z členského štátu A sa rozhodne rozšíriť svoje podnikanie otvorením prevádzkarne v členskom štáte B. S cieľom minimalizovať náklady sa tento startup rozhodne centralizovať ukladanie a spracúvanie údajov novej prevádzkarne na svojom serveri, ktorý sa nachádza v členskom štáte A. Členské štáty nesmú zakázať takéto snahy o centralizáciu IT, pokiaľ to nie je odôvodnené verejnou bezpečnosťou v súlade so zásadou proporcionality.

[53] Pojem „spracúvanie“ sa vymedzuje všeobecne [v článku 3 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii], a ako sa zdôrazňuje v odôvodnení 17, nariadenie by sa malo uplatňovať na spracúvanie v širokom zmysle, a to pri zahrnutí používania všetkých druhov IT systémov.

[54] Upozorňujeme, že nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii sa netýka požiadaviek na lokalizáciu údajov, ktoré ukladajú členské štáty pri uchovávaní iných ako osobných údajov v tretích krajinách a ktoré sa môžu uvádzať vo vnútroštátnych právnych poriadkoch. V záujme jasnosti treba uviesť, že všeobecné nariadenie o ochrane údajov sa vzťahuje na spracúvanie osobných údajov dotknutých osôb, ktoré sa nachádzajú v EÚ, prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v EÚ, pričom spracovateľská činnosť súvisí: a) s ponukou tovaru alebo služieb týmto dotknutým osobám v Únii bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba; alebo b) so sledovaním ich správania, pokiaľ ide o ich správanie na území Únie (pozri článok 3 ods. 2 všeobecného nariadenia o ochrane údajov).

Hoci sa nariadenie o voľnom toku iných ako osobných údajov neuplatňuje v prípade, že sa všetky činnosti spracúvania iných ako osobných údajov vykonávajú mimo EÚ, všeobecné nariadenie o ochrane údajov sa musí dodržiavať, ak sú súčasťou súboru údajov osobné údaje. V každom prípade sa musia dodržiavať najmä pravidlá prenosu osobných údajov do tretích krajín alebo do medzinárodných organizácií v súlade so všeobecným nariadením o ochrane údajov[55].

3.4 Činnosti týkajúce sa vnútornej organizácie členských štátov

V nariadení o voľnom toku iných ako osobných údajov sa členským štátom neukladá povinnosť outsourcingu poskytovania služieb v súvislosti s inými ako osobnými údajmi, ktoré chcú sami poskytovať alebo ich organizovať inými prostriedkami než na základe verejných zákaziek[56].

V článku 2 ods. 3 druhom pododseku nariadenia o voľnom toku iných ako osobných údajov sa uvádza:

„Týmto nariadením nie sú dotknuté zákony, iné právne predpisy a správne opatrenia, ktoré sa týkajú **vnútornej organizácie** členských štátov a ktorými sa rozdeľujú medzi verejnými orgánmi a verejnoprávnymi inštitúciami vymedzenými v článku 2 ods. 1 bode 4 smernice 2014/24/EÚ[57], právomoci a povinnosti súvisiace so **spracovaním údajov bez zmluvnej odmeny súkromných subjektov**, ako aj zákony, iné právne predpisy a správne opatrenia členských štátov, ktorými sa zabezpečuje vykonávanie uvedených právomocí a povinností.“[58]

Môžu existovať oprávnené záujmy, na základe ktorých by bolo možné zvoliť si tento druh „vlastného poskytovania“ služieb spracúvania údajov, ako je napríklad tzv. insourcing (využitie svojich vlastných zdrojov) alebo vzájomné dohody medzi orgánmi verejnej správy. Medzi typické príklady patrí používanie „vládneho cloudu“ alebo vláda, ktorá využíva

---

55 Pokiaľ ide o prenos osobných údajov do tretích krajín, pozri webovú stránku Komisie: 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_sk a *oznámenie Komisie Európskemu parlamentu a Rade – Výmena a ochrana osobných údajov v globalizovanom svete*, COM/2017/07 final, dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=COM%3A2017 %3A7 %3AFIN. Pokiaľ ide o Japonsko, Komisia 23. januára 2019 prijala rozhodnutie o primeranosti, ktoré umožní voľný pohyb osobných údajov medzi hospodárstvom Únie a Japonska so zárukami dôkladnej ochrany.

