II

(Nelegislatívne akty)

NARIADENIA

VYKONÁVACIE NARIADENIE KOMISIE 2019/1799

z 22. októbra 2019,

ktorým sa ustanovujú technické špecifikácie pre individuálne online systémy na zber vyhlásení podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/788 o európskej iniciatíve občanov

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2019/788 zo 17. apríla 2019 o európskej iniciatíve občanov ([1]), a najmä na jeho článok 11 ods. 5,

keďže:

(1) Nariadením (EÚ) 2019/788 sa stanovujú revidované pravidlá týkajúce sa európskej iniciatívy občanov a zrušuje sa nariadenie Európskeho parlamentu a Rady (EÚ) č. 211/2011 ([2]).

(2) V nariadení (EÚ) 2019/788 sa stanovuje, že na online zber vyhlásení o podpore pre registrované občianske iniciatívy musia organizátori využiť centrálny online systém na zber vyhlásení, ktorý zriadi a prevádzkuje Komisia. V záujme uľahčenia prechodu sa však organizátori môžu rozhodnúť pre používanie vlastného individuálneho online systému na zber vyhlásení pri iniciatívach zaregistrovaných podľa nariadenia (EÚ) 2019/788 do konca roka 2022.

(3) Podľa nariadenia (EÚ) 2019/788 by individuálny systém, ktorý sa používa na online zber vyhlásení o podpore, mal mať primerané technické a ochranné prvky s cieľom zabezpečiť, aby boli údaje počas celého postupu zberu bezpečne zozbierané, uložené a prenášané. Komisia by mala spolu s členskými štátmi vymedziť technické špecifikácie na splnenie požiadaviek na individuálne online systémy zberu.

(4) Pravidlami stanovenými v tomto nariadení sa nahrádzajú pravidlá stanovené vo vykonávacom nariadení Komisie (EÚ) č. 1179/2011 ([3]), ktoré sa preto stanú zastaranými.

(5) Cieľom technických a organizačných opatrení, ktoré sa majú vykonať, by malo byť predchádzanie akémukoľvek neoprávnenému spracovaniu osobných údajov, a to tak v čase návrhu systému, ako aj počas celého obdobia zberu, a ich ochrana proti náhodnému alebo nezákonnému zničeniu alebo náhodnej strate, zmene, neoprávnenému zverejneniu či prístupu k nim.

([1]) Ú. v. EÚ L 130, 17.5.2019, s. 55.
([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 211/2011 zo 16. februára 2011 o iniciatíve občanov (Ú. v. EÚ L 65, 11.3.2011, s. 1).
([3]) Vykonávacie nariadenie Komisie (EÚ) č. 1179/2011 zo 17. novembra 2011, ktorým sa ustanovujú technické špecifikácie pre online systémy zberu podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 211/2011 o iniciatíve občanov (Ú. v. EÚ L 301, 18.11.2011, s. 3).

(6) Organizátori by na tento účel mali uplatňovať primerané procesy riadenia rizík s cieľom identifikovať riziká pre ich systémy a určiť vhodné a primerané protiopatrenia na zníženie týchto rizík na prijateľnú úroveň. Organizátori by mali zistené riziká v oblasti bezpečnosti a ochrany údajov a opatrenia prijaté proti týmto rizikám riadne zdokumentovať so zreteľom na bezpečnostné pravidlá a požiadavky, ktoré uplatňuje certifikačný orgán. Bezpečnostné pravidlá a požiadavky by mali byť v súlade s nariadením (EÚ) 2019/788 a certifikačný orgán by ich mal na požiadanie poskytnúť.

(7) Vykonávaním technických špecifikácií stanovených v tomto nariadení by nemala byť dotknutá povinnosť organizátorov dodržiavať požiadavky na ochranu údajov podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 ([4]) vrátane možnej potreby posúdenia vplyvu na ochranu údajov.

(8) Zástupca skupiny organizátorov alebo prípadne právny subjekt uvedený v článku 5 ods. 7 uvedeného nariadenia sa v súvislosti so spracovaním osobných údajov v individuálnom online systéme na zber považujú za prevádzkovateľov údajov podľa nariadenia (EÚ) 2016/679.

(9) Organizátori, ktorí zavedú zmeny do svojho individuálneho online systému na zber vyhlásení po certifikácii systému, by to mali bez zbytočného odkladu oznámiť príslušnému certifikačnému orgánu, ak by zmena mohla ovplyvniť posúdenie, ktoré je základom certifikácie. Predtým sa organizátori môžu obrátiť na certifikačný orgán, aby si overili, či môže mať zmena takýto vplyv, a mala by sa preto oznámiť.

(10) S európskym dozorným úradníkom pre ochranu údajov sa konzultovalo v súlade s článkom 42 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([5]), pričom pripomienky predložil 16. septembra 2019. Uskutočnili sa konzultácie s Agentúrou Európskej únie pre sieťovú a informačnú bezpečnosť, ktorá predložila svoje pripomienky 18. júla 2019.

