II

(Neleģislatīvi akti)

REGULAS

KOMISIJAS ĪSTENOŠANAS REGULA (ES) Nr. 1179/2011

(2011. gada 17. novembris),

ar ko nosaka tehniskās specifikācijas vākšanas tiešsaistes sistēmām saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 211/2011 par pilsoņu iniciatīvu

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2011. gada 16. februāra Regulu (ES) Nr. 211/2011 par pilsoņu iniciatīvu [1] un jo īpaši tās 6. panta 5. punktu,

apspriedusies ar Eiropas Datu aizsardzības uzraudzītāju,

tā kā:

(1) Regula (ES) Nr. 211/2011 paredz, ka gadījumos, kad paziņojumi par atbalstu tiek vākti tiešsaistē, sistēmai, kas tiek izmantota šim nolūkam, ir jāatbilst noteiktām drošības un tehniskām prasībām un tai vajadzētu būt attiecīgās dalībvalsts iestāžu sertificētai.

(2) Vākšanas tiešsaistes sistēma Regulas (ES) Nr. 211/2011 izpratnē ir informācijas sistēma, kas sastāv no programmatūras, aparatūras, mitināšanas vides, darba procesiem un personāla, lai tiešsaistē vāktu paziņojumus par atbalstu.

(3) Regulā (ES) Nr. 211/2011 ir izklāstītas prasības, kurām vākšanas tiešsaistes sistēmām ir jāatbilst, lai tās varētu tikt sertificētas, un noteikts, ka Komisijai būtu jāpieņem tehniskās specifikācijas, lai īstenotu šīs prasības.

(4) Atvērtā tīmekļa lietotņu drošības projekta (*Open Web Application Security Project* (*OWASP*)) *Top 10 2010* projekts sniedz pārskatu par būtiskākajiem tīmekļa lietotņu drošības riskiem, kā arī instrumentiem, lai tos novērstu; tāpēc tehniskās specifikācijas balstās uz šā projekta secinājumiem.

(5) Tam, ka organizatori ir piemērojuši tehniskās specifikācijas, būtu jāgarantē, ka dalībvalstu iestādes sertificē vākšanas tiešsaistes sistēmas, un jāpalīdz nodrošināt, ka tiek īstenoti piemēroti tehniski un organizatoriski pasākumi, kas nepieciešami, lai izpildītu pienākumus, ko uzliek Eiropas Parlamenta un Padomes Direktīva 95/46/EK [2] par datu apstrādes pasākumu drošību, gan izveidojot apstrādes sistēmu, gan pašas apstrādes laikā, lai uzturētu drošību un tādējādi novērstu jebkādu neatļautu apstrādi, un aizsargātu personas datus pret nejaušu vai nelikumīgu iznīcināšanu vai nejaušu nozaudēšanu, izmainīšanu, neatļautu izpaušanu vai piekļuvi tiem.

(6) Sertificēšanas procesu būtu jāveicina tam, ka organizatori izmanto lietojumprogrammas, ko tiem sniegusi Komisija saskaņā ar Regulas (ES) Nr. 211/2011 6. panta 2. punktu.

(7) Pilsoņu iniciatīvu organizatoriem, tiešsaistē vācot paziņojumus par atbalstu, būtu jāpiemēro tehniskās specifikācijas, kas noteiktas šajā regulā, lai nodrošinātu apstrādāto datu aizsardzību. Ja apstrādi veic datu apstrādātājs, organizatoriem būtu jānodrošina, ka datu apstrādātājs darbojas, tikai ievērojot organizatoru norādījumus, un piemēro tehniskās specifikācijas, kas noteiktas šajā regulā.

(8) Šajā regulā ir ievērotas pamattiesības un principi, kas ietverti Eiropas Savienības Pamattiesību hartā, jo īpaši tās 8. pantā, kurā noteikts, ka ikvienai personai ir tiesības uz savu personas datu aizsardzību.

(9) Šajā regulā noteiktie pasākumi ir saskaņā ar atzinumu, ko sniegusi atbilstīgi Regulas (ES) Nr. 211/2011 20. pantam izveidotā komiteja,

[1] OV L 65, 11.3.2011., 1. lpp.

[2] OV L 281, 23.11.1995., 31. lpp.

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Tehniskās specifikācijas, kas minētas Regulas (ES) Nr. 211/2011 6. panta 5. punktā, ir izklāstītas pielikumā.

