II

(Muud kui seadusandlikud aktid)

MÄÄRUSED

KOMISJONI RAKENDUSMÄÄRUS (EL) nr 1179/2011,

17. november 2011,

millega kehtestatakse veebipõhiste kogumissüsteemide tehnilised spetsifikatsioonid vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) nr 211/2011 kodanikualgatuse kohta

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrust (EL) nr 211/2011 kodanikualgatuse kohta, [1] eriti selle artikli 6 lõiget 5,

olles konsulteerinud Euroopa Andmekaitseinspektoriga

ning arvestades järgmist:

(1) Määruses (EL) nr 211/2011 on sätestatud, et kui toetusavaldusi kogutakse veebipõhiselt, peaks sel eesmärgil kasutatav süsteem vastama teatud turvalisus- ja tehnilistele nõuetele ning süsteemil peab olema asjaomase liikmesriigi pädeva asutuse tõend.

(2) Määruse (EL) nr 211/2011 tähenduses on veebipõhine kogumissüsteem infosüsteem, mis koosneb tarkvarast, riistvarast, majutuskeskkonnast, äritoimingutest ja personalist ning mille eesmärk on koguda veebipõhiseid toetusavaldusi.

(3) Määruses (EL) nr 211/2011 on ette nähtud nõuded, millele veebipõhised kogumissüsteemid peavad tõendi saamiseks vastama, ning on sätestatud, et komisjon peaks nende nõuete rakendamiseks võtma vastu tehnilised spetsifikatsioonid.

(4) Avatud veebirakenduste turvalisuse projekti (Open Web Application Security Project – OWASP) projektis „Top 10 2010" esitatakse ülevaade veebirakenduse kõige olulisematest turvariskidest ning samuti vahendid nendega tegelemiseks; tehnilised spetsifikatsioonid toetuvad seetõttu selle projekti tulemustele.

(5) Tehniliste spetsifikatsioonide korraldajatepoolne rakendamine peaks tagama veebipõhiste kogumissüsteemide tõendamise liikmesriikide ametiasutustes ning aitama tagada, et nii töötlussüsteemi kavandamise kui ka tegeliku töötlemise ajal rakendatakse nõuetekohaseid tehnilisi ja organisatsioonilisi meetmeid, mida on vaja töötlustoimingute turvalisust käsitleva Euroopa Parlamendi ja nõukogu direktiiviga 95/46/EÜ [2] kehtestatud kohustuste täitmiseks, et säilitada turvalisus ning seeläbi hoida ära volitamata töötlemist ja kaitsta isikuandmeid juhusliku ja ebaseadusliku hävitamise või juhusliku kaotsimineku, muutmise, ebaseadusliku avalikustamise või juurdepääsu eest.

(6) Kui korraldajad kasutavad kooskõlas määruse (EL) nr 211/2011 artikli 6 lõikega 2 komisjoni loodud tarkvara, peaks tõendamisprotsess olema hõlpsam.

(7) Andmete kontrollijatena tegutsevad kodanikualgatuse korraldajad peaks veebipõhiste toetusavalduste kogumise ajal töödeldavate isikuandmete kaitse tagamiseks rakendama käesolevas määruses kehtestatud tehnilisi spetsifikatsioone. Kui töötlemist teeb andmetöötleja, peavad korraldajad tagama, et ta tegutseb vaid korraldajate antud juhiste alusel ning rakendab käesolevas määruses kehtestatud tehnilisi spetsifikatsioone.

(8) Käesolevas määruses austatakse põhiõigusi ja järgitakse Euroopa Liidu põhiõiguste hartas tunnustatud põhimõtteid, eriti selle artiklis 8 tunnustatud põhimõtet, mille kohaselt on igaühel õigus oma isikuandmete kaitsele.

(9) Käesoleva määrusega ette nähtud meetmed on kooskõlas määruse (EL) nr 211/2011 artikli 20 kohaselt asutatud komitee arvamusega,

[1] ELT L 65, 11.3.2011, lk 1.

