II

*(Muut kuin lainsäätämisjärjestyksessä hyväksyttävät säädökset)*

# ASETUKSET

## KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) N:o 1179/2011,

**annettu 17 päivänä marraskuuta 2011,**

**verkossa toteutettavien keruujärjestelmien teknisistä eritelmistä kansalaisaloitteesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 211/2011 mukaisesti**

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon kansalaisaloitteesta 16 päivänä helmikuuta 2011 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 211/2011 ([1]) ja erityisesti sen 6 artiklan 5 kohdan,

on kuullut Euroopan tietosuojavaltuutettua,

sekä katsoo seuraavaa:

(1) Asetuksessa (EU) N:o 211/2011 säädetään, että jos tuenilmaukset kerätään verkossa, tarkoitukseen käytettävän järjestelmän on täytettävä tietyt turvallisuusvaatimukset ja tekniset vaatimukset ja sitä varten on saatava todistus asianomaisen jäsenvaltion toimivaltaisilta viranomaisilta.

(2) Asetuksessa (EU) N:o 211/2011 tarkoitettu verkossa toteutettava keruujärjestelmä on tuenilmausten keräämiseen tarkoitettu tietojärjestelmä, joka koostuu ohjelmistosta, laitteistosta, ylläpitoympäristöstä, toimintaprosesseista ja henkilöstöstä.

(3) Asetuksessa (EU) N:o 211/2011 vahvistetaan ne vaatimukset, jotka verkossa toteutettavien keruujärjestelmien on täytettävä todistuksen saamiseksi, ja säädetään, että komission olisi hyväksyttävä tekniset eritelmät kyseisten vaatimusten täytäntöön panemiseksi.

(4) OWASP-hankkeen (Open Web Application Security Project) Top 10 2010 -asiakirjassa esitetään katsaus websovellusten tärkeimmistä turvallisuusriskeistä ja keinoista, joilla näitä riskejä voidaan torjua; nyt annettavissa teknisissä eritelmissä hyödynnetään tämän hankkeen tuloksia.

(5) Näitä teknisiä eritelmiä noudattamalla järjestäjät voivat todennäköisesti varmistaa verkossa toteutettavia keruujärjestelmiä varten tarvittavan todistuksen saannin jäsenvaltioiden viranomaisilta ja myötävaikuttaa siihen, että Euroopan parlamentin ja neuvoston direktiivissä 95/46/EY ([2]) säädettyjen, tietojenkäsittelyn turvallisuuteen liittyvien velvoitteiden noudattamisen edellyttämät asianmukaiset tekniset ja organisatoriset toimenpiteet toteutetaan sekä käsittelyn suunnittelu- että toteuttamisvaiheessa siten, että taataan turvallisuus, estetään luvaton käsittely ja suojataan henkilötiedot vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai tietojen antamiselta.

(6) Todistusten antamismenettely todennäköisesti helpottuu, jos järjestäjät käyttävät komission asetuksen (EU) N:o 211/2011 6 artiklan 2 kohdan mukaisesti käyttöön asettamaa ohjelmistoa.

(7) Kansalaisaloitteiden järjestäjien olisi rekisterinpitäjinä noudatettava tässä asetuksessa vahvistettuja teknisiä eritelmiä kerätessään tuenilmauksia verkossa, jotta käsiteltävien henkilötietojen suojaaminen voitaisiin varmistaa. Jos käsittelyn suorittaa henkilötietojen käsittelijä, järjestäjien olisi varmistettava, että tämä toimii ainoastaan järjestäjien ohjeiden mukaisesti ja noudattaa tässä asetuksessa vahvistettuja teknisiä eritelmiä.

(8) Asetuksessa kunnioitetaan perusoikeuksia ja noudatetaan periaatteita, jotka on vahvistettu Euroopan unionin perusoikeuskirjassa ja erityisesti sen 8 artiklassa, jossa todetaan, että jokaisella on oikeus henkilötietojensa suojaan.

