

**Vākšanas tiešsaistes sistēmas sertifikācijas pārbaudes lapa**

**1. Gadījumā, kad tiek izmantots Komisijas izstrādātais programmnodrošinājums:**

**Punkti 2.1 un 2.2:**

INFORMĀCIJAS DROŠĪBAS GARANTIJAS STANDARTI		STATUSS		
		Ieviests	Nav ieviests	Tiks pilnveidots
Prasības	Avots			
<p>Organizatori iesniedz dokumentus, kas pierāda, ka tie atbilst standartā ISO/IEC 27001 noteiktajām prasībām, bez pienākuma to formāli pārņemt. Šim nolūkam tie ir:</p> <p>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;</p> <p>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;</p> <p>c) rakstveidā noteikuši nenovērstos riskus;</p> <p>d) nodrošinājuši organizatoriskus līdzekļus, lai saņemtu informāciju par jauniem draudiem un drošības uzlabojumiem.</p>	<p><i>TS – 2.1. punkts</i></p>			

<p>Organizatori izvēlas drošības kontroles, kas balstās uz 2.1.punkta a) apakšpunktā noteikto riska analīzi, no šādiem standartiem:</p> <ol style="list-style-type: none"> <li>1) ISO/IEC 27002; vai</li> <li>2) Informācijas drošības foruma “Labas prakses standarta” (Information Security Forum’s “Standard of Good Practice”), lai risinātu šādus jautājumus:       <ol style="list-style-type: none"> <li>a) riska novērtējumi (ieteicama ISO/IEC 27005 vai cita īpaša un piemērota riska novērtēšanas metodoloģija);</li> <li>b) fiziskā un vides drošība;</li> <li>c) cilvēkresursu drošība;</li> <li>d) saziņas un operāciju pārvaldība;</li> <li>e) standarta piekļuves kontroles mehānismi papildus tiem, kas noteikti šajā īstenošanas regulā;</li> <li>f) informācijas sistēmu iegāde, izveidošana un uzturēšana;</li> <li>g) informācijas drošības starpgadījumu pārvaldība;</li> <li>h) pasākumi, lai labotu un mazinātu robus informācijas sistēmās, kuru rezultātā varētu notikt apstrādāto datu iznīcināšana, nejauša nozaudēšana, izmainīšana, neatļauta izpaušana vai piekļuve tiem;</li> <li>i) atbilstība;</li> <li>j) datortīklu drošība (ieteicams ISO/IEC 27033 vai “Labas prakses standarts” (SoGP)).</li> </ol> </li> </ol> <p>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.</p>	<p><i>TS – 2.2. punkts</i></p>			
---	--------------------------------	--	--	--

PRETPASĀKUMU STATUSA NOVĒRTĒJUMS			STATUSS				
			leviests	Nav ieviests	Pieņemts risks	Plānots	Nav piemērojams
Draudi	Pretpasākumi	Avots					
Bojāta autentifikācija un sesiju pārvaldība	paroles, sesiju ID un citi akreditācijas dati tiek nosūtīti, tikai izmantojot transporta slāņa drošību (Transport Layer Security (TLS))	TS – 2.7.3.g punkts					
Nepietiekoša Transporta slāņa ievainojamību izmantošana	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.	TS – 2.7.9.a punkts					
Nepietiekoša Transporta slāņa ievainojamību izmantošana	Sistēma piešķir karodziņu “drošs” visām jūtīgajām sīkdatnēm ( <i>cookies</i> ).	TS – 2.7.9.b punkts					
Nepietiekoša Transporta slāņa ievainojamību izmantošana	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.	TS – 2.7.9.c punkts					
Tīkla trafika noklausīšanās	Administrators piekļuvei vākšanas tiešsaistes sistēmas pārvaldības saskarnei ir īsa sesijas noildze (maksimāli 15 minūtes).	TS – 2.19.3 punkts					

