Projekts

LATVIJAS REPUBLIKAS MINISTRU KABINETS

2014.gada Noteikumi Nr.

Rīgā (prot. Nr. .§)

**Parakstu vākšanas tiešsaistes sistēmu drošības un tehniskās prasības**

Izdoti saskaņā ar

likuma „Par tautas nobalsošanu,

likumu ierosināšanu un Eiropas pilsoņu iniciatīvu”

 22.panta piekto daļu

**I Vispārīgie jautājumi**

1. Noteikumi nosaka:

1.1. drošības un tehniskās prasības parakstu vākšanas tiešsaistes sistēmai, lai nodrošinātu uzticamu un drošu parakstu vākšanu, izmantojot vienoto valsts un pašvaldību pakalpojumu portālu [www.latvija.lv](http://www.latvija.lv) (turpmāk – portāls) un citas parakstu vākšanas tiešsaistes sistēmas;

1.2. institūciju, kura izvērtē parakstu vākšanai izmantotās tiešsaistes sistēmas atbilstību šiem noteikumiem.

2. Lai nodrošinātu parakstu vākšanu elektroniski, tiek izveidota parakstu vākšanas tiešsaistes sistēma, izmantojot portālu (turpmāk - portāla parakstu vākšanas tiešsaistes sistēma), kuras pārzinis ir Centrālā vēlēšanu komisija (turpmāk – Komisija) un turētājs ir Valsts reģionālās attīstības aģentūra (turpmāk – Aģentūra). Portāla parakstu vākšanas tiešsaistes sistēma sastāv no šādām daļām:

2.1. parakstu vākšanas elektroniskā pakalpojuma (turpmāk – e - pakalpojums);

2.2. datu glabāšanas un parakstu pārbaudes sistēmas;

2.3. integrācijas saskarnes savākto parakstu saņemšanai no portāla un citām tiešsaistes sistēmām;

2.4. publiskas tīmekļa saskarnes ar informāciju par aktuālajām parakstu vākšanas iniciatīvām.

3. Parakstu vākšanu var organizēt, izmantojot privātpersonas parakstu vākšanas tiešsaistes sistēmu (turpmāk – privātpersonas parakstu vākšanas tiešsaistes sistēma), ja Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (turpmāk - sertificējošā institūcija) ir izsniegusi atbilstības sertifikātu, kas apliecina, ka privātpersonas parakstu vākšanas tiešsaistes sistēma atbilst šo noteikumu drošības un tehnisko parametru prasībām.

4. Persona, kas organizē un vada portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmas darbību, ir atbildīga par tās korektu izveidi, ieviešanu, uzturēšanu, izmantošanu, izmaiņu veikšanu un likvidēšanu atbilstoši šo noteikumu prasībām.

5. Šo noteikumu prasības neattiecas uz iekārtām, kuras fiziska persona izmanto parakstu iesniegšanai.

6. Informāciju par portāla elektroniski identificētu fizisko personu, kura parakstīšanās dienā atbilst likuma „Par tautas nobalsošanu, likuma ierosināšanu un Eiropas pilsoņu iniciatīvu” prasībām (turpmāk – vēlēšanu tiesības), portāla parakstu vākšanas tiešsaistes sistēmai no Iedzīvotāju reģistra sniedz Pilsonības un migrācijas lietu pārvalde, izmantojot tīmekļa pakalpi. Pilsonības un migrācijas lietu pārvalde ir tīmekļa pakalpes pārzinis un turētājs.

7. Aģentūra un Komisija sadarbojas ar Pilsonības un migrācijas lietu pārvaldi par tīmekļa pakalpes izmantošanu saskaņā ar šiem noteikumiem un Aģentūras apstiprinātajām vadlīnijām par Valsts informāciju sistēmu savietotāja izmantošanu, neslēdzot savstarpēju vienošanos.

**II Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmu drošības organizatoriskās prasības**

8. Portāla parakstu vākšanas tiešsaistes sistēma atbilst informācijas sistēmu vispārējās drošības normatīvo aktu prasībām un šo noteikumu prasībām.

9. Aģentūra ikgadējā Valsts informācijas sistēmas drošības audita ietvaros veic portāla parakstu vākšanas tiešsaistes sistēmas auditu atbilstoši šo noteikumu prasībām.

