FÖRSLAG

I enlighet med artikel 116.6 i lagen om elektronisk kommunikation (UL RS nr 130/22 och 18/23 – ZDU-1O) utfärdar Sloveniens byrå för kommunikationsnät och kommunikationstjänster, med beaktande av informationsförfarandet i enlighet med Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och föreskrifter för informationssamhällets tjänster, (EUT L 241, 17.9.2015, s. 1) följande:

ALLMÄN RÄTTSAKT
om ytterligare säkerhetskrav och begränsningar

Artikel 1
(Den allmänna rättsaktens innehåll)

I denna allmänna rättsakt föreskrivs följande:

1. Riktlinjer som ska följas av operatörer av mobilkommunikationsnät (nedan kallade *operatörer*) som tillhandahåller dessa nät till kritiska enheter som är förvaltare av kritisk infrastruktur inom andra områden av reglering av kritisk infrastruktur, i enlighet med den lagstiftning som reglerar kritisk infrastruktur (nedan kallade *förvaltare av kritisk infrastruktur*), leverantörer av samhällsviktiga tjänster enligt lagen om informationssäkerhet (nedan kallade*leverantörer av samhällsviktiga tjänster*), statliga förvaltningsorgan som fastställs i lagen om informationssäkerhet (nedan kallade *statliga förvaltningsorgan*) eller transportörer av viktiga delar av landets säkerhetssystem.
2. Kritiska delar av nätverket och tillhörande informationssystem med funktioner som avses i artikel 116.6 i lagen om elektronisk kommunikation (UL RS nr 130/22 och 18/23 – ZDU-1O (nedan kallad *lagen*), enligt bilagan, som utgör en integrerad del av denna allmänna rättsakt och upprättas i samarbete med det organ som ansvarar för informationssäkerhet.

Artikel 2
(Förklaring av termer)

(1) De termer som används i denna allmänna rättsakt betyder följande:

1. En leveranskedja är hela systemet med processer, personer, organisation och distribution vilka är involverade i konstruktion, produktion, lagring, distribution och leverans samt installation och underhåll av komponenter i kritiska linjesegment som är installerade i operatörens nätverk eller hos den leverantör av molntjänster som tillhandahåller sådana tjänster till operatören.

2. Kritiska delar av nätverket är de nätverkselement, funktioner, tjänster och stödjande informationssystem i fysisk form, programvara eller virtualiserad form hos operatören eller hos molntjänstleverantören, enligt förteckningen i bilagan till denna allmänna rättsakt.

3. Kritiska enheter är kritiska infrastrukturförvaltare inom andra områden av reglering av kritisk infrastruktur som fastställs i enlighet med den lagstiftning som styr området för kritisk infrastruktur, leverantörer av samhällsviktiga tjänster enligt lagen om informationssäkerhet, statliga förvaltningsorgan som fastställs i lagen om informationssäkerhet samt transportörer av viktiga delar av landets säkerhetssystem.

(2) Andra termer som används i denna allmänna rättsakt har samma betydelse som de definieras i lagen och den allmänna rättsakten om säkerhet för nät, tjänster och data.

Artikel 3
(Allmänna riktlinjer)

(1) Operatörer i leveranskedjan för komponenter i kritiska linjesegment och stödtjänster på tredje nivå för dessa komponenter ska beakta åtminstone följande riktlinjer under hela livscykeln för dessa komponenter:

