FORSLAG

I henhold til artikel 116, stk. 6, i lov om elektronisk kommunikation (UL RS nr. 130/22 og 18/23 – ZDU-1O) fastsætter Republikken Sloveniens agentur for kommunikationsnet og -tjenester følgende, under hensyntagen til informationsproceduren i overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1):

GENEREL LOV
om yderligere sikkerhedskrav og -restriktioner

Artikel 1
(Indholdet af den generelle lov)

Ved denne generelle lov fastsættes

1. retningslinjer, der skal følges af operatører af mobilkommunikationsnet (i det følgende benævnt "operatører"), som stiller disse net til rådighed for væsentlige enheder, der forvalter samfundskritisk infrastruktur inden for de øvrige områder af lovgivningen om samfundskritisk infrastruktur (i det følgende benævnt "forvaltere af kritisk infrastruktur"), udbydere af væsentlige tjenester som fastsat i loven om informationssikkerhed (i det følgende benævnt "udbydere af væsentlige tjenester"), statslige forvaltningsorganer som fastsat i lovgivningen om informationssikkerhed (i det følgende benævnt "statslige forvaltningsorganer") eller transportører af centrale dele af det nationale sikkerhedssystem
2. kritiske netkomponenter og tilhørende informationssystemer med den relevante funktionalitet, som omhandlet i artikel 116, stk. 6, i loven om elektronisk kommunikation (UL RS nr. 130/22 og 18/23 — ZDU-1O, i det følgende benævnt "loven") som anført i bilaget, der udgør en integrerende del af denne overordnede retsakt og er udarbejdet i samarbejde med den myndighed, der er ansvarlig for informationssikkerhed.

Artikel 2
(Begrebernes betydning)

(1) De begreber, der anvendes i den generelle lov, skal forstås som følger:

1. En forsyningskæde er hele systemet af processer, mennesker, organisation og distribution, der er involveret i udvikling, produktion, opbevaring, distribution og levering samt installation og vedligeholdelse af komponenter til kritiske netværkselementer, der er installeret i operatørens netværk eller hos den udbyder af cloudtjenester, der leverer disse tjenester til operatøren.

2. Kritiske netkomponenter er de netkomponenter, funktioner, tjenester og supporttjenester i informationssystemer i fysisk, software- eller virtualiseret form, der er placeret hos operatøren eller hos cloudtjenesteudbyderen, jf. listen i bilaget til denne generelle lov.

3. Kritiske enheder er de enheder, der forvalter kritisk infrastruktur inden for de øvrige områder af reguleringen af kritisk infrastruktur, der er fastlagt i overensstemmelse med loven om kritisk infrastruktur, udbydere af væsentlige tjenester som fastlagt i loven om informationssikkerhed, statslige forvaltningsorganer som fastlagt i loven om informationssikkerhed samt transportører af centrale dele af det nationale sikkerhedssystem.

(2) Andre udtryk, der anvendes i denne generelle lov, har den betydning, der er defineret i selve loven samt i den generelle lov om netværks-, tjeneste- og datasikkerhed.

Artikel 3
(Generelle retningslinjer)

(1) Operatører i forsyningskæden for komponenter til kritiske netkomponenter og supporttjenester på tredjepartsniveau for de pågældende komponenter skal som minimum tage hensyn til følgende retningslinjer i hele komponenternes livscyklus:

