

Prohlášení



Prohlášení 3/2021 k nařízení o soukromí a elektronických komunikacích Přijato dne 9. března 2021

Evropský sbor pro ochranu osobních údajů přijal toto prohlášení:

Evropský sbor pro ochranu osobních údajů (dále též „EDPB“) vítá dohodnutý mandát k vyjednávání přijatý Radou, který se týká ochrany soukromí a důvěrnosti při používání služeb elektronických komunikací („postoj Rady“), jako pozitivní krok směrem k novému nařízení o soukromí a elektronických komunikacích. Je nanejvýš důležité, aby byl obecný rámec EU pro ochranu údajů urychleně doplněn harmonizovanými pravidly pro elektronické komunikace.

Jak již bylo několikrát uvedeno¹, nařízení o soukromí a elektronických komunikacích nesmí za žádných okolností snížit úroveň ochrany, kterou poskytuje stávající směrnice o soukromí a elektronických komunikacích, nýbrž by mělo doplňovat GDPR tím, že poskytne další silné záruky důvěrnosti a ochrany všech druhů elektronické komunikace. Nařízení o soukromí a elektronických komunikacích nelze v žádném případě použít k faktické změně GDPR. V tomto ohledu postoj Rady vyvolává řadu obav a EDPB si přeje upozornit na otázky, které by se měly při nadcházejících jednáních řešit.

Tímto prohlášením není dotčeno případné budoucí podrobnější prohlášení Evropského sboru pro ochranu osobních údajů nebo stanovisko k postojům spolunormotvůrců.

Obavy týkající se zpracování a uchování údajů elektronické komunikace pro účely vymáhání práva a ochrany národní bezpečnosti

Pokud jde o čl. 6 odst. 1 písm. d) a čl. 7 odst. 4, EDPB znovu uvádí, že legislativní opatření, která vyžadují, aby poskytovatelé služeb elektronických komunikací uchovávali údaje elektronických komunikací, musí být v souladu s:

-) články 7 a 8 Listiny základních práv Evropské unie (dále jen „Listina“),
-) nejnovější judikaturou Soudního dvora EU („SDEU“)², jakož i
-) článkem 8 Evropské úmluvy o lidských právech.

Evropský sbor pro ochranu osobních údajů se domnívá, že nařízení o soukromí a elektronických komunikacích se nemůže odchýlit od uplatňování nejnovější judikatury SDEU, která zejména stanoví,

¹ Viz úplný seznam dokumentů týkajících se pravidel v oblasti soukromí a elektronických komunikací, který jakožto přílohu tohoto prohlášení vypracovaly EDPB a pracovní skupina zřízená podle článku 29.

² Spojené věci SDEU C-511/18, C-512/18 a C-520/18, věc C-623/17.

že články 7, 8, 11 a čl. 52 odst. 1 Listiny musí být vykládány v tom smyslu, že brání legislativním opatřením, která by jako preventivní opatření stanovila plošné a nerozlišující uchovávání provozních a lokalizačních údajů. Stanovit právní základ pro uchovávání údajů pro jiný účel, než je cílené uchovávání údajů pro účely vymáhání práva a ochrany národní bezpečnosti, Listina nedovoluje a v každém případě by takové uchovávání údajů muselo být přísně časově a věcně omezeno a také by muselo podléhat přezkumu ze strany soudu nebo nezávislého orgánu.

Pokud jde o vyloučení činností zpracování ze strany poskytovatelů z oblasti působnosti nařízení, EDPB se domnívá, že toto vyloučení je v rozporu s předpokladem jednotného rámce EU pro ochranu údajů. Evropský sbor pro ochranu osobních údajů nicméně zdůrazňuje, že v případě vyloučení se použije GDPR.

Důvěrnost elektronických komunikací vyžaduje zvláštní ochranu (články 6, 6a, 6b, 6c)

Právo na důvěrnost komunikace je základním právem chráněným podle článku 7 Listiny, který již byl proveden směrnicí o soukromí a elektronických komunikacích. Toto právo na důvěrnost musí být uplatněno na každou elektronickou komunikaci, bez ohledu na prostředky použité k odeslání, v klidu i při přenosu, od odesílatele k příjemci, a musí rovněž chránit integritu koncového zařízení každého uživatele.

Obecné zákazy s omezenými výjimkami pro zpracování osobních údajů

Evropský sbor pro ochranu osobních údajů plně podporuje přístup založený na obecných zákazech a s omezeními, konkrétními a jasně vymezenými (účelově orientovanými) výjimkami.

