II

(Nezakonodavni akti)

UREDBE

PROVEDBENA UREDBA KOMISIJE (EU) 2019/1799

od 22. listopada 2019.

o utvrđivanju tehničkih specifikacija za pojedinačne sustave internetskog prikupljanja u skladu s Uredbom (EU) 2019/788 Europskog parlamenta i Vijeća o europskoj građanskoj inicijativi

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2019/788 Europskog parlamenta i Vijeća od 17. travnja 2019. o europskoj građanskoj inicijativi ([1]), a posebno njezin članak 11. stavak 5.,

budući da:

(1) Uredbom (EU) 2019/788 utvrđuju se revidirana pravila o europskoj građanskoj inicijativi i stavlja izvan snage Uredba (EU) br. 211/2011 Europskog parlamenta i Vijeća ([2]).

(2) Uredbom (EU) 2019/788 propisuje se da za internetsko prikupljanje izjava o potpori registriranim inicijativama građana organizatori moraju upotrebljavati središnji sustav internetskog prikupljanja koji uspostavlja i vodi Komisija. Međutim, kako bi se olakšao prijelaz, organizatori mogu odlučiti upotrebljavati vlastiti pojedinačni sustav internetskog prikupljanja za inicijative registrirane na temelju Uredbe (EU) 2019/788 prije kraja 2022.

(3) U skladu s Uredbom (EU) 2019/788 pojedinačni sustav koji se upotrebljava za internetsko prikupljanje izjava o potpori trebao bi imati odgovarajuće tehničke i sigurnosne značajke kako bi se osiguralo da se podaci tijekom cijelog postupka prikupljaju, pohranjuju i prenose na siguran način. Komisija bi zajedno s državama članicama trebala utvrditi tehničke specifikacije koje pojedinačni sustavi internetskog prikupljanja moraju imati kako bi ispunili zahtjeve.

(4) Pravilima utvrđenima u ovoj Uredbi zamjenjuju se pravila utvrđena u Provedbenoj uredbi Komisije (EU) br. 1179/2011 ([3]), koja će stoga zastarjeti.

(5) Tehničkim i organizacijskim mjerama koje će se provesti trebalo bi nastojati spriječiti, u trenutku izrade sustava i tijekom cijelog razdoblja prikupljanja, svaku neovlaštenu obradu osobnih podataka te ih zaštititi od slučajnog ili nezakonitog uništavanja ili slučajnog gubitka, izmjene, neovlaštenog otkrivanja ili pristupa.

([1]) SL L 130, 17.5.2019., str. 55.
([2]) Uredba (EU) br. 211/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o građanskoj inicijativi (SL L 65, 11.3.2011., str. 1.).
([3]) Provedbena uredba Komisije (EU) br. 1179/2011 od 17. studenoga 2011. o utvrđivanju tehničkih specifikacija za sustave za online prikupljanje u skladu s Uredbom (EU) br. 211/2011 Europskog parlamenta i Vijeća o građanskoj inicijativi (SL L 301, 18.11.2011., str. 3.).

(6) U tu bi svrhu organizatori trebali primjenjivati odgovarajuće postupke upravljanja rizicima kako bi ustanovili kojim su rizicima njihovi sustavi izloženi te utvrdili prikladne i razmjerne protumjere za smanjenje tih rizika na prihvatljivu razinu. Organizatori bi trebali propisno dokumentirati utvrđene sigurnosne rizike i rizike za zaštitu podataka te mjere poduzete za suzbijanje tih rizika, uzimajući u obzir sigurnosna pravila i zahtjeve koje primjenjuje tijelo za potvrđivanje. Sigurnosna pravila i zahtjevi trebali bi biti u skladu s Uredbom (EU) 2019/788 te bi ih tijelo za potvrđivanje trebalo staviti na raspolaganje na zahtjev.

(7) Implementacija tehničkih specifikacija utvrđenih u ovoj Uredbi ne bi trebala dovesti u pitanje obvezu organizatorâ da ispune zahtjeve za zaštitu podataka koji proizlaze iz Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća ([4]), uključujući moguću potrebu za procjenom učinka na zaštitu podataka.

(8) Predstavnik skupine organizatora ili, ovisno o slučaju, pravni subjekt iz članka 5. stavka 7. te uredbe smatra se voditeljem obrade podataka na temelju Uredbe (EU) 2016/679 u vezi s obradom osobnih podataka u pojedinačnom sustavu internetskog prikupljanja.

(9) Organizatori koji svoj pojedinačni sustav internetskog prikupljanja izmijene nakon njegova potvrđivanja trebali bi bez nepotrebne odgode o tome izvijestiti relevantno tijelo za potvrđivanje ako bi izmjena mogla utjecati na procjenu na kojoj se potvrda temelji. Prije toga organizatori se mogu posavjetovati s tijelom za potvrđivanje kako bi provjerili može li izmjena imati takav utjecaj i trebaju li o njoj izvijestiti.