10. Prasības privātpersonas parakstu vākšanas tiešsaistes sistēmas darbībai:

10.1. nodrošina datu apstrādi atbilstoši fizisko personu datu aizsardzības normatīvo aktu prasībām;

10.2. nodrošina informācijas sistēmu drošības un organizatorisko pārvaldību saskaņā ar Latvijas nacionālo standartu LVS:ISO/IEC 27001:2014L „Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības”;

10.3. nodrošina vismaz šādu dokumentu sagatavošanu un apstiprināšanu:

10.3.1. risku novērtējums un akceptēto risku saraksts,

10.3.2. informācijas sistēmu drošības politika un noteikumi;

10.4. nodrošina organizatoriskos līdzekļus, lai saņemtu informāciju par jauniem draudiem un drošības uzlabojumiem, kā arī aprakstu (procedūru) par šādas informācijas saņemšanu;

10.5. saskaņā ar šo noteikumu 10.3.1.apakšpunktā minēto risku novērtējumu, veic drošības kontroles vismaz šādās jomās:

10.5.1. riska novērtējumos,

10.5.2. fiziska un vides drošībā,

10.5.4. cilvēkresursu drošībā,

10.5.5. saziņas un operāciju pārvaldībā,

10.5.6. standarta piekļuves kontroļu pārvaldībā,

10.5.7. informācijas sistēmu iegādē, izveidošanā, uzturēšanā un likvidēšanā,

10.5.8. informācijas drošības starpgadījumos un pakalpojumu nepārtrauktības pārvaldībā,

10.5.9. pasākumos, kas labotu un mazinātu ievainojamības informācijas sistēmās, kuru rezultātā varētu notikt apstrādāto datu iznīcināšana, nejauša nozaudēšana, izmainīšana, neatļauta izpaušana vai piekļuve tiem,

10.5.10. normatīvo aktu prasību atbilstībā,

10.5.11. datortīklu drošībā.

11. Lai parakstu vākšanu organizētu elektroniski ar privātpersonas parakstu vākšanas tiešsaistes sistēmas palīdzību, persona, kura minēta šo noteikumu 4. punktā, sertificējošā institūcijā iesniedz iesniegumu par privātpersonas paraksta vākšanas tiešsaistes sistēmas atbilstības sertifikāta saņemšanu, un šādu informāciju, ja tāda pēdējo 12 mēnešu laikā nav iesniegta:

11.1. ziņas par iesniedzēju (juridiskai personai – nosaukumu, reģistrācijas numuru, juridisko adresi, kontakttālruni un e-pasta adresi; fiziskai personai – vārdu, uzvārdu, deklarēto dzīvesvietas adresi, kontakttālruni un e-pasta adresi);

11.2. sistēmas tehnisko specifikāciju, kas vismaz ietver:

11.2.1. datortīkla slēguma shēmu izmantojamajām iekārtām un serveriem,

11.2.2 serveru datu glabāšanas iekārtu un tīkla iekārtu sarakstu, minot modeļu nosaukumus,

11.2.3. izmantojamās programmatūras sarakstu ar versijām,

11.2.4. iekārtu atrašanās vietas adresi,

11.3. sistēmas drošības politiku, drošības un lietošanas noteikumus;

11.4. risku novērtējuma dokumentu, kurā noteikta:

11.4.1. sistēmas darbības joma,

11.4.2. identificēto risku ietekme uz sistēmas darbību, tai skaitā novērtējot risku iestāšanās varbūtību, materiālos un nemateriālos zaudējumus, ietekmi uz sistēmas pieejamību, datu konfidencialitāti,

11.4.3. ja notikuši informācijas sistēmu drošības pārkāpumi, papildus informācijā iekļauj:

11.4.3.1. pretpasākumus, lai novērstu šādus pārkāpumus,

11.4.3.2. aizsardzības līdzekļus, kas tiks izmantoti, ja pārkāpumi atkārtojas,

11.4.3.3. uzskaitītos nenovērstos riskus,

11.4.3.4. nepieciešamos uzlabojumus, kas uzskaitīti prioritārā secībā;

11.5. tiešsaistes sistēmas pirmkodu, kas ietver visu pirmkodu, kas ir radīts vai mainīts veidojot sistēmu vai tās komponentes, piemēram, lietojumus, kas var tikt darbināti uz galaiekārtas;

11.6. iekšējā audita ziņojumu, kas satur privātpersonas parakstu vākšanas tiešsaistes sistēmas atbilstības izvērtējumu un pamatojumu šo noteikumu prasībām;

11.7. šo noteikumu 4.punktā minētās personas apliecinājumu, ka privātpersonas parakstu vākšanas tiešsaistes sistēma atbilst šiem noteikumiem;

11.8. servera vai serveru interneta protokola (turpmāk - IP) adresi vai IP adreses, no kuras privātpersonas parakstu vākšanas tiešsaistes sistēma iesniegs parakstus, izmantojot šo noteikumu 2.3.apakšpunktā minēto tīmekļa saskarni;

11.9. tīmekļa vietnes adresi (domēna vārdu, Domēna nosaukuma sistēmas adresi vai adreses, IP adresi vai IP adreses), kurā tiks vākti paraksti.