2. pants

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2011. gada 17. novembrī

Komisijas vārdā –
priekšsēdētājs
José Manuel BARROSO

PIELIKUMS

1. TEHNISKĀS SPECIFIKĀCIJAS, LAI ĪSTENOTU REGULAS (ES) Nr. 211/2011 6. PANTA 4. PUNKTA a) APAKŠPUNKTU

Lai novērstu paziņojumu par atbalstu automātisku iesniegšanu, izmantojot sistēmu, parakstītājs pirms paziņojuma par atbalstu iesniegšanas iziet pienācīgu verifikācijas procesu, kas atbilst pastāvošajai praksei. Viens no iespējamajiem verifikācijas procesiem ir stipru autentifikācijas attēla rakstzīmju (*CAPTCHA*) lietošana.

2. TEHNISKĀS SPECIFIKĀCIJAS, LAI ĪSTENOTU REGULAS (ES) Nr. 211/2011 6. PANTA 4. PUNKTA b) APAKŠPUNKTU

Informācijas aizsardzības standarti

2.1. Organizatori iesniedz dokumentus, kas pierāda, ka tie atbilst standartā ISO/IEC 27001 noteiktajām prasībām, bez pienākuma to formāli pārņemt. Šim nolūkam tie ir:

a) veikuši pilnīgu riska novērtējumu, kurā noteikta sistēmas darbības joma, parādīta ietekme uz darbību, gadījumā ja ir notikuši dažādi informācijas drošības pārkāpumi, uzskaitīti draudi informācijas sistēmai un tās ievainojamība, izveidots riska izvērtējuma dokuments, kurā ir uzskaitīti arī pretpasākumi, lai novērstu šādus draudus, un aizsardzības līdzekļi, kas tiks izmantoti, ja draudi rodas, un, visbeidzot, sagatavots saraksts, kurā prioritārā kārtībā uzskaitīti nepieciešamie uzlabojumi;

b) izstrādājuši un īstenojuši pasākumus, kā apieties ar risku, ņemot vērā personas datu aizsardzību un privātās dzīves un ģimenes dzīves aizsardzību, un pasākumus, kuri tiks veikti, gadījumā ja rodas risks;

c) rakstveidā noteikuši nenovērstos riskus;

d) nodrošinājuši organizatoriskus līdzekļus, lai saņemtu informāciju par jauniem draudiem un drošības uzlabojumiem.

2.2. Organizatori izvēlas drošības kontroles, kas balstās uz 2.1.punkta a) apakšpunktā noteikto riska analīzi, no šādiem standartiem:

1) ISO/IEC 27002; vai

2) Informācijas drošības foruma "Labas prakses standarta" (*Information Security Forum's "Standard of Good Practice"*),

lai risinātu šādus jautājumus:

a) riska novērtējumi (ieteicama ISO/IEC 27005 vai cita īpaša un piemērota riska novērtēšanas metodoloģija);

b) fiziskā un vides drošība;

c) cilvēkresursu drošība;

d) saziņas un operāciju pārvaldība;

e) standarta piekļuves kontroles mehānismi papildus tiem, kas noteikti šajā īstenošanas regulā;

f) informācijas sistēmu iegāde, izveidošana un uzturēšana;

g) informācijas drošības starpgadījumu pārvaldība;

h) pasākumi, lai labotu un mazinātu robus informācijas sistēmās, kuru rezultātā varētu notikt apstrādāto datu iznīcināšana, nejauša nozaudēšana, izmainīšana, neatļauta izpaušana vai piekļuve tiem;

i) atbilstība;

j) datortīklu drošība (ieteicams ISO/IEC 27033 vai "Labas prakses standarts").

Šo standartu piemērošanu var ierobežot un attiecināt tikai uz tām organizācijas daļām, kuras ir būtiskas vākšanas tiešsaistes sistēmai. Piemēram, cilvēkresursu drošību var attiecināt tikai uz personālu, kam ir fiziska vai tīkla piekļuve vākšanas tiešsaistes sistēmai, un fizisko/vides drošību var attiecināt tikai uz ēku (ēkām), kur tiek mitināta sistēma.

Funkcionālās prasības

2.3. Vākšanas tiešsaistes sistēma sastāv no tīmekļa lietotnes, kas izveidota, lai vāktu paziņojumus par atbalstu vienai pilsoņu iniciatīvai.