1. En enskild tillverkare eller leverantör och en tredjepartsleverantör av stödtjänster ska på grund av förbindelser och avtal med dem göra en riskbedömning i fråga om leveranser och potentiella effekter av tredje parts fysiska eller juridiska personer enligt offentlig eller privaträttslig lagstiftning (nedan kallade *tredje parter*), kompatibilitet med utrustning från andra tillverkare, produktkvalitet och produktsäkerhet samt potentiella negativa effekter på driften av operatörens tjänster och kritiska enheter,
2. att säkerheten är inbyggd och genomförd redan i utformningen och att kontrakten innehåller tidsfrister för att undanröja upplevda sårbarheter,
3. att viktiga säkerhetsdetaljer (tillgänglighet, konfidentialitet, integritet och äkthet) säkerställs under hela livscykeln för användningen,
4. att säkerheten och deras oavbrutna försörjning garanteras och det bekräftas att den stöder höga säkerhetsdetaljer i enlighet med internationellt erkända standarder (3GPP) och europeiska tekniska standarder (Etsi),
5. att de riktlinjer som avses i leden 2–4 i denna punkt är möjliga att kontrollera i avtalsdokumentationen med tillverkaren eller leverantören.
6. För varje tillverkare eller leverantör ska även de risker som är förknippade med rätten till användning av viktig teknik, vilka är nödvändiga för tillverkning och användning av utrustningen och riskerna i samband med tillhandahållande av utrustning, reservdelar eller stödtjänster på tredje nivå, bedömas och beaktas,
7. att de komponenter som används inte har olösta kända kritiska eller aktivt utnyttjade sårbarheter,
8. undvikande av en enda tillverkare eller leverantör, om detta är tekniskt genomförbart och ekonomiskt hållbart, i syfte att minska beroendet och öka motståndskraften vid kritiska komponenters sårbarheter, katastrofala nätfel eller hot mot säkerheten för kritiska enheters nät och tjänster från tredje fysiska eller juridiska enheter som omfattas av offentlig rätt eller privaträtt.

(2) Vid tillhandahållande av informations- och kommunikationsutrustning, system och tjänster ska operatörerna till fullo följa riktlinjerna från Europeiska unionens cybersäkerhetsbyrå (nedan kallad *Enisa*) och Europeiska unionens gällande förordningar om grundläggande säkerhetskrav vid upphandling av säkra IKT-produkter och IKT-tjänster. Byrån ska på sin webbplats offentliggöra länkar till aktuella Enisa-dokument och EU-förordningar inom ovannämnda område och hålla dem uppdaterade.

(3) Vid tillhandahållande av komponenter i kritiska linjesegment eller användning av molntjänster ska prioritet ges åt att välja komponenter från de tillverkare eller leverantörer eller tjänster från molntjänstleverantörer som har certifierats av organ för bedömning av överensstämmelse som har ackrediterats och, vid behov, auktoriserats på grundval av artikel 60.3 i Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (nedan kallad *förordningen*) för utfärdande av europeiska cybersäkerhetscertifikat på en viss säkerhetsnivå, i enlighet med artikel 52 i förordningen.

(4) Vid tillämpningen av föregående punkt ska operatören kontrollera en särskild webbplats som inrättats av Enisa i enlighet med artikel 55 i förordningen och som är avsedd att informera allmänheten om europeiska system för cybersäkerhetscertifiering, europeiska cybersäkerhetscertifikat och EU-försäkran om överensstämmelse, inbegripet information om europeiska system för cybersäkerhetscertifiering som inte längre är giltiga eller återkallade och utgångna europeiska cybersäkerhetscertifikat och EU-försäkran om överensstämmelse, och en databas med länkar till information om cybersäkerhet.

Artikel 4
(Riskbedömning)

(1) Vid fastställandet av komponenttillverkarens eller leverantörens och tjänsteleverantörens risk för kritiska delar av nätet tar operatören hänsyn till följande riskaspekter som den utvärderar.