(9) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EU) N:o 211/2011 20 artiklalla perustetun komitean lausunnon mukaiset,

([1]) EUVL L 65, 11.3.2011, s. 1.

([2]) EYVL L 281, 23.11.1995, s. 31.

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

*1 artikla*

Asetuksen (EU) N:o 211/2011 6 artiklan 5 kohdassa tarkoitetut tekniset eritelmät esitetään liitteessä.

*2 artikla*

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 17 päivänä marraskuuta 2011.

*Komission puolesta*
José Manuel BARROSO
*Puheenjohtaja*

*LIITE*

1. TEKNISET ERITELMÄT ASETUKSEN (EU) N:o 211/2011 6 ARTIKLAN 4 KOHDAN a ALAKOHDAN TÄYTÄNTÖÖNPANOA VARTEN

Jotta järjestelmän käytön yhteydessä estettäisiin tuenilmauksen lähettämisen automatisointi, allekirjoittajan on ennen tuenilmauksen lähettämistä käytävä läpi asianmukainen ja nykykäytännön mukainen tarkistusprosessi. Yksi mahdollisista tarkistusprosesseista on vahva ”captcha”-varmennus.

2. TEKNISET ERITELMÄT ASETUKSEN (EU) N:o 211/2011 6 ARTIKLAN 4 KOHDAN b ALAKOHDAN TÄYTÄNTÖÖNPANOA VARTEN

**Tietojen turvaamisen standardit**

2.1 Järjestäjien on toimitettava asiakirjat, jotka osoittavat, että he täyttävät standardin ISO/IEC 27001 vaatimukset, lukuun ottamatta standardin hyväksymistä. Tätä varten heidän on:

a) suoritettava täydellinen riskinarviointi, jossa yksilöidään järjestelmän laajuus, kuvataan tietojen turvaamiseen kohdistuvien erilaisten loukkausten vaikutukset toimintaan, luetellaan tietojärjestelmän uhat ja haavoittuvuudet ja johon sisältyy riskianalyysiasiakirja, jossa luetellaan myös vastatoimet tällaisten uhkien välttämiseksi sekä korjaavat toimet uhkien toteutuessa, ja joka sisältää luettelon parannuksista tärkeysjärjestyksessä;

b) suunniteltava ja toteutettava toimet henkilötietojen suojaan ja perhe- ja yksityiselämän suojaan kohdistuvien riskien hoitamiseksi sekä toimet, jotka toteutetaan riskin toteutuessa;

c) yksilöitävä muut riskit kirjallisesti;

d) esitettävä organisatoriset keinot saada palautetta uusista uhkista ja turvallisuuden parannuksista.

2.2 Järjestäjien on valittava turvallisuuden valvontamenetelmät 2.1 kohdan a alakohdassa tarkoitetun riskianalyysin pohjalta seuraavista standardeista

1) ISO/IEC 27002 tai

2) Information Security Forumin ”Standard of Good Practice”

seuraavien asioiden hoitamiseksi:

a) riskinarvioinnit (ISO/IEC 27005 tai muu erityinen ja soveltuva riskinarviointimenetelmä ovat suositeltavia);

b) fyysinen ja ympäristön turvallisuus;

c) henkilöstöturvallisuus;

d) viestintä ja toiminnan hallinta;

e) vakiopääsynvalvontatoimet niiden lisäksi, joista on säädetty tässä täytäntöönpanoasetuksessa;

f) tietojärjestelmien hankinta, kehitys ja ylläpito;

g) tietoturvaloukkausten hallinta;

h) toimet sellaisten tietojärjestelmiin kohdistuvien loukkausten korjaamiseksi ja lieventämiseksi, jotka johtaisivat käsiteltyjen henkilötietojen tuhoutumiseen tai vahingossa tapahtuvaan häviämiseen, muuttamiseen, luvattomaan luovuttamiseen tai saattamiseen muiden ulottuville;

i) vaatimustenmukaisuus;

j) tietokoneverkon turvallisuus (ISO/IEC 27033 tai SoGP ovat suositeltavia).