Je však znepokojen tím, že některé výjimky (zejména čl. 6 odst. 1 písm. c), čl. 6b odst. 1 písm. e), čl. 6b odst. 1 písm. f) a čl. 6c) zavedené Radou zřejmě umožňují velmi široké druhy zpracování, a připomíná, že je třeba tyto výjimky omezit na konkrétní a jasně vymezené účely. V každém případě by tyto zvláštní účely měly být výslovně uvedeny, aby byla zajištěna právní jistota a co nejvyšší stupeň ochrany.

Kromě toho by výjimky podle čl. 6 odst. 1 písm. b), c) a d), které umožňují přístup k údajům elektronických komunikací, včetně obsahu, za účelem zajištění bezpečnosti sítí a zařízení koncových uživatelů, mohly poskytovateli služeb elektronických komunikací nebo jejich zpracovatelům umožnit plný přístup k obsahu veškeré komunikace koncových uživatelů. Vzhledem k tomu, že by to mohlo ohrozit právo koncových uživatelů na důvěrnost a jejich očekávání v oblasti ochrany soukromí, musí být výjimky přiměřené a měly by být omezeny alespoň tak, aby bylo stanoveno, že to nesmí vést k systematickému sledování obsahu elektronické komunikace ani nemohou poskytovateli či zpracovatelům umožňovat obcházení případného šifrování.

V neposlední řadě by nařízení mělo zdůrazňovat úlohu anonymizace jako základní záruky, která by měla být systematicky upřednostňována, pokud jde o používání údajů elektronických komunikací.

Dostupné silné a důvěryhodné šifrování je v moderním digitálním světě nezbytné.

Silné nejmodernější šifrování by mělo být obecným pravidlem pro zajištění bezpečného, svobodného a spolehlivého toku údajů mezi občany, podniky a orgány státní správy a má zásadní význam pro zajištění souladu s povinnostmi v oblasti bezpečnosti vyplývajícími z GDPR, například pokud jde o zdravotní údaje a ochranu informačních systémů v souvislosti s rostoucími hrozbami. Koncové šifrování, od odesílatele po příjemce, je rovněž jediným způsobem, jak zajistit úplnou ochranu přenášených údajů. Jakýkoli pokus o oslabení šifrování, a to i pro účely, jako je národní bezpečnost, by

tyto ochranné mechanismy zcela znehodnotil v důsledku jejich možného neoprávněného použití. Šifrování musí zůstat standardizované, silné a účinné³.

Nové nařízení musí vynucovat požadavek na udělení souhlasu s používáním souborů cookies a podobných technologií a musí poskytovatelům služeb nabízet technické nástroje, které jim umožní tento souhlas jednoduše získat (článek 8⁴).

Potřeba přístupu zachovávajícího ochranu soukromí, pokud jde o řešení typu „ber, nebo nech být“.

Je třeba připomenout, že v souvislosti s pravidly ochrany soukromí v odvětví elektronických komunikací se použijí ustanovení o souhlasu podle GDPR. Evropský sbor pro ochranu osobních údajů se proto domnívá, že nutnost získat skutečný svobodný souhlas by měla poskytovatelům služeb bránit v používání nekalých praktik, jako je řešení typu „ber, nebo nech být“, které přístup ke službám a funkcím podmiňují souhlasem uživatele s uchováváním informací nebo získáním přístupu k informacím, které jsou již uchovávány v koncovém zařízení uživatele (tzv. „cookie walls“)⁵.

Evropský sbor pro ochranu osobních údajů zdůrazňuje potřebu zahrnout do nařízení o soukromí a elektronických komunikacích výslovné ustanovení, v němž by byl tento zákaz zakotven, aby uživatelé mohli profilování přijmout nebo odmítnout. Uživatelům by proto stejní poskytovatelé služeb měli navrhnout přiměřené alternativy. Tyto zásady by se měly uplatňovat stejným způsobem na všechny poskytovatele služeb bez ohledu na jejich odvětví činnosti nebo jejich stávající model financování (viz bod odůvodnění 21aa postoje Rady).

Měření návštěvnosti musí být omezeno na postupy nenarušující soukromí, u nichž není pravděpodobné, že by představovaly riziko pro ochranu soukromí uživatelů.