(2) Vid den värdering som avses i föregående punkt ska verksamhetsutövaren bedöma och beakta åtminstone följande:

1. Övergripande kvalitet (inklusive säkerhetsaspekter) och tillförlitlighet.
2. Graden av användning av öppna standarder och gränssnitt som förhindrar beroende och inlåsning av produkter från en viss tillverkare eller leverantör.
3. Efterlevnad av erkända internationella och europeiska tekniska standarder (3GPP, Etsi) och EU-bestämmelser och standardsäkerhetsinställningar i enlighet med yrkesmässiga rekommendationer (*GSMA Association*).
4. Graden av kompatibilitet med utrustning och nätverksfunktioner från tredje part.
5. Förmåga att tillhandahålla uppgraderingar och anpassningar.
6. Sårbarhetshanteringsprocessen, offentliggörande och aktuella processer med uppdateringar och korrigeringar.
7. Tillgång till och insyn i dokumentation avseende
   - nyckelfunktioner och information om säkerhet och andra funktioner i komponenten och möjliga inställningar och
   - programvara som används, inklusive öppen källkod (materiallista).
8. graden av beroende av stödtjänster på tredje nivå vid hantering och underhåll av utrustning, om operatören inte ensam utför dessa tjänster tillsammans med sina anställda.
9. En preliminär bedömning av utrustningens överensstämmelse eller en enhet som ska tillhandahålla en stödtjänst på tredje nivå, bestående av organ som ackrediterats i Europeiska unionen i enlighet med europeiska system för cybersäkerhetscertifiering. De ackrediterade organen offentliggörs i *Europeiska unionens officiella tidning*.

(3) Verksamhetsutövaren ska dokumentera riskfaktorerna och resultaten av riskbedömningen för varje utvald tillverkare, leverantör eller tredjepartsleverantör som avses i punkterna 2 och 3 i denna artikel och ska regelbundet uppdatera detta.

Artikel 5
(Allmänna riktlinjer för driften av kritiska linjesegment)

(1) Komponenterna i de kritiska linjesegmenten, deras drift och standardinställningar får inte innehålla tekniska egenskaper som skulle kunna inverka negativt på kritiska enheters säkerhet eller drift, bland annat till följd av sabotage, spionage, stöld av immateriella rättigheter eller terrorism.

(2) De kritiska linjesegmenten är i allmänhet belägna i Slovenien eller, med beaktande av alla säkerhetsrisker och säkerställande av en hög nivå av säkerhetsåtgärder, och om detta inte anges på annat sätt i tillämpliga förordningar, i Europeiska unionen. Operatören ska underrätta Sloveniens byrå för kommunikationsnät och kommunikationstjänster (nedan kallad *byrån*) och det organ som ansvarar för informationssäkerhet om planerade omplaceringar minst 30 dagar före omplaceringen utanför Europeiska unionen.

(3) Stödtjänster på tredje nivå för kritiska delar av nätverket utförs i allmänhet i Slovenien eller, med beaktande av alla säkerhetsrisker och säkerställande av en hög säkerhetsnivå, och om detta inte anges på annat sätt i tillämpliga förordningar, i Europeiska unionen. Operatören ska underrätta byrån och det organ som ansvarar för informationssäkerheten om den planerade flyttningen av deras stödtjänster på tredje nivå senast 30 dagar före omplaceringen utanför Europeiska unionens länder.

(4) Genomförandet av stödtjänster på tredje nivå får inte äventyra säkerheten eller driften av kritiska enheter eller nationella säkerhetstjänster.

(5) Operatören ska upprätta och regelbundet genomföra processen för identifiering av kritiska linjesegment. Detta måste utföras minst en gång om året eller när komponenter i kritiska linjesegment upphandlas.

(6) Om en enskild komponent endast delvis representerar ett kritiskt linjesegment ska den betraktas som en del av ett kritiskt linjesegment.

(7) Operatören ska föra en uppdaterad förteckning över alla komponenter i kritiska linjesegment, deras funktioner, platser, administratörer och chefer, deras tredjepartsleverantörer av stödtjänster och deras tillverkare eller leverantörer. På begäran ska förteckningen göras tillgänglig för byrån och ett organ med ansvar för informationssäkerhet.

Artikel 6
(Säkerhetsåtgärder för leverans av komponenter i kritiska linjesegment)

(1) Operatören ska vara känna till hela försörjningskedjan och de risker som är förknippade med den, inbegripet underleverantörer av enskilda komponenter i kritiska

linjesegment, vilket även omfattar krypteringsnycklar, UICC/eUICC och andra säkerhetselement, vars missbruk skulle kunna äventyra säkerheten för kritiska enheter.