Näiden standardien soveltaminen voidaan rajoittaa organisaation niihin osiin, jotka liittyvät verkossa toteutettavaan keruujärjestelmään. Esimerkiksi henkilöstöturvallisuus voidaan rajoittaa henkilöstöön, jolla on fyysinen tai verkkovälitteinen pääsy verkossa toteutettavaan keruujärjestelmään, ja fyysinen ja ympäristön turvallisuus voidaan rajoittaa rakennuksiin, joihin järjestelmä on sijoitettu.

**Toiminnan vaatimukset**

2.3 Verkossa toteutettava keruujärjestelmä koostuu web-pohjaisen sovelluksen esiintymästä, joka on määritetty keräämään tuenilmauksia yksittäiselle kansalaisaloitteelle.

2.4 Jos järjestelmän hallinnointi edellyttää erilaisia rooleja, on määritettävä useita pääsynvalvonnan tasoja pienimmän valtuuden periaatteella.

2.5 Yleisesti käytettävissä olevat ominaisuudet on selvästi erotettava ominaisuuksista, jotka on tarkoitettu hallinnointiin. Mikään pääsynvalvontamenetelmä ei saa vaikeuttaa järjestelmän julkisessa osassa olevien tietojen lukemista, mukaan luettuina aloitetta koskevat tiedot ja sähköiset tuenilmauslomakkeet. Aloitteen tukeminen on mahdollista vain järjestelmän julkisessa osassa.

2.6 Järjestelmän on kyettävä havaitsemaan ja estämään tuenilmausten kahdentaminen.

**Sovellustason turvallisuus**

2.7 Järjestelmä on suojattava asianmukaisesti tunnettuja haavoittuvuuksia ja hyväksikäyttömahdollisuuksia vastaan. Tätä varten sen on täytettävä muun muassa seuraavat vaatimukset:

2.7.1 Järjestelmä on suojattu käskyjen ujuttamista (injection flaws) vastaan esimerkiksi SQL-kyselyissä (Structured Query Language), LDAP-kyselyissä (Lightweight Directory Access Protocol), XPath-kyselyissä (XML Path Language), OS-kyselyissä (Operating System) tai ohjelmien argumenteissa. Tämä edellyttää järjestelmältä vähintään seuraavaa:

a) Kaikki käyttäjien syötteet validoidaan.

b) Validointi suoritetaan vähintään palvelinpuolen logiikassa.

c) Kaikessa tulkkien käytössä erotetaan varmentamaton data selkeästi komennosta tai kyselystä. SQL-kutsuissa tämä merkitsee sidottujen muuttujien (bind variables) käyttöä kaikissa valmistelluissa lausekkeissa ja tallennetuissa menettelyissä, ja dynaamisten kyselyjen välttämistä.

2.7.2 Järjestelmä on suojattu XSS-haavoittuvuuksia (Cross-Site Scripting) vastaan. Tämä edellyttää järjestelmältä vähintään seuraavaa:

a) Kaikki käyttäjien syötteet, jotka lähetetään takaisin selaimeen, tarkistetaan ja todetaan turvallisiksi (syötteiden validoinnin avulla).

b) Kaikki käyttäjien syötteet on puhdistettava asianmukaisesti ennen niiden sisällyttämistä tulostesivulle.

c) Tulosteen kunnollisella koodauksella varmistetaan, että nämä syötteet käsitellään selaimessa aina tekstinä. Aktiivista sisältöä ei käytetä.