[2] EÜT L 281, 23.11.1995, lk 31.

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Määruse (EL) nr 211/2011 artikli 6 lõikes 5 osutatud tehnilised spetsifikatsioonid on esitatud lisas.

Artikkel 2

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 17. november 2011

Komisjoni nimel
president
José Manuel BARROSO

LISA

1. TEHNILISED SPETSIFIKATSIOONID, MILLE EESMÄRK ON RAKENDADA MÄÄRUSE (EL) nr 211/2011 ARTIKLI 6 LÕIKE 4 PUNKTI a

Selleks et vältida toetusavalduste automaatset esitamist süsteemi kaudu, peab allakirjutanu enne toetusavalduse esitamist läbima kooskõlas kehtivate tavadega nõuetekohase tõendamisprotsessi. Üks võimalikest tõendamisprotsessidest on tugeva robotilõksu kasutamine.

2. TEHNILISED SPETSIFIKATSIOONID, MILLE EESMÄRK ON RAKENDADA MÄÄRUSE (EL) nr 211/2011 ARTIKLI 6 LÕIKE 4 PUNKTI b

Infokindluse standardid

2.1. Korraldajad esitavad enne vastuvõtmist dokumendid, mis tõendavad nende vastavust standardi ISO/IEC 27001 nõuetele. Sel eesmärgil on nad

a) teinud täieliku riskianalüüsi, kus on kindlaks määratud süsteemi ulatus, esitatud erinevate teabe tagamise rikkumise juhtude mõju ettevõtetele, loetletud infosüsteemi ohud ja nõrgad kohad, esitatud riskianalüüsi dokument, kus on muu hulgas ohtude vastumeetmete ja ohu ilmnemise korral võetavate kaitsemeetmete loetelu, ning viimasena on koostatud täienduste prioriteetnimekiri;

b) koostanud ja rakendanud riskikäsitlemise meetmed seoses isikuandmete, pere- ja eraelu kaitsega ning riski ilmnemise korral võetavad meetmed;

c) kirjalikult kindlaks määranud jääkriskid;

d) ette näinud organisatsioonilised vahendid tagasiside saamiseks uute ohtude ja turvalisuse täiendamise teemadel.

2.2. Korraldajad valivad punkti 2.1 alapunktis a esitatud riskianalüüsil põhineva turvakontrolli järgmiste standardite hulgast:

1) ISO/IEC 27002 või

2) infoturbefoorumi heade tavade standard,

et tegeleda järgmiste küsimustega:

a) riskihinnangud (soovitavalt ISO/IEC 27005 või muu spetsiifiline ja sobiv riskihindamismetoodika);

b) füüsiline turvalisus ja keskkonnaohutus;

c) inimressursside turvalisus;

d) teabevahetuse ja toimingute juhtimine;

e) juurdepääsukontrolli standardmeetmed lisaks käesolevas rakendusmääruses ettenähtutele;

f) infosüsteemide hankimine, väljatöötamine ja hooldus;

g) infoturbeintsidentide haldus;

h) infosüsteemis esinevate selliste rikkumiste heastamine ja leevendamine, mille tulemusel võib toimuda töödeldavate isikuandmete hävitamine või juhuslik kaotsiminek, muutmine, volitamata avalikustamine või juurdepääs;

i) nõuetele vastavus;

j) arvutivõrgu turvalisus (soovitavalt ISO/IEC 27033 või heade tavade standard).

Neid standardeid võib kohaldada vaid veebipõhise kogumissüsteemiga seotud organisatsiooni osade suhtes. Näiteks inimressursside turvalisus võib olla seotud nende isikutega, kellel on veebipõhisele kogumissüsteemile juurdepääs füüsiliselt või võrgu kaudu, ning füüsiline turvalisus / keskkonnaohutus seotud vaid süsteemi majutava(te) hoone(te)ga.

