

NARIŽENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2018/1807**ze dne 14. listopadu 2018****o rámci pro volný tok neosobních údajů v Evropské unii****(Text s významem pro EHP)**

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru ⁽¹⁾,

po konzultaci s Výborem regionů,

v souladu s řádným legislativním postupem ⁽²⁾,

vzhledem k těmto důvodům:

- (1) Digitalizace hospodářství nabírá na rychlosti. Informační a komunikační technologie již nejsou specifickým sektorem, nýbrž základem všech moderních inovativních ekonomických systémů a společností. Jádrem těchto systémů jsou elektronické údaje; analýzou těchto údajů či jejich spojením se službami a produkty lze vytvořit značnou hodnotu. Rychlý rozvoj ekonomiky založené na datech a nových technologiích, jako je umělá inteligence, produkty a služby internetu věcí, autonomní systémy a 5G, zároveň vyvolává nové právní otázky týkající se přístupu k údajům a jejich opakovaného použití, právní odpovědnosti, etiky a solidarity. Je třeba zvážit činnost zejména ve věci právní odpovědnosti, především prostřednictvím zavedení samoregulačních kodexů a dalších osvědčených postupů, a to s ohledem na doporučení, rozhodnutí a opatření přijatá bez zásahu člověka v celém hodnotovém řetězci zpracování údajů. Tato činnost může rovněž zahrnovat mj. vhodné mechanismy pro určení právní odpovědnosti pro převedení odpovědnosti mezi spolupracující služby, pojištění a audit.
- (2) Hodnotové řetězce údajů jsou postaveny na různých činnostech v oblasti údajů: vytváření a shromažďování údajů; agregace a organizování údajů; zpracování údajů, jejich analýza, uvádění na trh a šíření údajů; používání údajů včetně opakovaného použití. Základním stavebním kamenem jakéhokoli hodnotového řetězce údajů je účinně a efektivně fungující zpracování údajů. Nicméně takovému účinnému a efektivnímu fungování zpracování údajů a rozvoji ekonomiky založené na datech v Unii ztěžují zejména dva druhy překážek v oblasti mobility údajů a vnitřního trhu: požadavky na lokalizaci údajů stanovené orgány členských států a praxe obchodních proprietárních uzamčení (tzv. vendor lock-in) v soukromém sektoru.
- (3) Na služby zpracování údajů se vztahuje svoboda usazování a volný pohyb služeb podle Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“). Poskytování takových služeb však ztěžují nebo někdy znemožňují některé vnitrostátní, regionální nebo místní požadavky, aby údaje byly umístěny na určitém území.
- (4) Tyto překážky, které brání volnému pohybu služeb zpracování údajů a svobodě usazování poskytovatelů služeb zpracování údajů, vyplývají z požadavků vnitrostátních právních předpisů členských států, aby byly údaje pro účely zpracování umístěny v určité zeměpisné oblasti nebo na určitém území. Rovnocenný účinek mají i jiná pravidla nebo správní praxe ukládající zvláštní požadavky, které znesnadňují zpracování údajů mimo určitou zeměpisnou oblast nebo území v rámci Unie, například požadavky na použití technických prostředků, které jsou certifikovány nebo schváleny v konkrétním členském státě. 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. Toto nařízení v žádném případě neomezuje svobodu podniků uzavírat smlouvy, které stanoví, kde mají být údaje umístěny. Toto nařízení má tuto svobodu pouze podpořit tím, že zajistí, aby se dohodnuté umístění mohlo nacházet kdekoli v Unii.

⁽¹⁾ Úř. věst. C 227, 28.6.2018, s. 78.⁽²⁾ Postoj Evropského parlamentu ze dne 4. října 2018 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 6. listopadu 2018.

