

II

(Nelegislativní akty)

NAŘÍZENÍ

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2019/1799

ze dne 22. října 2019,

kterým se stanoví technické specifikace pro individuální online systémy sběru prohlášení o podpoře podle nařízení Evropského parlamentu a Rady (EU) 2019/788 o evropské občanské iniciativě

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2019/788 ze dne 17. dubna 2019 o evropské občanské iniciativě ⁽¹⁾, a zejména na čl. 11 odst. 5 uvedeného nařízení,

vzhledem k těmto důvodům:

- (1) Nařízení (EU) 2019/788 stanoví revidovaná pravidla pro evropskou občanskou iniciativu a zrušuje nařízení Evropského parlamentu a Rady (EU) č. 211/2011 ⁽²⁾.
- (2) Nařízení (EU) 2019/788 stanoví, že k online sběru prohlášení o podpoře registrovaných občanských iniciativ musí organizátoři využít centrálního online systému sběru zřízeného a provozovaného Komisí. K usnadnění přechodu si však organizátoři mohou v případě iniciativ zaregistrovaných do konce roku 2022 podle nařízení (EU) 2019/788 zvolit vlastní individuální online systém sběru.
- (3) Podle nařízení (EU) 2019/788 by měl mít individuální systém používaný pro online sběr prohlášení o podpoře odpovídající technické a bezpečnostní prvky, aby se zajistilo, že údaje jsou během celého sběru shromažďovány, ukládány a předávány bezpečným způsobem. Komise by společně s členskými státy měla stanovit technické specifikace pro zavedení požadavků na individuální online systémy sběru.
- (4) Pravidla stanovená v tomto nařízení nahrazují pravidla stanovená v prováděcím nařízení Komise (EU) č. 1179/2011 ⁽³⁾, která se proto stanou zastaralými.
- (5) Cílem technických a organizačních opatření, která mají být zavedena, by mělo být zabránění jakémukoli neoprávněnému zpracovávání osobních údajů a jejich ochraně před náhodným nebo nezákonným zničením nebo náhodnou ztrátou, změnou, neoprávněným poskytnutím nebo přístupem k nim, a to jak v době navrhování systému, tak po celé období sběru.

⁽¹⁾ Úř. věst. L 130, 17.5.2019, s. 55.⁽²⁾ Nařízení Evropského parlamentu a Rady (EU) č. 211/2011 ze dne 16. února 2011 o občanské iniciativě (Úř. věst. L 65, 11.3.2011, s. 1).⁽³⁾ Prováděcí nařízení Komise (EU) č. 1179/2011 ze dne 17. listopadu 2011, kterým se stanoví technické specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 211/2011 o občanské iniciativě (Úř. věst. L 301, 18.11.2011, s. 3).

- (6) Organizátoři by za tímto účelem měli uplatňovat přiměřené způsoby řízení rizik s cílem určit rizika pro své systémy a stanovit vhodná a přiměřená protipatření, aby tato rizika snížili na přijatelnou úroveň. Organizátoři by měli řádně zdokumentovat zjištěná bezpečnostní rizika, rizika spojená s ochranou údajů a opatření přijatá k odvrácení uvedených rizik, a to s ohledem na bezpečnostní pravidla a požadavky uplatňované orgánem ověřujícím soulad systému. Bezpečnostní pravidla a požadavky by měly být v souladu s nařízením (EU) 2019/788 a na požádání by je měl orgán ověřující soulad systému zpřístupnit.
- (7) Zavedením technických specifikací stanovených v tomto nařízení by neměla být dotčena povinnost organizátorů dodržovat požadavky na ochranu údajů vyplývající z nařízení Evropského parlamentu a Rady (EU) 2016/679 ⁽⁴⁾, včetně případné potřeby posouzení dopadu na ochranu údajů.
- (8) V souvislosti se zpracováním osobních údajů v individuálním online systému sběru se podle nařízení (EU) 2016/679 považuje za správce údajů zástupce skupiny organizátorů, nebo případně právní subjekt uvedený v čl. 5 odst. 7 zmíněného nařízení.
- (9) Organizátoři, kteří zavedou změny do svého individuálního online systému sběru poté, co byl ověřen soulad systému, by o tom měli bez zbytečného odkladu uvědomit příslušný orgán ověřující soulad systému, pokud by změna mohla ovlivnit posouzení, které je podkladem pro ověření souladu systému. Předtím si organizátoři mohou vyžádat vyjádření od orgánu ověřujícího soulad systému, aby si ověřili, zda může změna takový dopad mít, a měla by se proto oznámit.
- (10) V souladu s článkem 42 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ⁽⁵⁾ byl konzultován evropský inspektor ochrany údajů, který se k věci vyjádřil dne 16. září 2019. Byly vedeny konzultace s Agenturou Evropské unie pro bezpečnost sítí a informací, která podala připomínky dne 18. července 2019.
- (11) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného podle článku 22 nařízení (EU) 2019/788,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Technické specifikace uvedené v čl. 11 odst. 5 nařízení (EU) 2019/788 jsou stanoveny v příloze tohoto nařízení.

