EHDOTUS

Slovenian tasavallan viestintäverkoista ja -palveluista vastaava virasto säätää sähköisestä viestinnästä annetun lain (Slovenian virallinen lehti nro 130/22 ja 18/23 – ZDU-1O) 116 §:n 6 momentin nojalla seuraavaa ottaen huomioon teknisiä määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä 9 päivänä syyskuuta 2015 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/1535 (EUVL L 241, 17.9.2015, s. 1) mukaisen tiedotusmenettelyn:

YLEINEN LAKI
turvallisuutta koskevista lisävaatimuksista ja rajoituksista

1 §
(Yleisen lain sisältö)

Tässä yleisessä laissa säädetään

1. ohjeista, joita sellaisten matkaviestinverkkojen operaattoreiden, jäljempänä ’operaattorit’, jotka tarjoavat kyseisiä verkkoja kriittisille toimijoille ja jotka hallinnoivat kriittistä infrastruktuuria kriittisen infrastruktuurin sääntelyn muilla aloilla kriittisen infrastruktuurin alasta annetun lain määritelmän mukaisesti, jäljempänä ’kriittisen infrastruktuurin hallinnoijat’; tietoturvallisuudesta annetussa laissa määriteltyjen keskeisten palvelujen tarjoajien, jäljempänä ’keskeisten palvelujen tarjoajat’; tietoturvallisuudesta annetussa laissa määritettyjen valtionhallinnon elinten, jäljempänä ’valtionhallinnon elimet’; ja valtion turvallisuusjärjestelmän keskeisten osien toimijoiden on noudatettava; ja
2. verkon ja siihen liittyvien tietojärjestelmien kriittisistä elementeistä ja niiden toiminnoista, joita tarkoitetaan sähköisestä viestinnästä annetun lain (Slovenian virallinen lehti nro 130/22 ja 18/23 – ZDU-1O), jäljempänä ’laki’, sellaisena kuin se on liitteessä, joka on tämän yleisen lain erottamaton osa ja joka on laadittu yhteistyössä tietoturvasta vastaavan elimen kanssa, 116 §:n 6 momentissa.

2 §
(Määritelmät)

(1) Tässä yleisessä laissa käytetyillä käsitteillä tarkoitetaan seuraavaa:

1. ’Toimitusketju’ on koko järjestelmä, joka koostuu niistä menettelyistä, ihmisistä, organisaatiosta ja jakelusta, jotka ovat osallisia operaattorin verkossa tai operaattorille kyseisenlaisia palveluita toimittavan pilvipalvelun tarjoajan pilveen asennettujen kriittisten verkkoelementtien osien suunnittelussa, tuotannossa, varastoinnissa, jakelussa ja toimittamisessa sekä asentamisessa ja ylläpitämisessä.

2. ’Verkon kriittisiä elementtejä’ ovat fyysisessä, ohjelmisto- tai virtuaalisessa muodossa olevat verkkoelementit, toiminnot, palvelut ja niitä tukevat tietojärjestelmät operaattorin tai pilvipalvelun tarjoajan palvelussa, sellaisina kuin ne on lueteltu tämän yleisen lain liitteessä.

3. ’Kriittiset toimijat’ ovat kriittisen infrastruktuurin hallinnoijia kriittisen infrastruktuurin sääntelyn muilla aloilla, jotka määritellään kriittisen infrastruktuurin alasta annetun lain mukaisesti, sekä keskeisten palvelujen tarjoajia, jotka määritellään tietoturvasta annetussa laissa, valtionhallinnon elimet, jotka määritellään tietoturvasta annetussa laissa, sekä valtion turvallisuusjärjestelmän keskeisten osien toimijat.

(2) Muilla tässä yleisessä laissa käytetyillä käsitteillä on sama merkitys kuin laissa sekä verkkojen, palvelujen ja tietojen turvallisuudesta annetussa yleisessä laissa.