- (5) Mobilitě údajů v Unii současně brání i soukromá omezení: právní, smluvní a technické problémy, které uživatelům služeb zpracování údajů znesnadňují nebo znemožňují přenést své údaje od jednoho poskytovatele služeb k jinému nebo zpět do svých vlastních systémů informační technologie (dále jen „IT systémy“), a to nejen při ukončení smlouvy s poskytovatelem služeb.
- (6) Kombinace těchto překážek vede k nedostatečné konkurenci mezi poskytovateli cloudových služeb v Unii, k různým typům proprietárního uzamčení a k vážným problémům s mobilitou údajů. Politiky umístění údajů stejně tak omezují možnosti výzkumných a vývojářských společností k usnadnění spolupráce mezi firmami, univerzitami a jinými výzkumnými organizacemi s cílem podnítit inovace.
- (7) S cílem zajistit právní jistotu a z důvodu nutnosti zajistit rovné podmínky v rámci Unie je pro fungování vnitřního trhu nezbytný jednotný soubor pravidel pro všechny účastníky trhu. Za účelem odstranění překážek pro obchod a narušení hospodářské soutěže v důsledku rozdílů mezi vnitrostátními právními předpisy a zabránění vzniku dalších pravděpodobných překážek pro obchod a výrazných narušení hospodářské soutěže, je nezbytné přijmout jednotná pravidla, která se použijí ve všech členských státech.
- (8) Tímto nařízením není dotčen právní rámec o ochraně fyzických osob v souvislosti se zpracováním osobních údajů ani právní rámec týkající se respektování soukromého života a ochrany osobních údajů v elektronických komunikacích, a zejména nařízení Evropského parlamentu a Rady (EU) 2016/679 ⁽¹⁾ a směrnice Evropského parlamentu a Rady (EU) 2016/680 ⁽²⁾ a směrnice Evropského parlamentu a Rady 2002/58/ES ⁽³⁾.
- (9) Rozvíjející se internet věcí, umělá inteligence a strojové učení představují rozsáhlý zdroj neosobních údajů, například ve výsledku jejich využívání v automatizovaných postupech průmyslové výroby. Mezi konkrétní příklady neosobních údajů patří souhrnné a anonymizované soubory údajů používané pro analýzu údajů velkého objemu, údaje o postupech přesného zemědělství, které mohou přispět k monitorování a optimalizaci používání pesticidů a vody, nebo údaje o potřebě údržby průmyslových strojů. Pokud technologický rozvoj umožňuje konvertovat údaje na údaje osobní, má se s takovými anonymizovanými údaji zacházet jako s osobními údaji a má se na ně náležitým způsobem uplatnit nařízení (EU) 2016/679.
- (10) Podle nařízení (EU) 2016/679 členské státy nesmějí omezit ani zakázat volný pohyb osobních údajů v Unii z důvodů souvisejících s ochranou fyzických osob v souvislosti se zpracováním osobních údajů. Toto nařízení stanoví stejnou zásadu volného pohybu v Unii pro neosobní údaje, s výjimkou případů, kdy by omezení nebo zákaz ospravedlňovaly důvody veřejné bezpečnosti. Nařízení (EU) 2016/679 a toto nařízení poskytují soudržný soubor pravidel, která upravují volný pohyb různých typů údajů. Toto nařízení navíc nestanoví povinnost ukládat jednotlivé typy údajů odděleně.
- (11) K vytvoření rámce pro volný tok neosobních údajů v Unii a položení základů pro rozvoj ekonomiky založené na datech a zlepšení konkurenceschopnosti průmyslu Unie je nezbytné stanovit jasný, komplexní a předvídatelný právní rámec pro zpracování údajů jiných než osobních údajů na vnitřním trhu. Flexibilitu potřebnou k tomu, aby tento rámec mohl dostatečně zohlednit měnící se potřeby uživatelů, poskytovatelů služeb a vnitrostátních orgánů v Unii, by měl poskytnout přístup založený na zásadách, zajišťující spolupráci mezi členskými státy a také samoregulace. Aby se předešlo riziku překrývání se stávajícími mechanismy, a tím i vyšší zátěži členských států i podniků, neměla by být stanovena podrobná technická pravidla.
- (12) Toto nařízení by se nemělo týkat zpracování údajů, pokud je prováděno jako součást činnosti, jež nespadá do oblasti působnosti práva Unie. V souladu s článkem 4 Smlouvy o Evropské unii (dále jen „Smlouva o EU“) je vhodné připomenout, že za národní bezpečnost nesou výlučnou odpovědnost jednotlivé členské státy.

⁽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) (Úř. věst. L 119, 4.5.2016, s. 1).

⁽²⁾ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, s. 89).

⁽³⁾ 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).