<p>Neautorizēta piekļuve</p>	<p>Visi sistēmas aktivitātes žurnāli (<i>logs</i>) 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.</p> <p>Žurnālu saturs ietver vismaz:</p> <p>a) datumus un laikus, kad organizatori/administratori veic pieteikšanos (<i>log-on</i>) un veic atteikšanos (<i>log-off</i>) sistēmā;</p> <p>b) veiktos dublējumus;</p> <p>c) visas datubāzes administratoru veiktās izmaiņas un atjauninājumus.</p>	<p>TS – 2.16 punkts</p>					
	<p>Pastāv pienācīga drošības konfigurācija, kura nodrošina vismaz to, ka:</p> <p>a) visas programmatūras komponentes ir aktuālas un atjaunotas, tai skaitā operētājsistēma, tīmekļa/lietotnes serveris, datubāzes pārvaldības sistēma (DBMS), lietotnes un visas izejas kodu bibliotēkas;</p> <p>b) ir atspējoti, izņemti vai nav instalēti nevajadzīgi OS un tīmekļa/lietotnes servera pakalpojumi;</p> <p>c) sākotnējās konta paroles tiek grozītas vai tiek atspējotas;</p> <p>d) ir izveidota kļūdu apstrāde, lai novērstu steka izsekošanu (<i>stack trace</i>) vai citu pārlietu</p>	<p>TS – 2.7.6 punkts</p>					

	<p>daudz informācijas saturošu kļūdu paziņojumu noplūdi;</p> <p>e) drošības iestatījumi izstrādes struktūrās (<i>development frameworks</i>) un bibliotēkās tiek konfigurēti saskaņā ar labāko praksi, piemēram, OWASP vadlīnijām.</p>						
	<p>DBMS, kas tiek lietota, ir aktualizēta un tiek nepārtraukti uzlabota attiecībā uz jaunatklātiem ļaunprātīgas izmantošanas gadījumiem.</p>	<p><i>TS – 2.15 punkts</i></p>					
	<p>Fiziskā drošība</p> <p>Neatkarīgi no tā, kāda veida mitināšana (<i>hosting</i>) tiek lietota, iekārta, kas mitina lietotni, ir pienācīgi aizsargāta, kas nozīmē:</p> <p>a) mitināšanas telpas piekļuves kontroli un audita žurnālu;</p> <p>b) dublējumu datu fizisko aizsardzību pret zādzību vai nejaušu novietošanu nevietā;</p> <p>c) serveris, kas mitina lietotni, ir instalēts drošā statīvā.</p>	<p><i>TS – 2.17 punkts</i></p>					
	<p>Sistēma tiek mitināta uz servera, kas savienots ar internetu un kas ir instalēts “demilitarizētā zonā” (DMZ), un ko aizsargā uguns mūris.</p>	<p><i>TS – 2.18.1 punkts</i></p>					
	<p>Kad uguns mūra produkta attiecīgi jauninājumi un ielāpi kļūst publiski pieejami, tie tiek nekavējoties instalēti.</p>	<p><i>TS – 2.18.2 punkts</i></p>					
	<p>Visu ienākošo un no servera izejošo datu plūsmu (kas paredzēta vākšanas tiešsaistes sistēmai) pārbauda uguns mūra noteikumi, un tā tiek reģistrēta. Uguns mūra noteikumi neatļauj jebkādas plūsmas, kas nav vajadzīgas sistēmas drošai lietošanai un administrēšanai.</p>	<p><i>TS – 2.18.3 punkts</i></p>					

	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.	TS – 2.18.4 punkts					
	Pastāv lokālā tīkla (LAN) aizsardzības mehānismi, tādi kā: a) Layer 2 (L2) piekļuves saraksts / pārmijportu ( <i>switchport</i> ) drošība; b) neizmantoti pārmijporti tiek atspējoti; c) DMZ ir uz īpaša virtuālā lokālā tīkla (VLAN)/LAN; d) nevajadzīgos pārmijportos nav iespējots L2 trunking.	TS – 2.18.5 punkts					
	Kad attiecīgi jauninājumi un ielāpi OS, lietotņu izpildlaika versijām ( <i>runtimes</i> ), lietotnēm, kas darbojas uz servera, vai pretvīrusu programmām tiek publicētas, šādi jauninājumi vai ielāpi tiek nekavējoties instalēti.	TS – 2.19.4 punkts					
	Organizatoru klientu drošība Lai nodrošinātu gala-gala ( <i>end-to-end</i> ) drošību organizatori veic nepieciešamos pasākumus, lai aizsargātu savu klientu lietotni/ierīci, ko tie izmanto, lai pārvaldītu un piekļūtu vākšanas tiešsaistes sistēmai.	TS – 2.20 punkts					
	Lietotāji veic ar uzturēšanu nesaistītus uzdevumus ( <i>non-maintenance tasks</i> ) (piemēram, biroju automatizāciju) ar mazāko privilēģiju kopu, kas ir nepieciešamas to darbībai.	TS – 2.20.1 punkts					
	Kad OS, jebkādas instalētas lietotnes vai pretvīrusu programmas attiecīgi jauninājumi un ielāpi kļūst publiski pieejami, šādi jauninājumi vai ielāpi tiek nekavējoties instalēti.	TS – 2.20.2 punkts					