Funktsionaalsed nõuded

2.3. Veebipõhine kogumissüsteem koosneb veebipõhisest programmist, mis on kasutusele võetud toetusavalduste kogumiseks kindla kodanikualgatuse jaoks.

2.4. Kui süsteemi administreerimisel on vaja erinevaid rolle, tuleb kooskõlas vähima eelisõiguse põhimõttega kehtestada erineva tasemega pääsukontrollimehhanismid.

2.5. Avalikult juurde pääsetavad võimalused on selgelt eraldatud administratiivseks otstarbeks mõeldud võimalustest. Süsteemi avalikus osas kättesaadava teabe lugemist ei takista ükski pääsukontroll, sealhulgas teave algatuse ning toetusavalduse elektroonilise vormi kohta. Algatusele allkirja andmine on võimalik vaid avaliku osa kaudu.

2.6. Süsteem avastab ja takistab toetusavalduse mitmekordset esitamist.

Rakenduskihi turvalisus

2.7. Süsteemi kaitstakse nõuetekohaselt tuntud nõrkade kohtade ja vallutuste eest. Seetõttu peab süsteem muu hulgas vastama järgmistele nõuetele.

2.7.1. Süsteem kaitseb end SQL-injektsiooni (Structured Query Language), lihtsustatud kataloogisirvimise protokolli (Lightweight Directory Access Protocol (LDAP)) päringute, XPath (XML Path Language) päringute, operatsioonisüsteemi käskude või käsureaparameetrite eest. Sel eesmärgil on vähemalt nõutud, et

a) kasutaja sisestatud kõikide andmete õigsust kontrollitakse;

b) õigsuse kontrolli teeb vähemalt serveripoolne loogika;

c) interpretaatorite abil eraldatakse ebausaldusväärsed andmed käskudest või päringutest; SQL-kutsete puhul tähendab see seotud muutujate kasutamist kõigis parametriseeritavates päringutes ja salvestatud protseduurides ning dünaamiliste päringute vältimist.

2.7.2. Süsteem kaitseb end murdskriptimise (Cross-Site Scripting – XSS) eest. Sel eesmärgil on vähemalt nõutud, et

a) kontrollitakse brauserile tagasi saadetud kasutajasisendi turvalisust (sisendi õigsuse kontrollimise abil);

b) kogu kasutaja sisend töödeldakse enne selle sisestamist väljundlehele;

c) väljundi nõuetekohane kodeerimine tagab, et sellist sisendit käsitletakse brauseris alati tekstina. Aktiivset sisu ei kasutata.

2.7.3. Süsteemil on range autentimis- ja seansihaldus, mis vähemalt nõuab, et

a) mandaat on alati kaitstud, kui see salvestatakse räsimise või krüpteerimise teel. Räsi põhjal autentimise oht on maandatud;

b) mandaati ei saa ära arvata ega üle kirjutada nõrkade kontohaldusfunktsioonide kaudu (nt konto loomine, salasõna muutmine, salasõna taastamine, nõrgad seansi identifikaatorid);

c) seansi identifikaatoreid ja seansi andmeid ei näidata internetiaadressis (Uniform Resource Locator – URL);

d) seansi jagamise katsed ei saa seansi identifikaatoreid haavata;

e) seansi identifikaatorid aeguvad, mis tagab kasutajate väljalogimise;

f) seansi identifikaatoreid ei lasta pärast edukat sisselogimist ringlusesse;

g) salasõnad, seansi identifikaatorid ja muud mandaadid saadetakse vaid üle transpordikihi turbeprotokolli (Transport Layer Security – TLS);

h) süsteemi administraatoripoolne osa on kaitstud. Kui seda kaitseb ühefaktoriline autentimine, siis peab salasõna koosnema vähemalt kümnest märgist, mille hulgas on vähemalt üks täht, üks number ja üks erimärk. Alternatiivina võib kasutada kahefaktorilist autentimist. Kui kasutatakse vaid ühefaktorilist autentimist, siis interneti kaudu süsteemi administraatoriosale juurdepääsemiseks on vaja kaheastmelist kontrollimehhanismi, kusjuures üksikut faktorit täiendab mingi muu autentimisviis, näiteks SMSi teel edastatud ühekordne pääsuf-raas või -kood või asümmeetriliselt krüpteeritud suvaline väljakutsestring, mille peab dekrüpteerima süsteemile tundmatu korraldajate/administraatorite privaatvõtmega.