- (13) Volný tok údajů na území Unie bude hrát důležitou úlohu při docílení růstu a inovací založených na údajích. Veřejné orgány a veřejnoprávní subjekty členských států mohou mít, stejně jako podniky a spotřebitelé, prospěch ze svobodnější volby mezi poskytovateli služeb založených na údajích, konkurenčnějšími cenami a efektivnějšími službami poskytovanými občanům. Vzhledem k velkému množství údajů zpracovávaných veřejnými orgány a veřejnoprávními subjekty je mimořádně důležité, aby veřejné orgány a subjekty šly při zavádění služeb zpracování údajů příkladem a aby se v rámci využívání těchto služeb zdržely jakýchkoliv omezení týkajících se lokalizace údajů. Toto nařízení by se proto mělo vztahovat na veřejné orgány a veřejnoprávní subjekty. V tomto ohledu by se volný tok neosobních údajů, který stanovuje toto nařízení, měl použít i na všeobecné a konzistentní administrativní postupy a na jiné požadavky na lokalizaci údajů v oblasti zadávání veřejných zakázek, aniž by byla dotčena směrnice Evropského parlamentu a Rady 2014/24/EU ⁽¹⁾.
- (14) Stejně jako v případě směrnice 2014/24/EU nejsou tímto nařízením dotčeny právní a správní předpisy týkající se vnitřní organizace členských států a kterými se veřejným orgánům a subjektům 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 vykonávání těchto pravomocí a povinností. Ačkoli jsou veřejné orgány a veřejnoprávní subjekty vyzývány k tomu, aby zvážily hospodářské a jiné výhody zajištění služeb externími poskytovateli, mohou mít oprávněné důvody k tomu, aby si služby zajistily samy nebo aby byly služby dodány interně v rámci veřejné správy. Žádné ustanovení tohoto nařízení tudíž nezavazuje členské státy zadávat subdodávky nebo externalizovat poskytování služeb, jež si přejí poskytovat samy nebo je organizovat jiným způsobem než prostřednictvím zadávání veřejných zakázek.
- (15) Toto nařízení by se mělo vztahovat na fyzické nebo právnické osoby, jež poskytují služby zpracování údajů uživatelům, kteří mají bydliště nebo jsou usazeni v Unii, včetně osob, které poskytují služby zpracování údajů v Unii, aniž by v Unii byly usazené. Toto nařízení by se proto nemělo vztahovat na zpracování údajů, které probíhá mimo Unii, ani na požadavky na lokalizaci těchto údajů.
- (16) Tímto nařízením se nestanoví pravidla, která se týkají určení rozhodného práva v obchodních záležitostech, a proto jím není dotčeno nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ⁽²⁾. Zejména pokud právo rozhodné pro smlouvu nebylo zvoleno v souladu s uvedeným nařízením, řídí se smlouva o poskytování služeb v zásadě právními předpisy země, ve které má poskytovatel služeb obvyklé bydliště.
- (17) Toto nařízení by se mělo použít na zpracování údajů v nejširším slova smyslu a zahrnovat používání všech typů IT systémů, ať už jsou uloženy v prostorách uživatele, nebo zajišťovány externě poskytovatelem služeb. Mělo by se vztahovat na různé úrovně zpracování údajů, od uložení údajů (infrastruktura poskytovaná jako služba – Infrastructure-as-a-Service, IaaS) po zpracování údajů na platformách (platforma poskytovaná jako služba – Platform-as-a-Service, PaaS) nebo v aplikacích (software poskytovaný jako služba – Software-as-a-Service, SaaS).
- (18) Požadavky na lokalizaci údajů představují zjevnou překážku volnému poskytování služeb zpracování údajů v rámci Unie a na vnitřním trhu. Jako takové by měly být zakázány, ledaže by byly odůvodněny veřejnou bezpečností, jak ji vymezuje právo Unie, zejména ve smyslu článku 52 Smlouvy o fungování EU, a byly v souladu se zásadou proporcionality zakotvenou v článku 5 Smlouvy o EU. S cílem zajistit účinnost zásady volného toku neosobních údajů napříč hranicemi, aby se zajistilo rychlé odstranění stávajících požadavků na lokalizaci údajů a aby se umožnilo zpracování údajů na více místech v Unii z provozních důvodů, jakož i vzhledem k tomu, že toto nařízení stanoví opatření k zajištění dostupnosti údajů pro účely regulační kontroly, by členské státy neměly mít možnost odůvodnit požadavky ohledně umístění údajů jinými důvody, než je veřejná bezpečnost.
- (19) Pojem „veřejná bezpečnost“ ve smyslu článku 52 Smlouvy o fungování EU, jak jej vykládá Soudní dvůr, zahrnuje jak vnitřní, tak vnější bezpečnost členského státu, 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, 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. V souladu se zásadou proporcionality by požadavky na lokalizaci údajů, které jsou ospravedlněny důvody veřejné bezpečnosti, měly odpovídat sledovaným cílům a neměly by překračovat rámec toho, co je k dosažení daného cíle nezbytné.

⁽¹⁾ 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).

⁽²⁾ Nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I) (Úř. věst. L 177, 4.7.2008, s. 6).