(2) Operatören ska se till att säkerhetskraven mellan operatören och tillverkarna eller leverantörerna av komponenter av kritiska linjesegment eller dess leverantörer av stödtjänster på tredje nivå avtalas och dokumenteras och kräver att tillverkare eller leverantörer respekterar de överenskomna skyddsåtgärderna i hela leveranskedjan.

(3) För att förhindra att skadliga aktörer utnyttjar sårbarheter i tid ska operatören se till att tillverkaren eller leverantören av komponenter i ett kritiskt linjesegment enligt avtal förbinder sig att omedelbart informera operatören om den upptäckta sårbarheten och om åtgärder för att minska riskerna samt ge råd om skyddsåtgärder eller avhjälpande åtgärder som operatören kan vidta som svar på hotet.

(4) Operatören ska minst en gång om året kontrollera att åtkomsträttigheterna för kritiska linjesegment är adekvata eller utan dröjsmål uppdatera dem i enlighet med förändringar i organisationen eller på tredje nivås leverantörer av stödtjänster.

(5) Operatören ska undvika att bli beroende av en enskild leverantör eller tredjepartsleverantör (dvs. inlåsning av leverantörer), om detta är tekniskt genomförbart och ekonomiskt hållbart, i syfte att minska beroendet och öka motståndskraften hos kritiska komponenters sårbarhet, även genom att undvika långsiktiga avtal med enskilda tillverkare eller leverantörer eller leverantörer av stödtjänster på tredje nivå, eller ha möjlighet att ändra dem i syfte att minska störningar i tillhandahållandet av tjänster till kritiska enheter till lägsta möjliga nivå.

Artikel 7
(Avtalsvillkor med tillverkare, leverantörer eller tredjepartsleverantörer av supporttjänster)

För att säkerställa en hög säkerhetsnivå ska operatören inkludera åtminstone följande i nya avtalsvillkor med tillverkare, leverantörer eller tredjepartsleverantörer av stödtjänster:

1. En förklaring från tillverkaren eller leverantören om att komponenten eller dess standardinställningar inte har några papperslösa bakdörrar eller någon negativ inverkan på driften av kritiska enheter.
2. Ett åtagande från tillverkaren, leverantören eller tredjepartsleverantören att skydda de uppgifter som de får kännedom om under tillhandahållandet av tjänster eller tillgången till dem i samband med tillhandahållandet av åtkomsttjänsten.
3. Ett åtagande från tillverkaren, leverantören eller tredjepartsleverantören om att omedelbart informera operatören i händelse av överträdelser av skyddet av kommunikationsdata eller trafikdata som påverkar eller skulle kunna påverka operatören eller de kritiska enheter som avses i artikel 1.1 i denna allmänna rättsakt.
4. Ett åtagande från tillverkaren eller leverantören eller tredjepartsleverantören om att omedelbart underrätta operatören om alla säkerhetstillbud och sårbarheter som kan påverka säkerheten i nätverket, tillhörande tjänster eller uppgifter från operatören.
5. Ett åtagande från tillverkaren eller leverantören eller tredjepartsleverantören om att följa de säkerhetsstandarder och säkerhetsregler som fastställts av operatören och att vidta lämpliga säkerhetsåtgärder för att säkerställa säkerheten i informationssystem och informationsnät samt operatörens eller kritiska enheters data.

6. Operatörens förmåga att när som helst se över de miljöer, förfaranden, säkerhetsåtgärder och verktyg som används av tredjepartsleverantören av stödtjänster vid åtkomst till operatörens nätverk och data.
7. Tillverkarens eller leverantörens eller tredjepartsleverantörens ansvar för skador som skulle orsakas av identifierade sårbarheter eller missbruk av komponenter i kritiska linjesegment, deras standardinställning eller under tillhandahållandet av stödtjänster på tredje nivå som tillverkaren eller leverantören eller stödleverantören på tredje nivå har försummat eller avsiktligt genomfört.
8. En skyldighet att regelbundet utbilda personalen hos tillverkaren eller leverantören eller leverantören av stödtjänster på tredje nivå i datasäkerhets- och informationssystem samt datanät.