2.7.4. Süsteemis ei ole ebaturvalisi objekti otseviiteid. Sel eesmärgil on vähemalt nõutud, et

a) piiratud ressursside otseviidete puhul kontrollib programm, et kasutajal on volitused pääseda juurde taotletud ressurssidele;

b) kui tegemist on kaudse viitega, siis otseviite ühendus on piiratud antud kasutajale mõeldud väärtustega.

2.7.5. Süsteem kaitseb end CSRF defekti (Cross-Site Request Forgery flaw) eest.

2.7.6. Kasutatakse nõuetekohast turvakonfiguratsiooni, mis nõuab vähemalt, et

a) kõik tarkvarakomponendid on ajakohastatud, sealhulgas operatsioonisüsteem, veebi-/programmiserver, andmebaasihaldur (DBMS), programmid ja kõik kooditeegid;

b) operatsioonisüsteem ja veebi-/programmiserveri tarbetud teenused blokeeritakse, eemaldatakse või neid ei installeerita;

c) kontode vaikimisi salasõnad muudetakse või blokeeritakse;

d) rakendatakse veahaldust, et vältida pinulogi ja teiste üliinformatiivsete veateadete lekkimist;

e) arendusraamistike ja teekide turvaseaded on konfigureeritud kooskõlas parimate tavadega, näiteks OWASPi juhistega.

2.7.7. Süsteem tagab andmete krüpteerimise järgmiselt:

a) elektroonilises vormingus isikuandmed krüpteeritakse ladustamise või edastamise korral liikmesriikide pädevatele asutustele kooskõlas määruse (EL) nr 211/2011 artikli 8 lõikega 1, kusjuures võtmeid hallatakse ja varundatakse eraldi;

b) tugevaid standardalgoritme ja tugevaid võtmeid kasutatakse kooskõlas rahvusvaheliste standarditega. Rakendatakse võtmehaldust;

c) salasõnad räsitakse tugeva standardalgoritmi abil ja selleks kasutatakse sobivat soola;

d) kõik võtmed ja salasõnad kaitstakse volitamata juurdepääsu eest.

2.7.8. Süsteem piirab juurdepääsu URL-ile, tuginedes kasutaja pääsutasemele ja -lubadele. Sel eesmärgil on vähemalt nõutud, et

a) juhul, kui lehele juurdepääsu autentimiseks ja volituste kontrollimiseks kasutatakse väliseid turvamehhanisme, tuleb need iga lehe puhul nõuetekohaselt konfigureerida;

b) juhul, kui kasutatakse kaitset koodi tasemel, tuleb seda rakendada iga nõutava lehe puhul.

2.7.9. Süsteem kasutab piisavat transpordikihi kaitset. Selleks kasutatakse kõiki järgmisi meetmeid või vähemalt sama tugevaid meetmeid:

a) mis tahes tundlikule ressursile juurdepääsemiseks nõuab süsteem kõige uuemat hüperteksti edastusprotokolli üle turvasoklite kihi (HTTPS), kasutades sertifikaate, mis on kehtivad, mille tähtaeg ei ole saabunud, mis ei ole tühistatud ning sobivad kõikide saidi kasutatavate domeenidega;

b) süsteem seab turvalipu kõikidele tundlikele küpsistele;

c) server konfigureerib kooskõlas parimate tavadega TLS-pakkuja üksnes krüpteerimisalgoritmide toetamiseks. Kasutajaid teavitatakse kohustusest võimaldada TSL tugi oma brauseris.