56 Odôvodnenie 14 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

57 V článku 2 ods. 1 bode 4 smernice Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES, Ú. v. EÚ L 94, 28.3.2014, s. 65 – 242 sa stanovuje, že „„verejnoprávne inštitúcie sú inštitúcie‘, ktoré majú všetky tieto charakteristické znaky: a) sú zriadené na osobitný účel uspokojovania potrieb vo všeobecnom záujme, pričom nemajú priemyselnú ani komerčnú povahu; b) majú právnu subjektivitu a c) sú z väčšej časti financované štátnymi, regionálnymi alebo miestnymi orgánmi alebo inými verejnoprávnymi inštitúciami; alebo ich riadenie podlieha dohľadu týchto orgánov alebo inštitúcií; alebo majú správnu, riadiacu alebo dozornú radu, v ktorej viac ako polovicu členov menujú štátne, regionálne alebo miestne orgány alebo iné verejnoprávne inštitúcie“.

58 V odôvodnení 13 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii sa poukazuje na to, že nariadením nie je dotknutá smernica 2014/24/EÚ.

centralizovanú IT agentúru na poskytovanie služieb spracúvania údajov pre verejné inštitúcie a orgány.

V nariadení o voľnom toku iných ako osobných údajov sa však členské štáty nabádajú k tomu, aby zvážili hospodársku efektívnosť a iné výhody využívania externých poskytovateľov služieb[59],[60]. Len čo vnútroštátne orgány začnú s „outsourcingom“ spracúvania údajov so zmluvnou odmenou pre súkromné subjekty a začne prebiehať spracúvanie v EÚ, na takéto spracúvanie údajov sa bude vzťahovať nariadenie o voľnom toku iných ako osobných údajov, čo znamená, že na všeobecné a administratívne postupy vnútroštátnych orgánov sa bude vzťahovať zásada voľného toku iných ako osobných údajov. Musia sa zdržať najmä zavádzania obmedzení lokalizácie údajov, napr. pri tendroch v rámci verejného obstarávania[61].

4. Samoregulačné prístupy podporujúce voľný tok údajov

Samoregulácia prispieva k inováciám a dôvere medzi účastníkmi trhu a má potenciál lepšie reagovať na zmeny na trhu. V tomto oddiele sa uvádza prehľad samoregulačných iniciatív v oblasti spracúvania osobných údajov aj iných ako osobných údajov.

4.1 Prenos údajov a zmena poskytovateľov cloudových služieb

Jedným z cieľov nariadenia o voľnom toku iných ako osobných údajov je vyhnúť sa praktikám odkázanosti na určitého dodávateľa. Tieto praktiky sa vyskytujú vtedy, keď používatelia nemôžu zmeniť poskytovateľa služieb, pretože ich údaje sú „uzamknuté“ v systéme poskytovateľa, napríklad z dôvodu špecifického formátu údajov alebo zmluvných podmienok, a nemôžu sa preniesť mimo IT systému predajcu. Prenos údajov bez prekážok je dôležitý pre to, aby používatelia mali možnosť slobodne si vybrať medzi poskytovateľmi služieb spracúvania údajov, čím sa zabezpečí účinná hospodárska súťaž na trhu.

Prenosnosť údajov medzi podnikmi je čoraz dôležitejšia v celej škále digitálnych priemyselných odvetví vrátane cloudových služieb.

Podľa článku 6 nariadenia o voľnom toku iných ako osobných údajov Komisia s cieľom prispieť ku konkurencieschopnému dátovému hospodárstvu podporuje a uľahčuje tvorbu samoregulačných kódexov správania na úrovni EÚ (ďalej len „kódexy správania“). Poskytuje sa v ňom základ pre odvetvie na vytvorenie samoregulačných kódexov správania pri zmene poskytovateľa služieb a prenose údajov medzi rôznymi IT systémami.