Artikel 8
(Regler för åtkomst till och användning av kritiska linjesegment)

(1) När operatören fysiskt eller logistiskt får tillgång till komponenterna i kritiska linjesegment, deras inställningar och operatörens data som lagras, bearbetas eller modifieras i dem, ska operatören säkerställa att

1. åtkomsten är strikt begränsad till personer som tidigare har auktoriserats,
2. alla arbeten på kritiska linjesegment som utförs på plats eller via fjärråtkomst styrs av operatören,
3. tvåfaktorsautentisering utförs för användare som tilldelas de högsta rättigheterna för åtkomst till enskilda komponenter i kritiska linjeelement, deras inställningar eller de data som lagras eller behandlas där,
4. varje behörig person som beviljas åtkomst har ett unikt användarkonto och ett unikt lösenord,
5. endast lösenord används som ändras regelbundet eller omedelbart vid upptäckt missbruk och innehåller minst 15 tecken bestående av versaler och gemener, siffror och specialtecken, om programvaran tillåter detta,
6. begreppet nolltolerans eller nolltillit tillämpas när så är möjligt vid åtkomst,
7. säkerheten för kommunikationsförbindelsen från den behöriga användaren till de enskilda komponenterna skyddas genom kryptering, med beaktande av den senaste tekniska utvecklingen och bästa industriella praxis på området informationssäkerhet, eller rekommenderas av etablerade institutioner på informationssäkerhetsområdet,
8. en outplånlig registrering av åtkomster och åtkomstförsök görs, som bevaras i minst sex månader, inklusive en säkerhetskopia, men också kan ske under en längre period, om analysen av riskhanteringen och bedömningen av den godtagbara risknivån visar att riskerna bör hanteras på ett tillfredsställande sätt genom att föra loggar under en längre period,
9. registrering och övervakning av alla programvaruinterventioner på komponenter utförs där så är möjligt, inklusive konfigurationsändringar, register, inklusive en säkerhetskopia av dessa uppgifter, ska bevaras så länge som anges i föregående punkt,
10. tillgången till enskilda komponenter och till uppgifter som lagras eller behandlas på dem är tidsbegränsad och öppen endast under den tid som det nödvändiga arbetet pågår.

(2) Vid åtkomst till enskilda komponenter i kritiska linjesegment för personal eller anställda hos en tredjepartsleverantör av stödtjänster ska de

1. endast använda en säker mellanliggande särskild arbetsstation (hoppserver, på engelska *jump server*), som ska vara föremål för regelbundna säkerhetskontroller,
2. installera endast på en särskild arbetsstation de absolut nödvändiga verktygen, komponenterna och aktiva tjänsterna för att få åtkomst till andra resurser i nätverket som är absolut nödvändiga och måste uppdateras med de senaste säkerhetskorrigeringarna,
3. använda säkra kryptografiska operationer och nycklar på en särskild arbetsstation, som måste vara belägen i operatörens nätverk och som endast operatören har kontroll över,
4. varje åtkomst godkänns och aktiveras av operatören manuellt och endast så länge åtkomsten pågår,
5. alla åtkomster och aktiviteter kontrolleras fysiskt och registreras av operatören,
6. tvåfaktorsautentisering och lösenord ska användas som är minst 15 tecken långa och innehåller versaler och gemener, siffror och specialtecken, som ska ändras på grundval av bedömda risker.

(3) Innan operatören överför tjänsten att förvalta, underhålla eller uppdatera kritiska linjesegment eller deras enskilda komponenter till en tredje part, ska den kontrollera och säkerställa att tredje parten har minst samma eller bättre säkerhetsmekanismer och processer för säkerhetsriskhantering jämfört med sina mekanismer och processer. Den ska omedelbart informera den berörda kritiska enheten, byrån och det organ som ansvarar för informationssäkerhet om avsikten att överföra den.