12. Sertificējošā institūcija izskata šo noteikumu 11.punktā minēto iesniegumu un pievienoto informāciju, un izsniedz atbilstības sertifikātu vai pieņem lēmumu par atteikumu izsniegt atbilstības sertifikātu Administratīvā procesa likumā noteiktā kārtībā un termiņā.

13. Atbilstības sertifikāta izsniegšanas gadījumā, sertificējošā institūcija informē šo noteikumu 4. punktā minēto personu un nodod informāciju Aģentūrai un Komisijai par izsniegto atbilstības sertifikātu un šo noteikumu 11.8.apakšpunktā minēto IP adresi vai IP adresēm.

14. Aģentūra pēc šo noteikumu 13.punktā minētās informācijas saņemšanas 10 darba dienu laikā privātpersonas parakstu vākšanas tiešsaistes sistēmai piešķir piekļuvi šo noteikumu 2.3. apakšpunktā minētajai tīmekļa saskarnei savākto parakstu iesniegšanai.

15. Sertificējošai institūcijai ir šādas tiesības:

15.1. veikt drošības auditu vai pārbaudi privātpersonas parakstu vākšanas tiešsaistes sistēmai, tai skaitā visam sistēmas dzīves cikla laikā veidotajam vai mainītajam pirmkodam;

15.2. ja drošības audita vai pārbaudes laikā tiek konstatēts, ka privātpersonas parakstu vākšanas tiešsaistes sistēma neatbilst šo noteikumu prasībām, pieņemt lēmumu par atbilstības sertifikātu anulēšanu;

15.3. var pieņemt lēmumu par atbilstības sertifikāta anulēšanu arī bez drošības audita vai pārbaudes, ja tiek konstatēta privātpersonas parakstu vākšanas tiešsaistes sistēmas neatbilstība šo noteikumu prasībām.

16. Šo noteikumu 15.2. un 15.3. minētos lēmumus var pārsūdzēt tiesā Administratīvā procesa likumā noteiktā kārtībā.

17. Šo noteikumu 15.2. vai 15.3.punktā pieņemtā lēmuma gadījumā, sertificējošā institūcija par to informē šo noteikumu 4.punktā minēto personu un Komisiju, kā arī nosūta Aģentūrai pieprasījumu bloķēt piekļuvi šo noteikumu 2.3. apakšpunktā minētajai tīmekļa saskarnei.

18. No šo noteikumu 15.2. vai 15.3.punktā minētā lēmuma pieņemšanas dienas, privātpersonas parakstu vākšanas tiešsaistes sistēmas darbība tiek apturēta un tai tiek bloķēta piekļuve šo noteikumu 2.3. punktā minētai saskarnei.

19. Ja portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmai ir noticis drošības incidents, tad persona, kas minēta šo noteikumu 4.punktā, nekavējoties, bet ne vēlāk kā 24 stundu laikā, par to informē Sertificējošo institūciju.

20. Fizisko personu datu apstrādes mērķis portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmai ir parakstu vākšana konkrētajai iniciatīvai. Fizisko personu datus iznīcina saskaņā ar šo noteikumu 33. punktā minēto.

21. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmas esošo datu, kas ir radušies parakstu vākšanas laikā, kā arī šo noteikumu 56.punktā minētās informācijas glabāšanas laiks nepārsniedz vienu gadu pēc Komisijas lēmuma par parakstu vākšanas rezultātiem pieņemšanas. Šis noteikumu punkts neattiecas uz sistēmas pirmkodu un fizisko personu datiem.

**III Tehniskās prasības portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmām**

22. Atbilstoši Elektroniski dokumentu likumam, portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma parakstu vākšanai izmanto elektroniski parakstītu teksta datni UTF-8 kodējumā, kas satur tādu pašu informāciju kā Komisijas apstiprināta parauga veidlapa.

23. Komisija nodrošina, ka šo noteikumu 22.punktā minētā datne tiek aizsargāta ar fiziskās aizsardzības metodēm.

24. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmas lietotāju saskarne tīmekļa lapā, kurā tiek veikta parakstu vākšana vai lietojumā, kas darbojas uz lietotāja iekārtas, nodrošina iespēju fiziskai personai parakstīties, izmantojot secīgas un vienkārši saprotamas darbības tīmekļa pārlūkā.

25. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma pirms datnes parakstīšanas viegli salasāmā veidā attēlo šo noteikumu 22.punktā minētās datnes saturu un informāciju par datnes parakstītāju.

26. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma nodrošina fiziskai personai šo noteikumu 22.punktā minēto datni parakstīt ar drošu elektronisko parakstu.

27. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma nodrošina aizsardzību pret automatizētu parakstu iesniegšanu.

28. Portāla parakstu vākšanas tiešsaistes sistēma nodrošina personai izvēles iespēju saņemt informāciju par savu dalību parakstu vākšanā, identificējoties savā portāla profilā.

29. Portāla parakstu vākšanas tiešsaistes sistēmā parakstīšanās tiesības tiek piešķirtas portāla elektroniski identificētai fiziskai personai, kura atbilst vēlēšanu tiesībām, pēc personas datu atbilstības pārbaudes Iedzīvotāju reģistrā.

30. Privātpersonas parakstu vākšanas tiešsaistes sistēma var veikt vēlēšanu tiesību pārbaudi tikai par tām fizikām personām, kuras sevi ir identificējušas Privātpersonas parakstu vākšanas tiešsaistes sistēmā, izmantojot Iedzīvotāju reģistra servisu, normatīvajos aktos noteiktajā kārtībā, sedzot Iedzīvotāju reģistra tiešsaistes da­tu pārraides sistēmas tehniskā pieslēguma konfigurēšanas izmaksas saskaņā ar Pilsonības un migrācijas lietu pārvaldes maksas pakalpojumu cenrādi. Vēlēšanu tiesību pārbaudi Iedzīvotāju reģistrā veic bez maksas.

31. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma savākto parakstu iesniegšanai tiešsaistē Komisijai izmanto šo noteikumu 2.3.apakšpunktā minēto tīmekļa saskarni.

32. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma pēc paraksta iesniegšanas šo noteikumu 2.2. apakšpunktā minētajai sistēmai un šo noteikumu 44. punktā minētās pārbaudes veikšanas, fiziskai personai attēlo informāciju par parakstu nosūtīšanas rezultātu.

33. E – pakalpojums un privātpersonas parakstu vākšanas tiešsaistes sistēma nodrošina šo noteikumu 22.punktā minētās parakstītās datnes dzēšanu, nesaglabājot fiziskās personas datus un parakstītās datnes, ja izpildās viens no šādiem nosacījumiem:

33.1. tiklīdz parakstītā datne ir veiksmīgi iesniegta, izmantojot šo noteikumu 2.3 punktā minēto tīmekļa saskarni;

33.2. iesniedzot parakstīto datni, izmantojot šo noteikumu 2.3. punktā minēto tīmekļa saskarni, ir notikusi kļūda, kas neizslēdz iespēju veiksmīgi iesniegt to pašu datni vēlāk, un fiziskā persona nav devusi piekrišanu mēģināt iesniegt datni atkāroti;

33.3. iesniedzot parakstīto datni, izmantojot šo noteikumu 2.3. punktā minēto tīmekļa saskarni, ir notikusi kļūda, kas izslēdz iespēju iesniegt to pašu datni atkārtoti.

34. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma publiski, neveicot fiziskas personas identifikāciju, nodrošina šādas informācijas pieejamību:

34.1. parakstu vākšanas iniciatīvas grupas nosaukumu, adresi, e-pasta adresi un kontakttālruni;

34.2. likumprojekta, Satversmes grozījumu projekta vai Saeimas atsaukšanas ierosinājuma tekstu un parakstu vākšanas termiņu;

34.3. savākto parakstu indikatīvo skaitu par konkrēto iniciatīvu;

34.4. šo noteikumu 4.punktā minētās personas nosaukumu, adresi, e-pasta adresi un kontakttālruni.

35. Portālā publicē un uztur informāciju par visām notikušajām parakstu vākšanām sākot ar 2015.gada 1.janvāri, norādot šo noteikumu 34.1. un 34.2. apakšpunktā minēto informāciju un savākto parakstu skaitu saskaņā ar Komisijas lēmumu par parakstu vākšanas rezultātiem.