Pri tvorbe takýchto kódexov správania pri prenose údajov by sa malo zohľadniť viacero aspektov, a to najmä:

---

59 Odôvodnenie 14 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

60 Externým poskytovateľom služieb by bol akýkoľvek subjekt, ktorý nie je „verejnoprávnou inštitúciou“, ako sa stanovuje v článku 2 ods. 1 bode 4 smernice Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES, Ú. v. EÚ L 94, 28.3.2014, s. 65 – 242.

61 Odôvodnenie 13 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

- **najlepšie postupy** na uľahčenie zmeny poskytovateľa služieb a prenosu údajov pomocou štruktúrovaného, bežne používaného a strojovo čitateľného formátu;
- **minimálne požiadavky na informácie** s cieľom zabezpečiť, aby profesionálnym používateľom boli poskytované pred uzatvorením zmluvy dostatočne podrobné a jasné informácie, pokiaľ ide o procesy, technické požiadavky, časové rámce a poplatky, ktoré sa uplatňujú, ak sa profesionálny používateľ rozhodne pre iného poskytovateľa služieb alebo chce preniesť údaje späť do svojich vlastných IT systémov;
- **prístupy k systémom certifikácie** pre lepšiu porovnateľnosť cloudových služieb a
- **plány v oblasti komunikácie** s cieľom zvýšiť informovanosť o kódexoch správania.

Na trhu s cloudovými službami začala Komisia uľahčovať prácu pracovných skupín zainteresovaných strán v oblasti cloud computingu na digitálnom jednotnom trhu, ktoré združujú odborníkov z oblasti cloud computingu a profesionálnych používateľov vrátane malých a stredných podnikov. V tejto fáze jedna podskupina vytvára samoregulačné kódexy správania pri prenose údajov a zmene poskytovateľa cloudových služieb (pracovná skupina SWIPO) [62] a ďalšia podskupina pracuje na vývoji certifikácie bezpečnosti cloudových služieb (pracovná skupina CSPCERT)[63].

Pracovná skupina SWIPO vytvára kódexy správania vzťahujúce sa na celé spektrum cloudových služieb: infraštruktúra ako služba (Infrastructure as a Service – IaaS), platforma ako služba (Platform as a Service – PaaS) a softvér ako služba (Software as a Service – SaaS).

Komisia očakáva, že rôzne kódexy správania budú doplnené **vzorovými zmluvnými doložkami**[64]. Tie umožnia dostatočnú technickú a právnu špecifickosť pri praktickom vykonávaní a uplatňovaní kódexov správania, ktoré budú mať osobitný význam pre malé a stredné podniky. Vypracovanie vzorových zmluvných doložiek je naplánované po vypracovaní kódexov správania (ktoré by mali byť hotové do 29. novembra 2019).

V súlade s článkom 8 nariadenia o voľnom toku iných ako osobných údajov Komisia zhodnotí vykonávanie nariadenia do 29. novembra 2022. To umožní posúdiť: i) vplyv na voľný tok údajov v Európe; ii) uplatňovanie nariadenia, najmä na zmiešané súbory údajov; iii) mieru, do akej členské štáty účinne zrušili existujúce neodôvodnené obmedzenia lokalizácie údajov; a iv) trhovú účinnosť kódexov správania v oblasti prenosu údajov a zmeny poskytovateľa cloudových služieb.

62 The Cloud Switching and Porting Data Working Group (pracovná skupina pre zmenu poskytovateľov cloudových služieb a prenos údajov).

63 The European Cloud Service Provider Certification Working Group (pracovná skupina pre európsku certifikáciu poskytovateľov cloudových služieb). Pozri aj oddiel 4.3.

64 Pozri odôvodnenie 30 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii.

Pojem prenosnosť a vzájomné pôsobenie so všeobecným nariadením o ochrane údajov

Obe nariadenia[65] sa týkajú prenosnosti údajov a ich cieľom je uľahčiť prenos údajov z jedného IT prostredia do druhého, t. j. buď do systémov iného poskytovateľa, alebo do systémov na určenom mieste. Tým sa zabraňuje odkázanosti na určitého dodávateľa a posilňuje sa hospodárska súťaž medzi poskytovateľmi služieb. Nariadenia sa však líšia svojím prístupom k prenosnosti, pokiaľ ide o vzťah medzi cieľovými záujmovými skupinami a právnou povahou ustanovení.