2.4. Ja sistēmas administrēšanai ir nepieciešamas vairākas lomas, tad tiek izveidoti dažādi piekļuves kontroles līmeņi, ievērojot mazākās konfidencialitātes pielaides principu.

2.5. Publiski pieejamās funkcijas ir skaidri nodalītas no funkcijām, kas ir paredzētas administrēšanas mērķiem. Nekāda piekļuves kontrole neliedz lasīt informāciju, kas ir pieejama sistēmas publiskajā daļā, ieskaitot informāciju par iniciatīvu un paziņojuma par atbalstu elektronisko veidlapu. Parakstīšanās par iniciatīvu ir iespējama, tikai izmantojot šo publisko daļu.

2.6. Sistēma atklāj un novērš paziņojumu par atbalstu dubultu iesniegšanu.

Lietotnes līmeņa drošība

2.7. Sistēma ir pienācīgi aizsargāta pret zināmām ievainojamībām un ļaunprātīgu izmantošanu. Šajā nolūkā tā cita starpā atbilst šādām prasībām:

2.7.1. Sistēma ir aizsargāta pret injekcijas kļūdām, piemēram, strukturētās vaicājumu valodas (*SQL*) vaicājumiem, direktoriju vieglpiekļuves protokola (*LDAP*) vaicājumiem, *XML* valodas *XPath* vaicājumiem (*XML Path Language* (*XPath*) *queries*), operētājsistēmas (OS) komandām vai programmas argumentiem (*program arguments*). Šim nolūkam ir vismaz nepieciešams, ka:

a) visi lietotāju ievadītie dati tiek validēti;

b) validēšanu veic vismaz servera puses loģika (*server-side logic*);

c) izmantojot jebkādus interpretatorus, neuzticami dati ir skaidri nodalīti no komandas vai vaicājuma. Attiecībā uz *SQL* vaicājumiem tas nozīmē saistošo mainīgo (*bind variables*) izmantošanu visos sagatavotajos priekšrakstos un saglabātajos procesos un izvairīšanos no dinamiskiem vaicājumiem.

2.7.2. Sistēma ir aizsargāta pret starpvietņu skriptošanu (*XSS*). Šim nolūkam ir vismaz nepieciešams, ka:

a) visi lietotāju ievadītie dati, kas tiek nosūtīti atpakaļ uz pārlūkprogrammu, tiek validēti (izmantojot ievadīto datu validāciju);

b) visi lietotāju ievadītie dati ir pienācīgi kodēti, pirms tie tiek iekļauti izvades lapā;

c) pienācīga izvaddatu kodēšana nodrošina, ka šādi ievadītie dati vienmēr tiek apstrādāti kā teksts pārlūkprogrammā. Netiek izmantots aktīvs saturs.

2.7.3. Sistēmai ir stipra autentificēšanas un sesiju pārvaldība, kam vismaz ir nepieciešams, ka:

a) akreditācijas dati, kad tos saglabā, vienmēr tiek aizsargāti, izmantojot jaukšanu vai šifrēšanu. Risks, ka kāda persona autentificējas, izmantojot jaukšanas apiešanu (*pass-the-hash*), ir samazināts;

b) akreditācijas datus nevar uzminēt vai pārrakstīt vāju konta pārvaldības funkciju dēļ (piemēram, konta izveidošana, paroles maiņa, paroles atgūšana, vāji sesiju identifikatori (ID));

c) sesiju ID un sesiju dati netiek atklāti vienotajā resursu vietrādī (*URL*);

d) sesiju ID nav neaizsargāti pret sesiju fiksācijas uzbrukumiem;

e) sesiju ID noilgst, kas nodrošina, ka lietotāji pārtrauc savienojumu;

f) sesiju ID netiek rotēti pēc veiksmīgas pieteikšanās;

g) paroles, sesiju ID un citi akreditācijas dati tiek nosūtīti, tikai izmantojot transporta slāņa drošību (*Transport Layer Security* (*TLS*));

h) sistēmas administrācijas daļa ir aizsargāta. Ja tā ir aizsargāta ar vienfaktora autentificēšanu, tad parole sastāv vismaz no desmit zīmēm, kuru skaitā ir vismaz viens burts, viens cipars un viena īpašā zīme. Var arī izmantot divfaktoru autentificēšanu. Ja tiek izmantota tikai vienfaktora autentificēšana, tā ietver divu soļu verifikācijas mehānismu, lai piekļūtu sistēmas administrācijas daļai caur internetu, kurā vienfaktora autentificēšanu pastiprina cits autentificēšanas mehānisms, piemēram, vienreiz izmantojama piekļuves frāze/kods, kas tiek nosūtīts ar *SMS*, vai asimetriski šifrēta nejaušu pārbaužu virkne, ko atšifrē, izmantojot organizatoru/administratoru personisko atslēgu, kas nav zināma sistēmai.