2.7.3 Järjestelmässä on vahva todentamis- ja istuntojen hallinta, mikä edellyttää vähintään seuraavaa:

a) Valtuustiedot (credentials) suojataan aina kun ne tallennetaan tiivistämällä (hashing) tai salakirjoituksella (encryption). Riskiä todennetusta pääsystä ”pass-the-hash”-tekniikalla on lievennetty.

b) Valtuustietoja ei voi arvata tai päällekirjoittaa heikkojen tilinhallinnointitoimintojen vuoksi (esim. tilin luonti, salasanan muuttaminen, salasanan palautus, heikot istuntotunnisteet (session IDs)).

c) Istuntotunnisteita ja istuntodataa ei paljasteta URL-osoitteessa.

d) Istuntotunnisteet eivät ole haavoittuvia istunnon ennaltamääräämishyökkäykselle (session fixation).

e) Istuntotunnisteilla on aikakatkaisu, jolla varmistetaan käyttäjien uloskirjautuminen.

f) Istuntotunnisteita ei kierrätetä onnistuneen sisäänkirjautumisen jälkeen.

g) Salasanat, istuntotunnisteet ja muut valtuustiedot lähetetään ainoastaan TLS-protokollaa käyttäen (Transport Layer Security).

h) Järjestelmän hallinnointiosio on suojattu. Jos se on suojattu yhden tekijän todennuksella (single-factor authentication), salasanassa on oltava vähintään 10 merkkiä, joista vähintään yksi on kirjain, yksi numero ja yksi erikoismerkki. Vaihtoehtoisesti voidaan käyttää kahden tekijän todennusta (two-factor authentication). Pelkkää yhden tekijän todennusta käytettäessä pääsy järjestelmän hallinnointiosioon internetin kautta edellyttää kaksivaiheista tarkistusmekanismia, jossa yhden tekijän todennusta täydennetään muulla todentamiskeinolla, esimerkiksi tekstiviestinä lähetettävällä kertaluonteisella salalauseella/koodilla tai epäsymmetrisesti salakirjoitetulla sattumanvaraisella haastemerkkijonolla (challenge string), joka avataan järjestäjän/ylläpitäjän yksityisellä avaimella, jota järjestelmä ei tunne.

2.7.4 Järjestelmässä ei ole turvaamattomia suoria objektiviittauksia. Tämä edellyttää järjestelmältä vähintään seuraavaa:

a) Suorissa viittauksissa rajoitettuihin resursseihin sovellus tarkistaa, että käyttäjällä on valtuudet päästä nimenomaan pyydettyyn resurssiin.

b) Jos viittaus on epäsuora, yhdistäminen suoraan viittaukseen rajoittuu senhetkiselle käyttäjälle sallittuihin arvoihin.

2.7.5 Järjestelmä on suojattu XSRF-haavoittuvuuksia (Cross-Site Request Forgery) vastaan.

2.7.6 Järjestelmässä on käytössä asianmukaiset turvallisuusasetukset, mikä edellyttää vähintään seuraavaa:

a) Kaikki ohjelmistokomponentit ovat ajan tasalla, mukaan luettuina käyttöjärjestelmä, web-/sovelluspalvelin, tietokannan hallintajärjestelmä (Data Base Management System (DBMS), sovellukset ja kaikki koodikirjastot.

b) Käyttöjärjestelmän ja web-/sovelluspalvelimen tarpeettomat palvelut on deaktivoitu, poistettu kokonaan tai jätetty asentamatta.

c) Tilien oletussalasanat on muutettu tai poistettu käytöstä.

d) Virheenkäsittely on hoidettu siten, että jäljityspinojen (stack traces) ja muiden liian informatiivisten virhesanomien vuotaminen ei ole mahdollista.

e) Kehitysympäristöjen ja kirjastojen turvallisuusasetukset ovat parhaiden käytäntöjen, kuten OWASP-suuntaviivojen, mukaiset.