Právo na prenosnosť osobných údajov podľa článku 20 všeobecného nariadenia o ochrane údajov sa zameriava na vzťah medzi dotknutou osobou a prevádzkovateľom. Týka sa práva dotknutej osoby získať osobné údaje, ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, a bez prekážok ich preniesť inému prevádzkovateľovi alebo do vlastných skladovacích kapacít od prevádzkovateľa, ktorému boli osobné údaje poskytnuté[66]. Dotknuté osoby sú v tomto vzťahu zvyčajne spotrebiteľmi rôznych online služieb, ktoré si želajú zmeniť poskytovateľa služieb.

V článku 6 nariadenia o voľnom toku iných ako osobných údajov sa nestanovuje právo profesionálnych používateľov na prenos údajov, ale uvádza sa v ňom samoregulačný prístup s dobrovoľnými kódexmi správania pre odvetvie. Zároveň sa zameriava na situáciu, keď profesionálny používateľ zabezpečí externé spracovanie svojich údajov treťou stranou, ktorá ponúka službu spracúvania údajov[67]. V súlade s článkom 3 ods. 8 nariadenia o voľnom toku iných ako osobných údajov „profesionálny používateľ“ môže byť „fyzická alebo právnická osoba vrátane verejného orgánu a verejnoprávnej inštitúcie, ktorá využíva služby spracúvania údajov alebo o ne žiada na účely súvisiace so svojou obchodnou, podnikateľskou, remeselnou alebo profesijnou činnosťou alebo so svojou úlohou“.

V praxi sa prenosnosť podľa článku 6 nariadenia o voľnom toku iných ako osobných údajov týka interakcií medzi podnikmi medzi profesionálnym používateľom (ktorý sa môže v prípadoch, ktoré zahŕňajú spracúvanie osobných údajov, kvalifikovať ako „prevádzkovateľ“ v súlade so všeobecným nariadením o ochrane údajov) a poskytovateľom služieb (ktorý sa podobne v niektorých prípadoch môže kvalifikovať ako „spracovateľ“).

---

65 Článok 6 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii a článok 20 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

66 Pozri: Pracovná skupina zriadená podľa článku 29: *Usmernenia k právu na prenosnosť údajov.* WP 242 rev.01, prijaté 13. decembra 2016, naposledy revidované a prijaté 5. apríla 2017.

67 V odôvodnení 29 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii sa uvádza: „Zatiaľ čo jednotliví spotrebitelia majú výhody z existujúceho práva Únie [t. j. všeobecného nariadenia o ochrane údajov], možnosť zmeniť poskytovateľa služieb sa pre tých používateľov, ktorí konajú v rámci ich obchodnej alebo podnikateľskej činnosti neuľahčuje.“

Napriek rozdielom sa môžu vyskytnúť situácie, keď by sa na prenos údajov vzťahovalo nariadenie o voľnom toku iných ako osobných údajov aj všeobecné nariadenie o ochrane údajov, a to v súvislosti so zmiešanými súbormi údajov.

Príklad:

Podnik využívajúci cloudové služby sa rozhodne zmeniť svojho poskytovateľa cloudových služieb a preniesť všetky údaje novému poskytovateľovi. Zmena poskytovateľa služieb a prenos údajov sú zahrnuté v zmluve medzi zákazníkom a poskytovateľom cloudových služieb. Ak starý poskytovateľ cloudových služieb dodržiava kódex správania vypracovaný podľa nariadenia o voľnom toku iných ako osobných údajov, prenos údajov sa musí uskutočniť v súlade s požiadavkami, ktoré sú v ňom stanovené.

Ak sú súčasťou prenášaných súborov údajov aj osobné údaje, prenos musí byť v súlade so všetkými príslušnými ustanoveniami všeobecného nariadenia o ochrane údajov, pričom sa musí zabezpečiť najmä to, aby nový poskytovateľ cloudových služieb spĺňal platné požiadavky, napríklad bezpečnosť[68].