36. Portāls nodrošina pārbaudi vai fiziskā persona iepriekš nav parakstījusies konkrētajā parakstu vākšanā.

37. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma nodrošina iespēju saglabāt unikālu vienoto resursu vietrādi (turpmāk - URL) arī uz atsevišķu parakstu vākšanas iniciatīvas vietni, kurā atspoguļota informācija par iniciatīvu un kurā ir iespējams vākt parakstus.

38. Ja vienu parakstu vākšanas tiešsaistes sistēmu izmanto dažādām parakstu vākšanas iniciatīvām, portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmai ir jānodrošina funkcionalitātes un informācijas nodalīšana starp iniciatīvām.

39. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmai ir skaidri nodalītas funkcijas neidentificētai fiziskai personai, elektroniski identificētai fiziskai personai un sistēmas administratoram.

**IV Specifiskās tehniskās prasības datu glabāšanas un parakstu pārbaudes sistēmai**.

40. Datu glabāšanas un parakstu pārbaudes sistēma nodrošina;

40.1. parakstu saņemšanu no portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmas;

40.2. informācijas par fizisku personu, kas parakstījusies klātienē, ievadi;

40.3. šo noteikumu 22.punktā minētās parakstītās datnes un šo noteikumu 45.punktā minētās informācijas glabāšanu;

40.4.fizisko personu parakstu pārbaudi;

40.5. parakstu skaitīšanu un informācijas sniegšanu par parakstu skaitu;

40.6. fizisko personu, kas piedalījušies parakstu vākšanā, reģistrāciju.

41. Datu glabāšanas un parakstu pārbaudes sistēma datu saņemšanai no privātpersonas parakstu vākšanas tiešsaistes sistēmas ievēro šādas prasības:

41.1. nodrošina parakstus saņemšanu tikai no sertificētām sistēmām, kas pieprasījumos norāda korektu autentifikācijas informāciju un kas pieslēdzas no šo noteikumu 11.8 apakšpunktā norādītās IP adreses vai IP adresēm;

41.2. parakstu saņemšanai izmanto šo noteikumu 2.3 apakšpunktā minēto tīmekļa saskarni, kas nodrošina ar drošu elektronisko parakstu parakstītas datnes saņemšanu.

42. Aģentūra publicē šo noteikumu 2.3. apakšpunktā minētās tīmekļa saskarnes specifikāciju un pirmkoda piemēru izmantošanai.

43. Šo noteikumu 4.punktā minētā persona noslēdz vienošanos ar Aģentūru par iespēju tai bez atlīdzības izmantot šo noteikumu 2.3. apakšpunktā minēto tīmekļa saskarni testēšanas vajadzībām.

44. Saņemot šo noteikumu 22.punktā minēto datni ar parakstu vai parakstiem, izmantojot šo noteikumu 2.3.apakšpunktā minēto tīmekļa saskarni, datu glabāšanas un parakstu pārbaudes sistēma veic šādas pārbaudes un darbības, un par to rezultātu nodod informāciju portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmai, kas iesniegusi parakstīto datni:

44.1. pārbauda vai fiziska persona iepriekš nav parakstījusies konkrētajā parakstu vākšanā;

44.2. pārbauda vai šo noteikumu 22.punktā minētās saglabātās parakstītās datnes saturs atbilst šo noteikumu 22.punktā minētā teksta datnes saturam;

44.3 vai Komisijas paraksts atbilst šo noteikumu 22.punktā minētajam parakstam un ir derīgs;

44.4. vai fiziskās personas drošs elektroniskais paraksts ir derīgs;

44.5. vai šo noteikumu 22.punktā minētā parakstītā datne ir veiksmīgi saglabāta Datu glabāšanas un parakstu pārbaudes sistēmā.

45. Datu glabāšanas un parakstu pārbaudes sistēma nodrošina iespēju Komisijai un likuma „Par tautas nobalsošanu, likuma ierosināšanu un Eiropas pilsoņu iniciatīvu” 22.panta otrās daļas un daļas un 25.5 panta otrās daļas minētajām institūcijām un personām, ievadīt informāciju par fizisko personu, kas parakstījusies uz Komisijas apstiprināta parauga veidlapām. Zvērināti notāri var neizmantot minēto sistēmu.

46. Informāciju par identificētu fizisko personu, kuras paraksts, saskaņā ar  likuma „Par tautas nobalsošanu, likuma ierosināšanu un Eiropas pilsoņu iniciatīvu”, apliecinājis zvērināts notārs, Komisijai, pēc tās pieprasījuma, elektroniski nodod Latvijas Zvērinātu notāru padome.