2.7.4. Sistēmai nav nedrošas tiešās objektu atsauces. Šim nolūkam ir vismaz nepieciešams, ka:

a) attiecībā uz tiešajām atsaucēm uz ierobežotiem resursiem lietotne pārbauda, ka lietotājs ir sankcionēts piekļūt attiecīgajam pieprasītajam resursam;

b) ja atsauce ir netiešā atsauce, tiešās atsauces kartēšana ir aprobežota ar vērtībām, kas ir sankcionētas tikai attiecībā uz pašreizējo lietotāju.

2.7.5. Sistēma aizsargā pret starpvietņu pieprasījumu viltošanas kļūdu.

2.7.6. Pastāv pienācīga drošības konfigurācija, kura nodrošina vismaz to, ka:

a) visas programmatūras komponentes ir aktuālas, tai skaitā operētājsistēma, tīmekļa/lietotnes serveris, datubāzes pārvaldības sistēma (*DBMS*), lietotnes un visas kodu bibliotēkas;

b) ir atspējoti, izņemti vai nav instalēti nevajadzīgi OS un tīmekļa/lietotnes servera pakalpojumi;

c) sākotnējās konta paroles tiek grozītas vai tiek atspējotas;

d) ir izveidota kļūdu apstrāde, lai novērstu steka izsekošanu (*stack trace*) vai citu pārlieku daudz informācijas saturošu ziņojumu noplūdi;

e) drošības iestatījumi izstrādes struktūrās (*development frameworks*) un bibliotēkās tiek konfigurēti saskaņā ar labāko praksi, piemēram, *OWASP* vadlīnijām.

2.7.7. Sistēma nodrošina datu šifrēšanu šādi:

a) personas dati elektroniskā formātā tiek šifrēti, kad tie tiek saglabāti vai nosūtīti kompetentajām iestādēm dalībvalstīs saskaņā ar Regulas (ES) Nr. 211/2011 8. panta 1. punktu, kodu pārvaldīšanai un dublikātu sagatavošanai notiekot atsevišķi;

b) tiek lietoti stipri standarta algoritmi un stipras atslēgas saskaņā ar starptautiskajiem standartiem. Pastāv kodu pārvaldības sistēma;

c) paroles tiek jauktas ar stipru standarta algoritmu, un tiek izmantots pienācīgs "sāls" (*salt*);

d) visas atslēgas un paroles tiek aizsargātas no nesankcionētas piekļuves.

2.7.8. Sistēma ierobežo *URL* piekļuvi, balstoties uz lietotāju piekļuves līmeņiem un atļaujām. Šim nolūkam ir vismaz nepieciešams, ka:

a) ja tiek lietoti ārējie drošības mehānismi, lai nodrošinātu autentifikācijas un sankcionēšanas pārbaudes lapas piekļuvei, tiem ir jābūt pienācīgi konfigurētiem attiecībā uz katru lapu;

b) ja tiek lietota kodu līmeņa aizsardzība, kodu līmeņa aizsardzībai ir jābūt katrai nepieciešamajai lapai.

2.7.9. Sistēma lieto pietiekamu transporta slāņa aizsardzību (*Transport Layer Protection*). Šim nolūkam pastāv visi no šiem pasākumiem vai līdzvērtīga spēka pasākumi:

a) sistēmai ir nepieciešama visaktuālākā hiperteksta drošas pārsūtīšanas protokola versija (*HTTPS*), lai piekļūtu jebkādiem sensitīviem resursiem, izmantojot spēkā esošus sertifikātus, kuru termiņš nav beidzies, kas nav atsaukti un atbilst visiem vietnē lietotajiem domēniem;

b) sistēma piešķir karodziņu "drošs" visām jūtīgajām sīkdatnēm;

c) serveris konfigurē *TLS* sniedzēju, lai tas atbalstītu tikai šifrēšanas algoritmus, kas atbilst labākajai praksei. Lietotāji tiek informēti, ka tiem ir jāatļauj *TLS* atbalsts savā pārlūkprogrammā.