3 §
(Yleiset ohjeet)

(1) Operaattoreiden kriittisten verkkoelementtien osien toimitusketjussa ja näitä osia koskevissa kolmannen tason tukipalveluissa on otettava huomioon vähintään seuraavat ohjeet kyseisten osien koko elinkaaren ajan:

1. yksittäisen valmistajan tai toimittajan ja kolmannen tason tukipalvelujen tarjoajan on niihin liittyvien suhteiden ja niiden kanssa tehtyjen sopimusten vuoksi tehtävä riskinarviointi, joka koskee kolmansien osapuolten luonnollisten henkilöiden tai oikeushenkilöiden, jäljempänä ’kolmannet osapuolet’, toimituksia ja mahdollisia vaikutuksia, yhteensopivuutta muiden valmistajien laitteiden kanssa, tuotteiden laatua ja turvallisuutta sekä mahdollisia kielteisiä vaikutuksia operaattorin palveluiden ja kriittisten toimijoiden toimintaan;
2. turvallisuuden on oltava sisäänrakennettua ja toteutettu jo suunnittelun yhteydessä, ja sopimuksissa on määritettävä määräajat havaittujen haavoittuvuuksien poistamiselle;
3. keskeiset turvaominaisuudet (käytettävyys, luottamuksellisuus, eheys ja aitous) on varmistettava osien käytön koko elinkaaren ajan;
4. turvallisuus ja osien keskeytymätön toimitus on taattava ja tiukkojen turvaominaisuuksien tukeminen on varmistettava kansainvälisesti tunnustettujen standardien (3GPP) ja eurooppalaisten teknisten standardien (ETSI) mukaisesti;
5. tämän momentin 2–4 kohdassa tarkoitettujen ohjeiden on oltava todennettavissa valmistajan tai toimittajan kanssa tehdyissä sopimusasiakirjoissa;
6. kunkin valmistajan tai toimittajan osalta on arvioitava ja otettava huomioon myös laitteiden valmistuksen ja käytön kannalta välttämättömien keskeisten teknologioiden käyttöoikeuksiin liittyvät riskit sekä laitteiden, varaosien tai kolmannen tason tukipalvelujen toimittamiseen liittyvät riskit;
7. käytetyillä osilla ei tule olla ratkaisemattomia tunnettuja kriittisiä tai aktiivisesti hyödynnettyjä haavoittuvuuksia;
8. mikäli teknisesti mahdollista ja taloudellisesti kestävää, yksittäisen valmistajan tai toimittajan käyttämistä on vältettävä, jotta voidaan vähentää riippuvuutta ja parantaa häiriönsietokykyä kriittisten osien haavoittuvuuksien, verkon täydellisen toimintahäiriön tai kriittisten toimijoiden verkkojen ja palvelujen turvallisuuteen kohdistuvan uhan sattuessa, kun tällaisesta vastaisivat kolmannen osapuolen julkis- tai yksityisoikeudelliset luonnolliset henkilöt tai oikeushenkilöt.

(2) Operaattoreiden on noudatettava tieto- ja viestintälaitteita, -järjestelmiä ja -palveluja toimittaessaan täysimääräisesti Euroopan unionin kyberturvallisuusviraston, jäljempänä ’ENISA’, ohjeita ja voimassa olevia Euroopan unionin säädöksiä, jotka koskevat turvallisuutta koskevia perusvaatimuksia hankittaessa turvallisia tieto- ja viestintätekniikan tuotteita ja

palveluja. Virasto julkaisee verkkosivustollaan linkkejä edellä mainittuun alaan liittyviin ajankohtaisiin ENISAn asiakirjoihin ja EU:n säädöksiin ja pitää linkkejä ajan tasalla.

(3) Kriittisten verkkoelementtien osia toimitettaessa tai pilvipalveluja käytettäessä etusijalle on asetettava osien valitseminen niiltä valmistajilta tai toimittajilta tai palveluiden valitseminen niiltä pilvipalvelun tarjoajilta, jotka ovat saaneet sertifioinnin vaatimustenmukaisuuden arviointilaitoksilta, jotka on akkreditoitu ja tarvittaessa valtuutettu Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta 17 päivänä huhtikuuta 2019 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881, jäljempänä ’asetus’, 60 artiklan 3 kohdan nojalla eurooppalaisten kyberturvallisuussertifikaattien myöntämiseksi asetuksen 52 artiklassa tarkoitetulla määritetyllä varmuustasolla.