1. For individuelle producenter eller udbydere og for udbydere af supporttjenester på tredjepartsniveau skal de, i kraft af deres forbindelser og aftaler med disse parter, gennemføre en risikovurdering for såvidt angår levering og de potentielle indvirkninger fra tredjeparts fysiske eller juridiske personer under offentlig eller privat ret (i det følgende benævnt "tredjeparter"), komponenternes kompatibilitet med udstyr fra andre producenter, deres produktkvalitet og produktsikkerhed samt potentielle negative indvirkninger på driften af operatørens tjenester og kritiske enheder.
2. At sikkerhed allerede i designfasen er indbygget og implementeret, og at kontrakterne indeholder tidsfrister for afhjælpning af eventuelle mangler.
3. At de centrale sikkerhedsfunktioner (tilgængelighed, fortrolighed, integritet og autenticitet) er sikret gennem brugstiden i hele deres livscyklus.
4. At sikkerhed og uafbrudt forsyning er garanteret, og at det er bekræftet, at de understøtter avancerede sikkerhedsfunktioner i overensstemmelse med de internationalt anerkendte standarder (3GPP) og de europæiske tekniske standarder (ETSI).
5. At de retningslinjer, der henvises til i punkt 2 til 4 i dette afsnit, kan verificeres i kontraktdokumenterne med producenten eller med leverandøren.
6. At der for hver producent eller leverandør også foretages en vurdering af og tages hensyn til de risici, der er forbundet med brugsrettighederne til de nøgleteknologier, der er nødvendige for fremstilling og brug af udstyret, samt de risici, der er forbundet med levering af udstyr, reservedele eller supporttjenester på tredjepartsniveau.
7. At de anvendte komponenter ikke har uafklarede kendte kritiske eller aktivt udnyttede svagheder.
8. At det er teknisk muligt og økonomisk bæredygtigt at undgå en enkelt producent eller leverandør med det formål at begrænse afhængigheden og øge modstandsdygtigheden i tilfælde af svagheder i kritiske komponenter, katastrofale netværkssvigt eller sikkerhedstrusler mod kritiske enheders net og tjenester fra tredjeparts fysiske eller juridiske enheder, der er underlagt offentlig eller privat lovgivning.

(2) Ved levering af informations- og kommunikationsudstyr, -systemer og -tjenester skal operatørerne fuldt ud overholde retningslinjerne fra Den Europæiske Unions Agentur for

Cybersikkerhed (i det følgende benævnt "ENISA") samt gældende EU-regulering om grundlæggende sikkerhedskrav ved indkøb af sikre IKT-produkter og -tjenester. Agenturet skal på sin hjemmeside offentliggøre links til gældende ENISA-dokumenter og EU-regulering på ovennævnte område og holde disse ajour.

(3) Ved levering af kritiske netkomponenter eller ved brug af cloudtjenester skal det prioriteres at vælge komponenter fra de producenter eller leverandører eller udbydere af cloudtjenester, der er certificeret af overensstemmelsesvurderingsorganer, der er akkrediteret og om nødvendigt godkendt på grundlag af artikel 60, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (i det følgende benævnt "forordningen") med henblik på udstedelse af europæiske cybersikkerhedsattester på et bestemt tillidsniveau som fastsat i forordningens artikel 52.

(4) Med henblik på foregående stykke kontrollerer operatøren et særligt websted, der er oprettet af ENISA i overensstemmelse med forordningens artikel 55, og som har til formål at informere offentligheden om europæiske cybersikkerhedscertificeringsordninger, europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer, herunder oplysninger om europæiske cybersikkerhedscertificeringsordninger, der ikke længere er gyldige eller er tilbagekaldt, samt udløbne europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer og en database med links til information om cybersikkerhed.

Artikel 4
(Risikovurdering)

(1) Når operatøren fastlægger risikoen i forbindelse med producenten eller leverandøren af komponenter og leverandøren af tjenester på tredjepartsniveau for de kritiske netkomponenter, tager operatøren hensyn til og evaluerer nedenstående risikoaspekter.

(2) I den vurdering, der henvises til i foregående afsnit, skal operatøren som minimum vurdere og tage højde for