2.7.10. Süsteem kaitseb end kontrollimata ümbersuunamiste ja edastamiste eest.

Andmebaasi turvalisus ja andmete terviklus

2.8. Juhul, kui erinevad kodanikualgatused kasutavad veebipõhiste kogumissüsteemide puhul ühist riistvara ja operatsioonisüsteemi, siis ei jaga nad omavahel andmeid, sealhulgas juurdepääsu/krüpteerimise mandaate. Lisaks kajastub see riskihinnangutes ja rakendatavates vastumeetmetes.

2.9. Maandatud on oht, et keegi autendib end andmebaasis räsi põhjal.

2.10. Allakirjutanute esitatud andmed on juurdepääsetavad vaid andmebaasi administraatorile/korraldajale.

2.11. Allakirjutanutelt kogutavad haldusmandaadid, isikuandmed ja nende varundatud andmed kaitstakse tugevate krüpteerimisalgoritmide abil kooskõlas punkti 2.7.7 alapunktiga b. Krüptimata kujul võib süsteemis siiski ladustada selle liikmesriigi, kus toetusavaldusi loetletakse, toetusavalduse esitamise kuupäeva ja keele, milles allakirjutanu toetusavalduse vormi täitis.

2.12. Allakirjutanutel on juurdepääs esitatud andmetele toetusavalduse vormi täitmise seansi ajal. Kui toetusavalduse vorm on esitatud ja seanss suletakse, ei ole esitatud andmed enam juurdepääsetavad.

2.13. Allakirjutanute isikuandmed, sealhulgas varundatud andmed, on kättesaadavad krüpteeritud vormingus vaid süsteemis. Kui riiklikud asutused soovivad kooskõlas määruse (EL) nr 211/2011 artikliga 8 andmeid vaadata või nende õigsust kontrollida, võivad korraldajad krüpteeritud andmeid edastada vastavalt punkti 2.7.7 alapunktile a.

2.14. Toetusavalduse vormi sisestatud andmete püsivus on atomaarne. See tähendab, et pärast seda, kui kasutaja on sisestanud toetusavalduse vormi kõik vajalikud üksikasjad ja valideerib oma otsuse algatust toetada, siis süsteem kas edastab kõik vormi andmed andmebaasi või ei salvesta vea esinemise korral mitte midagi. Süsteem teavitab kasutajat taotluse edukast või edutust salvestamisest.

2.15. Kasutatav andmebaasihaldus on ajakohane ja seda paigatakse pidevalt uute avastatud vallutuste korral.

2.16. Kogu süsteemi tegevus logitakse. Süsteem teeb kindlaks, et erandeid ja teisi allpool loetletud turvalisusega seotud sündmusi salvestavaid auditilogisid saab esitada ja neid hoitakse seni, kuni andmed hävitatakse kooskõlas määruse (EL) nr 211/2011 artikli 12 lõigetega 5 ja 3. Logid on nõuetekohaselt kaitstud, näiteks salvestades need krüpteeritud kujul. Korraldajad/administraatorid kontrollivad logisid korrapäraselt kahtlase tegevuse suhtes. Logid sisaldavad vähemalt järgmist:

a) korraldajate/administraatorite sisse- ja väljalogimise kuupäevi ja kellaaegu;

b) tehtud varundamisi;

c) kõiki andmebaasi administraatori muudatusi ja uuendusi.

Taristu turvalisus – füüsiline asukoht, võrgutaristu ja serveri keskkond

2.17. *Füüsiline turvalisus*

Olenemata sellest, millist majutust kasutatakse, peab programmi majutav masin olema nõuetekohaselt kaitstud ning tagama, et

a) kontrollitakse majutusalale juurdepääsu ja koostatakse auditilogi;

b) varundatud andmed on füüsiliselt kaitstud varguse või tahtmatu ümberpaigutamise eest;

c) programmi majutav server on paigaldatud turvalisele püstikule.

2.18. *Võrguturvalisus*

2.18.1. Süsteemi majutatakse välisvõrguga suhtlevas serveris, mis on paigutatud demilitaarsesse tsooni (DMZ) ja kaitstud tulemüüriga.