(4) Edellisen momentin soveltamiseksi operaattorin on tarkastettava asetuksen 55 artiklan mukaisesti ENISAn perustama erityinen verkkosivusto, jonka tarkoituksena on tiedottaa yleisölle eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, eurooppalaisista kyberturvallisuussertifikaateista ja EU-vaatimustenmukaisuusilmoituksista, mukaan lukien tiedot eurooppalaisista kyberturvallisuuden sertifiointijärjestelmistä, jotka eivät ole enää voimassa, tai kumotuista ja umpeutuneista eurooppalaisista kyberturvallisuussertifikaateista ja EU-vaatimustenmukaisuusilmoituksista, sekä tietorekisteri kyberturvallisuustietoja koskevista linkeistä.

4 §
(Riskinarviointi)

(1) Määrittäessään osien valmistajan tai toimittajan ja kolmannen tason palvelujen tarjoajan riskiä verkon kriittisten elementtien osalta operaattori ottaa huomioon seuraavat arvioitavat riskinäkökohdat.

(2) Operaattorin on edellisessä momentissa tarkoitetussa arvioinnissa arvioitava ja otettava huomioon vähintään seuraavat seikat:

1. yleinen laatu (mukaan lukien turvallisuusnäkökohdat) ja luotettavuus;
2. sellaisten avointen standardien ja rajapintojen käyttötaso, joilla estetään riippuvuutta tietyn valmistajan tai toimittajan tuotteista tai toimittajalukkiutumista;
3. tunnustettujen kansainvälisten ja eurooppalaisten teknisten standardien (3GPP, ETSI) ja Euroopan unionin säädösten ja oletusarvoisten turvallisuusasetusten noudattaminen ammatillisten suositusten (matkapuhelinoperaattorien järjestö GSMA Association) mukaisesti;
4. yhteensopivuuden taso kolmannen osapuolen laitteiden ja verkkotoimintojen kanssa;
5. kyky tarjota päivityksiä ja mukautuksia;
6. haavoittuvuuksien hallinnointi, paljastaminen ja ajantasainen menettely päivitysten ja korjausten avulla;
7. seuraavien asiakirjojen saatavuus ja avoimuus:
   - tärkeimmät toiminnot ja tiedot osan turvallisuudesta ja muista ominaisuuksista sekä mahdollisista asetuksista, ja
   - käytetyt ohjelmistot, mukaan lukien avoin lähdekoodi (ohjelmistosisältöluettelo – SBOM);

8. riippuvuuden taso kolmannen tason tukipalveluista laitteiden hallinnoinnissa ja ylläpidossa, jos operaattori ei suorita näitä palveluja yksin työntekijöidensä avustuksella;
9. alustava arviointi sellaisen laitteen tai yksikön vaatimustenmukaisuudesta, jolla Euroopan unionissa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti akkreditoidut elimet tarjoaisivat kolmannen tason tukipalveluja; kyseiset akkreditoidut elimet on julkaistu Euroopan unionin virallisessa lehdessä.

(3) Operaattorin on dokumentoitava riskitekijät ja riskinarvioinnin tulokset kustakin tämän pykälän 2 ja 3 momentissa tarkoitetusta valitusta valmistajasta tai toimittajasta tai kolmannen tason palvelujen tarjoajasta ja päivitettävä tiedot säännöllisesti.

5 §
(Yleiset ohjeet kriittisten verkkoelementtien toiminnasta)

(1) Kriittisten verkkoelementtien osat, niiden toiminta ja oletusasetukset eivät saa sisältää teknisiä ominaisuuksia, jotka voisivat vaikuttaa kielteisesti kriittisten toimijoiden turvallisuuteen tai toimintaan muun muassa sabotaasin, vakoilun, teollis- ja tekijänoikeuksien varastamisen tai terrorismin vuoksi.

(2) Kriittiset verkkoelementit sijaitsevat yleensä Slovenian tasavallassa tai ottaen huomioon kaikki turvallisuusriskit ja varmistaen korkean turvallisuustason Euroopan unionissa, jollei sovellettavista säännöksistä muuta johdu. Operaattorin on ilmoitettava Slovenian viestintäverkoista ja -palveluista vastaavalle virastolle, jäljempänä ’virasto’, ja tietoturvasta vastaavalle elimelle suunnitellusta muutostaan vähintään 30 päivää ennen muuttoa Euroopan unionin ulkopuolelle.