1. den overordnede kvalitet (herunder sikkerhedsaspekter) og pålidelighed
2. graden af anvendelse af åbne standarder og grænseflader, der hindrer afhængighed og fastlåsning til produkter fra en bestemt producent eller leverandør
3. overholdelsen af de anerkendte internationale og europæiske tekniske standarder (3GPP, ETSI) samt EU's regler og standardsikkerhedsindstillinger i overensstemmelse med anbefalingerne fra fagfolk i branchen (GSMA Association)
4. graden af kompatibilitet med udstyr og netværksfunktioner fra tredjeparter
5. evnen til at levere opgraderinger og brugertilpasninger
6. processen for håndtering af sikkerhedssvagheder, offentliggørelsen af disse samt den løbende proces med opdateringer og fejlrettelser
7. dokumentationens tilgængelighed og gennemsigtighed vedrørende
   - nøglefunktioner og information om komponentens sikkerhed og øvrige funktioner og mulige indstillinger
   - den anvendte software, herunder open source-koden (Software Bill of Materials – SBOM)

8. graden af afhængighed af supporttjenester på tredjepartsniveau i forbindelse med håndtering og vedligeholdelse af udstyr, hvis operatøren ikke udfører disse tjenester alene med sine medarbejdere
9. foreløbig vurdering af overensstemmelsen af udstyret eller den enhed, der skal levere en supporttjeneste på tredjepartsniveau, foretaget af organer, der er akkrediteret i EU i henhold til de europæiske cybersikkerhedscertificeringsordninger, hvor de akkrediterede organer offentliggøres i *Den Europæiske Unions Tidende*.

(3) Operatøren skal dokumentere risikofaktorerne og resultaterne af risikovurderingen for hver enkelt udvalgt producent eller leverandør eller tredjepartsleverandør, jf. stk. 2 og 3 i denne artikel, og skal regelmæssigt ajourføre disse.

Artikel 5
(Generelle retningslinjer for driften af kritiske netelementer)

(1) De kritiske netkomponenter, deres drift og standardindstillinger må ikke indebære tekniske forhold, der kan påvirke sikkerheden eller driften af de kritiske enheder negativt, bl.a. ved sabotage, spionage, tyveri af intellektuel ejendom eller terrorisme.

(2) De kritiske netkomponenter er som hovedregel placeret i Republikken Slovenien eller, under hensyntagen til alle sikkerhedsrisici og med et højt niveau af sikkerhedsforanstaltninger, i EU, hvis der ikke er fastsat andet i gældende regler. Operatøren skal underrette Republikken Sloveniens agentur for kommunikationsnet og -tjenester (i det følgende benævnt "agenturet") samt den myndighed, der er ansvarlig for informationssikkerhed, om den påtænkte flytning mindst 30 dage før den påtænkte udflytning til et land uden for EU.

(3) Supporttjenester på tredjepartsniveau for kritiske elementer i netværket leveres generelt i Republikken Slovenien eller, under hensyntagen til alle sikkerhedsrisici og med et højt niveau af sikkerhedsforanstaltninger, og hvis dette ikke er specificeret på anden vis i gældende regler, i EU. Operatøren skal underrette agenturet og myndigheden med ansvar for informationssikkerhed om den påtænkte flytning mindst 30 dage før den påtænkte udflytning til et land uden for EU.

(4) Anvendelsen af supporttjenester på tredjepartsniveau må ikke bringe sikkerheden eller driften af kritiske enheders tjenester eller den nationale sikkerhed i fare.

(5) Operatøren skal etablere og regelmæssigt gennemføre en proces til identifikation af kritiske netkomponenter. Dette skal ske mindst én gang om året, eller når de kritiske netkomponenter indkøbes.

(6) Hvis en individuel komponent kun delvist udgør en kritisk netkomponent, skal den betragtes som en del af en kritisk netkomponent.

(7) Operatøren skal føre en ajourført liste over alle kritiske netkomponenters elementer, deres funktioner, placeringer, forvaltere og administratorer, deres leverandører af supporttjenester på tredjepartsniveau og disses producenter eller leverandører. Listen skal efter anmodning stilles til rådighed for agenturet og for en myndighed med ansvar for informationssikkerhed.

Artikel 6
(Sikkerhedsforanstaltninger i forbindelse med levering af kritiske netkomponenter)

(1) Operatøren skal have kendskab til hele forsyningskæden og de risici, der er forbundet med den, herunder underleverandører af individuelle komponenter til kritiske netkomponenter, som også omfatter krypteringsnøgler, UICC/eUICC og øvrige sikkerhedselementer, hvis misbrug kan bringe de kritiske enheders sikkerhed i fare.

