II

(Muud kui seadusandlikud aktid)

MÄÄRUSED

KOMISJONI RAKENDUSMÄÄRUS (EL) 2019/1799,

22. oktoober 2019,

millega vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2019/788 kodanikualgatuse kohta kehtestatakse toetusavalduste kogumise veebipõhiste üksiksüsteemide tehnilised kirjeldused

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrust (EL) 2019/788 kodanikualgatuse kohta, ([1]) eriti selle artikli 11 lõiget 5,

ning arvestades järgmist:

(1) Määrusega (EL) 2019/788 on muudetud Euroopa kodanikualgatust käsitlevaid eeskirju ning tunnistatud kehtetuks Euroopa Parlamendi ja nõukogu määrus (EL) nr 211/2011 ([2]).

(2) Määruses (EL) 2019/788 on sätestatud, et registreeritud kodanikualgatuste toetusavalduste veebipõhiseks kogumiseks peavad korraldajad kasutama komisjoni loodud ja käitatavat veebipõhist toetusavalduste kogumise kesksüsteemi. Et aga hõlbustada sellele üleminekut, võivad korraldajad enne 2022. aasta lõppu määruse (EL) 2019/788 kohaselt registreeritud algatuste puhul siiski otsustada, et nad kasutavad oma veebipõhist toetusavalduste kogumise üksiksüsteemi.

(3) Määruse (EL) 2019/788 kohaselt peaks toetusavalduste veebipõhiseks kogumiseks kasutatavate üksiksüsteemide tehnilised ja turvaomadused olema piisavad, et tagada andmete turvaline kogumine, säilitamine ja edastamine kogu menetluse vältel. Komisjon peaks koos liikmesriikidega määrama kindlaks tehnilised kirjeldused toetusavalduste kogumise veebipõhiste üksiksüsteemide nõuete rakendamiseks.

(4) Käesolevas määruses sätestatud eeskirjad asendavad komisjoni rakendusmääruses (EL) nr 1179/2011 ([3]) sätestatud eeskirjad, mis kaotavad seetõttu asjakohasuse.

(5) Rakendatavate tehniliste ja korralduslike meetmete eesmärk peaks olema vältida nii süsteemi loomise ajal kui ka kogu andmete kogumise perioodil isikuandmete loata töötlemist ja kaitsta neid juhusliku või ebaseadusliku hävitamise või juhusliku kaotsimineku, muutmise, loata avalikustamise või juurdepääsu eest.

([1]) ELT L 130, 17.5.2019, lk 55.
([2]) Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 211/2011 kodanikualgatuse kohta (ELT L 65, 11.3.2011, lk 1).
([3]) Komisjoni 17. novembri 2011. aasta rakendusmäärus (EL) nr 1179/2011, millega kehtestatakse veebipõhiste kogumissüsteemide tehnilised spetsifikatsioonid vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) nr 211/2011 kodanikualgatuse kohta (ELT L 301, 18.11.2011, lk 3).

(6) Selleks peaksid korraldajad rakendama asjakohaseid riskijuhtimismenetlusi, et tuvastada nende süsteemidega seotud riskid ning määrata kindlaks asjakohased ja proportsionaalsed vastumeetmed, et vähendada neid riske vastuvõetava tasemeni. Korraldajad peaksid nõuetekohaselt dokumenteerima tuvastatud turva- ja andmekaitseriskid ning nende riskide maandamiseks võetud meetmed, võttes arvesse sertifitseerimisasutuse kohaldatavaid turvaeeskirju ja -nõudeid. Turvaeeskirjad ja -nõuded peaksid olema kooskõlas määrusega (EL) 2019/788 ning sertifitseerimisasutus peaks need taotluse korral kättesaadavaks tegema.

(7) Käesolevas määruses sätestatud tehniliste kirjelduste rakendamine ei tohiks piirata korraldajate kohustust järgida Euroopa Parlamendi ja nõukogu määrusest (EL) 2016/679 ([4]) tulenevaid andmekaitsenõudeid, sealhulgas võimalikku vajadust koostada andmekaitsealane mõjuhinnang.

(8) Korraldajate rühma või vajaduse korral kõnealuse määruse artikli 5 lõikes 7 osutatud juriidilise isiku esindajat käsitatakse seoses isikuandmete töötlemisega toetusavalduste kogumise veebipõhises üksiksüsteemis määruse (EL) 2016/679 kohaste vastutatavate töötlejatena.

(9) Korraldajad, kes pärast süsteemi sertifitseerimist muudavad oma veebipõhist toetusavalduste kogumise süsteemi, peaksid juhul, kui muudatus võib mõjutada sertifitseerimise aluseks olevat hinnangut, teavitama asjaomast sertifitseerimisasutust sellest põhjendamatu viivituseta. Enne seda võivad korraldajad küsida sertifitseerimisasutuselt nõu, et kontrollida, kas muudatusel võib olla selline mõju, millisel juhul tuleks sellest teatada.