- (20) Aby se zajistilo účinné uplatňování zásady volného toku neosobních údajů přes hranice a předešlo se vzniku nových překážek bránících hladkému fungování vnitřního trhu, měly by členské státy Komisi neprodleně sdělit každý návrh aktu, který zavádí nový požadavek na lokalizaci údajů nebo mění stávající požadavek na lokalizaci údajů. Tyto návrhy aktů by měly být předkládány a posuzovány v souladu se směrnicí Evropského parlamentu a Rady (EU) 2015/1535 ⁽¹⁾.
- (21) Kromě toho by za účelem odstranění možných stávajících překážek členské státy měly během přechodného období 24 měsíců od počátku používání tohoto nařízení provést přezkum stávajících právních nebo správních předpisů obecné povahy, které stanovují požadavky na lokalizaci údajů, a veškeré takové požadavky na lokalizaci údajů, u kterých mají za to, že jsou v souladu s tímto nařízením, sdělit i s jejich odůvodněním Komisi. To by mělo Komisi umožnit přezkoumání souladu veškerých zbývajících požadavků na lokalizaci údajů. Komise by měla mít případně možnost, vznést vůči dotčenému členskému státu připomínky. Tyto připomínky by mohly obsahovat doporučení, aby členský stát požadavek ohledně umístění údajů změnil nebo zrušil.
- (22) Povinnost sdělovat Komisi stávající požadavky na lokalizaci údajů a návrhy aktů zavedená tímto nařízením by se měla uplatnit na regulační požadavky na lokalizaci údajů a na návrhy aktů obecné povahy, a nikoliv na rozhodnutí určená konkrétní fyzické či právnické osobě.
- (23) Za účelem zajištění transparentnosti požadavků na lokalizaci údajů stanovených v právních a správních předpisech obecné povahy členských států určených fyzickým a právnickým osobám, např. poskytovatelům služeb a uživatelům služeb zpracování údajů, by členské státy měly zveřejnit informace o takových opatřeních na jednotném vnitrostátním online informačním místě a pravidelně je aktualizovat. Alternativně by měly členské státy poskytovat takové aktualizované informace informačnímu místu zřízenému jiným aktem Unie. Aby byly fyzické a právnické osoby řádně informovány o požadavcích na lokalizaci údajů platných v Unii, měly by členské státy oznámit adresy těchto jednotných informačních míst Komisi. Komise by měla tyto informace zveřejnit na svých internetových stránkách společně s pravidelně aktualizovaným konsolidovaným seznamem všech požadavků na lokalizaci údajů, které jsou platné v jednotlivých členských státech, včetně souhrnných informací o těchto požadavcích.
- (24) Požadavky na lokalizaci údajů často pocházejí z nedostatku důvěry v přeshraniční zpracování údajů a vycházejí z předpokládané nedostupnosti údajů pro účely příslušných orgánů členských států, například pro inspekci a audit za účelem regulační kontroly či dozoru. Tento nedostatek důvěry nelze překonat pouze tím, že smluvní podmínky zakazující příslušným orgánům při výkonu jejich úředních povinností zákonný přístup k údajům budou prohlášeny za neplatné. Proto by toto nařízení mělo jasně stanovit, že jím nejsou dotčeny pravomoci příslušných orgánů požadovat nebo získat přístup k údajům v souladu s právem Unie nebo vnitrostátním právem a že přístup příslušných orgánů k údajům nelze odmítnout na základě toho, že údaje jsou zpracovávány v jiném členském státě. Příslušné orgány by mohly uložit funkční požadavky na podporu přístupu k údajům, např. požadavek, aby se popisy systému uchovávaly v příslušném členském státě.
- (25) Fyzické nebo právnické osoby, které jsou povinny poskytnout údaje příslušným orgánům, mohou těmto povinností dostát tím, že příslušným orgánům poskytnou a zaručí účinný a včasný elektronický přístup k údajům bez ohledu na členský stát, na jehož území jsou tyto údaje zpracovávány. Uvedený přístup může být zajištěn konkrétními podmínkami ve smlouvách mezi fyzickou nebo právnickou osobou, která je povinna poskytnout přístup, a poskytovatelem služeb.
- (26) Jestliže je fyzická nebo právnická osoba povinna poskytnout údaje a tuto povinnost nesplní, měl by mít příslušný orgán možnost požádat o pomoc příslušné orgány v ostatních členských státech. V takových případech by příslušné orgány měly použít zvláštní nástroje pro spolupráci podle práva Unie nebo mezinárodních dohod v závislosti na předmětu dané věci, tedy v oblastech, jako je policejní spolupráce, trestní nebo civilní soudnictví či

⁽¹⁾ Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1).

správních záležitosti, jde například o rámcové rozhodnutí Rady 2006/960/SVV ⁽¹⁾, směrnici Evropského parlamentu a Rady 2014/41/EU ⁽²⁾, Úmluvu Rady Evropy o kyberkriminalitě ⁽³⁾, nařízení Rady (ES) č. 1206/2001 ⁽⁴⁾, směrnici Rady 2006/112/ES ⁽⁵⁾ a nařízení Rady (EU) č. 904/2010 ⁽⁶⁾. Pokud takové zvláštní mechanismy spolupráce neexistují, měly by příslušné orgány vzájemně spolupracovat prostřednictvím určených jednotných kontaktních míst s cílem poskytnout přístup k požadovaným údajům.

