**Informatīvais ziņojums**

**“Par atbildīgās iestādes noteikšanu dalībai Eiropas Kiberdrošības sertifikācijas grupā ”**

# 1.   Ievads

Informatīvais ziņojums “Par atbildīgās iestādes noteikšanu dalībai Eiropas Kiberdrošības sertifikācijas grupā” (turpmāk – ziņojums) sagatavots, ņemot vērā Eiropas Komisijas (turpmāk – EK) 2019. gada 9. jūlija vēstuli Nr. (2019)4374176 ar lūgumu līdz 2019. gada 5. septembrim iesniegt EK informāciju par nacionālo pārstāvi Eiropas Kiberdrošības sertifikācijas grupā (turpmāk – ECCG).

2019. gada 27. jūnijā spēkā stājās Eiropas Parlamenta un Padomes Regula (ES) 2019/881 par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju (turpmāk – regula).

Regulas mērķis ir noteikt 1) ENISA (Eiropas Savienības Kiberdrošības aģentūras) mērķus, uzdevumus un organizatoriskos aspektus un 2) satvaru, kurā jāizveido Eiropas kiberdrošības sertifikācijas shēmas, lai Eiropas Savienībā (turpmāk – ES) informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) produktiem, pakalpojumiem un procesiem nodrošinātu pietiekami augstu kiberdrošības līmeni. Regula paredz arī ECCG izveidi.

Ziņojuma mērķis ir informēt par ECCG un identificēt atbildīgo iestādi, kas nodrošinās nacionālo interešu pārstāvību šajā grupā.

# 2.   Eiropas Kiberdrošības sertifikācijas grupa (ECCG)

Regula paredz izveidot pirmo ES mēroga kiberdrošības sertifikācijas shēmu, kas kalpotu kā apliecinājums sertificēto produktu, procesu un pakalpojumu kiberdrošībai.

Kiberdrošības sertifikācija ir nepieciešama, lai vairotu uzticēšanos produktiem, pakalpojumiem un procesiem, kā arī stiprinātu to drošību, – tas ir nozīmīgs priekšnosacījums digitālā vienotā tirgus pienācīgai darbībai. Sertifikācijas shēmā paredzētas noteiktas prasības, pēc kuru izpildes IKT produkts, pakalpojums vai process atkarībā no tā atbilstības līmeņa varēs saņemt Eiropas kiberdrošības sertifikātu vai ES atbilstības apliecinājumu.

Dalībvalstīm regulā izvirzīti vairāki uzdevumi kiberdrošības sertifikācijas shēmu ieviešanai, kas ietver arī valstu kiberdrošības sertifikācijas iestāžu noteikšanu un atbilstības pārbaužu veikšanu. Lai konsekventi piemērotu Eiropas kiberdrošības sertifikācijas satvaru, regulas 62. pants paredz izveidot ECCG, ko veido valstu kiberdrošības sertifikācijas iestāžu vai citu attiecīgo valsts iestāžu pārstāvji. Dalībvalstis var arī deleģēt citai dalībvalstij savu pārstāvību ECCG. Saskaņā ar regulas 62. panta 4. punktu ECCG uzdevumi ir šādi:

1. dot padomus un palīdzēt EK tās darbā, lai konsekventi īstenotu un piemērotu kiberdrošības sertifikāciju, īpaši attiecībā uz ES mainīgo darba programmu, kiberdrošības sertifikācijas politikas jautājumiem, politiskās pieejas koordināciju un Eiropas kiberdrošības sertifikācijas shēmu izveidi;
2. palīdzēt, dot padomus Eiropas Savienības Kiberdrošības aģentūrai (turpmāk – ENISA) un sadarboties ar to saistībā ar kandidātshēmas izveidošanu;
3. pieņemt atzinumu par ENISA izveidotajām kandidātshēmām;
4. pieprasīt ENISA izveidot kandidātshēmas;
5. pieņemt EK adresētus atzinumus par esošo Eiropas kiberdrošības sertifikācijas shēmu uzturēšanu un pārskatīšanu;
6. izvērtēt attiecīgās attīstības tendences kiberdrošības sertifikācijas jomā un īstenot informācijas un labas prakses apmaiņu kiberdrošības sertifikācijas shēmu jautājumos;
7. sekmēt valstu kiberdrošības sertifikācijas iestāžu sadarbību, izmantojot spēju veidošanu un informācijas apmaiņu, jo īpaši – ieviešot efektīvas informācijas apmaiņas metodes kiberdrošības sertifikācijas aspektos;
8. atbalstīt salīdzinošās izvērtēšanas mehānismu īstenošanu saskaņā ar Eiropas kiberdrošības sertifikācijas shēmā paredzētajiem noteikumiem;
9. veicināt Eiropas kiberdrošības sertifikācijas shēmu saskaņošanu ar starptautiski atzītiem standartiem, to starpā pārskatot esošās Eiropas kiberdrošības sertifikācijas shēmas un attiecīgajā gadījumā iesakot ENISA sadarboties ar attiecīgajām starptautiskajām standartizācijas organizācijām, lai novērstu trūkumus vai nepilnības pieejamajos starptautiski atzītajos standartos.

Paredzēts, ka ieinteresētās personas un attiecīgās trešās personas varēs uzaicināt apmeklēt ECCG sanāksmes un piedalīties tās darbā.

Eiropas Komisija ar ENISA palīdzību nodrošinās ECCG darbību.