2.18.2. Kui tulemüüri uuendused ja parandused tehakse avalikuks, paigaldatakse need viivitamata.

2.18.3. Kogu (veebipõhise kogumissüsteemi jaoks mõeldud) serverisse sisenevat ja serverist väljuvat liiklust kontrollib tulemüür ja see tegevus logitakse. Tulemüüri eeskirjad keelavad kogu tarbetu liikluse, et süsteemi saaks turvaliselt kasutada ja hallata.

2.18.4. Veebipõhine kogumissüsteem peab olema majutatud piisava kaitsega tootmiskeskkonnas, mis on eraldatud nendest keskkondadest, mida kasutatakse mittetootmiskeskkondade, näiteks arendus- või testimiskeskkondade majutamiseks.

2.18.5. Rakendatakse kohtvõrgu turvameetmeid, näiteks järgmiseid:

a) 2. andmelülikihi (L2) juurdepääsunimekiri / kommutaatori pordi turvalisus;

b) kasutamata kommutaatori pordid on välja lülitatud;

c) demilitariseeritud tsoon asub privaatses virtuaalkohtvõrgus (VLAN);

d) mittevajalike portide puhul ei võimaldata andmelülikihi (L2) otseühendust.

2.19. *Operatsioonisüsteemi ja võrgu-/programmiserveri turvalisus*

2.19.1. Rakendatakse nõuetekohast turvakonfiguratsiooni, mis hõlmab punktis 2.7.6 loetletud elemente.

2.19.2. Programmid töötavad vähimate vajalike õigustega.

2.19.3. Administraatori juurdepääsul veebipõhise kogumise süsteemi haldusliidesele on lühike seansiaeg (maksimaalselt 15 minutit).

2.19.4. Kui avalikustatakse asjakohased operatsioonisüsteemi täiendused ja parandused, programmide käitusajad, serveritel töötavad programmid või pahavaratõrje, tuleb sellised parandused viivitamata paigaldada.

2.19.5. Maandatud on oht, et keegi autendib end andmebaasis räsi põhjal.

2.20. *Korraldaja turvameetmed kliendi suhtes*

Korraldajad võtavad otspunktturvalisuse tagamiseks vajalikud meetmed, et turvata oma kliendi programm/seade, mida kasutatakse veebipõhise kogumise süsteemi haldamiseks ja sellele juurde pääsemiseks, näiteks:

2.20.1. kasutajad täidavad hooldusega mitteseotud ülesandeid (näiteks bürooautomaatikat) vähimate töötamiseks vajalike õigustega;

2.20.2. kui operatsioonisüsteemi, paigaldatud programmide või pahavaratõrje täiendused ja parandused tehakse avalikuks, paigaldatakse need viivitamata.

3. TEHNILISED SPETSIFIKATSIOONID, MILLE EESMÄRK ON RAKENDADA MÄÄRUSE (EL) nr 211/2011 ARTIKLI 6 LÕIKE 4 PUNKTI c

3.1. Süsteemis on võimalus teha iga liikmesriigi jaoks aruanne, kus on loetletud algatus ja allakirjutanute isikuandmed, mida selle liikmesriigi pädev asutus peab kontrollima.

3.2. Allakirjutanute toetusavalduste eksportimine on võimalik määruse (EL) nr 211/2011 III lisas esitatud vormingus. Süsteem võib lisaks pakkuda võimalust eksportida toetusavaldusi koostalitlusvõimelises vormingus, näiteks laiendatav märgistuskeel (Extensible Markup Language – XML).

3.3. Eksporditud toetusavaldustele pannakse asjaomaste liikmesriikide jaoks märge *piiratud kasutusega* ja sildistatakse *isikuandmetena.*

3.4. Eksporditud andmete elektroonilist edastamist liikmesriikidele turvatakse pealtkuulamise eest, kasutades selleks otspunktkrüpteerimist.