	Pastāv pienācīga drošības konfigurācija, iesklaujot visus elementus, kas ir uzskaitīti TS 2.7.6. punktā.	TS – 2.19.1 punkts					
Neautorizēta piekļuve	Aplikācijas darbojas ar zemāko privilēģiju kopu, kādas ir nepieciešamas to darbībai.	TS – 2.19.2 punkts					
	Risks, kādai personai autentificēties sistēmā, izmantojot “jaušanas apiešanu” ( <i>pass-the-hash</i> ), ir samazināts.	TS – 2.19.5 punkts					

REGULAS (EU) Nr. 211/2011 PUNKTA 6(4)(c) PRASĪBU IEVIEŠANA		STATUSS		
		leviets	Nav ieviests	Tiks pilnveidots
Prasības	Avots			
Eksportēto datu elektroniska nosūtīšana dalībvalstīm tiek aizsargāta pret pārtveršanu, izmantojot piemērotu gala-gala ( <i>end-to-end</i> ) šifrēšanu.	TS – 3.4 punkts			



**2. Gadījumā, kad netiek izmantots Komisijas izstrādātais programmnodrošinājums:**

INFORMĀCIJAS DROŠĪBAS GARANTIJAS STANDARTI		STATUSS		
		ieviests	Nav ieviests	Tiks pilnveidots
Prasības	Avots			
<p>Organizatori iesniedz dokumentus, kas pierāda, ka tie atbilst standartā ISO/IEC 27001 noteiktajām prasībām, bez pienākuma to formāli pārņemt. Šim nolūkam tie ir:</p> <p>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;</p> <p>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;</p> <p>c) rakstveidā noteikuši nenovērstos riskus;</p> <p>d) nodrošinājuši organizatoriskus līdzekļus, lai saņemtu informāciju par jauniem draudiem un drošības uzlabojumiem.</p>	TS – 2.1. punkts			

<p>Organizatori izvēlas drošības kontroles, kas balstās uz 2.1.punkta a) apakšpunktā noteikto riska analīzi, no šādiem standartiem:</p> <ol style="list-style-type: none"> <li>1) ISO/IEC 27002; vai</li> <li>2) Informācijas drošības foruma “Labas prakses standarta” (Information Security Forum’s “Standard of Good Practice”), lai risinātu šādus jautājumus:       <ol style="list-style-type: none"> <li>a) riska novērtējumi (ieteicama ISO/IEC 27005 vai cita īpaša un piemērota riska novērtēšanas metodoloģija);</li> <li>b) fiziskā un vides drošība;</li> <li>c) cilvēkresursu drošība;</li> <li>d) saziņas un operāciju pārvaldība;</li> <li>e) standarta piekļuves kontroles mehānismi papildus tiem, kas noteikti šajā īstenošanas regulā;</li> <li>f) informācijas sistēmu iegāde, izveidošana un uzturēšana;</li> <li>g) informācijas drošības starpgadījumu pārvaldība;</li> <li>h) pasākumi, lai labotu un mazinātu robus informācijas sistēmās, kuru rezultātā varētu notikt apstrādāto datu iznīcināšana, nejauša nozaudēšana, izmaiņšana, neatļauta izpaušana vai piekļuve tiem;</li> <li>i) atbilstība;</li> <li>j) datortīklu drošība (ieteicams ISO/IEC 27033 vai “Labas prakses standarts” (SoGP)).</li> </ol> </li> </ol> <p>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.</p>	<p><i>TS – 2.2. punkts</i></p>			
--	--------------------------------	--	--	--