(4) Operatören ska kontrollera det faktiska läget för säkerhetsprocesserna innan tjänsterna börjar tillhandahållas och därefter minst en gång om året. Operatören ska föra register över interna granskningar och kontroller av tillhandahållandet av tredjepartsstödtjänster och bevara dem under hela den tid då tjänsterna tillhandahålls och under ett år efter det att de upphört att gälla, dock inte längre än fem år.

ÖVERGÅNGS- OCH SLUTBESTÄMMELSE

Artikel 9
(Övergångsbestämmelser)

(1) Verksamhetsutövaren ska underrätta byrån och det organ som ansvarar för informationssäkerheten om de befintliga platserna för kritiska linjesegment inom 30 dagar efter det att denna allmänna rättsakt har trätt i kraft.

(2) Operatören ska underrätta byrån och det organ som ansvarar för informationssäkerhet om de befintliga platserna för stödtjänster på tredje nivå för kritiska linjesegment inom 30 dagar efter det att denna allmänna rättsakt har trätt i kraft.

(3) Byrån ska för första gången offentliggöra de handlingar som avses i artikel 3.2 i denna allmänna rättsakt från och med den dag då den träder i kraft.

FÖRSLAG

Artikel 10
(Ikraftträdande)

Denna allmänna rättsakt träder i kraft den trettionde dagen efter det att den har offentliggjorts i Republiken Sloveniens kungörelseorgan, varigenom operatörerna får använda utrustningen och upprätthålla tillhandahållandet av stödtjänster på tredje nivå fram till utgången av de tidsfrister som anges i artikel 312.2 och 312.3 i lagen.

Nej _____ mag. Marko

Mišmaš

Ljubljana, den _____ direktör

EVA 2023-3150-0034

FÖRSLAG

Bilaga

Förteckning över kritiska linjesegment och tillhörande informationssystem:

Kritiska linjesegment	**Nätverks- och informationssystemens funktioner**
Prenumeranthantering och krypteringsmekanismer	- sessionshantering (röst och data), - autentisering av användare och utrustning med nätverket, - hantering och lagring av nycklar för auktorisation av abonnenter och nätverkskomponenter (UICC/eUICC, digitala certifikat/HSM), - funktioner för säker autentisering, skydd av kommunikationsintegritet (kryptering) och lagring av användarnycklar samt nätverks- och hanteringskomponenter, - förvaltning av åtkomsträttigheter,
sammankoppling,	- värdtjänstfunktioner och gränssnitt till andra nätverk och tjänster,
hanterade nättjänster,	- registrering och auktorisation av nättjänster, - lagring och behandling av kommunikations-, lokaliserings- och trafikuppgifter, - exponering av nätverks- och nätverksfunktioner för externa applikationer och tjänster,
förvaltning och orkestrering av virtualiserade nätverksfunktioner (NFV) och nätverksorkestrering (MANO), inklusive virtualiseringsinfrastruktur,	- ledningsfunktioner för orkestrering och konfiguration av NFV, oavsett typ av genomförande (VM, behållare, mikrotjänster), - virtualiseringsfunktioner för implementering och användning av NFV, - NSSF(Nätverksskivningsvalfunktion, på engelska *Network Slice Selection Function*),
radioaccessnät,	- basstationer som stöder 5G-teknik eller högre,
ledningssystem och andra stödsystem,	- övervaka driften och förvaltningen av mobilkommunikationsnätet, inbegripet åtkomstdelen (RAN/O-RAN), - system för att upptäcka säkerhetshändelser, avvikelser, hot och deras hantering (säkerhetsfunktioner inklusive SIEM/SOAR).
laglig avlyssning,	- funktioner för den behöriga myndighetens tillgång till kommunikationsinnehåll och uppgifter om användartrafik.