Článek 2

1. Organizátoři zajistí, aby jejich individuální online systém sběru byl po celé období sběru v souladu s technickými specifikacemi stanovenými v příloze.
2. Organizátoři bez zbytečného prodlení oznámí příslušnému orgánu členského státu uvedenému v čl. 11 odst. 3 nařízení (EU) 2019/788 změny, které jsou do systému nebo podpůrných organizačních opatření zavedeny poté, co uvedený orgán ověřil soulad systému, pokud tyto změny mohou mít dopad na posouzení, které je podkladem pro ověření souladu. Předtím si organizátoři mohou vyžádat vyjádření od příslušného orgánu, zda může změna takový dopad mít.

⁽⁴⁾ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

⁽⁵⁾ Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

Článek 3

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

Použije se ode dne 1. ledna 2020.

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

V Bruselu dne 22. října 2019.

Za Komisi
předseda
Jean-Claude JUNCKER

PŘÍLOHA

1. TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. 11 ODS. 4 PÍSM. A) NAŘÍZENÍ (EU) 2019/788

Systém zavádí technická opatření zajišťující, aby prohlášení o podpoře mohly podávat pouze fyzické osoby. Technická opatření nevyžadují, aby bylo shromažďováno a uchováno více osobních údajů, než je uvedeno v příloze III nařízení (EU) 2019/788.

2. TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. 11 ODS. 4 PÍSM. B) NAŘÍZENÍ (EU) 2019/788

Organizátoři zavedou přiměřená a účinná technická a organizační opatření k řízení rizik ohrožujících bezpečnost sítí a informačních systémů, které při svých operacích používají, aby se zajistilo, že informace poskytnuté o iniciativě v online systému sběru a zveřejněné online odpovídají informacím o iniciativě zveřejněným v registru uvedeném v čl. 6 odst. 5 nařízení (EU) 2019/788.

Organizátoři zajistí, aby:

- a) informace poskytnuté o iniciativě v online systému sběru odpovídaly informacím zveřejněným v registru;
- b) systém podával informace o iniciativě zveřejněné v registru dříve, než občan předloží prohlášení o podpoře;
- c) byla zavedena bezpečnostní opatření zajišťující, že pole pro vkládání údajů v prohlášeních o podpoře se zobrazují společně s informacemi o iniciativě, aby se zabránilo riziku, že prohlášení o podpoře budou v důsledku nedostatečného popisu příslušné iniciativy předložena k jiné iniciativě;
- d) systém zajišťoval, že po předložení prohlášení budou údaje v prohlášeních o podpoře uloženy spolu s informacemi o iniciativě;
- e) byla zavedena bezpečnostní opatření, která zamezí neoprávněným změnám informací poskytnutých o iniciativě v online systému sběru.

3. TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. 11 ODS. 4 PÍSM. C) NAŘÍZENÍ (EU) 2019/788

Systém zajistí, aby prohlášení o podpoře byla předkládána v souladu s datovými poli uvedenými v příloze III nařízení (EU) 2019/788.

Systém zajistí, aby osoba mohla předložit prohlášení o podpoře pouze poté, co potvrdí, že si přečetla prohlášení o ochraně soukromí uvedené v příloze III nařízení (EU) 2019/788.

4. TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. 11 ODS. 4 PÍSM. D) NAŘÍZENÍ (EU) 2019/788**4.1. Správa**

4.1.1. Skupina organizátorů jmenuje bezpečnostního pracovníka odpovědného za bezpečnost systému a bezpečné předávání shromážděných prohlášení o podpoře příslušnému orgánu odpovědného členského státu. Bezpečnostní pracovník dohlíží na postupy zabezpečení informací a na technická a organizační bezpečnostní opatření k zajištění bezpečného sběru, uchovávání a předávání údajů poskytovaných podepsanými osobami.