Príklad:

V prípade, že sa banka rozhodne zmeniť svojho poskytovateľa správy vzťahov s klientmi, je možné, že niektoré (osobné a iné ako osobné) údaje musia prejsť od starého poskytovateľa novému. Tieto údaje budú následne podliehať rôznym regulačným požiadavkám, pričom niektoré z nich budú vyplývať zo všeobecného nariadenia o ochrane údajov a iné zase z nariadenia o voľnom toku iných ako osobných údajov.

4.2 Kódexy správania a systémy certifikácie týkajúce sa ochrany osobných údajov

Kódexy správania a systémy certifikácie sa môžu použiť na dokázanie plnenia povinností vyplývajúcich zo všeobecného nariadenia o ochrane údajov (pozri článok 24 ods. 3 a článok 28 ods. 5).

V súlade s článkom 40 ods. 1 a článkom 42 ods. 1 všeobecného nariadenia o ochrane údajov by členské štáty, orgány dohľadu, Európsky výbor pre ochranu údajov a Komisia mali nabádať odvetvie, aby vytvorilo kódexy správania a zaviedlo certifikačné mechanizmy na ochranu údajov.

Združenia alebo iné orgány zastupujúce konkrétnu kategóriu prevádzkovateľov alebo spracovateľov môžu vypracovať kódex správania pre konkrétny sektor. Návrh kódexu je

[68] Pozri: Pracovná skupina zriadená podľa článku 29: *stanovisko č. 05/2012 o cloud computingu*, prijaté 1. júla 2012, WP196, v ktorom sa spresňuje postavenie a povinnosti používateľov cloudu a poskytovateľov *cloudových* služieb v súvislosti so spracúvaním osobných údajov.

potrebné predložiť na schválenie príslušnému orgánu dohľadu[69]. Ak sa návrh kódexu správania týka činností spracúvania vo viacerých členských štátoch, orgán dohľadu ho musí pred schválením predložiť Európskemu výboru pre ochranu údajov. Výbor potom vydá svoje stanovisko k tomu, či je návrh kódexu v súlade so všeobecným nariadením o ochrane údajov.

Európsky výbor pre ochranu údajov uverejnil svoje usmernenie 1/2019 o kódexe správania a monitorovacích orgánoch v súlade so všeobecným nariadením o ochrane údajov[70]. Toto usmernenie zahŕňa informácie o vypracovaní kódexov správania, kritériá na ich schválenie a ďalšie užitočné informácie. Podobne aj v usmernení Európskeho výboru pre ochranu údajov 1/2018 o certifikácii a identifikácii certifikačných kritérií v súlade s článkami 42 a 43 všeobecného nariadenia o ochrane údajov sa uvádzajú informácie o certifikácii podľa uvedeného nariadenia a vypracovaní a schvaľovaní certifikačných kritérií[71].

Príklady kódexov správania, ktoré vytvorilo odvetvie cloud computingu:

Kódex správania EÚ v oblasti cloud computingu, ktorého vypracovanie podporila Komisia, bol vypracovaný v spolupráci so skupinou pre otázky cloud computingu pozostávajúcou z vybraných zástupcov priemyselných odvetví – Cloud Select Industry Group (C-SIG) na základe smernice o ochrane údajov[72] a následne všeobecného nariadenia o ochrane údajov. Kódex správania EÚ v oblasti cloud computingu sa vzťahuje na celé spektrum cloudových služieb, ako sú softvér ako služba (Software as a Service – SaaS), platforma ako služba (Platform as a Service – PaaS) a infraštruktúra ako služba (Infrastructure as a Service – IaaS)[73].

Kódex správania poskytovateľov služieb cloudovej infraštruktúry v Európe (CISPE)[74] sa zameriava na poskytovateľov IaaS. Kódex správania CISPE pozostáva z požiadaviek týkajúcich sa poskytovateľov IaaS, ktorí pôsobia ako spracovatelia údajov podľa všeobecného nariadenia o ochrane údajov. Zároveň sa v ňom uvádzajú ustanovenia o riadiacej štruktúre na vykonávanie a uplatňovanie kódexu.