(2) Operatøren skal sikre, at sikkerhedskravene mellem operatøren og producenterne eller leverandørerne af kritiske netkomponenter eller tredjepartsleverandører af supporttjenester er kontraktligt aftalt og dokumenteret, og kræve, at producenterne eller leverandørerne respekterer de aftalte sikkerhedsforanstaltninger i hele forsyningskæden.

(3) For at forhindre, at ondsindede aktører omgående udnytter eventuelle sikkerhedshuller, skal operatøren sikre, at producenten eller leverandøren af kritiske netkomponenter kontraktligt forpligter sig til omgående at underrette operatøren om det opdagede sikkerhedshul og om foranstaltninger til risikoreduktion samt rådgive om beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som operatøren kan træffe som reaktion på truslen.

(4) Operatøren skal mindst en gang om året kontrollere, om adgangsrettighederne til kritiske netkomponenter er tilstrækkelige, eller straks ajourføre dem i overensstemmelse med ændringer i organisationen eller hos udbydere af supporttjenester på tredjepartsniveau.

(5) Operatøren skal forhindre sin afhængighed af en individuel leverandør eller udbyder af supporttjenester på tredjepartsniveau (dvs. "leverandørbinding"), hvor dette er teknisk muligt og økonomisk bæredygtigt, med det formål at reducere afhængigheden og øge modstandsdygtigheden i tilfælde af svagheder ved kritiske komponenter, også ved at undgå langsigtede kontrakter med individuelle producenter eller leverandører eller udbydere af supporttjenester på tredjepartsniveau eller ved at have mulighed for at ændre disse med det formål at reducere afbrydelser i leveringen af tjenester til kritiske enheder til det lavest mulige niveau.

Artikel 7
(Kontraktvilkår med producenter, leverandører eller udbydere af supporttjenester på tredjepartsniveau)

For at sikre et højt sikkerhedsniveau skal operatøren som minimum medtage følgende i nye aftalevilkår med producenter, leverandører eller udbydere af supporttjenester på tredjepartsniveau:

1. en erklæring fra producenten eller leverandøren om, at komponenten eller dens standardindstillinger ikke har udokumenterede smuthuller eller nogen negativ indvirkning på driften af de kritiske enheder
2. en forsikring fra producenten, leverandøren eller tredjepartsudbyderen om at beskytte de data, som de får kendskab til under levering af tjenester eller adgang til disse i forbindelse med leveringen af en adgangstjeneste

3. en forsikring fra producenten, leverandøren eller tredjepartsudbyderen om straks at informere operatøren i tilfælde af overtrædelser af beskyttelsen af kommunikationsdata eller trafikdata, der påvirker eller kan påvirke operatøren eller de kritiske enheder, der er omhandlet i artikel 1, stk. 1, i denne generelle lov
4. en forsikring fra producenten, leverandøren eller tredjepartsudbyderen om straks at underrette operatøren om enhver sikkerhedshændelse og svaghed, der kan påvirke sikkerheden af operatørens netværk, tilhørende tjenester eller data
5. en forpligtelse fra producentens, leverandørens eller tredjepartsudbyderens side til at overholde de sikkerhedsstandarder og -regler, der er fastsat af operatøren, og til at træffe passende sikkerhedsforanstaltninger med henblik på at garantere sikkerheden af it-systemer og netværk samt operatørens eller den kritiske enheds data
6. operatørens mulighed for til enhver tid at gennemgå de forhold, procedurer, sikkerhedsforanstaltninger og værktøjer, der anvendes af udbyderen af supporttjenester på tredjepartsniveau, når denne tilgår operatørens netværk og data
7. producentens, leverandørens eller tredjeparts supportudbyderens ansvar for skader, der måtte forårsages af identificerede sikkerhedshuller eller misbrug af komponenter i kritiske netkomponenter, af deres standardindstillinger eller under levering af tredjeparts supporttjenester, som producenten, leverandøren eller tredjeparts supportudbyderen har forsømt eller bevidst implementeret
8. en forpligtelse til regelmæssigt at uddanne producentens, leverandørens eller tredjeparts supportudbyders personale inden for datasikkerhed og it-systemer og -netværk.