Postoj Rady vytváří novou výjimku pro měření návštěvnosti, jak naznačuje pracovní skupina zřízená podle článku 29⁶. Odchyłka pro měření návštěvnosti navrhovaná Radou je však formulována příliš široce a mohla by vést k příliš širokému výkladu toho, co by mohlo spadat do oblasti působnosti odchyłky, což by následně mohlo vést ke snížení úrovně ochrany koncových zařízení koncových uživatelů.

Evropský sbor pro ochranu osobních údajů proto zdůrazňuje, že výjimka pro měření návštěvnosti by měla být omezena na základní analýzu, která je nezbytná pro analýzu funkčnosti služby požadované uživatelem, měla by být omezena pouze na poskytování statistických údajů provozovateli služeb a musí být uplatňována provozovatelem nebo jeho zpracovateli. Toto zpracování proto samo o sobě ani v kombinaci s jinými řešeními pro sledování nemůže vést k žádnému vyčleňování nebo profilování uživatelů ze strany poskytovatele nebo jiných správců údajů. Kromě toho by služba měření návštěvnosti neměla umožňovat shromažďování informací týkajících se využívání konkrétních internetových stránek/aplikací uživateli a měla by zahrnovat uživatelsky přívětivý mechanismus, jehož pomocí se lze jakémukoliv sběru údajů vyhnout.

³Prohlášení pracovní skupiny zřízené podle článku 29 o šifrování a jeho dopadu na ochranu jednotlivců v souvislosti se zpracováním jejich osobních údajů v EU, 11. dubna 2018, k dispozici na adrese: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

⁴ Jakož i související body odůvodnění (20aaaa a 21aa postoje Rady).

⁵ Jak již bylo uvedeno v prohlášení Evropského sboru pro ochranu osobních údajů o revizi nařízení o soukromí a elektronických komunikacích přijatém dne 25. května 2018, k dispozici na adrese:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_privacy_cs.pdf a v pokynech EDPB č. 5/2019 k souhlasu podle nařízení 2016/679, bod 39, k dispozici na adrese: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_cs.pdf.

⁶ Viz též stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies (WP 194), s. 10. K dispozici na adrese: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf.

Účinný způsob, jak získávat souhlas v případě internetových stránek a mobilních aplikací (článek 4a)

Evropský sbor pro ochranu osobních údajů se domnívá, že nařízení o soukromí a elektronických komunikacích by mělo zlepšit stávající situaci tím, že vrátí kontrolu uživatelům a bude řešit „únavu z poskytování souhlasu“. Článek 4a by měl jít dál a vyžadovat, aby byl v prohlížečích a operačních systémech zaveden uživatelsky vstřícný a účinný mechanismus, jenž správcům umožní získat souhlas, aby byly zajištěny rovné podmínky pro všechny zúčastněné strany. Oblast působnosti nařízení by měla rovněž výslovně zahrnovat poskytovatele prohlížečů a operačních systémů.

Nastavení ochrany soukromí by mělo standardně zachovávat právo na ochranu osobních údajů a integritu koncových zařízení uživatelů a mělo by usnadňovat vyjádření a odvolání souhlasu způsobem, který je jednoduchý, závazný a vůči všem stranám vymahatelný.

Další zpracování pro slučitelné účely (článek 6c a čl. 8 odst. 1 písm. g))

V souvislosti s probíhajícími diskusemi o dalším zpracování metadat/údajů elektronických komunikací shromažďovaných prostřednictvím souborů cookies a podobných technologií EDPB znovu zdůrazňuje, že podporuje přístup nařízení o soukromí a elektronických komunikacích, který původně navrhla Evropská komise a následně uplatnil i Evropský parlament, jenž je založen na obecném zákazu a následných omezených výjimkách a použití souhlasu. Další zpracování pro slučitelné účely s sebou nese riziko narušení ochrany poskytované nařízením o soukromí a elektronických komunikacích, zejména pro zpracování metadat elektronických komunikací, a to tím, že umožní, aby zpracování pro jakýkoli účel, který poskytovatel služby považuje za oprávněný, splňovalo ustanovení o „slučitelnosti“, přestože normotvůrce jednoznačně usiloval o omezení jeho použití na konkrétní účely v případě neexistence souhlasu. Evropský sbor pro ochranu osobních údajů by rád zdůraznil, že výše uvedené údaje mohou být i po anonymizaci dále zpracovány i bez souhlasu a bez vytváření rizik pro uživatele.