---

69 Pozri článok 40 ods. 5 a článok 55 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

70 Európsky výbor pre ochranu údajov: *usmernenie 1/2019 o kódexe správania a monitorovacích orgánoch v súlade s nariadením 2016/679*, prijaté 12. februára 2019, verzia na verejnú konzultáciu, k dispozícii online na adrese: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en.

71 Európsky výbor pre ochranu údajov: *usmernenie 1/2018 o certifikácii a identifikácii certifikačných kritérií v súlade s článkami 42 a 43 nariadenia 2016/679*, prijaté 23. januára 2019, k dispozícii online na adrese: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en.

72 Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (dátum ukončenia platnosti: 24. mája 2018).

73 Viac informácií o kódexe správania EÚ v oblasti cloud computingu nájdete na: https://eucoc.cloud/en/home.html.

74 Viac informácií o kódexe správania CISPE nájdete na: https://cispe.cloud/code-of-conduct/.

Kódex správania Cloud Security Alliance pre súlad so všeobecným nariadením o ochrane údajov sa zameriava na všetky zainteresované strany v oblasti cloud computingu a európskych právnych predpisov v oblasti osobných údajov, ako sú poskytovatelia cloudových služieb, zákazníci a potenciálni zákazníci využívajúci cloudové služby, audítori a sprostredkovatelia pôsobiaci v oblasti cloud computingu. Kódex správania sa vzťahuje na celé spektrum poskytovateľov cloudových služieb[75].

4.3 Posilnenie dôvery v cezhraničné spracúvanie údajov – certifikácia bezpečnosti

Ako sa uvádza v odôvodnení 33 nariadenia o voľnom toku iných ako osobných údajov, zvýšením dôvery v bezpečnosť cezhraničného spracúvania údajov by sa mala znížiť tendencia účastníkov trhu a verejného sektora využívať lokalizáciu údajov ako prostriedok na zaistenie bezpečnosti údajov. Spolu s balíkom právnych predpisov o kybernetickej bezpečnosti, ktorý navrhla Komisia v roku 2017[76], pracovná skupina CSPCERT pripravuje odporúčania na účely zriadenia európskeho systému certifikácie v oblasti cloud computingu, ktoré budú predložené Komisii. Takýto systém môže uľahčiť voľný pohyb údajov, umožniť lepšiu porovnateľnosť cloudových služieb a podporovať využívanie cloudu. Komisia môže požiadať Agentúru Európskej únie pre kybernetickú bezpečnosť (ENISA), aby pripravila kandidátsky systém v súlade s príslušnými ustanoveniami aktu o kybernetickej bezpečnosti[77]. Takýto systém môže pozostávať z osobných aj iných ako osobných údajov. Okrem aktu o kybernetickej bezpečnosti sa všeobecné nariadenie o ochrane údajov, ako sa zdôrazňuje v oddiele 4.2, môže použiť aj na preukázanie existencie primeraných záruk týkajúcich sa bezpečnosti údajov[78].

Záverečné poznámky

Dosiahnutie právnej istoty a dôvery v spracúvanie údajov je nevyhnutné na to, aby mohla EÚ využívať údaje v čo najväčšej miere a aby sa hodnotové reťazce mohli rozvíjať naprieč všetkými sektormi a hranicami. Tento cieľ zabezpečujú obe nariadenia a obe sa zameriavajú na voľný pohyb údajov. Nariadenie o voľnom toku iných ako osobných údajov a všeobecné nariadenie o ochrane údajov spolu vytvárajú základ pre voľný tok všetkých údajov v Európskej únii a pre vysoko konkurencieschopné európske dátové hospodárstvo.

---

75 Viac informácií o kódexe správania Cloud Security Alliance nájdete na: *https*://gdpr.cloudsecurityalliance.org/.

76 Viac informácií sa uvádza na adrese: https://ec.europa.eu/digital-single-market/en/cyber-security.

77 Nariadenie Európskeho parlamentu a Rady zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti).

78 Pozri odôvodnenie 74 aktu o kybernetickej bezpečnosti.