- (27) Pokud žádost o poskytnutí pomoci obnáší získání přístupu dožádaného orgánu do jakýchkoli prostor fyzické nebo právnické osoby, včetně přístupu k jakýmkoli zařízením a prostředkům pro zpracování údajů, musí být takový přístup v souladu s právem Unie nebo vnitrostátním procesním právem, včetně případného požadavku získat předem soudní povolení.
- (28) Toto nařízení by nemělo uživatelům umožňovat, aby se pokoušeli obcházet uplatňování vnitrostátního práva. Proto je třeba stanovit, že členské státy mohou ukládat účinné, přiměřené a odrazující sankce uživatelům, kteří příslušným orgánům brání v získání přístupu k jejich údajům potřebným k výkonu úředních povinností příslušných orgánů podle práva Unie a vnitrostátního práva. V naléhavých případech, pokud uživatel zneužívá svá práva, by členské státy měly mít možnost uložit přísně přiměřená dočasná opatření. Jakákoli dočasná opatření, která vyžadují přemístění údajů na dobu přesahující 180 dní od přemístění, by znamenala odchylku od zásady volného pohybu údajů na značně dlouhé období, a měla by být proto oznámena Komisi, aby ta přezkoumala, zda jsou slučitelná s právem Unie.
- (29) Podstatným faktorem přispívajícím k tomu, že uživatelé mají možnost výběru a na trzích služeb zpracování údajů probíhá účinná hospodářská soutěž, je možnost bez obtíží údaje přenést. Skutečné nebo domnělé obtíže při přenášení údajů přes hranice rovněž podkopávají důvěru profesionálních uživatelů ve využívání přeshraničních nabídek, a tím i jejich důvěru ve vnitřní trh. Zatímco individuální spotřebitelé požívají výhod zakotvených ve stávajícím právu Unie, uživatelům jednajícím v rámci své podnikatelské nebo profesní činnosti není změna poskytovatele služeb usnadňována. K rozvoji hospodářské soutěže na vnitřním trhu služeb zpracování údajů přispívají rovněž jednotné technické požadavky v celé Unii, ať už je jich dosaženo technickou harmonizací, vzájemným uznáváním nebo dobrovolnou harmonizací.
- (30) Aby mohli profesionální uživatelé plně využít výhod konkurenčního prostředí, měli by mít možnost činit informovaná rozhodnutí a snadno porovnávat jednotlivé složky různých služeb zpracování údajů nabízených na vnitřním trhu, včetně smluvních podmínek upravujících přenášení údajů při ukončení smlouvy. V zájmu sladění s inovačním potenciálem trhu a zohlednění zkušeností a odborných znalostí poskytovatelů služeb a profesionálních uživatelů služeb zpracování údajů by podrobné informační a provozní požadavky ohledně přenesení údajů měly být definovány ze strany účastníků trhu prostřednictvím samoregulace, kterou podpoří, usnadní a monitoruje Komise, a to ve formě kodexů chování Unie, jež mohou zahrnovat vzorové smluvní podmínky.
- (31) V zájmu účinnosti a usnadnění změny poskytovatele služeb a přenesení údajů by uvedené kodexy chování měly být komplexní a měly by zahrnovat alespoň klíčové aspekty, které jsou důležité v rámci procesu přenosu údajů, jako jsou postupy zálohování údajů a místa uložení záloh, dostupné formáty a nosiče údajů, požadované IT konfigurace a minimální přenosové rychlosti sítě, dále pak doba potřebná k zahájení procesu přenesení a doba, po kterou údaje zůstanou k dispozici pro přenesení, jakož i záruky, pokud jde o přístup k údajům v případě úpadku poskytovatele služeb. Tyto kodexy chování by rovněž měly jasně stanovit, že proprietární uzamčení není přijatelnou obchodní praxí, měly by prosazovat technologie, které zvyšují důvěru, a měly by být pravidelně aktualizovány, aby držely krok s vývojem technologií. Komise by měla zajistit, aby v průběhu tohoto procesu byly konzultovány všechny příslušné zúčastněné strany, včetně sdružení malých a středních podniků, začínajících podniků, uživatelů a poskytovatelů cloudových služeb. Komise by měla hodnotit vývoj a účinnost provádění těchto kodexů chování.

⁽¹⁾ Rámcové rozhodnutí Rady 2006/960/SVV ze dne 18. prosince 2006 o zjednodušení výměny operativních a jiných informací mezi donucovacími orgány členských států Evropské unie (Úř. věst. L 386, 29.12.2006, s. 89).

⁽²⁾ Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech (Úř. věst. L 130, 1.5.2014, s. 1).

⁽³⁾ Úmluva Rady Evropy o kyberkriminalitě, CETS č. 185.

⁽⁴⁾ Nařízení Rady (ES) č. 1206/2001 ze dne 28. května 2001 o spolupráci soudů členských států při dokazování v občanských nebo obchodních věcech (Úř. věst. L 174, 27.6.2001, s. 1).

⁽⁵⁾ Směrnice Rady 2006/112/ES ze dne 28. listopadu 2006 o společném systému daně z přidané hodnoty (Úř. věst. L 347, 11.12.2006, s. 1).

⁽⁶⁾ Nařízení Rady (EU) č. 904/2010 ze dne 7. října 2010 o správní spolupráci a boji proti podvodům v oblasti daně z přidané hodnoty (Úř. věst. L 268, 12.10.2010, s. 1).