2.7.7 Järjestelmä mahdollistaa tietojen salakirjoituksen seuraavasti:

a) Sähköiset henkilötiedot salakirjoitetaan, kun ne tallennetaan tai siirretään jäsenvaltioiden toimivaltaisille viranomaisille asetuksen (EU) N:o 211/2011 8 artiklan 1 kohdan mukaisesti, ja avainten hallinnointi ja varmuuskopiointi tapahtuu eriytetysti.

b) Vahvoja standardialgoritmeja ja vahvoja avaimia käytetään kansainvälisten standardien mukaisesti. Avainten hallinnointi on käytössä.

c) Salasanat tiivistetään vahvalla standardialgoritmilla ja niissä käytetään asianmukaista suolaa (salt).

d) Kaikki avaimet ja salasanat suojataan luvattomalta pääsyltä.

2.7.8 Järjestelmä rajoittaa URL-osoitteeseen pääsyä käyttäjän pääsytasojen ja käyttövaltuuksien perusteella. Tämä edellyttää järjestelmältä vähintään seuraavaa:

a) Jos sivulle pääsyn edellyttämissä todentamis- ja lupatarkistuksissa käytetään ulkoisia turvallisuusmekanismeja, nämä on määritettävä asianmukaisesti jokaiselle sivulle.

b) Jos käytössä on kooditason suojaus, sitä on käytettävä jokaiselle pyydettävälle sivulle.

2.7.9 Järjestelmässä käytetään riittävää TLS-suojausta. Tämä edellyttää kaikkia seuraavista toimista tai vähintään yhtä tehokkaita toimia:

a) Järjestelmä vaatii HTTPS-protokollan (Hypertext Transfer Protocol Secure) uusimman version salliakseen pääsyn kaikkiin arkaluonteisiin resursseihin todistuksilla (certificates), jotka ovat voimassa, jotka eivät ole vanhentuneet, joita ei ole peruutettu ja jotka vastaavat kaikkia sivuston käyttämiä verkkoalueita.

b) Järjestelmä asettaa ”turvallinen”-tunnisteen kaikkiin arkaluonteisiin evästeisiin.

c) Palvelin määrittää TLS:n tarjoajan tukemaan ainoastaan parhaiden käytäntöjen mukaisia salakirjoitusalgoritmeja. Käyttäjille ilmoitetaan, että heidän on sallittava TLS-tuki selaimissaan.

2.7.10 Järjestelmä on suojattu validoimattomia uudelleen- ja edelleenohjauksia vastaan.

**Tietokannan turvallisuus ja tietojen eheys**

2.8 Jos eri kansalaisaloitteiden verkossa toteutettavissa keruujärjestelmissä käytetään yhteisiä laitteisto- ja käyttöjärjestelmäresursseja, niissä ei saa jakaa dataa, mukaan luettuina pääsyn/salakirjoituksen valtuustiedot. Tämä on otettava huomioon myös riskinarvioinnissa ja toteutettavissa vastatoimissa.

2.9 Riskiä todennetusta pääsystä tietokantaan ”pass-the-hash”-tekniikalla on lievennetty.

2.10 Allekirjoittajien toimittamat tiedot ovat ainoastaan tietokannan ylläpitäjän/järjestäjän saatavissa.

2.11 Hallinnolliset valtuustiedot, allekirjoittajilta kerätyt henkilötiedot ja niiden varmuuskopiot on suojattu vahvoin salakirjoitusalgoritmein 2.7.7 kohdan b alakohdan mukaisesti. Järjestelmään voidaan kuitenkin tallentaa ilman salakirjoitusta jäsenvaltio, jossa tuenilmaus lasketaan, tuenilmauksen lähetyspäivämäärä sekä kieli, jolla allekirjoittaja täytti tuenilmauslomakkeen.

2.12 Allekirjoittajien saatavissa ovat ainoastaan tiedot, jotka toimitetaan siinä istunnossa, jossa he täyttävät tuenilmauslomakkeen. Kun tuenilmauslomake on toimitettu, istunto suljetaan eivätkä toimitetut tiedot ole enää saatavissa.