(3) Verkon kriittisiä elementtejä koskevia kolmannen tason tukipalveluja tarjotaan yleensä Slovenian tasavallassa tai ottaen huomioon kaikki turvallisuusriskit ja korkean turvallisuustason varmistamisen Euroopan unionissa, jollei sovellettavista säännöksistä muuta johdu. Operaattorin on ilmoitettava virastolle ja tietoturvasta vastaavalle elimelle kolmannen tason tukipalvelujensa suunnitellusta muutosta vähintään 30 päivää ennen muuttoa Euroopan unionin valtioiden ulkopuolelle.

(4) Kolmannen tason tukipalvelujen toteuttaminen ei saa vaarantaa kriittisten toimijoiden palvelujen turvallisuutta tai toimintaa tai kansallista turvallisuutta.

(5) Operaattorin on määritettävä kriittisten verkkoelementtien tunnistamisen menettely ja käytettävä sitä säännöllisesti. Sitä on käytettävä vähintään kerran vuodessa tai aina, kun hankitaan kriittisten verkkoelementtien osia.

(6) Jos yksittäinen osa edustaa vain osittain kriittistä verkkoelementtiä, sitä on pidettävä osana kriittistä verkkoelementtiä.

(7) Operaattorin on pidettävä ajantasaista luetteloa kaikista kriittisten verkkoelementtien osista, niiden toiminnoista, sijainneista, ylläpitäjistä ja hallinnoijista, niiden kolmannen tason tukipalvelujen tarjoajista ja niiden valmistajista tai toimittajista. Luettelo on asetettava viraston ja tietoturvasta vastaavan elimen saataville pyynnöstä.

6 §
(Kriittisten verkkoelementtien osien toimituksia koskevat turvatoimenpiteet)

(1) Operaattorin on oltava tietoinen koko toimitusketjusta ja siihen liittyvistä riskeistä, mukaan lukien kriittisten verkkoelementtien yksittäisten osien alihankkijat; tähän kuuluvat myös salausavaimet, UICC-/eUICC-kortit ja muut turvatekijät, joiden väärinkäyttö voisi vaarantaa kriittisten toimijoiden turvallisuuden.

(2) Operaattorin on varmistettava, että operaattorin ja kriittisten verkkoelementtien osien valmistajien tai toimittajien tai kolmannen tason tukipalvelujen tarjoajien välisistä turvallisuusvaatimuksista sovitaan ja että ne dokumentoidaan ja että valmistajat tai toimittajat noudattavat sovittuja turvatoimenpiteitä koko toimitusketjussa.

(3) Jotta voidaan estää ajoissa haitallisia toimijoita hyödyntämästä haavoittuvuuksia, operaattorin on varmistettava, että kriittisen verkkoelementin osien valmistaja tai toimittaja sitoutuu sopimusperusteisesti ilmoittamaan välittömästi operaattorille havaitusta haavoittuvuudesta ja toimenpiteistä riskien vähentämiseksi ja neuvomaan suoja- tai korjaustoimenpiteistä, joita operaattori voi toteuttaa uhan torjumiseksi.

(4) Operaattorin on tarkistettava vähintään kerran vuodessa kriittisten verkkoelementtien käyttöoikeuksien riittävyys tai päivitettävä ne viipymättä organisaatiossa tai kolmannen tason tukipalvelujen tarjoajien osalta tapahtuneiden muutosten mukaisesti.

(5) Operaattorin on huolehdittava, että se ei ole riippuvainen yksittäisestä toimittajasta tai kolmannen tason palvelujen tarjoajasta (ns. ’toimittajariippuvuus’), jos se on teknisesti mahdollista ja taloudellisesti kestävää, jotta voidaan vähentää riippuvuutta ja lisätä häiriönsietokykyä kriittisten osien haavoittuvuuksien tapauksessa, myös välttämällä pitkäaikaisia sopimuksia yksittäisten valmistajien tai toimittajien tai kolmannen tason tukipalvelujen tarjoajien kanssa tai varmistamalla mahdollisuuden muuttaa sopimuksia, jotta kriittisille toimijoille tarjottavien palvelujen tarjoamisen häiriöt saataisiin mahdollisimman alhaiselle tasolle.