- (32) Pokud příslušný orgán v jednom členském státě žádá o pomoc jiný členský stát, aby získal přístup k údajům podle tohoto nařízení, měl by prostřednictvím určeného jednotného kontaktního místa předložit určenému jednotnému kontaktnímu místu dožádaného členského státu řádně odůvodněnou žádost včetně písemného vysvětlení svých důvodů a právních základů, na jejichž základě o přístup k údajům usiluje. Jednotné kontaktní místo určené členským státem, jehož pomoc je požadována, by mělo usnadnit předání žádosti příslušnému orgánu v dožádaném členském státě. V zájmu zajištění účinné spolupráce by orgán, kterému je žádost předána, měl bez zbytečného prodlení v reakci na žádost pomoc poskytnout, nebo informovat o obtížích s vyhověním žádosti o poskytnutí pomoci či o svých důvodech pro zamítnutí žádosti.
- (33) Posílením důvěry v bezpečnost přeshraničního zpracování údajů by se měla omezit tendence účastníků trhu a veřejného sektoru používat lokalizaci údajů jako náhražku bezpečnosti údajů. Měla by se tím zlepšit i právní jistota pro společnosti, pokud jde o soulad s platnými bezpečnostními požadavky při externím zajišťování činností v oblasti zpracování údajů poskytovateli služeb, včetně těch v ostatních členských státech.
- (34) Na zpracování údajů v jiném členském státě by se měly i nadále vztahovat veškeré bezpečnostní požadavky týkající zpracování údajů, které jsou na základě práva Unie nebo vnitrostátního práva, jež je v souladu s právem Unie, důvodně a přiměřeně uplatňovány v členském státě, v němž mají bydliště nebo jsou usazené fyzické nebo právnické osoby, o jejichž údaje se jedná. Tyto fyzické nebo právnické osoby by měly mít možnost splnit tyto požadavky buď samy, nebo prostřednictvím smluvních ujednání ve smlouvách s poskytovateli služeb.
- (35) Bezpečnostní požadavky stanovené na vnitrostátní úrovni by měly být nezbytné a přiměřené bezpečnostním rizikům pro zpracování údajů v oblasti působnosti vnitrostátních právních předpisů, kterými jsou tyto požadavky stanoveny.
- (36) Směrnice Evropského parlamentu a Rady (EU) 2016/1148⁽¹⁾ stanoví právní opatření s cílem posílit celkovou úroveň kybernetické bezpečnosti v Unii. Služby zpracování údajů představují jednu z digitálních služeb, na něž se uvedená směrnice vztahuje. Podle uvedené směrnice členské státy zajistí, aby poskytovatelé digitálních služeb určili a přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž jsou vystaveny sítě a informační systémy, které využívají. Tato opatření by měla zajišťovat úroveň bezpečnosti odpovídající existující míře rizika, přičemž by měla zohledňovat bezpečnost systémů a zařízení, řešení incidentů, řízení kontinuity provozu, monitorování, audity a testování a soulad s mezinárodními normami. Komise má tyto prvky blíže upřesnit v prováděcích aktech podle uvedené směrnice.
- (37) Komise by měla předložit zprávu o provádění tohoto nařízení, zejména s cílem určit, zda jsou nutné změny zohledňující vývoj techniky nebo vývoj na trhu. Zpráva by měla zejména vyhodnotit toto nařízení, především jeho uplatňování pokud jde o soubory údajů obsahující jak osobní, tak neosobní údaje, a dále uplatňování výjimky z důvodu veřejné bezpečnosti. Předtím, než se začne používat toto nařízení, by Komise také měla zveřejnit pokyny ohledně toho, jak postupovat v případě souborů údajů obsahujících jak osobní, tak neosobní údaje, aby podniky, včetně malých a středních podniků, lépe chápaly vzájemné působení tohoto nařízení a nařízení (EU) 2016/679 a zajistily dodržování obou uvedených nařízení.
- (38) Toto nařízení respektuje základní práva a ctí zásady uznávané zejména Listinou základních práv Evropské unie a mělo by být vykládáno a uplatňováno v souladu s těmito právy a zásadami, včetně práv na ochranu osobních údajů, svobodu projevu a informací a svobodu podnikání.
- (39) Jelikož cíle tohoto nařízení, totiž zajištění volného toku jiných než osobních údajů v Unii, nemůže být dosaženo uspokojivě členskými státy, ale spíše jej, z důvodu jeho rozsahu a účinků, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o EU. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení tohoto cíle,

⁽¹⁾ Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

PŘIJALY TOTO NAŘÍZENÍ:

Článek 1

Předmět

Toto nařízení má za cíl zajistit volný tok jiných než osobních údajů v rámci Unie tím, že stanoví pravidla, pokud jde o požadavky na lokalizaci údajů, dostupnost údajů příslušným orgánům a přenos údajů pro profesionální uživatele.

Článek 2

Oblast působnosti

1. Toto nařízení se použije na zpracování elektronických údajů jiných než osobních údajů v Unii, které je
 - a) poskytováno jako služba uživatelům, kteří mají bydliště nebo jsou usazení v Unii, bez ohledu na to, zda je v Unii usazen poskytovatel služeb; nebo
 - b) prováděno fyzickou nebo právníckou osobou, která má bydliště nebo je usazena v Unii, pro její vlastní potřebu.
2. 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.
3. Toto nařízení se nevztahuje na činnosti, které nespádají do oblasti působnosti práva Unie.