4.1.2. Organizátoři mohou požádat příslušný vnitrostátní orgán uvedený v čl. 11 odst. 3 nařízení (EU) 2019/788, aby stanovil příslušná bezpečnostní pravidla a požadavky na ověřování souladu individuálních online systémů sběru. Příslušný orgán stanoví bezpečnostní pravidla a požadavky zpravidla do jednoho měsíce od obdržení žádosti. Příslušná bezpečnostní pravidla a požadavky musí být v souladu se stávajícími příslušnými vnitrostátními nebo mezinárodními bezpečnostními normami.

- 4.1.3. Bezpečnostní pravidla a požadavky na ověřování souladu systému řeší rizika vymezená v oddíle 4.2 a zohledňují specifikace v oddíle 4.3.

4.2. Zabezpečení informací

- 4.2.1. Organizátoři používají postupy řízení rizik k identifikaci rizik spojených s používáním svých systémů, i pokud jde o práva a svobody podepsaných osob, a ke stanovení vhodných a přiměřených opatření k předcházení a zmírnění dopadu událostí ovlivňujících bezpečnost sítí a informačních systémů, které používají při svých operacích.

Postup řízení rizik se zaměří zejména na rizika spojená s důvěrností a integritou informací v systému. Tato rizika mohou vyplývat z hrozeb, mezi které patří:

- a) chyby uživatelů;
- b) chyby správce systému/zabezpečení;
- c) chyby v konfiguraci;
- d) napadení malwarem;
- e) náhodné změny informací;
- f) poskytnutí nebo únik informací;
- g) zranitelnost softwaru;
- h) neoprávněný přístup;
- i) zachycení nebo odposlech informací;
- j) rizika související s ochranou údajů.

- 4.2.2. Organizátoři předloží dokumentaci prokazující, že:

- a) posoudili rizika systému;
- b) stanovili vhodná opatření k předcházení a zmírnění dopadu událostí ovlivňujících bezpečnost systému;
- c) určili zbytková rizika;
- d) zavedli opatření a ověřili jejich provádění;
- e) zajistili organizační prostředky k získávání informací o nových hrozbách a zlepšeních v oblasti bezpečnosti;
- f) v průběhu celého období sběru splňují požadavky na ověřování souladu stanovené v čl. 11 odst. 4 nařízení (EU) 2019/788, včetně zavedení nezbytných postupů, jimiž se splnění požadavků zajistí.

- 4.2.3. Opatření k předcházení a zmírnění dopadu událostí ovlivňujících bezpečnost systémů se týkají těchto oblastí:

- a) bezpečnosti lidských zdrojů;
- b) kontroly přístupu;
- c) kryptografických kontrol;
- d) fyzické a environmentální bezpečnosti;
- e) bezpečnosti operací;
- f) bezpečnosti komunikací;
- g) pořízení, vývoje a údržby systému;
- h) řízení incidentů v oblasti bezpečnosti informací;
- i) souladu s požadavky.

Uplatňování těchto bezpečnostních opatření se může omezovat jen na části organizace, které souvisejí s online systémem sběru. Například bezpečnost lidských zdrojů se může omezovat na pracovníky, kteří mají fyzický nebo logický přístup k online systému sběru, a fyzická/environmentální bezpečnost se může omezovat na budovy, v nichž se systém nachází.

- 4.2.4. Pokud organizátoři využívají zpracovatele pro vývoj nebo zavádění online systémů sběru nebo jejich částí, poskytnou dokumentaci, na jejímž základě se orgán ověřující soulad ujistí o tom, že jsou zavedeny nezbytné bezpečnostní kontroly.

4.3. **Šifrování údajů**

Systém zajišťuje toto šifrování údajů:

- a) osobní údaje v elektronickém formátu se šifrují při ukládání nebo odesílání příslušným orgánům členských států v souladu s nařízením (EU) 2019/788, přičemž klíče se spravují a zálohují odděleně;
 - b) v souladu s mezinárodními normami (např. norma ETSI) se používají odpovídající standardní algoritmy a klíče. Zavádí se správa klíčů;
 - c) všechny klíče a hesla jsou chráněny před neoprávněným přístupem.
-