Nos termos do artigo 116.º, n.º 6, da Lei das Comunicações Eletrónicas (UL RS n.ºs 130/22 e 18/23 — ZDU-10), a Agência das Redes e Serviços de Comunicação da República da Eslovénia, tendo em conta o procedimento de informação em conformidade com a Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (JO L 241 de 17.9.2015, p. 1), tem a seguinte redação:

LEI GERAL **sobre requisitos e restrições de segurança adicionais**

Artigo 1.º **(Conteúdo da lei geral)**

A presente lei geral prevê:

1. diretrizes a seguir pelos operadores de redes de comunicações móveis (a seguir designados «operadores») que fornecem essas redes a entidades críticas que são gestores de infraestruturas fundamentais noutras áreas da regulamentação das infraestruturas críticas, tal como especificado na legislação que rege a área das infraestruturas fundamentais (a seguir designados «gestores de infraestruturas fundamentais»), prestadores de serviços essenciais, tal como determinado pela lei que rege a segurança da informação (a seguir designados «prestadores de serviços essenciais»), órgãos da administração pública, tal como determinado pela lei que rege a segurança da informação (a seguir designados «organismos da administração pública») ou transportadoras de partes essenciais do sistema de segurança do país; e
2. elementos fundamentais da rede e sistemas de informação associados com as suas funcionalidades a que se refere o artigo 116.º, n.º 6, da Lei das Comunicações Eletrónicas (UL RS n.ºs 130/22 e 18/23 – ZDU-10; a seguir designado por «Lei»), tal como consta do anexo, que faz parte integrante da presente lei geral e é elaborado em cooperação com o organismo responsável pela segurança da informação.

Artigo 2.º **(Significado dos termos)**

(1) Os termos utilizados nesta lei geral significam:

1. Uma cadeia de abastecimento é todo o sistema de processos, pessoas, organização e distribuição envolvidos na conceção, produção, armazenamento, distribuição e fornecimento, bem como na instalação e manutenção de componentes de elementos críticos da rede instalados na rede do operador ou no prestador de serviços de computação em nuvem que presta esses serviços ao operador.
2. Os elementos fundamentais da rede são os elementos da rede, as funções, os serviços e os sistemas de informação de suporte em suporte físico, informático ou

PROPOSTA

virtualizado no operador ou no prestador de serviços de computação em nuvem, tal como enumerados no anexo da presente lei geral.

3. As entidades fundamentais são gestores de infraestruturas fundamentais noutros domínios da regulamentação das infraestruturas cruciais determinados em conformidade com a legislação que rege o domínio das infraestruturas fundamentais, prestadores de serviços essenciais tal como determinado pela lei que rege a segurança da informação, os órgãos da administração pública, tal como determinado pela lei que rege a segurança da informação e os transportadores de partes essenciais do sistema de segurança do país.

(2) Outros termos utilizados nesta lei geral têm o mesmo significado que o definido pela Lei e pela Lei Geral sobre a Segurança das Redes, Serviços e Dados.

Artigo 3.º (Diretrizes gerais)

(1) Os operadores da cadeia de abastecimento dos componentes de elementos fundamentais da rede e dos serviços de apoio de terceiro nível para esses componentes devem ter em conta, pelo menos, as seguintes orientações ao longo de todo o ciclo de vida desses componentes:

1. no caso de um fabricante ou fornecedor individual e de um prestador de serviços de apoio de nível terceiro devido a relações e acordos com eles, devem realizar uma avaliação dos riscos em termos de fornecimento e potenciais impactos por terceiros, singulares ou coletivas de direito público ou privado (a seguir designados «terceiros»), de compatibilidade com equipamentos de outros fabricantes, de qualidade e segurança dos produtos e de potenciais impactos negativos no funcionamento dos serviços do operador e das entidades fundamentais;
2. que a segurança já está integrada e implementada na conceção e que os contratos incluem prazos para a eliminação de vulnerabilidades percebidas;
3. que os principais elementos de segurança (disponibilidade, confidencialidade, integridade e autenticidade) são assegurados ao longo de todo o ciclo de vida da sua utilização,
4. que a segurança e o seu fornecimento ininterrupto estão garantidos e confirma-se que suporta elementos de segurança elevados, em conformidade com as normas internacionalmente reconhecidas (3GPP) e as normas técnicas europeias (ETSI);
5. que as orientações referidas nos pontos 2 a 4 do presente número são verificáveis na documentação contratual com o fabricante ou o fornecedor;
6. para cada fabricante ou fornecedor, os riscos associados aos direitos de utilização das tecnologias-chave necessários para o fabrico e a utilização do equipamento e os riscos relacionados com o fornecimento de equipamentos, peças sobresselentes ou serviços de apoio de terceiro nível são igualmente avaliados e tidos em conta;
7. que os componentes utilizados não apresentam vulnerabilidades críticas ou exploradas ativamente não resolvidas;
8. evitar um único fabricante ou fornecedor, sempre que tal seja tecnicamente viável e economicamente sustentável, com o objetivo de reduzir a dependência e aumentar a resiliência em caso de vulnerabilidades críticas dos componentes, falha catastrófica da rede ou ameaça à segurança das redes e serviços de

entidades críticas por entidades naturais ou jurídicas terceiras de direito público ou privado.