2.7.10. Sistēma aizsargā pret neatļautu novirzīšanu un pārvirzīšanu.

Datubāzu drošība un datu integritāte

2.8. Gadījumos, kad vākšanas tiešsaistes sistēmām, kas tiek izmantotas pilsoņu iniciatīvām, ir kopīga aparatūra un operētājsistēmu resursi, tās neapmainās ar datiem, tai skaitā piekļuves/šifrēšanas akreditācijas datiem. Turklāt tas ir atspoguļots riska novērtējumā un īstenotajos pretpasākumos.

2.9. Risks, ka kāda persona autentificējas, izmantojot "jaukšanas apiešanu", ir samazināts.

2.10. Dati, ko sniedz parakstītāji, ir pieejami tikai datubāzes administratoram/organizatoram.

2.11. Administratīvie akreditācijas dati, personas dati, kas ir savākti no parakstītājiem, un to dublikāti tiek aizsargāti, izmantojot stiprus šifrēšanas algoritmus saskaņā ar 2.7.7. punkta b) apakšpunktu. Tomēr sistēmā nešifrēti var saglabāt dalībvalsti, kurai tiks pieskaitīts paziņojums par atbalstu, paziņojuma par atbalstu iesniegšanas datumu un valodu, kurā parakstītājs aizpildīja paziņojumu par atbalstu.

2.12. Parakstītājiem ir piekļuve tikai datiem, kas ir ievadīti sesijā, kurā tie pabeidz aizpildīt paziņojuma par atbalstu veidlapu. Līdzko paziņojums par atbalstu ir iesniegts, iepriekšējā sesija tiek slēgta un ievadītajiem datiem vairs nevar piekļūt.

2.13. Parakstītāja personas dati ir pieejami tikai sistēmā, ieskaitot dublikātu šifrētā formātā. Datu apskates vai sertificēšanas nolūkā, ko veic valsts iestādes saskaņā ar Regulas (ES) Nr. 211/2011 8. pantu, organizatori var eksportēt šifrētos datus saskaņā ar 2.7.7.punkta a) apakšpunktu.

2.14. Paziņojumā par atbalstu ievadīto datu inertība ir atomiska. Tas nozīmē, ka, līdzko lietotājs paziņojuma par atbalstu veidlapā ir ievadījis visu nepieciešamo informāciju un validējis savu lēmumu atbalstīt iniciatīvu, sistēma vai nu nodod visus veidlapas datus datubāzei, vai – kļūdas gadījumā – nesaglabā nekādus datus. Sistēma informē lietotāju par viņa pieprasījuma veiksmīgu vai neveiksmīgu apstrādāšanu.

2.15. *DBMS*, kas tiek lietota, ir aktualizēta un tiek nepārtraukti uzlabota attiecībā uz jaunatklātiem ļaunprātīgas izmantošanas gadījumiem.

2.16. Visi sistēmas aktivitātes žurnāli ir vietā. Sistēma nodrošina, ka visus audita žurnālus, kas reģistrē izņēmumus un citus ar drošību saistītus notikumus, kuri uzskaitīti turpmāk, var ģenerēt un saglabāt, līdz dati ir iznīcināti saskaņā ar Regulas (ES) Nr. 211/2011 12. panta 3. vai 5. punktu. Žurnāli tiek pienācīgi aizsargāti, piemēram, saglabājot tos šifrētos datu nesējos. Organizatori/administratori regulāri pārbauda žurnālus attiecībā uz aizdomīgu darbību. Žurnālu saturs ietver vismaz:

a) datumus un laikus, kad organizatori/administratori veic pieteikšanos un veic atteikšanos;

b) veiktos dublējumus;

c) visas datubāzes administratoru izmaiņas un atjauninājumus.

Infrastruktūras drošība – fiziskā atrašanās vieta, tīkla infrastruktūra un serveru vide

2.17. *Fiziskā drošība*

Neatkarīgi no tā, kāda veida mitināšana tiek lietota, iekārta, kas mitina lietotni, ir pienācīgi aizsargāta, kas nozīmē:

a) mitināšanas telpas piekļuves kontroli un audita žurnālu;

b) dublējumu datu fizisko aizsardzību pret zādzību vai nejaušu novietošanu nevietā;

c) serveris, kas mitina lietotni, ir instalēts drošā statīvā.