# 3.  Situācijas raksturojums

#

Regulas sadaļa par kiberdrošības sertifikācijas satvaru aptver divas jomas – kiberdrošība un sertifikācija. Saskaņā ar regulas 62. panta 2. punktu par ECCG pārstāvi valsts nominē valstu kiberdrošības sertifikācijas iestāžu vai citu attiecīgo valsts iestāžu pārstāvjus. EK 2019. gada 9. jūlija vēstulē Nr. (2019)4374176 norādīts, ka tiek sagaidīts, ka deleģētie pārstāvji ir speciālisti kiberdrošības sertifikācijas jomā.

Izvērtējot faktisko situāciju, ir secināms, ka šobrīd Latvijā nav:

1) valsts kiberdrošības sertifikācijas iestādes;

2) vienas atsevišķas iestādes, kura būtu kompetenta gan sertifikācijas, gan kiberdrošības jautājumos.

Atbildība par kiberdrošības un sertifikācijas jautājumiem ir sadalīta starp vairākām iestādēm. Saskaņā ar Ministru kabineta 2003. gada 29. aprīļa noteikumu Nr. 236 “Aizsardzības ministrijas nolikums” 5.15.1 apakšpunktu AM uzdevums ir koordinēt informācijas tehnoloģiju drošības politikas veidošanu un īstenošanu.

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (turpmāk – CERT.LV) novēro un analizē kibertelpā notiekošo, reaģē uz informācijas tehnoloģiju drošības incidentiem un koordinē to novēršanu, veic pētniecisko darbu, kā arī organizē izglītojošus pasākumus un apmācības. Tā veic arī citus Informācijas tehnoloģiju drošības likumā noteiktos pienākumus un ir Latvijas Universitātes Matemātikas un informātikas institūta (turpmāk – LU MII) struktūrvienība.

 Savukārt Ekonomikas ministrijas (turpmāk – EM) uzdevumos ir izstrādāt politiku standartizācijas, akreditācijas un metroloģijas jomā, kā arī koordinēt nacionālo standartizācijas, akreditācijas, metroloģijas un tirgus uzraudzības sistēmu (Ministru kabineta 2010. gada 23. marta noteikumu Nr. 271 “Ekonomikas ministrijas nolikums” 5.6. apakšpunkts). Saskaņā ar Ministru kabineta 2018. gada 27. februāra noteikumu Nr. 111 “Valts aģentūras “Latvijas Nacionālais akreditācijas birojs” nolikums” 3. punktu Latvijas Nacionālais akreditācijas birojs (turpmāk – LATAK) savā darbībā īsteno nacionālās akreditācijas institūcijas funkcijas. LATAK ir EM pārraudzībā.

Balstoties uz EM uzticētajām funkcijām, kā arī kompetenci atbilstības novērtēšanas un sertificēšanas jautājumos, AM ierosina uz ECCG sēdēm, kas skar sertifikāciju, piesaistīt ekspertus no EM.

Ņemot vērā CERT.LV uzticētās funkcijas un kompetenci informācijas tehnoloģiju drošības apdraudējumos, AM ierosina uz ECCG sēdēm, kas skar informācijas tehnoloģiju drošības apdraudējumus, piesaistīt ekspertus no CERT.LV.

**4.  Piedāvātais risinājums**

Saskaņā ar regulas 62. panta 2. punktu par ECCG pārstāvi valsts nominē valstu kiberdrošības sertifikācijas iestāžu vai citu attiecīgo valsts iestāžu pārstāvjus. ECCG galvenais uzdevums ir dot padomus un palīdzēt EK tās darbā, lai konsekventi īstenotu un piemērotu Eiropas kiberdrošības sertifikācijas satvaru, kā arī palīdzēt ENISA un cieši sadarboties ar to kiberdrošības sertifikācijas kandidātshēmu izveidē.

Latvijā kiberdrošības sertifikācijas jomā nav valsts kiberdrošības sertifikācijas iestādes un atbildība par kiberdrošības un sertifikācijas jautājumiem ir sadalīta starp vairākām iestādēm. Lai Latvija veiksmīgi iesaistītos Eiropas kiberdrošības sertifikācijas satvara veidošanā, nepieciešams izvēlēties iestādi, kura spētu nodrošināt Latvijas pārstāvību ECCG un koordinēt kiberdrošības sertifikācijas jautājumus starp kompetentajām iestādēm.

Tā kā AM kompetence ietver kiberdrošības jautājumus un AM spēj nodrošināt pastāvīgu pārstāvību ECCG sēdēs, jānosaka, ka AM deleģē pārstāvi darbam ECCG, kā arī koordinē kiberdrošības sertifikācijas jautājumus starp kompetentajām iestādēm. Vienlaikus, tā kā EM pārziņā ir atbilstības novērtēšana un sertifikācija un CERT.LV ir atbildīgs par informācijas tehnoloģiju drošības apdraudējumu novērošanu, EM un CERT.LV jānodrošina ekspertīze savas kompetences jautājumos un jāpiedalās ECCG sēdēs, ja nepieciešams. Informācijas tehnoloģiju drošības likuma 4. panta otrā daļa nosaka, ka LU MII ir AM pakļautībā, tādēļ atsevišķs lēmums par atbalsta sniegšanu AM nav nepieciešams.

Ministru prezidenta biedrs, aizsardzības ministrs Artis Pabriks

Z. Jēkabsone, 67335352

zane.jekabsone@mod.gov.lv