*Projekts*

LATVIJAS REPUBLIKAS MINISTRU KABINETS

2018. gada Noteikumi Nr.

Rīgā (prot. Nr. . §)

**Noteikumi par drošības incidenta būtiskuma kritērijiem, informēšanas kārtību un ziņojuma saturu**

Izdoti saskaņā ar

Informācijas tehnoloģiju drošības likuma

6. panta septīto daļu

1. Noteikumi nosaka informācijas tehnoloģiju drošības incidenta (turpmāk – drošības incidents) būtiskuma kritērijus, informēšanas kārtību un ziņojuma saturu.

2. Drošības incidentam ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību, ja tas:

2.1. ilgst vairāk nekā 24 stundas, neatkarīgi no skarto lietotāju skaita;

2.2. skar no 1% līdz 10% (ieskaitot) pamatpakalpojuma lietotājus un ilgst vismaz 4 stundas;

2.3. skar no 10% līdz 15% (ieskaitot) pamatpakalpojuma lietotājus un ilgst vismaz 2 stundas;

2.4. skar vairāk nekā 15% pamatpakalpojuma lietotājus un ilgst vismaz 1 stundu;

2.5. skar vismaz vienu pamatpakalpojuma lietotāju, kurš ir lielo uzņēmumu sarakstā;

2.6. skar vairāk nekā ¼ daļu no pamatpakalpojuma lietotājiem kādā no Latvijas plānošanas reģioniem;

2.7. skar pamatpakalpojuma lietotājus vismaz vēl vienā citā Eiropas Savienības dalībvalstī un ilgst vismaz divas stundas.

3. Drošības incidentam ir būtiska ietekme uz digitālā pakalpojuma sniegšanu, ja tas ilgst vairāk nekā divas stundas.

4. Pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs četru stundu laikā pēc tam, kad konstatēts drošības incidents, kas būtiski ietekmējis pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu, vai, tiklīdz tas kļuvis iespējams, elektroniski iesniedz kompetentajai Drošības incidentu novēršanas institūcijai sākotnējo ziņojumu, kurā norādīta pieteicēja kontaktinformācija (vārds un uzvārds, ieņemamais amats, elektroniskā pasta adrese un telefona numurs) un visa tam pieejamā informācija par konstatēto drošības incidentu, tajā skaitā:

4.1. drošības incidenta konstatēšanas laiks un ilgums;

4.2. pakalpojums, kuru drošības incidents ir skāris;

4.3. drošības incidenta apraksts;

4.4. procentuālais vai skaitliskais skarto lietotāju skaits, ko skāris drošības incidents;

4.5. veiktās darbības saistībā ar drošības incidenta novēršanu;

4.6. drošības incidenta skartās Eiropas Savienības dalībvalstis;

4.7. plānotais drošības incidenta novēršanas laiks;

4.8. nepieciešamais atbalsta apjoms no kompetentās Drošības incidentu novēršanas institūcijas;

4.9. cita informācija, kas attiecas uz drošības incidentu.

5. Ja pamatpakalpojuma sniedzējs ir atkarīgs no digitālā pakalpojuma sniedzēja, kuru ir skāris šo noteikumu 3. punktā minētais drošības incidents, tas papildus šo noteikumu 4. punktā minētajai informācijai norāda informāciju par digitālā pakalpojuma sniedzēju.

6. Kompetentā Drošības incidentu novēršanas institūcija, saņemot šo noteikumu 4. punktā minēto sākotnējo ziņojumu, reģistrē to un elektroniski vai telefoniski informē pamatpakalpojuma sniedzēju vai digitālā pakalpojuma sniedzēju par sākotnējā ziņojuma saņemšanu.

7. Pamatpakalpojuma sniedzējs un digitālā pakalpojuma sniedzējs līdz šo noteikumu 8. punktā minētā gala ziņojuma iesniegšanai informē kompetento Drošības incidentu novēršanas institūciju par izmaiņām informācijā, kas norādīta šo noteikumu 4. punktā minētajā sākotnējā ziņojumā.

8. Pamatpakalpojuma sniedzējs un digitālā pakalpojuma sniedzējs 10 darba dienu laikā pēc drošības incidenta, kas būtiski ietekmējis pamatpakalpojuma nepārtrauktību vai digitālā pakalpojuma sniegšanu, novēršanas elektroniski iesniedz kompetentajai Drošības incidentu novēršanas institūcijai gala ziņojumu, kurā norādīts:

8.1. pakalpojums, kuru drošības incidents ir skāris;

8.2. drošības incidenta apraksts;

8.3. drošības incidenta novēršanas ilgums;

8.4. procentuālais vai skaitliskais skarto lietotāju skaits, ko skāris drošības incidents;

8.5. drošības incidenta radīto apzināto zaudējumu apmērs. Ja nav iespējams noteikt precīzu zaudējuma apmēru, novērtē zaudējumu kopumā;

8.6 drošības incidenta iespējamā izcelsme un iemesls;

8.7. drošības incidenta skartās Eiropas Savienības dalībvalstis;

8.8. cita informācija, kas attiecas uz drošības incidentu.

9. Šo noteikumu 4. un 8. punktā minētos ziņojumus pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs elektroniski nosūta uz kompetentās Drošības incidentu novēršanas institūcijas elektronisko pasta adresi [cert@cert.lv](mailto:cert@cert.lv) (Latvijas Universitātes Matemātikas un informātikas institūts) un [info@milcert.mil.lv](mailto:info@milcert.mil.lv) (Militārās izlūkošanas un drošības dienests). Gadījumā, ja interneta pieslēgums nav pieejams, pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs šo noteikumu 4. punktā minēto informāciju kompetentajai Drošības incidentu novēršanas institūcijai sniedz pa tālruni 67085888 (Latvijas Universitātes Matemātikas un informātikas institūts) vai 25404404 (Militārās izlūkošanas un drošības dienests).

**Informatīva atsauce uz Eiropas Savienības direktīvām**

Noteikumos iekļautas tiesību normas, kas izriet no Eiropas Parlamenta un Padomes 2016. gada 6. jūlija direktīvas (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

Ministru prezidents Māris Kučinskis

Aizsardzības ministrs Raimonds Bergmanis