(10) U skladu s člankom 42. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([5]) provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka, koji je komentare dostavio 16. rujna 2019. Provedeno je savjetovanje s Agencijom Europske unije za mrežnu i informacijsku sigurnost, koja je komentare dostavila 18. srpnja 2019.

(11) Mjere predviđene ovom Uredbom u skladu su s mišljenjem Odbora uspostavljenog člankom 22. Uredbe (EU) 2019/788,

DONIJELA JE OVU UREDBU:

Članak 1.

Tehničke specifikacije iz članka 11. stavka 5. Uredbe (EU) 2019/788 utvrđene su u Prilogu ovoj Uredbi.

Članak 2.

1. Organizatori su dužni pobrinuti se za to da njihov pojedinačni sustav internetskog prikupljanja bude u skladu s tehničkim specifikacijama utvrđenima u Prilogu tijekom cijelog razdoblja prikupljanja.

2. Organizatori su dužni bez nepotrebne odgode izvijestiti nadležno tijelo države članice iz članka 11. stavka 3. Uredbe (EU) 2019/788 o izmjenama sustava ili organizacijskih mjera potpore koje su uvedene nakon što je tijelo potvrdilo sustav ako te izmjene mogu utjecati na procjenu na kojoj se potvrda temelji. Prije toga organizatori se mogu posavjetovati s nadležnim tijelom o tome bi li izmjena mogla imati takav utjecaj.

([4]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

([5]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

Članak 3.

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Primjenjuje se od 1. siječnja 2020.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 22. listopada 2019.

Za Komisiju
Predsjednik
Jean-Claude JUNCKER

PRILOG

1. **TEHNICKE SPECIFIKACIJE ZA PROVEDBU CLANKA 11. STAVKA 4. TOCKE (A) UREDBE (EU) 2019/788**

U sustavu se primjenjuju tehničke mjere kojima se postiže da izjave o potpori mogu podnijeti samo fizičke osobe. Zbog tih se tehničkih mjera ne smije prikupljati i pohranjivati više osobnih podataka nego što je navedeno u Prilogu III. Uredbi (EU) 2019/788.

2. **TEHNICKE SPECIFIKACIJE ZA PROVEDBU CLANKA 11. STAVKA 4. TOCKE (B) UREDBE (EU) 2019/788**

Organizatori su dužni uvesti primjerene i učinkovite tehničke i organizacijske mjere za upravljanje sigurnosnim rizicima kojima su izloženi mrežni i informacijski sustavi kojima se služe u poslovanju kako bi informacije o inicijativi koje su navedene u sustavu internetskog prikupljanja i predstavljene javnosti na internetu odgovarale informacijama o inicijativi objavljenima u registru iz članka 6. stavka 5. Uredbe (EU) 2019/788.

Organizatori su dužni pobrinuti se za sljedeće:

(a) informacije o inicijativi navedene u sustavu internetskog prikupljanja odgovaraju informacijama objavljenima u registru;

(b) informacije o inicijativi objavljene u registru sustav prikazuje prije nego što građanin podnese izjavu o potpori;

(c) primjenjuju se sigurnosne mjere koje omogućuju da se polja za unos podataka u izjavama o potpori prikazuju zajedno s informacijama o inicijativi kako bi se spriječilo podnošenje izjava o potpori za neku drugu inicijativu zbog pogrešnog prikazivanja inicijative;

(d) sustav je izveden tako da se podaci iz izjava o potpori nakon podnošenja pohranjuju zajedno s informacijama o inicijativi;

(e) primjenjuju se sigurnosne mjere protiv neovlaštenih izmjena informacija o inicijativi u sustavu internetskog prikupljanja.

3. **TEHNICKE SPECIFIKACIJE ZA PROVEDBU CLANKA 11. STAVKA 4. TOCKE (C) UREDBE (EU) 2019/788**

Sustav mora biti izveden tako da se izjave o potpori dostavljaju u skladu s poljima za unos podataka iz Priloga III. Uredbi (EU) 2019/788.

Sustav mora biti izveden tako da osoba može podnijeti izjavu o potpori tek nakon što potvrdi da je pročitala izjavu o zaštiti osobnih podataka iz Priloga III. Uredbi (EU) 2019/788.

4. **TEHNICKE SPECIFIKACIJE ZA PROVEDBU CLANKA 11. STAVKA 4. TOCKE (D) UREDBE (EU) 2019/788**

4.1. **Upravljanje**

4.1.1. Skupina organizatora imenuje službenika za sigurnost koji je odgovoran za sigurnost sustava i siguran prijenos prikupljenih izjava o potpori nadležnom tijelu odgovorne države članice. Službenik za sigurnost nadzire postupke osiguravanja informacija i tehničke i organizacijske sigurnosne mjere kako bi se zajamčili sigurno prikupljanje, pohrana i prijenos podataka koje su dostavili potpisnici.