FUNKCIONĀLĀS PRASĪBAS		STATUSS		
		Ieviests	Nav ieviests	Tiks pilnveidots
Prasības	Avots			
Vākšanas tiešsaistes sistēma sastāv no tīmekļa lietotnes, kas izveidota, lai vāktu paziņojumus par atbalstu vienai pilsoņu iniciatīvai.	<i>TS– 2.3 punkts</i>			
Ja sistēmas administrēšanai ir nepieciešamas vairākas lomas, tad tiek izveidoti dažādi piekļuves kontroles līmeņi, ievērojot mazāko privilēģiju principu.	<i>TS– 2.4 punkts</i>			
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.	<i>TS– 2.5 punkts</i>			
Sistēma atklāj un novērš paziņojumu par atbalstu dubultu iesniegšanu.	<i>TS–2.6 punkts</i>			

PRETPASĀKUMU STATUSA NOVĒRTĒJUMS			STATUSS				
			leviests	Nav ieviests	Pieņemts risks	Plānots	Nav piemērojams
Draudi	Pretpasākumi	Avots					
Injeksija	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 ( <i>program arguments</i> ).	TS – 2.7.1 punkts					
Injeksija	Visi lietotāju ievadītie dati tiek validēti.	TS – 2.7.1.a punkts					
Injeksija	Validēšanu veic vismaz servera puses loģika ( <i>server-side logic</i> ).	TS – 2.7.1.b punkts					
Injeksija	Izmantojot jebkādu interpretatoru, neuzticami dati ir skaidri nodalīti no komandas vai vaicājuma. Attiecībā uz SQL vaicājumiem tas nozīmē saistošo mainīgo ( <i>bind variables</i> ) izmantošanu visos sagatavotajos priekšrakstos un saglabātajos procesos, un izvairīšanos no dinamiskiem vaicājumiem.	TS – 2.7.1.c punkts					
starpvietņu skriptošana (XSS)	Visi lietotāju ievadītie dati, kas tiek nosūtīti atpakaļ uz pārlūkprogrammu, tiek validēti (izmantojot ievadīto datu validāciju).	TS – 2.7.2.a punkts					
starpvietņu skriptošana (XSS)	Visi lietotāju ievadītie dati ir pienācīgi kodēti ( <i>escaped</i> ), pirms tie tiek iekļauti izvades lapā.	TS – 2.7.2.b punkts					
starpvietņu skriptošana (XSS)	Pienācīga izvaddatu kodēšana nodrošina, ka šādi ievadītie dati vienmēr tiek apstrādāti kā teksts pārlūkprogrammā. Netiek izmantots aktīvs saturs.	TS – 2.7.2.c punkts					
Bojāta autentifikācija un	Sistēmai ir stipra autentificēšana un sesiju pārvaldība.	TS – 2.7.3 punkts					

sesiju pārvaldība								
Bojāta autentifikācija un sesiju pārvaldība	Akreditācijas dati ( <i>credentials</i> ), kad tos saglabā, vienmēr tiek aizsargāti, izmantojot jaukšanu vai šifrēšanu. Risks, kādam autentificēties sistēmā lietojot 'jaukšanas-apiešanu' ( <i>'pass-the-hash'</i> ) ir mazināts.	TS – 2.7.3.a punkts						
Bojāta autentifikācija un sesiju pārvaldība	Akreditācijas datus nevar uzminēt vai pārrakstīt vāju konta pārvaldības funkciju dēļ (piemēram - konta izveidošana, paroles maiņa, paroles atgūšana, vāji sesiju identifikatori (ID)).	TS – 2.7.3.b punkts						
Bojāta autentifikācija un sesiju pārvaldība	Sesiju ID un sesiju dati netiek atklāti vienotajā resursu vietrādī (URL).	TS – 2.7.3.c punkts						
Bojāta autentifikācija un sesiju pārvaldība	Sesiju ID nav ievainojami pret sesiju fiksācijas uzbrukumiem.	TS – 2.7.3.d punkts						
Bojāta autentifikācija un sesiju pārvaldība	Sesiju ID noilgst, kas nodrošina, ka lietotāji pārtrauc savienojumu.	TS – 2.7.3.e punkts						
Bojāta autentifikācija un sesiju pārvaldība	Sesiju ID netiek rotēti pēc veiksmīgas pieteikšanās.	TS – 2.7.3.f punkts						
Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana	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, šifra atslēgu pārvaldīšanai un dublikātu sagatavošanai notiekot atsevišķi.	TS – 2.7.7.a punkts						
Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana	Tiek lietoti stipri standarta algoritmi un stipras šifru atslēgas saskaņā ar starptautiskajiem standartiem. Pastāv šifru atslēgu pārvaldības sistēma.	TS – 2.7.7.b punkts						

Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana	Paroles tiek jauktas ( <i>hashed</i> ) ar stipru standarta algoritmu, un tiek izmantots pienācīgs "sāls" ( <i>salt</i> ).	TS – 2.7.7.c punkts					
Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana	Visas atslēgas un paroles tiek aizsargātas no nesankcionētas piekļuves.	TS – 2.7.7.d punkts					
Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana	Administratīvie akreditācijas dati, personas dati, kas ir savākti no parakstītājiem, un to dublikāti tiek aizsargāti, izmantojot stiprus šifrēšanas algoritmus atbilstoši TS 2.7.7(b) punkta prasībām. Tomēr, dalībvalsts, kurā tiks skaitīti atbalsta paziņojumi, atbalsta paziņojuma iesniegšanas datums un valoda, kurā parakstītājs ir aizpildījis atbalsta paziņojumu, sistēma var tikt uzglabāti nešifrētā veidā.	TS – 2.11 punkts					
Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana	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 TS 2.7.7(a) punktu.	TS – 2.13 punkts					
URL piekļuves ierobežošanas kļūda	Ja tiek lietoti ārējie drošības mehānismi, lai nodrošinātu autentifikācijas un sankcionēšanas pārbaudes lapas piekļuvei, tiem ir jābūt pienācīgi konfigurētiem attiecībā uz katru lapu.	TS – 2.7.8.a punkts					
URL piekļuves ierobežošanas kļūda	Ja tiek lietota koda līmeņa aizsardzība, koda līmeņa aizsardzībai ir jābūt katrai nepieciešamajai lapai.	TS – 2.7.8.b punkts					
Brute Force uzbrukums	Sistēmas administrācijas daļa ir aizsargāta. Ja tā ir aizsargāta ar vien-faktora autentificēšanu, tad parole sastāv vismaz no desmit zīmēm, kuru skaitā ir vismaz viens burts, viens cipars un viena īpašā zīme. Var arī izmantot div-faktoru autentificēšanu. Gadījumā ja tiek lietota tikai vien-faktora autentificēšanās,	TS – 2.7.3.h punkts					

	tā satur divu soļu verifikācijas mehānismu, lai piekļūtu sistēmas administrēšanas sadaļai caur Internet. Kurā viens faktors ir papildināts lietojot citus autentifikācijas paņēmienus, tādus kā vienreiz lietojumu piekļuves frāzi/kodu caur SMS vai asimetriski šifrētu gadījuma izaicinājuma virkni ( <i>challenge string</i> ), kuru atšifrē lietojot organizatora/administratorsa privāto atslēgu, kura nav zināma sistēmai.						
Neautorizēta piekļuve	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.	<i>TS – 2.12 punkts</i>					
Neautorizēta piekļuve	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.	<i>TS – 2.8 punkts</i>					
Neautorizēta piekļuve	Dati, ko sniedz parakstītāji, ir pieejami tikai datubāzes administratoram/organizatoram.	<i>TS – 2.10 punkts</i>					
Neautorizēta piekļuve	Lietotnes darbojas, izmantojot vizemāko privilēģiju kopu, kas tām ir nepieciešams, lai darbotos.	<i>TS – 2.19.2 punkts</i>					
Aplikāciju kļūda	Paziņojumā par atbalstu ievadīto datu noturība 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.	<i>TS – 2.14 punkts</i>					
Bojāta autentifikācija un sesiju pārvaldība	Paroles, sesiju ID un citi akreditācijas dati tiek nosūtīti, tikai izmantojot transporta slāņa drošību (Transport Layer Security (TLS))	<i>TS – 2.7.3.g punkts</i>					