(10) Euroopa andmekaitseinspektoriga on konsulteeritud vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([5]) artiklile 42 ja ta esitas oma märkused 16. septembril 2019. Euroopa Liidu Võrgu- ja Infoturbeametiga on konsulteeritud ja ta esitas oma märkused 18. juulil 2019.

(11) Käesoleva määrusega ette nähtud meetmed on kooskõlas määruse (EL) 2019/788 artikli 22 kohaselt asutatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Määruse (EL) 2019/788 artikli 11 lõikes 5 osutatud tehnilised kirjeldused esitatakse käesoleva määruse lisas.

Artikkel 2

1. Korraldajad tagavad, et nende veebipõhine toetusavalduste kogumise üksiksüsteem vastab kogu kogumisperioodi jooksul lisas sätestatud tehnilistele kirjeldustele.

2. Korraldajad teavitavad määruse (EL) 2019/788 artikli 11 lõikes 3 osutatud liikmesriigi pädevat asutust põhjendamatu viivituseta, kui nad on süsteemi või toetavaid korralduslikke meetmeid muutnud pärast seda, kui kõnealune asutus on süsteemi sertifitseerinud, ja kui need muudatused võivad mõjutada sertifitseerimise aluseks olevat hinnangut. Enne seda võivad korraldajad küsida pädevalt asutuselt nõu, kas muudatusel võib olla selline mõju.

([4]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

([5]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

Artikkel 3

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Seda kohaldatakse alates 1. jaanuarist 2020.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 22. oktoober 2019

Komisjoni nimel
President
Jean-Claude JUNCKER

LISA

1. **TEHNILISED KIRJELDUSED MÄÄRUSE (EL) 2019/788 ARTIKLI 11 LÕIKE 4 PUNKTI A RAKENDAMISEKS**

Süsteemi puhul tuleb võtta tehnilised meetmed, et toetusavaldusi saaksid esitada üksnes füüsilised isikud. Tehniliste meetmetega ei nõuta, et kogutaks ja säilitataks rohkem isikuandmeid, kui on loetletud määruse (EL) 2019/788 III lisas.

2. **TEHNILISED KIRJELDUSED MÄÄRUSE (EL) 2019/788 ARTIKLI 11 LÕIKE 4 PUNKTI B RAKENDAMISEKS**

Et tagada veebipõhises toetusavalduste kogumise süsteemis algatuse kohta esitatud ja avalikkusele veebis esitatud teabe vastavus määruse (EL) 2019/788 artikli 6 lõikes 5 osutatud registris avaldatud teabele, kehtestavad korraldajad asjakohased ja tõhusad tehnilised ja korralduslikud meetmed, et juhtida nende tegevuses kasutatavate võrgu- ja infosüsteemide turvariske.

Korraldajad tagavad, et:

a) veebipõhises toetusavalduste kogumise süsteemis algatuse kohta esitatud teave vastab registris avaldatud teabele;

b) süsteemis on esitatud teave registris avaldatud algatuse kohta enne, kui kodanik toetusavalduse esitab;

c) kehtivad turvameetmed, millega tagatakse, et toetusavalduste andmeväljad esitatakse koos algatust käsitleva teabega, et vältida ohtu, et toetusavaldused esitatakse vale algatuse kuvamise tõttu teise algatuse kohta;

d) süsteemiga tagatakse, et pärast toetusavalduse esitamist salvestatakse andmed koos algatust käsitleva teabega;

e) kehtivad turvameetmed, millega välditakse veebipõhise toetusavalduste kogumise süsteemis algatust käsitleva teabe ilma loata muutmist.

3. **TEHNILISED KIRJELDUSED MÄÄRUSE (EL) 2019/788 ARTIKLI 11 LÕIKE 4 PUNKTI C RAKENDAMISEKS**

Süsteemiga tagatakse, et toetusavaldused esitatakse vastavalt määruse (EL) 2019/788 III lisas esitatud andmeväljadele.

Süsteemiga tagatakse, et isik saab esitada toetusavalduse alles pärast seda, kui ta on kinnitanud, et ta on lugenud määruse (EL) 2019/788 III lisas esitatud isikuandmete kaitse avaldust.

4. **TEHNILISED KIRJELDUSED MÄÄRUSE (EL) 2019/788 ARTIKLI 11 LÕIKE 4 PUNKTI D RAKENDAMISEKS**

4.1. **Juhtimine**

4.1.1. Korraldajate rühm nimetab ametisse turbeametniku, kes vastutab süsteemi turvalisuse ja kogutud toetusavalduste turvalise edastamise eest vastutava liikmesriigi pädevale asutusele. Turvaametnik teeb järelevalvet infokindluse protsesside ning tehniliste ja korralduslike turvameetmete üle, et tagada allakirjutanute esitatud andmete turvaline kogumine, säilitamine ja edastamine.