7 §
(Sopimusehdot valmistajien, toimittajien tai kolmannen tason tukipalvelujen tarjoajien kanssa)

Korkean turvallisuustason varmistamiseksi operaattorin on sisällytettävä uusiin sopimusehtoihin valmistajien, toimittajien tai kolmannen tason tukipalvelujen tarjoajien kanssa vähintään seuraavat seikat:

1. valmistajan tai toimittajan lausunto siitä, että osassa tai sen oletusasetuksissa ei ole dokumentoimattomia takaportteja tai että niillä ei ole kielteisiä vaikutuksia kriittisten toimijoiden toimintaan;
2. valmistajan tai toimittajan tai kolmannen tason palvelujen tarjoajan sitoumus suojata tiedot, joita ne saavat palvelujen tarjoamisen aikana tai joihin ne pääsevät yhteyspalvelun tarjoamisen yhteydessä;
3. valmistajan tai toimittajan tai kolmannen tason palvelujen tarjoajan sitoumus ilmoittaa välittömästi operaattorille, jos viestintätietojen tai liikennetietojen suojaa on rikottu

niin, että se vaikuttaa tai voisi vaikuttaa operaattoriin tai tämän yleisen lain 1 §:n 1 momentissa tarkoitettuihin kriittisiin toimijoihin;

4. valmistajan tai toimittajan tai kolmannen tason palvelujen tarjoajan sitoumus ilmoittaa välittömästi operaattorille kaikista tietoturvapoikkeamista ja haavoittuvuuksista, jotka voisivat vaikuttaa operaattorin verkon, siihen liittyvien palvelujen tai tietojen turvallisuuteen;
5. valmistajan tai toimittajan tai kolmannen tason palvelujen tarjoajan sitoumus noudattaa operaattorin asettamia turvallisuusstandardeja ja -sääntöjä ja toteuttaa asianmukaiset turvatoimenpiteet tietojärjestelmien ja -verkkojen turvallisuuden sekä operaattorin tai kriittisen toimijan tietojen varmistamiseksi;
6. operaattorin mahdollisuus tarkastella kolmannen tason tukipalvelujen tarjoajan käyttämiä ympäristöjä, menettelyjä, turvatoimenpiteitä ja välineitä, kun tarjoaja käyttää operaattorin verkkoa ja tietoja milloin tahansa;
7. valmistajan tai toimittajan tai kolmannen tason tukipalvelujen tarjoajan vastuu vahingosta, joka aiheutuisi kriittisten verkkoelementtien osien tunnistetuista haavoittuvuuksista tai väärinkäytöstä, niiden oletusasetuksista tai sellaisten kolmannen tason tukipalvelujen tarjoamisen yhteydessä, jotka valmistaja tai toimittaja tai kolmannen tason tukipalvelujen tarjoaja on laiminlyönyt tai tarkoituksellisesti toteuttanut;
8. velvollisuus kouluttaa säännöllisesti valmistajan tai toimittajan tai kolmannen tason tukipalvelujen tarjoajan henkilöstöä tietoturva- ja tietojärjestelmien ja -verkkojen alalla.

8 §
(Kriittisiin verkkoelementteihin pääsyä ja niiden käyttöä koskevat säännöt)

(1) Operaattorin on varmistettava fyysisesti tai loogisesti tapahtuvan, kriittisten verkkoelementtien osiin, niiden asetuksiin ja niihin tallennettuihin, käsiteltyihin tai muutettuihin operaattorin tietoihin pääsyn yhteydessä, että