4.1.2. Organizatori mogu od nacionalnog nadležnog tijela iz članka 11. stavka 3. Uredbe (EU) 2019/788 zatražiti da dostavi primjenjiva sigurnosna pravila i zahtjeve za potvrđivanje pojedinačnih sustava internetskog prikupljanja. Nadležno tijelo sigurnosna pravila i zahtjeve u pravilu dostavlja u roku od mjesec dana od primitka zahtjeva. Primjenjiva sigurnosna pravila i zahtjevi moraju biti u skladu s postojećim odgovarajućim nacionalnim ili međunarodnim sigurnosnim standardima.

4.1.3. Sigurnosnim pravilima i zahtjevima za potvrđivanje sustava suzbijaju se rizici iz odjeljka 4.2. te se pritom uzimaju u obzir specifikacije iz odjeljka 4.3.

4.2. **Osiguravanje informacija**

4.2.1. Organizatori s pomoću postupaka upravljanja rizikom utvrđuju rizike povezane s upotrebom njihovih sustava, uključujući rizike za prava i slobode potpisnika, te određuju prikladne i razmjerne mjere za sprečavanje i ublažavanje učinka incidenata koji utječu na sigurnost mrežnih i informacijskih sustava kojima se služe u poslovanju.

Postupak upravljanja rizikom posebno je usmjeren na rizike povezane s povjerljivošću i cjelovitošću podataka u sustavu. Ti rizici mogu biti posljedica prijetnji, uključujući:

(a) korisničke pogreške;

(b) pogreške administratora sustava/administratora za sigurnost;

(c) pogreške u konfiguraciji;

(d) infekcija zlonamjernim programima;

(e) nenamjerna izmjena informacija;

(f) otkrivanje ili curenje informacija;

(g) ranjivosti softvera;

(h) neovlašten pristup;

(i) presretanje ili prisluškivanje prometa;

(j) rizici za zaštitu podataka.

4.2.2. Organizatori dostavljaju dokumentaciju kojom dokazuju da su učinili sljedeće:

(a) procijenili rizike sustava;

(b) odredili prikladne mjere za sprečavanje i ublažavanje učinka incidenata koji utječu na sigurnost sustava;

(c) utvrdili preostale rizike;

(d) uveli mjere i provjerili kako se provode;

(e) osigurali organizacijska sredstva za zaprimanje informacija o novim prijetnjama i poboljšanjima sigurnosti;

(f) osigurali da se zahtjevi za potvrđivanje iz članka 11. stavka 4. Uredbe (EU) 2019/788 poštuju tijekom cijelog postupka prikupljanja, među ostalim uvođenjem postupaka potrebnih da se to postigne.

4.2.3. Mjere za sprečavanje i ublažavanje učinka incidenata koji utječu na sigurnost sustava obuhvaćaju sljedeća područja:

(a) sigurnost ljudskih potencijala;

(b) kontrolu pristupa;

(c) kriptografske kontrole;

(d) fizičku sigurnost i sigurnost okruženja;

(e) sigurnost operacija;

(f) sigurnost komunikacija;

(g) nabavu, razvoj i održavanje sustava;

(h) upravljanje incidentima povezanima sa sigurnošću informacija;

(i) usklađenost.

Primjena navedenih sigurnosnih mjera može se ograničiti na dijelove organizacije koji su relevantni za sustav internetskog prikupljanja. Na primjer, sigurnost ljudskih potencijala može se ograničiti na osoblje koje ima fizički ili mrežni pristup sustavu za internetsko prikupljanje, a fizička sigurnost/sigurnost okruženja može se ograničiti na zgradu u kojoj je sustav smješten.

4.2.4. Ako se organizatori koriste uslugama izvršitelja obrade kako bi razvili ili pustili u rad sustav internetskog prikupljanja ili neke njegove dijelove, organizatori su dužni dostaviti dokumentaciju na temelju koje tijelo za potvrđivanje može utvrditi primjenjuju li se potrebne sigurnosne kontrole.

4.3. **Šifriranje podataka**

Sustav mora omogućivati sljedeće šifriranje podataka:

(a) osobni podaci u elektroničkom obliku šifriraju se pri pohrani ili prijenosu nadležnim tijelima država članica u skladu s Uredbom (EU) 2019/788, uz odvojeno upravljanje ključevima i izradu sigurnosnih kopija;

(b) upotrebljavaju se odgovarajući standardni algoritmi i odgovarajući ključevi u skladu s međunarodnim normama (kao što je norma ETSI). Primjenjuje se upravljanje ključevima;

(c) svi ključevi i lozinke zaštićeni su od neovlaštenog pristupa.