(11) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru zriadeného podľa článku 22 nariadenia (EÚ) 2019/788,

PRIJALA TOTO NARIADENIE:

Článok 1

Technické špecifikácie uvedené v článku 11 ods. 5 nariadenia (EÚ) 2019/788 sú stanovené v prílohe k tomuto nariadeniu.

Článok 2

1. Organizátori zabezpečia, aby bol ich individuálny online systém na zber vyhlásení v súlade s technickými špecifikáciami stanovenými v prílohe počas celého obdobia zberu.

2. Organizátori bez zbytočného odkladu oznámia príslušnému orgánu členského štátu uvedenému v článku 11 ods. 3 nariadenia (EÚ) 2019/788 zmeny, ktoré boli zavedené v systéme alebo v podporných organizačných opatreniach po tom, ako tento orgán udelil osvedčenie systému, ak tieto zmeny môžu ovplyvniť posúdenie, ktoré je základom certifikácie. Predtým sa organizátori môžu obrátiť na príslušný orgán, aby si overili, či môže mať zmena takýto vplyv.

([4]) 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).

([5]) 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).

Článok 3

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Uplatňuje sa od 1. januára 2020.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 22. októbra 2019

Za Komisiu
predseda
Jean-Claude JUNCKER

PRÍLOHA

1. **TECHNICKÉ ŠPECIFIKÁCIE, KTORÝCH ÚČELOM JE VYKONÁVANIE ČLÁNKU 11 ODS. 4 PÍSM. A) NARIADENIA (EÚ) 2019/788**

V systéme sa musia zaviesť technické opatrenia, ktorými sa zabezpečí, aby vyhlásenia o podpore mohli predkladať iba fyzické osoby. Technické opatrenia nesmú vyžadovať, aby sa zbieralo a uchovávalo viac osobných údajov, ako sú tie, ktoré sú uvedené v prílohe III k nariadeniu (EÚ) 2019/788.

2. **TECHNICKÉ ŠPECIFIKÁCIE, KTORÝCH ÚČELOM JE VYKONÁVANIE ČLÁNKU 11 ODS. 4 PÍSM. B) NARIADENIA (EÚ) 2019/788**

Organizátori zavedú primerané a účinné technické a organizačné opatrenia na riadenie rizík spojených s bezpečnosťou sietí a informačných systémov, ktoré používajú pri svojich činnostiach, s cieľom zabezpečiť, aby informácie poskytnuté o iniciatíve v online systéme na zber vyhlásení a zverejnené online zodpovedali informáciám o iniciatíve uverejneným v registri, ktorý sa uvádza v článku 6 ods. 5 nariadenia (EÚ) 2019/788.

Organizátori zabezpečia, aby:

a) informácie o iniciatíve poskytnuté v online systéme na zber zodpovedali informáciám uverejneným v registri;

b) systém prezentoval informácie o iniciatíve uverejnené v registri predtým, ako občan predloží vyhlásenie o podpore;

c) boli zavedené bezpečnostné opatrenia na zabezpečenie toho, aby sa polia vo vyhláseniach o podpore, do ktorých sa vpisujú údaje, prezentovali spolu s informáciami o iniciatíve, s cieľom predísť riziku, že sa vyhlásenia o podpore predložia k inej iniciatíve v dôsledku skreslenia informácií o iniciatíve;

d) systém zabezpečoval, že sa po odoslaní údajov údaje vo vyhláseniach o podpore uložia spolu s informáciami o iniciatíve;

e) sa zaviedli bezpečnostné opatrenia, aby sa zabránilo nepovoleným zmenám informácií poskytovaných o iniciatíve v online systéme na zber.

3. **TECHNICKÉ ŠPECIFIKÁCIE, KTORÝCH ÚČELOM JE VYKONÁVANIE ČLÁNKU 11 ODS. 4 PÍSM. C) NARIADENIA (EÚ) 2019/788**

V systéme sa zabezpečí, aby sa vyhlásenia o podpore predkladali v súlade s údajmi uvedenými v prílohe III k nariadeniu (EÚ) 2019/788.

V systéme sa zabezpečí, aby osoba mohla vyhlásenie o podpore predložiť až po tom, ako potvrdí, že si prečítala vyhlásenie o ochrane osobných údajov uvedené v prílohe III k nariadeniu (EÚ) 2019/788.

4. **TECHNICKÉ ŠPECIFIKÁCIE, KTORÝCH ÚČELOM JE VYKONÁVANIE ČLÁNKU 11 ODS. 4 PÍSM. D) NARIADENIA (EÚ) 2019/788**

4.1. **Správa**

4.1.1. Skupina organizátorov nominuje bezpečnostného pracovníka zodpovedného za bezpečnosť systému a bezpečný prenos zozbieraných vyhlásení o podpore príslušnému orgánu zodpovedného členského štátu. Bezpečnostný pracovník dohliada na procesy zabezpečovania informácií a technické a organizačné bezpečnostné opatrenia na zaistenie bezpečného zberu, uchovávania a prenosu údajov, ktoré poskytli signatári.