Artikel 8
(Regler for adgang til og brug af kritiske netkomponenter)

(1) Når operatøren har fysisk eller teknisk adgang til kritiske netkomponenter, til deres indstillinger og til de data, som operatøren har gemt, behandlet eller ændret i disse, skal operatøren sikre

1. at adgangen er strengt begrænset til personer, der tidligere er blevet autoriseret
2. at alt arbejde på kritiske netkomponenter, der udføres på stedet eller via fjernadgang, kontrolleres af operatøren
3. at der foretages multifaktorgodkendelse af brugere, der er tildelt de højeste niveauer af rettigheder til adgang til individuelle kritiske netkomponenter, deres indstillinger og til de data, som operatøren har gemt, behandlet eller ændret deri
4. at enhver autoriseret person, der gives dataadgang, får tildelt en unik brugerkonto og adgangskode
5. at der kun anvendes adgangskoder, der ændres regelmæssigt eller straks i tilfælde af opdaget misbrug, og som indeholder mindst 15 tegn og omfatter store og små bogstaver, tal og specialtegn, hvis softwaren tillader dette
6. at begrebet nultolerance eller tillid implementeres i adgangen, hvor dette er muligt
7. at sikkerheden i kommunikationsforbindelsen fra den autoriserede bruger til de enkelte komponenter beskyttes ved brug af kryptering, under hensyntagen til den seneste teknologiske udvikling og bedste praksis inden for branchen for it-sikkerhed, eller som anbefalet af etablerede institutioner inden for it-sikkerhed
8. at der foretages en uudslettelig registrering af adgang og adgangsforsøg, som opbevares i mindst seks måneder, herunder en sikkerhedskopi, men som også kan være i en længere periode, når analysen af risikostyringen og vurderingen af det acceptable risikoniveau viser, at risiciene håndteres hensigtsmæssigt ved at opbevare logfilerne over en længere periode

9. at der foretages registrering og overvågning af alle softwareindgreb på komponenter, herunder konfigurationsændringer, hvor dette er muligt; registreringer, herunder en sikkerhedskopi af de nævnte data, bliver opbevaret så længe som angivet i foregående punkt
10. at adgangen til de individuelle komponenter og til de data, der gemmes eller behandles på disse, er tidsbegrænset og kun åben, så længe det nødvendige arbejde pågår.

(2) I tilfælde af at personale eller ansatte hos en tredjepartsleverandør af supporttjenester får adgang til individuelle kritiske netkomponenter, skal de pågældende

1. udelukkende anvende en sikker, mellemliggende særlig arbejdsstation ("jumpserver"), som skal underkastes regelmæssig sikkerhedskontrol
2. på en særlig arbejdsstation udelukkende installere de absolut nødvendige værktøjer, komponenter og aktive tjenester til at få adgang til andre ressourcer på netværket, som er absolut nødvendige, og som skal være opdateret med de seneste sikkerhedsopdateringer
3. anvende sikre kryptografiske processer og nøgler på en særlig arbejdsstation, som skal være placeret i operatørens netværk, og som udelukkende er under dennes kontrol
4. ved hver adgang godkendes og aktiveres manuelt af operatøren og kun for adgangens varighed
5. kontrolleres og registreres fysisk for hver adgang og aktivitet af operatøren
6. benytte to-faktor-autentifikation og adgangskoder, der er mindst 15 tegn lange og omfatter store og små bogstaver, tal og specialtegn, som skal ændres på grundlag af vurderede risici.