2.18. *Tīkla drošība*

2.18.1. Sistēma tiek mitināta uz servera, kas savienots ar internetu un kas ir instalēts "demilitarizētā zonā" (*DMZ*), un ko aizsargā ugunsmūris.

2.18.2. Kad ugunsmūra produkta attiecīgi jauninājumi un ielāpi kļūst publiski pieejami, tie tiek nekavējoties instalēti.

2.18.3. Visu ienākošo un no servera izejošo datu plūsmu (kas paredzēta vākšanas tiešsaistes sistēmai) pārbauda ugunsmūra noteikumi, un tā tiek reģistrēta. Ugunsmūra noteikumi neatļauj jebkādas plūsmas, kas nav vajadzīgas sistēmas drošai lietošanai un administrēšanai.

2.18.4. Vākšanas tiešsaistes sistēma ir jāmitina uz pienācīgi aizsargāta produkcijas tīkla segmenta, kas ir nodalīts no segmentiem, kurus izmanto neproduktīvas sistēmas, piemēram, izstrādes vai testēšanas vidēm.

2.18.5. Pastāv lokālā tīkla (*LAN*) aizsardzības mehānismi, piemēram:

a) *Layer 2* (*L2*) piekļuves saraksts/pārmijportu drošība;

b) neizmantoti pārmijporti tiek atspējoti;

c) *DMZ* ir uz īpaša virtuālā lokālā tīkla (*VLAN*)/*LAN*;

d) nevajadzīgos pārmijportos nav iespējots *L2 trunking*.

2.19. *OS un tīmekļa/lietotnes servera drošība*

2.19.1. Pastāv pienācīga drošības konfigurācija, ieskaitot elementus, kas ir uzskaitīti 2.7.6. punktā.

2.19.2. Lietotnes darbojas, izmantojot viszemāko privilēģiju komplektu, kas tām ir nepieciešams, lai darbotos.

2.19.3. Administratora piekļuvei vākšanas tiešsaistes sistēmas pārvaldības saskarnei ir īsa sesijas noildze (maksimāli 15 minūtes).

2.19.4. Kad attiecīgi OS jauninājumi un ielāpi, lietotņu izpildlaiki, lietotnes, kas darbojas uz servera, vai pretvīrusu programmas tiek publiskotas, šādi jauninājumi vai ielāpi tiek nekavējoties instalēti.

2.19.5. Risks, ka kāda persona autentificējas sistēmā, izmantojot "jaukšanas apiešanu", ir samazināts.

2.20. *Organizatoru klientu drošība*

Abpusējas drošības labad organizatori veic nepieciešamos pasākumus, lai aizsargātu savu klientu lietotni/ierīci, ko tie izmanto, lai pārvaldītu un piekļūtu vākšanas tiešsaistes sistēmai, piemēram:

2.20.1. lietotāji veic ar uzturēšanu nesaistītus uzdevumus (*non-maintenance tasks*) (piemēram, biroju automatizāciju) ar mazāko privilēģiju skaitu, kas ir nepieciešams to darbībai;

2.20.2. kad OS, jebkādas instalētas lietotnes vai pretvīrusu programmas attiecīgi jauninājumi un ielāpi kļūst publiski pieejami, šādi jauninājumi vai ielāpi tiek nekavējoties instalēti.

3. TEHNISKĀS SPECIFIKĀCIJAS, LAI ĪSTENOTU REGULAS (ES) Nr. 211/2011 6. PANTA 4. PUNKTA c) APAKŠPUNKTU

3.1. Sistēma sniedz iespēju attiecībā uz katru dalībvalsti iegūt ziņojumu, kurā iekļauta iniciatīva un parakstītāju personas dati, pēc šīs dalībvalsts kompetentās iestādes veiktās verifikācijas.

3.2. Eksportēt parakstītāju paziņojumus par atbalstu ir iespējams Regulas (ES) Nr. 211/2011 III pielikumā noteiktajā formātā. Sistēma var nodrošināt iespēju eksportēt paziņojumu par atbalstu sadarbspējīgā formātā, piemēram, paplašināmās iezīmēšanas valodā (*XML*).

3.3. Eksportētie paziņojumi par atbalstu tiek iezīmēti kā "*ierobežotai izplatīšanai*" attiecīgajai dalībvalstij un marķēti ar atzīmi "*personas dati*".

3.4. Eksportēto datu elektroniska nosūtīšana dalībvalstīm tiek aizsargāta pret pārtveršanu, izmantojot piemērotu pilnīgu šifrēšanu.