2.13 Allekirjoittajien henkilötiedot, mukaan luettuna varmuuskopio, ovat järjestelmässä ainoastaan salakirjoitetussa muodossa. Järjestäjät voivat viedä salakirjoitetut tiedot 2.7.7 kohdan a alakohdan mukaisesti tietojen tarkistuttamiseksi ja vahvistuttamiseksi kansallisilla viranomaisilla asetuksen (EU) N:o 211/2011 8 artiklan mukaisesti.

2.14 Tuenilmauslomakkeeseen täytettävien tietojen pysyvyys on atomaarinen. Tämä tarkoittaa sitä, että kun käyttäjä on antanut kaikki tarvittavat tiedot tuenilmauslomakkeelle ja validoi päätöksensä tukea aloitetta, järjestelmä joko vie kaikki lomakkeen tiedot onnistuneesti tietokantaan tai, virheen sattuessa, epäonnistuu siinä tallentamatta mitään tietoja. Järjestelmä ilmoittaa käyttäjälle tämän pyynnön käsittelyn onnistumisesta tai epäonnistumisesta.

2.15 Käytettävä tietokannan hallintajärjestelmä (DBMS) on ajantasainen ja siihen asennetaan jatkuvasti korjauspäivityksiä uusimpia todettuja hyväksikäyttötapoja vastaan.

2.16 Kaikki järjestelmän toimintalokit ovat käytössä. Järjestelmässä on varmistettava, että poikkeuksia ja muita alla lueteltuja turvallisuuden kannalta merkityksellisiä tapahtumia kirjaavia jäljityslokeja voidaan tuottaa ja säilyttää, kunnes tiedot tuhotaan asetuksen (EU) N:o 211/2011 12 artiklan 3 tai 5 kohdan mukaisesti. Lokit on suojattu asianmukaisesti esimerkiksi tallentamalla ne salakirjoitettuun tietovälineeseen. Järjestäjien/ylläpitäjien on säännöllisesti tarkistettava lokit epäilyttävän toiminnan varalta. Lokin on sisällettävä vähintään:

a) järjestäjien/ylläpitäjien sisään- ja uloskirjausten päivämäärät ja kellonajat

b) varmuuskopioiden ottamiset

c) kaikki tietokannan ylläpitäjän muutokset ja päivitykset.

**Infrastruktuurin turvallisuus – fyysinen sijainti, verkkoinfrastruktuuri ja palvelinympäristö**

2.17 *Fyysinen turvallisuus*

Käytettävästä palvelin-ylläpitoratkaisusta (hosting) riippumatta kone, jossa sovellusta ylläpidetään, on asianmukaisesti suojattu, mukaan luettuna:

a) palvelin-ylläpitoalueen pääsynvalvonta- ja jäljitysloki

b) varmuuskopiotietojen fyysinen suojaaminen varkautta tai häviämistä vastaan

c) sovelluksen ylläpitopalvelimen asentaminen suojattuun telineeseen.

2.18 *Verkon turvallisuus*

2.18.1 Järjestelmää ylläpidetään demilitarisoidulle alueelle (DMZ) asennetussa internetin suuntaisessa palvelimessa, joka on suojattu palomuurilla.

2.18.2 Kun palomuurista julkaistaan merkityksellisiä ohjelmisto- ja korjauspäivityksiä, tällaiset päivitykset asennetaan tarkoituksenmukaisella tavalla.

2.18.3 Kaikki palvelimeen saapuva ja sieltä lähtevä liikenne (verkossa toteutettavaa keruujärjestelmää varten) käy läpi palomuurin sääntöjen mukaisen tarkastuksen ja kirjataan lokiin. Palomuurin säännöissä on kiellettävä kaikki liikenne, joka ei ole tarpeen järjestelmän turvatun käytön ja ylläpidon kannalta.