1. pääsyoikeus on annettu vain henkilöille, jotka on valtuutettu tähän aiemmin;
2. operaattori valvoo kaikkia kriittisiin verkkoelementteihin liittyviä toimia, jotka suoritetaan paikan päällä tai etäyhteyden kautta;
3. monivaiheinen tunnistaminen suoritetaan käyttäjille, joille annetaan suurimmat oikeudet kriittisten verkkoelementtien yksittäisiin osiin, niiden asetuksiin tai tallennettuihin tai käsiteltyihin tietoihin pääsyyn;
4. jokaisella valtuutetulla henkilöllä, jolle on myönnetty pääsyoikeus, on yksilöllinen käyttäjätili ja salasana;
5. käytetään ainoastaan salasanoja, jotka vaihdetaan säännöllisesti tai välittömästi havaitun väärinkäytön yhteydessä ja jotka sisältävät vähintään 15 merkkiä ja joissa on suuria ja pieniä kirjaimia, numeroita ja erikoismerkkejä, jos ohjelmisto sen sallii;
6. nollatoleranssin tai luottamuksen käsite otetaan käyttöön pääsyoikeuden osalta mahdollisuuksien mukaan;
7. valtuutetun käyttäjän viestintäyhteyden turvallisuus yksittäisiin osiin on suojattu salauksella ottaen huomioon tekniikan viimeisin kehitys ja parhaat käytännöt tietoturvan alalla tai tietoturvan alalla vakiintuneiden laitosten suositukset;
8. tietoihin pääsy ja pääsy-yritykset tallennetaan vähintään kuuden kuukauden ajaksi muodossa, jota ei voi muokata, mukaan lukien varmuuskopion avulla, mutta ajanjakso voi olla myös pidempi, jos riskinhallinnan analyysin ja hyväksyttävän riskitason arvioinnin mukaan riskejä olisi hallinnoitava asianmukaisesti säilyttämällä tallennettuja tietoja pidempään;

9. kaikkien osien ohjelmistotoiminnot tallennetaan ja niitä seurataan mahdollisuuksien mukaan, mukaan lukien muutokset kokoonpanossa. Rekisteröityjä tietoja, mukaan lukien näiden tietojen varmuuskopiota, on säilytettävä niin kauan kuin edellisessä momentissa on ilmoitettu;
10. pääsy yksittäisiin osiin ja niihin tallennettuihin tai niissä käsiteltyihin tietoihin on määräaikainen ja avoin vain tarvittavan toimen ajaksi.

(2) Jos kolmannen tason tukipalvelujen tarjoajan henkilöstöllä tai työntekijöillä on pääsy kriittisten verkkoelementtien yksittäisiin osiin, niiden on

1. käytettävä vain suojattua erityistä välitason työasemaa (eng. ”jump server”), jolle tehdään säännöllisiä turvallisuustarkastuksia;
2. asennettava erityiselle työasemalle vain sellaisia ehdottoman välttämättömiä työkaluja, osia ja aktiivisia palveluita verkon muiden resurssien käyttämiseksi, jotka on päivitettävä uusimmilla tietoturvakorjauksilla;
3. käytettävä suojattuja salaustoimintoja ja -avaimia erityisellä työasemalla, jonka on oltava operaattorin verkossa ja joka on sen yksinomaisessa valvonnassa;
4. operaattori hyväksyy ja aktivoi jokaisen pääsyn manuaalisesti ja vain pääsylle tarvittavaksi ajaksi;
5. operaattori valvoo pääsyä ja toimia ja rekisteröi kaikki pääsyt ja toimet fyysisesti;
6. käytettävä kaksivaiheista todennusta ja vähintään 15 merkin pituisia salasanoja, jotka sisältävät isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä ja jotka on vaihdettava arvioitujen riskien perusteella.

(3) Ennen kuin operaattori siirtää kriittisten verkkoelementtien tai niiden yksittäisten osien hallinta-, ylläpito- tai päivityspalvelun kolmannelle osapuolelle, sen on tarkistettava ja varmistettava, että tällä on käytössä vähintään samat tai paremmat tietoturvamekanismit ja turvallisuudenhallintamenettelyt kuin operaattorilla. Sen on ilmoitettava siirtoaikomuksestaan välittömästi asianomaiselle kriittiselle toimijalle, virastolle ja tietoturvasta vastaavalle elimelle.