Nedrošu tiešo objektu atsauču ievainojamību izmantošana	Sistēmai nav nedrošas tiešās objektu atsauces.	TS – 2.7.4 punkts					
Nedrošu tiešo objektu atsauču ievainojamību izmantošana	Attiecībā uz tiešajām atsaucēm uz ierobežotiem resursiem lietotne pārbauda, ka lietotājs ir sankcionēts piekļūt attiecīgajam pieprasītajam resursam.	TS – 2.7.4.a punkts					
Nedrošu tiešo objektu atsauču ievainojamību izmantošana	Ja atsauce ir netiešā atsauce, tiešās atsauces kartēšana ir aprobežota ar vērtībām, kas ir sankcionētas tikai attiecībā uz pašreizējo lietotāju.	TS – 2.7.4.b punkts					
Nepietiekoša Transporta slāņa ievainojamību izmantošana	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.	TS – 2.7.9.a punkts					
Nepietiekoša Transporta slāņa ievainojamību izmantošana	Sistēma piešķir karodziņu “drošs” visām jūtīgajām sīkdatnēm ( <i>cookies</i> ).	TS – 2.7.9.b punkts					
Nepietiekoša Transporta slāņa ievainojamību izmantošana	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.	TS – 2.7.9.c punkts					
Tīkla trafika noklausīšanās	Administrators piekļuvei vākšanas tiešsaistes sistēmas pārvaldības saskarnei ir īsa sesijas noildze (maksimāli 15 minūtes).	TS – 2.19.3 punkts					
Neautorizēta piekļuve	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 iegūt 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	TS – 2.16 punkts					



	<p>Žurnālus attiecībā uz aizdomīgu darbību. Žurnālu saturs ietver vismaz:</p> <ul style="list-style-type: none"> <li>a) datumus un laikus, kad organizatori/administratori veic pieteikšanos (<i>log-on</i>) un veic atteikšanos (<i>log-off</i>) sistēmā;</li> <li>b) veiktos dublējumus;</li> <li>c) visas datubāzes administratoru izmaiņas un atjauninājumus.</li> </ul>						
	<p>Pastāv pienācīga drošības konfigurācija, kura nodrošina vismaz to, ka:</p> <ul style="list-style-type: none"> <li>a) visas programmatūras komponentes ir aktuālas, tai skaitā operētājsistēma, tīmekļa/lietotnes serveris, datubāzes pārvaldības sistēma (DBMS), lietotnes un visas kodu bibliotēkas;</li> <li>b) ir atspējoti, izņemti vai nav instalēti nevajadzīgi OS un tīmekļa/lietotnes servera pakalpojumi;</li> <li>c) sākotnējās konta paroles tiek grozītas vai tiek atspējotas;</li> <li>d) ir izveidota kļūdu apstrāde, lai novērstu steka izsekošanu (<i>stack trace</i>) vai citu pārlietu daudz informācijas saturošu kļūdu paziņojumu noplūdi;</li> <li>e) drošības iestatījumi izstrādes struktūrās (<i>development frameworks</i>) un bibliotēkās tiek konfigurēti saskaņā ar labāko praksi, piemēram, OWASP vadlīnijām.</li> </ul>	TS – 2.7.6 punkts					
	<p>DBMS, kas tiek lietota, ir aktualizēta un tiek nepārtraukti uzlabota attiecībā uz jaunatklātiem ļaunprātīgas izmantošanas gadījumiem (<i>exploits</i>).</p>	TS – 2.15 punkts					
	<p>Fiziskā drošība Neatkarīgi no tā, kāda veida mitināšana tiek lietota, iekārta, kas mitina lietotni, ir pienācīgi aizsargāta, kas nozīmē:</p> <ul style="list-style-type: none"> <li>a) mitināšanas telpas piekļuves kontroli un audita žurnālu;</li> <li>b) dublējumu datu fizisko aizsardzību pret zādzību vai nejaušu novietošanu nevietā;</li> <li>c) serveris, kas mitina lietotni, ir instalēts drošā statīvā.</li> </ul>	TS – 2.17 punkts					

	Sistēma tiek mitināta uz servera, kas savienots ar internetu un kas ir instalēts "demilitarizētā zonā" (DMZ), ko aizsargā uguns mūris.	TS – 2.18.1 punkts					
	Kad uguns mūra produkta attiecīgi jauninājumi un ielāpi kļūst publiski pieejami, tie tiek nekavējoties instalēti.	TS – 2.18.2 punkts					
	Visu ienākošo un no servera izejošo datu plūsmu (kas paredzēta vākšanas tiešsaistes sistēmai) pārbauda uguns mūra noteikumi, un tā tiek reģistrēta. Uguns mūra noteikumi neatļauj jebkādas plūsmas, kas nav vajadzīgas sistēmas drošai lietošanai un administrēšanai.	TS – 2.18.3 punkts					
	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.	TS – 2.18.4 punkts					
	Pastāv lokālā tīkla (LAN) aizsardzības mehānismi, piemēram: a) Layer 2 (L2) piekļuves saraksts / pārmijportu ( <i>switchport</i> ) drošība; b) neizmantojie pārmijporti tiek atspējoti; c) DMZ ir atsevišķā virtuālā lokālā tīklā (VLAN)/LAN; d) nevajadzīgos pārmijportos nav iespējots L2 trunking.	TS – 2.18.5 punkts					
	Kad attiecīgi jauninājumi un ielāpi OS, lietotņu izpildlaika versijām ( <i>runtimes</i> ), lietotnēm, kas darbojas uz servera, vai pretvīrusu programmām tiek publiskas, šādi jauninājumi vai ielāpi tiek nekavējoties instalēti.	TS – 2.19.4 punkts					