47. Lai nodrošinātu informācijas ievadi par fizisko personu šo noteikumu 45. un 46. punktā minētajā gadījumā, Datu glabāšanas un parakstu pārbaudes sistēma nodrošina šādu funkcionalitāti:

47.1. veic pārbaudi vai fiziska persona iepriekš nav parakstījusies konkrētajā parakstu vākšanā;

 47.2. veic personas datu atbilstības pārbaudi Iedzīvotāju reģistrā - vai fiziskai personai ir vēlēšanu tiesības parakstīšanās laikā;

47.3. Komisijai un likuma „Par tautas nobalsošanu, likuma ierosināšanu un Eiropas pilsoņu iniciatīvu” 22.panta otrās daļas un 25.5 panta otrās daļas minētajām institūcijām un personām nodrošināt iespēju apstiprināt fiziskās personas klātienē veikto parakstu. Zvērināti notāri var neizmantot minēto sistēmu.

48. Pēc parakstu vākšanas beigām un pēc Komisijas parakstu pārbaudes no apstiprināta parauga veidlapām, Datu glabāšanas un parakstu pārbaudes sistēma nodrošina uzkrāto parakstu skaitīšanu un derīgo parakstu skaitu apkopojumu.

49. Komisijai veicot parakstu derīguma pārbaudi, Datu glabāšanas un parakstu pārbaudes sistēma, papildus šo noteikumu 44. un 47. punktā veiktajām pārbaudēm, veic visu šo noteikumu 22.punktā minēto saglabāto parakstu datņu un šo noteikumu 45. un 46. punktā minēto ierakstu pārbaudes, nosakot:

49.1. personas datu atbilstības pārbaudi Iedzīvotāju reģistrā - vai fiziskai personai ir vēlēšanu tiesības parakstīšanās laikā;

49.2. vai fiziskā persona iepriekš nav parakstījusies konkrētajā parakstu vākšanā.

50. Datu glabāšanas un parakstu pārbaudes sistēma nodrošina publiski pieejamu šo noteikumu 2.4.punktā minēto saskarni (vismaz JSON formātā), kas par katru parakstu vākšanas iniciatīvu nodrošina vismaz šādas informācijas izsniegšanu:

50.1 Iniciatīvas nosaukums, Iniciatīvas grupas nosaukums, likumprojekta, Satversmes grozījumu projekta vai Saeimas atsaukšanas ierosinājuma tekstu un parakstu vākšanas termiņu,

50.2. parakstu vākšanas laikā savākto parakstu indikatīvo skaitu, kas reģistrēti šo noteikumu 2.2. punktā minētajā sistēmā;

50.3 pēc parakstu saskaitīšanas - kopējais derīgo parakstu skaits pēc to saskaitīšanas.

**V Drošības prasības lietojumiem, kas nodrošina tiešsaistes parakstu vākšanu**

51. Portālu un privātpersonu parakstu vākšanas tiešsaistes sistēmām, ir jābūt aizsargātām pret zināmām ievainojamībām un ļaunprātīgu izmantošanu saskaņā ar labo praksi un tām ir jāatbilst vismaz šādām prasībām:

51.1. nodrošināta aizsardzība pret injekcijas kļūdām (piemēram, SQL injekcija, XML valodas Xpath injekcija, operētājsistēmas komandu injekcija), ar šādām minimālajām prasībām:

51.1.1. pārbaudes veikšana visiem datiem, kas saņemti no ārpuses, tai skaitā fiziskās personas ievadītiem datiem,

51.1.2. ievaddatu pārbaudes veikšana vismaz servera pusē (lietojumā, kas darbojas uz servera),

51.1.3. jebkādu interpretējamu pieprasījumu izmantošanas gadījumā, piemēram SQL teikumi, ievaddatu nodalīšana no komandas vai vaicājuma;

51.2. nodrošināta aizsardzība pret starpvietņu skriptēšanas kļūdām (XSS) ar šādām minimālām prasībām:

51.2.1. pārbaudes veikšana visiem datiem, kas tiek nosūtīti uz pārlūkprogrammu,

51.2.2. nodrošināta visu parādāmo pārlūkprogrammā datu pienācīga kodēšana;

51.3. nodrošināta stipra autentificēšanās un sesiju pārvaldība, ar vismaz šādām minimālām prasībām:

51.3.1. tiek nodrošināts, lai akreditācijas datus nevar uzminēt vai pārrakstīt vāju lietotāja konta pārvaldības funkciju dēļ,

51.3.2. tiek nodrošināts, ka jebkādus sesijas datus, tai skaitā identifikatorus, nedrīkst atklāt URL,