Budoucí úloha dozorových úřadů, Evropského sboru pro ochranu osobních údajů a mechanismu spolupráce (články 18 až 20)

Evropský sbor pro ochranu osobních údajů připomíná, že mají-li být na jednotném digitálním trhu zaručeny rovné podmínky, je nezbytné zajistit v celé EU harmonizovaný výklad a prosazování všech ustanovení o zpracovávání údajů obsažených v nařízení o soukromí a elektronických komunikacích.

Dohled nad ustanoveními o ochraně soukromí podle nařízení o soukromí a elektronických komunikacích by měl být za účelem další podpory jednotnosti svěřen příslušným dozorovým úřadům podle GDPR.

Evropský sbor pro ochranu osobních údajů by rád připomněl, že existuje jasné propojení pravomocí mezi vnitrostátními orgány příslušnými podle stávající směrnice o soukromí a elektronických komunikacích a úřady pro ochranu údajů. Ustanovení budoucího nařízení o soukromí a elektronických komunikacích týkající se ochrany soukromí by neměla být uplatňována izolovaně, neboť jsou provázána se zpracováním osobních údajů a s GDPR.

V zájmu sladění vysoké úrovně ochrany osobních údajů s právní a procesní jistotou by proto vnitrostátní orgány odpovědné za prosazování GDPR měly být pověřeny dohledem nad ustanoveními budoucího nařízení o soukromí a elektronických komunikacích, která se týkají zpracování osobních údajů, jak původně navrhla Evropská komise⁷.

⁷ Evropská komise, Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), 10. ledna 2017, k dispozici na adrese: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52017PC0010> a

Evropský sbor pro ochranu osobních údajů konstatuje, že na rozdíl od původního návrhu Evropské komise byly z postoje Rady odstraněny všechny odkazy na mechanismus spolupráce a jednotnosti stanovený v kapitole VII GDPR. Z výše uvedených důvodů EDPB znovu připomíná, že dokonalé sladění s rámcem pro spolupráci a jednotnost GDPR je pro nařízení o soukromí a elektronických komunikacích nezbytným předpokladem, který mu umožní dosáhnout jeho cílů, zabrání roztříštěnosti při jeho prosazování a uplatňování a také sníží zátěž pro poskytovatele, kteří by se jinak museli obracet na možná více než 27 dozorových úřadů.

Pokud by příslušné vnitrostátní orgány, které nejsou členy Evropského sboru pro ochranu osobních údajů, musely s tímto sborem spolupracovat, jak v současné době předpokládá postoj Rady, jejich schopnost včas přispívat k jednotnému uplatňování nařízení o soukromí a elektronických komunikacích by se snížila, což by mělo nepříznivý dopad na digitální ekonomiku i ochranu základních práv.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)

PŘÍLOHA: Seznam předchozích dokumentů vypracovaných Evropským sborem pro ochranu osobních údajů a pracovní skupinou zřízenou podle článku 29

-) Stanovisko 1/2009 k návrhům, kterými se mění směrnice 2002/58/ES o ochraně soukromí v elektronických komunikacích (směrnice o soukromí a elektronických komunikacích), k dispozici na adrese: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_cs.pdf.
-) Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies (WP 194), k dispozici na adrese: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf.
-) Stanovisko č. 3/2016 k hodnocení a přezkumu směrnice o soukromí a elektronických komunikacích (WP 240), k dispozici na adrese https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.
-) Stanovisko pracovní skupiny zřízené podle článku 29 k návrhu nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), k dispozici na adrese: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.
-) Prohlášení pracovní skupiny zřízené podle článku 29 o šifrování a jeho dopadu na ochranu jednotlivců v souvislosti se zpracováním jejich osobních údajů v EU, Brusel, 11. dubna 2018, k dispozici na adrese: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.
-) Prohlášení Evropského sboru pro ochranu osobních údajů o revizi nařízení o soukromí a elektronických komunikacích a jejím dopadu na ochranu fyzických osob v souvislosti se soukromím a důvěrným charakterem jejich komunikace, přijaté dne 25. května 2018, k dispozici na adrese: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_cs.pdf.
-) Prohlášení Evropského sboru pro ochranu osobních údajů č. 3/2019 o revizi nařízení o soukromí a elektronických komunikacích, přijaté dne 13. března 2019, k dispozici na adrese: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_cs.pdf.
-) Prohlášení k nařízení o soukromí a elektronických komunikacích a budoucí úloze dozorových úřadů a EDPB, přijaté dne 19. listopadu 2020, k dispozici na adrese: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-eprivacy-regulation-and-future-role-supervisory_cs.