(4) Operaattorin on todennettava turvallisuusmenettelyjen tosiasiallinen tila ennen palvelun tarjoamisen aloittamista ja sen jälkeen vähintään kerran vuodessa. Operaattorin on pidettävä kirjaa kolmansien osapuolten tukipalvelujen tarjoamista koskevista sisäisistä arvioinneista ja valvonnasta ja säilytettävä kirjanpito palvelujen tarjoamisen ajan ja yhden vuoden ajan niiden päättymisen jälkeen, kuitenkin enintään viiden vuoden ajan.

SIIRTYMÄ- JA LOPPUSÄÄNNÖKSET

9 §
(Siirtymäsäännökset)

(1) Operaattorin on ilmoitettava virastolle ja tietoturvasta vastaavalle elimelle kriittisten verkkoelementtien olemassa olevista sijainneista 30 päivän kuluessa tämän yleisen lain voimaantulosta.

(2) Operaattorin on ilmoitettava virastolle ja tietoturvasta vastaavalle elimelle kriittisten verkkoelementtien kolmannen tason tukipalvelujen olemassa olevista sijainneista 30 päivän kuluessa tämän yleisen lain voimaantulosta.

(3) Virasto julkaisee ensimmäisen kerran tämän yleisen lain 3 §:n 2 momentissa tarkoitetut asiakirjat lain voimaantulopäivästä alkaen.

10 §
(Voimaantulo)

Tämä yleinen laki tulee voimaan kolmantenakymmenentenä päivänä sen jälkeen, kun se on julkaistu Slovenian virallisessa lehdessä, ja operaattorit voivat käyttää laitteita ja ylläpitää kolmannen tason tukipalvelujen tarjoamista lain 312 §:n 2 ja 3 momentissa säädettyjen määräaikojen päättymiseen saakka.

Nro _____ maisteri Marko

Mišmaš

Ljubljana, _____ [päivämäärä] johtaja

EVA 2023-3150-0034

EHDOTUS

Liite

Luettelo kriittisistä verkkoelementeistä ja niihin liittyvistä tietojärjestelmistä:

Kriittiset verkkoelementit	**Verkko- ja tietojärjestelmien toiminnot**
Tilaajan hallinta- ja salausmekanismit	- istuntojen hallinta (ääni ja tiedot), - käyttäjien ja laitteiden tunnistaminen verkossa, - tilaajien ja verkko-osien valtuuttamiseen käytettyjen avainten hallinta ja tallentaminen (UICC/eUICC, digitaaliset varmenteet / HSM), - toiminnot turvalliseen tunnistamiseen, viestinnän eheyden suojaamiseen (salaus) ja käyttäjäavainten ja verkko- ja hallintaosien säilyttämiseen, - käyttöoikeuksien hallinnointi
Yhteenliittäminen	- verkkoisännöintitoiminnot ja liitännät muihin verkkoihin ja palveluihin
Hallinnoidut verkkopalvelut	- verkkopalvelujen rekisteröinti ja valtuuttaminen, - viestintä-, sijainti- ja liikennetietojen tallentaminen ja käsittely, - verkon ja verkkotoimintojen altistuminen ulkoisille sovelluksille ja palveluille
Virtuaalisten verkkotoimintojen (NFV) hallinta ja orkestrointi ja verkon orkestrointi (MANO), mukaan lukien virtualisointi-infrastruktuuri	- NFV:n orkestroinnin ja konfiguroinnin hallintatoiminnot toteutustyypistä riippumatta (virtuaalikone, säiliö, mikropalvelut), - NFV:n toteuttamiseen ja käyttöön liittyvät virtualisointitoiminnot, - verkon viipaloinnin valitsemistoiminto (NSSF)
Radioliityntäverkko	- tukiasemat, jotka tukevat vähintään 5G-teknologiaa
Hallintajärjestelmät ja muut tukijärjestelmät	- matkapuhelinverkon toiminnan ja hallinnoinnin seuranta, mukaan lukien liittymäosa (RAN/O-RAN), - järjestelmät turvallisuustapahtumien, poikkeavuuksien, uhkien ja niiden hallinnan havaitsemiseksi (turvallisuustoiminnot, mukaan lukien SIEM/SOAR)
Laillinen telekuuntelu	- toimivaltaisen viranomaisen tehtävät, jotka koskevat pääsyä viestintäsisältöön ja käyttäjäliikennettä koskeviin tietoihin