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 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.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

- 1) „údaji“ údaje jiné než osobní údaje ve smyslu čl. 4 bodu 1 nařízení (EU) 2016/679;
- 2) „zpracováním“ jakákoliv operace nebo soubor operací s údaji nebo soubory údajů v elektronické podobě, prováděné pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
- 3) „návrhem aktu“ text vypracovaný za účelem jeho přijetí jako právního nebo správního předpisu obecné povahy, přičemž je ve fázi přípravy, kdy v něm ještě mohou být provedeny podstatné změny;
- 4) „poskytovatelem služby“ fyzická nebo právnícká osoba, která poskytuje služby zpracování údajů;
- 5) „požadavkem na lokalizaci údajů“ jakákoliv 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;
- 6) „příslušným orgánem“ orgán členského státu nebo jakýkoli jiný subjekt oprávněný podle vnitrostátního práva vykonávat veřejnou funkci nebo vykonávat veřejnou moc, který má podle práva Unie nebo vnitrostátního práva pravomoc získat přístup k údajům zpracovávaným fyzickou nebo právníckou osobou pro účely výkonu svých úředních povinností;
- 7) „uživatel“ fyzická nebo právnícká osoba, včetně veřejného orgánu nebo veřejnoprávního subjektu, která využívá nebo požaduje službu zpracování údajů;
- 8) „profesionálním uživatelem“ fyzická nebo právnícká osoba, 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.

Článek 4

Volný pohyb údajů v Unii

1. Požadavky na lokalizaci údajů jsou zakázány, ledaže jsou odůvodněny veřejnou bezpečností v souladu se zásadou proporcionality.

Prvním pododstavcem tohoto odstavce není dotčen odstavec 3 ani požadavky na lokalizaci údajů stanovené na základě stávajícího práva Unie.

2. Členské státy okamžitě sdělí Komisi každý návrh aktu, kterým se zavádí nový požadavek na lokalizaci údajů nebo mění stávající požadavek na lokalizaci údajů, v souladu s postupy stanovenými v článcích 5, 6 a 7 směrnice (EU) 2015/1535.

3. Do 30. května 2021 členské státy zajistí zrušení všech stávajících požadavků na lokalizaci údajů stanovených v právních nebo správních předpisech obecné povahy, které nejsou v souladu s odstavcem 1 tohoto článku.

Pokud se členský stát domnívá, že stávající požadavek na lokalizaci údajů je v souladu s odstavcem 1 tohoto článku, a může proto zůstat v platnosti, sdělí toto opatření týkající se požadavku do 30. května 2021 Komisi spolu s důvody pro jeho zachování v platnosti. Aniž je dotčen článek 258 Smlouvy o fungování EU, Komise do šesti měsíců od obdržení uvedeného sdělení přezkoumá, zda je takové opatření v souladu s odstavcem 1 tohoto článku, a případně vznesе vůči dotčenému členskému státu připomínky, včetně doporučení, aby toto opatření v případě potřeby změnil nebo zrušil.

4. Členské státy zveřejní podrobnosti o veškerých požadavcích na lokalizaci údajů, které byly stanoveny v právních nebo správních předpisech obecné povahy a jsou platné na jejich území, prostřednictvím jednotného vnitrostátního online informačního místa, které průběžně aktualizují, nebo poskytují tyto aktualizované podrobné informace o veškerých takových požadavcích na lokalizaci údajů ústřednímu informačnímu místu zřízenému jiným aktem Unie.

5. Členské státy informují Komisi o adrese svého jednotného informačního místa uvedeného v odstavci 4. Komise zveřejní odkazy na tato místa na svých internetových stránkách, spolu s pravidelně aktualizovaným a konsolidovaným seznamem všech požadavků na lokalizaci údajů podle odstavce 4, včetně souhrnných informací o těchto požadavcích.

Článek 5

Dostupnost údajů příslušným orgánům

1. Tímto nařízením nejsou dotčeny pravomoci příslušných orgánů požadovat nebo získat přístup k údajům pro účely výkonu jejich úředních povinností v souladu s právem Unie nebo vnitrostátním právem. Přístup k údajům nelze příslušným orgánům odmítnout na základě toho, že údaje jsou zpracovávány v jiném členském státě.

2. Pokud příslušný orgán poté, co požádal o přístup k údajům uživatele, tento přístup nezíská a pokud podle práva Unie nebo mezinárodních dohod neexistuje zvláštní mechanismus spolupráce za účelem výměny údajů mezi příslušnými orgány různých členských států, může požádat o pomoc příslušný orgán v jiném členském státě v souladu s postupem stanoveným v článku 7.

3. Pokud žádost o poskytnutí pomoci obnáší získání přístupu dožádaného orgánu do jakýchkoli prostor fyzické nebo právnické osoby, včetně přístupu k jakýmkoli zařízením a prostředkům pro zpracování údajů, musí být takový přístup v souladu s právem Unie nebo vnitrostátním procesním právem.

4. Členské státy mohou ukládat účinné, přiměřené a odrazující sankce za nedodržení povinnosti, pokud jde o poskytování údajů, v souladu s právem Unie a vnitrostátním právem.

V případě zneužití práva ze strany uživatele, může členský stát vůči tomuto uživateli uložit přísně přiměřená dočasná opatření, pokud je takový krok opodstatněn naléhavou potřebou přístupu k údajům, přičemž je třeba zohlednit zájem dotčených stran. Pokud dočasné opatření ukládá přemístění údajů na dobu přesahující 180 dní od přemístění, je tato skutečnost v průběhu této 180denní lhůty sdělena Komisi. Komise v nejkratší možné době posoudí opatření a jeho slučitelnost s právem Unie a případně přijme nezbytná opatření. Komise sdílí informace o zkušenostech získaných v tomto ohledu s jednotnými kontaktními místy členských států uvedenými v článku 7.