4.1.2. Korraldajad võivad paluda määruse (EL) 2019/788 artikli 11 lõikes 3 osutatud riiklikul pädeval asutusel esitada toetusavalduste kogumise veebipõhiste süsteemide sertifitseerimise turvaeeskirjad ja -nõuded. Pädev asutus esitab turvaeeskirjad ja -nõuded reeglina ühe kuu jooksul pärast taotluse saamist. Kohaldatavad turvaeeskirjad ja -nõuded peavad olema kooskõlas kehtivate asjaomaste riiklike või rahvusvaheliste turvastandarditega.

4.1.3. Süsteemi sertifitseerimise turvaeeskirjades ja -nõuetes käsitletakse punktis 4.2 määratletud riske ja võetakse arvesse punktis 4.3 esitatud kirjeldusi.

4.2. **Infokindlus**

4.2.1. Korraldajad kasutavad riskijuhtimismenetlusi, et tuvastada oma süsteemide kasutamisega seotud riskid, sealhulgas allakirjutanute õiguste ja vabadustega seotud riskid, ning määrata kindlaks asjakohased ja proportsionaalsed meetmed, et ennetada ja leevendada selliste intsidentide mõju, mis mõjutavad nende tegevuses kasutatavate võrgu- ja infosüsteemide turvalisust.

Riskijuhtimismenetluses keskendutakse eelkõige riskidele, mis on seotud süsteemis oleva teabe konfidentsiaalsuse ja terviklikkusega. Mõningad nendest riskidest võivad tuleneda järgmistest ohtudest:

a) kasutajate vead;

b) süsteemi-/turvahalduri vead;

c) seadistusvead;

d) pahavaraga nakatumine;

e) teabe juhuslik muutmine;

f) teabe avaldamine või lekked;

g) tarkvara haavatavus;

h) loata juurdepääs;

i) andmeliikluse jälgimine või pealtkuulamine;

j) andmekaitseriskid.

4.2.2. Korraldajad esitavad dokumendid, millest nähtub, et nad:

a) on hinnanud süsteemi riske;

b) on kindlaks määranud asjakohased meetmed süsteemi turvalisust mõjutavate intsidentide mõju ennetamiseks ja leevendamiseks;

c) on tuvastanud jääkriskid;

d) on rakendanud meetmeid ja kontrollinud nende rakendamist;

e) on ette näinud korralduslikud vahendid info saamiseks uute ohtude ja turvalisuse täiendamise teemadel;

f) täidavad kogu teabekogumise protsessi vältel määruse (EL) 2019/788 artikli 11 lõikes 4 sätestatud sertifitseerimisnõudeid ja on selle tagamiseks kehtestanud vajalikud protsessid.

4.2.3. Süsteemide turvalisust mõjutavate intsidentide ennetamise ja leevendamise meetmed hõlmavad järgmisi valdkondi:

a) personali turvalisus;

b) juurdepääsukontroll;

c) krüptograafilised kontrollid;

d) füüsiline turvalisus ja keskkonnaohutus;

e) toimingute turvalisus;

f) teabeedastuse turvalisus;

g) süsteemi soetamine, arendamine ja hooldamine;

h) infoturbeintsidentide haldus;

i) nõuetele vastavus.

Nende turvameetmete kohaldamist võib piirata vaid veebipõhise kogumissüsteemiga seotud organisatsiooni osadega. Näiteks personali turvalisus võib olla piiratud nende isikutega, kellel on veebipõhisele kogumissüsteemile füüsiline või loogiline juurdepääs, ning füüsiline turvalisus/keskkonnaohutus võib olla piiratud vaid süsteemi majutava(te) hoone(te)ga.

4.2.4. Kui korraldajad kasutavad veebipõhiste toetusavalduste kogumise süsteemide või nende osade arendamiseks või kasutuselevõtuks töötlejat, esitavad korraldajad dokumendid, mis võimaldavad sertifitseerimisasutusel teha kindlaks, kas on kehtestatud vajalikud turvakontrolli meetmed.

4.3. **Andmete krüpteerimine**

Süsteemiga nähakse ette andmete järgmine krüpteerimine:

a) elektroonilises vormingus isikuandmed krüpteeritakse, kui neid säilitatakse või need edastatakse liikmesriikide pädevatele asutustele kooskõlas määrusega (EL) 2019/788, kusjuures võtmeid hallatakse ja varundatakse eraldi;

b) sobivaid standardalgoritme ja sobivaid võtmeid kasutatakse kooskõlas rahvusvaheliste standarditega (näiteks ETSI standard). Rakendatakse võtmehaldust;

c) kõiki võtmeid ja salasõnu tuleb kaitsta volitamata juurdepääsu eest.