51.3.3. sesijas identifikatorus aizsargāšana pret sesijas fiksācijas uzbrukumiem,

51.3.4. nodrošināta sesiju noilguma funkcionalitāte,

51.3.5. akreditācijas datu un sesiju informācijas nosūtīšanai izmantot tikai transporta slāņa drošību (TLS),

51.3.6. ja administratora saskarnei netiek izmantota divu faktoru autentifikācija, paroļu veidošanai izmanto stipra loģiskā politika;

51.4. piekļuve resursiem ar tiešo atsauci tiek nodrošināta tā, lai pārbaude par tiesībām piekļūt resursam tiek veikta, pirms informācijas nosūtīšanas;

51.5. nodrošināta aizsardzība pret starpvietņu pieprasījumu viltošanas kļūdu (XSRF);

51.6. nodrošināta pienācīgas sistēmas šāda drošības konfigurēšana:

51.6.1. visas izmantojamās programmatūras komponentes ir aktuālas, tai skaitā operētājsistēmas, tīmekļa vai lietotnes serveris, datubāzes pārvaldības sistēma, lietotnes un visas kodu bibliotēkas,

51.6.2. ir atspēkoti vai nav instalēti nevajadzīgas operētājsistēmas, tīmekļa vai lietotnes servera un datubāzes pārvaldības sistēmas pakalpojumi,

51.6.3. ir izveidota kļūdu apstrāde, lai novērstu pārlieku daudz informācijas saturošu ziņojumu noplūdi,

51.6.4. drošības iestādījumi izstrādes ietvaros un bibliotēkās ir konfigurēti saskaņā ar labo praksi, piemēram, atvērtā tīmekļa lietotņu drošības projekta vadlīnijām;

51.7. nodrošina šādu šifrēšanu:

51.7.1. šifrē personas datus, kas tiek saglabāti elektroniskā formātā,

51.7.2. šifrē vai izmanto pienācīgu transporta slāņa aizsardzību (Transport Layer Protection) pārsūtot personas datus elektroniski.

51.7.2. lieto stiprus šifrēšanas algoritmus un stipras atslēgas,

51.7.3. jābūt šifrēšanas atslēgu pārvaldības procedūrai,

51.7.4. saglabājot paroles datubāzē, tās jauc ar stipru standarta jaucējsummas algoritmu un jāpievieno pienācīgu kriptogrāfisko jaucējvērtību “*salt*”,

51.7.5. visas paroles un šifrēšanas atslēgas pienācīgi aizsargā;

51.8. saitēm (URL) ir nodrošināta piekļuves kontrole, kas pārbauda tiesības piekļūt resursam to atverot;

51.9. tiek izmantota pietiekama transporta slāņa aizsardzība (Transport Layer Protection) ar šādām minimālām prasībām:

51.9.1. piekļuvei sistēmai izmanto aktuāla hiperteksta drošas pārsūtīšanas protokola (HTTPS) versiju, izmantojot spēkā esošus sertifikātus, kuru termiņš nav beidzies, tie nav atsaukti un ir atbilstoši domēnam, kurā tos izmanto,

51.9.2. izmanto tikai tādus šifrēšanas algoritmus, kas atbilst labai praksei;

51.10. nodrošināta aizsardzība pret neatļautu novirzīšanu vai pārvirzīšanu.

52. Ja privātpersonas parakstu vākšanas tiešsaistes sistēma, izmanto kopīgu aparatūru, operētājsistēmu vai datubāzes pārvaldības sistēmu ar citām sistēmām, to atspoguļo risku novērtējumā un īstenotajos risku novēršanas pretpasākumos.

53. Portālu un privātpersonas parakstu vākšanas tiešsaistes sistēmai administrēšanas un pārvaldības piekļuves funkcionalitātei nodrošina piekļuvi tikai tām personām, kurām sistēmā esošā informācija atbilstošā apjomā ir nepieciešama darba pienākumu veikšanai administrēšanas tehnoloģiskā procesa nodrošināšanai.

54. Personas, kura apkalpo sistēmu, darba līgumā vai amata aprakstā iekļauj nosacījumus par konfidencialitātes prasību ievērošanu attiecībā uz datiem, kuri nonāk šīs personas rīcībā, veicot darba pienākumus. Ja sistēmu apkalpo trešā persona (piemēram, komersants vai pašnodarbināta persona), konfidencialitātes prasības nosaka dokumentā, ar kuru nodibina tiesiskās attiecības.