Článek 6

Přenesení údajů

1. S cílem přispět konkurenceschopné ekonomice založené na datech Komise podporuje a usnadňuje tvorbu samoregulačních kodexů chování na úrovni Unie (dále jen „kodexy chování“), které vycházejí ze zásad transparentnosti a interoperability, zohledňují otevřené standardy a stanoví pokyny mimo jiné pro tyto otázky:
 - a) osvědčené postupy pro usnadnění změny poskytovatele služeb nebo přenos údajů ve strukturovaném, běžně používaném a strojově čitelném formátu, včetně otevřených standardních formátů, pokud je to nezbytné nebo to požaduje poskytovatel služeb, který údaje dostává;
 - b) minimální požadavky na informace, které zajistí, aby profesionálním uživatelům před uzavřením smlouvy o zpracování údajů byly poskytnuty dostatečně podrobné, jasné a transparentní 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;
 - c) přístupy k systémům certifikace, které usnadňují porovnávání produktů a služeb zpracování údajů pro profesionální uživatele, přičemž zohledňují stanovené vnitrostátní nebo mezinárodní normy usnadňující srovnatelnost těchto produktů a služeb. Tyto přístupy mohou mimo jiné zahrnovat řízení jakosti, řízení bezpečnosti informací, řízení kontinuity provozu a řízení v oblasti životního prostředí;
 - d) plány v oblasti komunikace uplatňující multidisciplinární přístup s cílem zvýšit informovanost příslušných zúčastněných stran o kodexech chování.
2. Komise zajistí, aby byly kodexy chování připravovány v úzké spolupráci se všemi příslušnými zúčastněnými stranami, včetně sdružení malých a středních podniků a začínajících podniků, uživatelů a poskytovatelů cloudových služeb.
3. Komise podněcuje poskytovatele služeb k tomu, aby přípravu kodexů chování dokončili do 29. listopadu 2019 a účinně je provedli do 29. května 2020.

Článek 7

Postup spolupráce mezi orgány

1. Každý členský stát určí jednotné kontaktní místo, které jedná s jednotnými kontaktními místy ostatních členských států a s Komisí v otázkách uplatňování tohoto nařízení. Členské státy oznámí Komisi určená jednotná kontaktní místa a veškeré jejich pozdější změny.
2. Pokud příslušný orgán v jednom členském státě žádá o pomoc jiný členský stát za účelem získání přístupu k údajům, předloží určenému jednotnému kontaktnímu místu dožádaného členského státu řádně odůvodněnou žádost. Žádost musí obsahovat písemné vysvětlení důvodů, na jejichž základě členský stát usiluje o přístup k údajům a právní základy jeho žádosti.
3. Jednotné kontaktní místo určí, který orgán jeho členského státu je příslušný, a žádost obdrženou podle odstavce 2 tomuto příslušnému orgánu předá.
4. Takto dožádaný příslušný orgán bez zbytečného odkladu a ve lhůtě přiměřené naléhavosti žádosti odpoví, a to sdělením požadovaných údajů, nebo informováním dožadujícího příslušného orgánu o tom, že nepovažuje podmínky pro podání žádosti o pomoc podle tohoto nařízení za splněné.
5. Veškeré informace vyměňované v souvislosti s pomocí, o kterou bylo požádáno a která byla poskytnuta podle čl. 5 odst. 2, se použijí pouze v souvislosti se záležitostmi, v níž bylo o pomoc požádáno.
6. Jednotná kontaktní místa poskytují uživatelům souhrnné informace o tomto nařízení, a to i pokud jde o kodexy chování.

Článek 8

Hodnocení a pokyny

1. Nejpozději 29. listopadu 2022 Komise předloží Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru zprávu hodnotící provádění tohoto nařízení, zejména pokud jde o:
 - a) uplatňování tohoto nařízení, zejména pokud jde o soubory údajů obsahující jak osobní, tak neosobní údaje, s ohledem na vývoj na trhu a na technologický vývoj, který může rozšířit možnosti deanonymizace údajů;

- b) provádění čl. 4 odst. 1 členskými státy, a to zejména výjimky z důvodu veřejné bezpečnosti; a
 - c) přípravu a účinné provádění kodexů chování a účinné poskytování informací ze strany poskytovatelů služeb.
2. K vypracování zprávy uvedené v odstavci 1 poskytnou členské státy Komisi potřebné informace.
3. Do 29. května 2019 zveřejní Komise pokyny k vzájemnému působení tohoto nařízení a nařízení (EU) 2016/679, zejména pokud jde o soubory údajů obsahující jak osobní, tak neosobní údaje.

Článek 9

Závěrečná ustanovení

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení se použije po šesti měsících od vyhlášení.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

Ve Štrasburku dne 14. listopadu 2018.

Za Evropský parlament
předseda
A. TAJANI

Za Radu
předsedkyně
K. EDTSTADLER