(3) Inden operatøren overdrager administration, vedligeholdelse eller opdatering af kritiske netkomponenter eller deres individuelle komponenter til en tredjepart, skal operatøren kontrollere og sikre, at denne som minimum har de samme eller bedre sikkerhedsmekanismer og sikkerhedsstyringsprocesser på plads i forhold til operatørens egne mekanismer og processer. Operatøren skal straks underrette den pågældende kritiske enhed, agenturet samt myndigheden med ansvar for informationssikkerhed om den påtænkte overdragelse.

(4) Operatøren skal kontrollere sikkerhedsprocessernes faktiske tilstand, inden tjenesteydelsen påbegyndes, og derefter mindst en gang om året. Operatøren skal føre fortegnelser over interne revisioner og kontroller af leveringen af tredjepartssupporttjenester og opbevare disse, så længe tjenesterne leveres og i et år efter deres ophør, dog højst fem år.

OVERGANGSBESTEMMELSER OG AFSLUTTENDE BESTEMMELSER

Artikel 9
(Overgangsbestemmelser)

(1) Operatøren skal senest 30 dage efter ikrafttrædelsen af denne generelle lov underrette agenturet og myndigheden med ansvar for informationssikkerhed om de eksisterende placeringer af de kritiske netkomponenter.

(2) Operatøren skal senest 30 dage efter ikrafttrædelsen af denne generelle lov underrette agenturet og myndigheden med ansvar for informationssikkerhed om de eksisterende placeringer af supporttjenester på tredjepartsniveau for kritiske netkomponenter.

(3) Agenturet skal for første gang offentliggøre de dokumenter, der er omhandlet i artikel 3, stk. 2, i denne generelle lov på datoen for dens ikrafttræden.

Artikel 10
(Ikrafttræden)

Denne generelle lov træder i kraft på tredivtedagen efter dens offentliggørelse i Republikken Sloveniens officielle tidende, hvorved operatører kan anvende udstyret og opretholde leveringen af supporttjenester på tredjepartsniveau indtil udløbet af de frister, der er angivet i lovens artikel 312, stk. 2 og 3.

Nr. _____ mag. Marko Mišmaš

Ljubljana, den _____ direktør

EVA 2023-3150-0034

FORSLAG

Bilag

Liste over kritiske netkomponenter og tilhørende informationssystemer:

Kritiske netkomponenter	**Net- og informationssystemernes funktionaliteter**
Abonnentstyring og krypteringsmekanismer	- Sessionshåndtering (tale og data), - autentificering af brugere og udstyr i netværket, - styring og opbevaring af nøgler til autorisation af abonnenter og netkomponenter (UICC/eUICC, digitale certifikater/HSM), - funktioner til sikker autentificering, beskyttelse af kommunikationens integritet (kryptering) og opbevaring af brugernøgler, netværks- og administrationskomponenter, - styring af adgangsrettigheder.
Tilslutninger	- Hostingfunktioner og grænseflader til andre netværk og tjenester.
Administrerede nettjenester	- Registrering og godkendelse af nettjenester, - opbevaring og behandling af kommunikations-, lokaliserings- og trafikdata, - netværks- og netværksfunktioners eksponering for eksterne applikationer og tjenester.
Styring og tilrettelæggelse af virtuelle netværksfunktioner (NFV) og netværkstilrettelæggelse (MANO), herunder virtualiseringsinfrastruktur.	- Management-funktioner i forbindelse med tilrettelæggelse og konfigurering af NFV uanset implementeringstype (VM, container, microservices), - virtualiseringsfunktioner til implementering og brug af NFV, - Network Slice Selection Function (NSSF).
Netværk til trådløs adgang	- Ladestationer, der understøtter 5G-teknologi eller derover.
Managementsystemer og andre supportsystemer	- Overvågning af drift og styring af mobilkommunikationsnettet, herunder adgangsdelen (RAN/O-RAN), - systemer til detektering af sikkerhedshændelser, uregelmæssigheder, trusler og håndtering heraf (sikkerhedsfunktioner, herunder SIEM/SOAR).
Lovlig aflytning	- Funktioner, der giver den kompetente myndighed adgang til kommunikationsindhold og data om brugertrafik.