2.18.4 Verkossa toteutettavaa keruujärjestelmää on ylläpidettävä asianmukaisesti suojatussa tuotantoverkon segmentissä, joka on erotettu segmenteistä, joilla ylläpidetään muita kuin tuotantoverkon segmenttejä, kuten kehitys- tai testausympäristöistä.

2.18.5 Lähiverkon (LAN) turvatoimet ovat käytössä, mukaan luettuina:

a) Layer 2 -pääsylista (L2) / porttikytkinten suojaaminen (port switch security)

b) käyttämättömät kytkentäportit on deaktivoitu

c) DMZ-alue on erillisessä virtuaalilähiverkossa (VLAN)/LAN

d) L2-rinnakkaiskäyttö (L2 trunking) ei ole mahdollista tarpeettomissa porteissa.

2.19 *Käyttöjärjestelmän ja web-/sovelluspalvelimen turvallisuus*

2.19.1 Asianmukaiset turvallisuusasetukset ovat käytössä, mukaan luettuina 2.7.6 kohdassa luetellut elementit.

2.19.2 Sovellusten toiminta edellyttää mahdollisimman pieniä valtuuksia.

2.19.3 Ylläpitäjän pääsy verkossa toteutettavan keruujärjestelmän hallinnointiliittymään on ajallisesti rajoitettu lyhyellä istunnon aikakatkaisulla (enintään 15 minuuttia).

2.19.4 Kun käyttöjärjestelmästä, sovellusten suoritusajoista, palvelimella suoritettavista sovelluksista tai haittaohjelmien torjuntaohjelmista julkaistaan merkityksellisiä ohjelmisto- ja korjauspäivityksiä, tällaiset päivitykset asennetaan tarkoituksenmukaisella tavalla.

2.19.5 Riskiä todennetusta pääsystä järjestelmään ”pass-the-hash”-tekniikalla on lievennetty.

2.20 *Järjestäjän asiakaspuolen turvallisuus*

Päästä päähän ulottuvan turvallisuuden mahdollistamiseksi järjestäjien on tarpeellisin toimin suojattava asiakassovellus/-laite, jolla he hallinnoivat verkossa toteutettavaa keruujärjestelmää ja pääsevät siihen, kuten:

2.20.1 Käyttäjät suorittavat muita kuin ylläpitotehtäviä (kuten toimistoautomaatiotehtäviä) niin vähäisin valtuuksin kuin on tarpeen niiden hoitamiseksi.

2.20.2 Kun käyttöjärjestelmästä, mistä tahansa asennetuista sovelluksista tai haittaohjelmien torjuntaohjelmista julkaistaan merkityksellisiä ohjelmisto- ja korjauspäivityksiä, tällaiset päivitykset asennetaan tarkoituksenmukaisella tavalla.

3. TEKNISET ERITELMÄT ASETUKSEN (EU) N:o 211/2011 6 ARTIKLAN 4 KOHDAN c ALAKOHDAN TÄYTÄNTÖÖNPANOA VARTEN

3.1 Järjestelmän avulla voidaan tuottaa kustakin jäsenvaltiosta raportti, jossa luetellaan aloitteen tiedot ja allekirjoittajien henkilötiedot kulloisenkin jäsenvaltion toimivaltaisen viranomaisen tarkistettavaksi.

3.2 Allekirjoittajien tuenilmausten vienti on mahdollista asetuksen (EU) N:o 211/2011 liitteessä III kuvatussa muodossa. Järjestelmässä voi lisäksi olla mahdollisuus viedä tuenilmauksia jossain yhteentoimivassa muodossa, kuten XML (Extensible Markup Language).

3.3 Viedyt tuenilmaukset on varustettava luonnehdinnalla *rajoitettuun jakeluun* kyseiselle jäsenvaltiolle ja merkinnällä *henkilötietoja*.

3.4 Vietyjen tietojen sähköinen lähettäminen jäsenvaltioille on suojattava salakuuntelulta (eavesdropping) käyttäen soveltuvaa päästä päähän -salakirjoitusta.