55. Datu dublikātus (rezerves kopijas) aizsargā, izmantojot stipru šifrēšanas algoritmu un atslēgas.

56. Informācijas sistēmu audita žurnālos reģistrē izņēmumus un citus ar drošību saistīti notikumus. Sistēmu administratoriem ir pienākums regulāri pārbaudīt sistēmu audita žurnālus attiecībā uz aizdomīgu darbību. Minimālā informācija, ko saglabā sistēmu audita žurnālos ir:

56.1. datums un laiks, kad sistēmas administratori veic pieslēgšanos vai atslēgšanos;

56.2. datums un laiks, kad ir veikta datu dublēšana (datu rezerves kopēšana);

56.3. datums un laiks, kad ir veiktas izmaiņas sistēmā vai programmatūras atjaunināšana.

**VI Drošības prasības informācijas sistēmu infrastruktūrai, kas nodrošina tiešsaistes parakstu vākšanu**

57. Neatkarīgi no tā, kur ir izmitināta portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma un kas nodrošina izmitināšanu, parakstu vākšanas tiešsaistes sistēma pienācīgi aizsargā vismaz ar šādām prasībām:

57.1. izmitināšanas telpām nodrošināta piekļuves kontrole un visi apmeklējumi tiek reģistrēti audita žurnālā;

57.2. nodrošina dublējamo datu aizsargāšanu pret zādzību vai nejaušu novietošanu nevietā;

57.3. nodrošina servera vai serveru novietošanu drošā statnē.

58. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmu izmitina uz servera vai serveriem, kuri fiziski atrodas Latvijas teritorijā, un kas ir savienoti ar internetu un nodalīti ar ugunsmūri aizsargātā „demilitarizētā zonā”.

59. Ugunsmūra programmatūras versijai ir jābūt aktuālai.

60. Ugunsmūrim ir jāpārbauda un jāreģistrē visa saņemto un nosūtāmo datu plūsma no „demilitarizētās zonas”. Ugunsmūris atļauj piekļuvi tikai tādām datu plūsmām, kas nepieciešamas sistēmas darbībai vai administrēšanai.

61. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēma atrodas pienācīgi aizsargātā tīkla segmentā, kas ir nodalīts no testēšanas un izstrādes sistēmām.

62. Lokālā tīkla segmentā, kur atrodas sistēma, piemēro šādus aizsardzības mehānismus:

62.1. nodrošina pārmijportu piekļuves sarakstu komutatorā, kur katram tā pārmijportam tiek piekārtots saraksts ar iekārtu aparatūras adresēm, kuras var pārmijportu izmantot, vai pārmijportu drošību, kas ir tīkla komutatoru konfigurācija, kas neļauj pievienot komutatora pārmijportiem neautorizētas iekārtas;

62.2. atspēko neizmantotos pārmijportus;

62.3. nodrošināt demilitarizētās zonas atrašanos nodalītā lokālā tīklā vai nodalītā virtuālā lokālā tīklā;

62.4. nodrošināt, ka nevajadzīgos pārmijportos nav iespējama piekļuve virtuālajiem lokālajiem tīkliem (IEEE 802.1Q - VLAN).

63. Portāla un privātpersonas parakstu vākšanas tiešsaistes sistēmai nodrošina šādu servera un operētājsistēmas aizsargāšanu:

63.1. nodrošināt atbilstošu drošības konfigurāciju, ieskaitot elementus, kas uzskaitīti šo noteikumu 51.6. apakšpunktā;

63.2. nodrošināt lietotnes darbošanos, izmantojot viszemāko privilēģiju komplektu, kas tām ir nepieciešams, lai darbotos;

63.3. sistēmu administratoru piekļuvei nodrošināt parakstu vākšanas sistēmām sesijas noildzi, nepārsniedzot 15 minūtes;

63.4. pēc attiecīgo operētājsistēmas un izmantojamo lietotņu jauninājumu, ielāpu un pretvīrusu programmatūras atjauninājumu publicēšanas, nekavējoties uzsākt to uzstādīšanu.

**VII. Noslēguma jautājumi**

64. Noteikumi stājas spēkā 2015.gada 1.janvārī.

Ministru prezidente L.Straujuma

Vides aizsardzības un

reģionālās attīstības ministrs R. Naudiņš

Iesniedzējs:

Vides aizsardzības un

reģionālās attīstības ministrs R. Naudiņš

Vīza:

valsts sekretārs G. Puķītis

14.07.2014

3484

K.Jansons

kaspars.jansons@varam.gov.lv

66016567