4.1.2. Organizátori môžu požiadať príslušný vnútroštátny orgán uvedený v článku 11 ods. 3 nariadenia (EÚ) 2019/788, aby poskytol uplatniteľné bezpečnostné pravidlá a požiadavky na certifikáciu jednotlivých online systémov na zber. Príslušný orgán poskytne bezpečnostné pravidlá a požiadavky spravidla do jedného mesiaca po prijatí žiadosti. Uplatniteľné bezpečnostné pravidlá a požiadavky musia byť v súlade s existujúcimi príslušnými vnútroštátnymi alebo medzinárodnými bezpečnostnými normami.

4.1.3. Bezpečnostné pravidlá a požiadavky na certifikáciu systému musia obsahovať riešenia rizík vymedzených v oddiele 4.2 a zohľadňovať špecifikácie uvedené v oddiele 4.3.

4.2. **Informačná bezpečnosť**

4.2.1. Organizátori musia používať procesy riadenia rizík na identifikáciu rizík spojených s používaním svojich systémov vrátane práv a slobôd signatárov a na stanovenie vhodných a primeraných opatrení na predchádzanie a zmierňovanie vplyvu incidentov ovplyvňujúcich bezpečnosť sietí a informačných systémov, ktoré používajú pri svojej prevádzke.

Proces riadenia rizík má byť zameraný najmä na riziká súvisiace s dôvernosťou a integritou informácií v systéme. Tieto riziká môžu byť výsledkom hrozieb vrátane:

a) chýb používateľov;

b) chýb správcu systému/bezpečnostného správcu;

c) chýb v konfigurácii;

d) infekcie malvérom;

e) náhodnej zmeny informácií;

f) zverejnenia informácií alebo únikov informácií;

g) zraniteľnosti softvéru;

h) neoprávneného prístupu;

i) zachytenia alebo odpočúvania;

j) rizík spojených s ochranou údajov.

4.2.2. Organizátori musia poskytnúť dokumentáciu preukazujúcu, že:

a) posúdili riziká systému;

b) stanovili vhodné opatrenia na predchádzanie a zmierňovanie dôsledkov incidentov ovplyvňujúcich bezpečnosť systému;

c) identifikovali reziduálne riziká;

d) vykonali opatrenia a overili ich vykonávanie;

e) zabezpečili organizačné prostriedky na získanie informácií, pokiaľ ide o nové hrozby a vylepšenia bezpečnosti;

f) dodržiavajú počas celého procesu zberu požiadavky na certifikáciu stanovené v článku 11 ods. 4 nariadenia (EÚ) 2019/788 vrátane zavedenia potrebných procesov na ich zabezpečenie.

4.2.3. Opatrenia na predchádzanie a zmierňovanie vplyvu incidentov ovplyvňujúcich bezpečnosť systémov zahŕňajú tieto oblasti:

a) bezpečnosť ľudských zdrojov;

b) kontrola prístupu;

c) kryptografické kontroly;

d) fyzická a environmentálna bezpečnosť;

e) bezpečnosť prevádzky,

f) komunikačná bezpečnosť;

g) kúpa, vývoj a údržba systémov;

h) riadenie incidentov informačnej bezpečnosti;

i) súlad.

Uplatňovanie týchto bezpečnostných opatrení môže byť obmedzené na časti organizácie, ktoré súvisia s online systémom na zber. Napríklad bezpečnosť ľudských zdrojov môže byť obmedzená na personál, ktorý má fyzický alebo logický prístup k online systému na zber, a fyzická/environmentálna bezpečnosť môže byť obmedzená na budovy, v ktorých je systém umiestnený.

4.2.4. Ak organizátori využívajú spracovateľa údajov na vývoj alebo zavádzanie online systémov na zber alebo ich častí, organizátori poskytnú dokumentáciu, ktorá certifikačnému orgánu umožní zistiť, či sú zavedené potrebné bezpečnostné kontroly.

4.3. **Šifrovanie údajov**

Systém zabezpečí takéto šifrovanie údajov:

a) osobné údaje v elektronickom formáte sú šifrované pri ukladaní alebo posielaní príslušným orgánom členských štátov v súlade s nariadením (EÚ) 2019/788, kľúče sa spravujú a zálohujú osobitne;

b) používať sa musia primerané štandardné algoritmy a primerané kľúče v súlade s medzinárodnými normami (ako napríklad s normou ETSI). Zavedený musí byť systém riadenia kľúčov;

c) všetky kľúče a heslá musia byť zabezpečené proti neoprávnenému prístupu.