	<p>Organizatoru klientu drošība.          Lai nodrošinātu gala-gala (<i>end-to-end</i>) drošību organizatori veic nepieciešamos pasākumus, lai aizsargātu savu klientu lietotni/ierīci, ko tie izmanto, lai pārvaldītu un piekļūtu vākšanas tiešsaistes sistēmai.</p>	<i>TS – 2.20 punkts</i>					
	<p>Lietotāji veic ar uzturēšanu nesaistītus uzdevumus (<i>non-maintenance tasks</i>) (piemēram, biroju automatizāciju) ar mazāko privilēģiju kopu, kas ir nepieciešamas to darbībai.</p>	<i>TS – 2.20.1 punkts</i>					
	<p>Kad OS, jebkādas instalētas lietotnes vai pretvīrusu programmas attiecīgi jauninājumi un ielāpi kļūst publiski pieejami, šādi jauninājumi vai ielāpi tiek nekavējoties instalēti.</p>	<i>TS – 2.20.2 punkts</i>					
	<p>Sistēma aizsargā pret starpvietņu pieprasījumu viltošanas (<i>cross-site forgery</i>) kļūdu.</p>	<i>TS – 2.7.5 punkts</i>					
	<p>Sistēma aizsargā pret neatļautu novirzīšanu un pārvirzīšanu.</p>	<i>TS – 2.7.10 punkts</i>					
	<p>Risks, ka kāda persona autentificējas datubāzē, izmantojot “jaukšanas apiešanu” (<i>pass-the-hash</i>), ir samazināts.</p>	<i>TS – 2.9 punkts</i>					
	<p>Pastāv pienācīga drošības konfigurācija, iekļaujot visus elementus, kas ir uzskaitīti TS 2.7.6. punktā.</p>	<i>TS – 2.19.1 punkts</i>					
	<p>Risks, kādai personai autentificēties sistēmā, izmantojot “jaukšanas apiešanu” (<i>pass-the-hash</i>), ir samazināts.</p>	<i>TS – 2.19.5 punkts</i>					

REGULAS (EU) Nr. 211/2011 PUNKTA 6(4)(c) PRASĪBU IEVIEŠANA		STATUSS		
		Ieviests	Nav ieviests	Tiks pilnveidots
Prasības	Avots			
Sistēma sniedz iespēju attiecībā uz katru dalībvalsti iegūt ziņojumu, kurā iekļauta iniciatīva un parakstītāju personas dati, kas paredzēti šīs dalībvalsts kompetentās iestādes verifikāciju veikšanai.	TS – 3.1 punkts			
Eksportēt parakstītāju paziņojumus par atbalstu ir iespējams Regulas (ES) Nr. 211/2011 III pielikumā noteiktajā formātā. Sistēma var nodrošināt iespēju eksportēt paziņojumu par atbalstu savietojamā formātā, piemēram, paplašināmās iezīmēšanas valodā (XML).	TS – 3.2 punkts			
Eksportētie paziņojumi par atbalstu tiek iezīmēti kā “ierobežotai izplatīšanai” attiecīgajai dalībvalstij un marķēti ar atzīmi “personas dati”.	TS – 3.3 punkts			
Eksportēto datu elektroniska nosūtīšana dalībvalstīm tiek aizsargāta pret pārtveršanu, izmantojot piemērotu pilnīgu ( <i>end-to-end</i> ) šifrēšanu.	TS – 3.4 punkts			

REGULAS (EU) Nr. 211/2011 PUNKTA 6(4)(a) PRASĪBU IEVIEŠANA		STATUSS		
		Ieviests	Nav ieviests	Tiks pilnveidots
Prasības	Avots			
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.	TS – 1. punkts			