(2) Ao fornecerem equipamentos, sistemas e serviços de informação e comunicação, os operadores devem cumprir plenamente as orientações da Agência da União Europeia para a Cibersegurança (a seguir designada «ENISA») e os regulamentos válidos da União Europeia relativos aos requisitos básicos de segurança aquando da aquisição de produtos e serviços de TIC seguros. A Agência publica no seu sítio da Web ligações para os atuais documentos da ENISA e regulamentos da UE no domínio acima referido e mantém-nas atualizadas.

(3) Ao fornecer componentes de elementos de rede fundamentais ou utilizar serviços de computação em nuvem, deve ser dada prioridade à escolha de componentes dos fabricantes ou fornecedores ou serviços de prestadores de serviços de computação em nuvem que tenham sido certificados por organismos de avaliação da conformidade acreditados e, se necessário, autorizados com base no artigo 60.º, n.º 3, do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (a seguir designado «Regulamento») para a emissão de certificados europeus de cibersegurança a determinados níveis de garantia, tal como determinado no artigo 52.º do regulamento.

(4) Para efeitos do número anterior, o operador verifica um sítio da Web especial, criado pela ENISA em conformidade com o artigo 55.º do Regulamento, destinado a informar o público sobre os sistemas europeus de certificação da cibersegurança, os certificados europeus de cibersegurança e as declarações UE de conformidade, incluindo informações relativas aos sistemas europeus de certificação da cibersegurança que deixaram de ser válidos ou revogados e caducados e caducados, bem como um repositório de ligações para informações sobre cibersegurança.

Artigo 4.º (Avaliação do risco)

(1) Ao determinar o risco do fabricante ou fornecedor de componentes e do prestador de serviços de terceiro nível para os elementos críticos da rede, o operador tem em conta os seguintes aspetos de risco, que avalia.

(2) Na avaliação referida no número anterior, o operador deve avaliar e ter em conta, pelo menos:

1. A qualidade global (incluindo aspetos de segurança) e fiabilidade;
2. O nível de utilização de normas e interfaces abertas que impeçam a dependência e a vinculação aos produtos de um determinado fabricante ou fornecedor;
3. O cumprimento das normas técnicas internacionais e europeias reconhecidas (3GPP, ETSI) e dos regulamentos da União Europeia e dos parâmetros de segurança por defeito, em conformidade com as recomendações profissionais (Associação SGMA);
4. O nível de compatibilidade com equipamentos e funções de rede de terceiros;
5. A capacidade de fornecer atualizações e personalizações;

PROPOSTA

6. O processo de gestão de vulnerabilidades, a sua divulgação e o processo atualizado com atualizações e correções;
 7. A disponibilidade e transparência da documentação relativa a:
 - As funções-chave e informações sobre segurança e outras características do componente e possíveis definições, e
 - O software utilizado, incluindo código de código aberto (Lista de materiais — SBOM);
 8. O nível de dependência dos serviços de apoio de terceiro nível na gestão e manutenção de equipamentos, se o operador não executar esses serviços sozinho com os seus empregados;
 9. A avaliação preliminar da conformidade do equipamento ou de uma entidade que preste um serviço de apoio de terceiro nível por organismos acreditados na União Europeia de acordo com os sistemas europeus de certificação da cibersegurança, em que os organismos acreditados são publicados no *Jornal Oficial da União Europeia*.
- (3) O operador deve documentar os fatores de risco e os resultados da avaliação dos riscos para cada fabricante, fornecedor ou prestador de serviços de terceiro nível selecionado a que se referem os n.ºs 2 e 3 do presente artigo, e deve atualizá-lo regularmente.

Artigo 5.º

(Diretrizes gerais sobre o funcionamento dos elementos fundamentais da rede)

- (1) Os componentes dos elementos fundamentais da rede, o seu funcionamento e as predefinições não devem conter características técnicas suscetíveis de afetar negativamente a segurança ou o funcionamento das entidades fundamentais, nomeadamente devido à sabotagem, espionagem, roubo de propriedade intelectual ou terrorismo.
- (2) Os elementos fundamentais da rede estão geralmente localizados na República da Eslovénia ou, tendo em conta todos os riscos de segurança e assegurando um elevado nível de medidas de segurança, e se tal não for especificado em contrário pela regulamentação aplicável, na União Europeia. O operador deve informar a Agência das Redes e Serviços de Comunicação da República da Eslovénia (a seguir designada «a Agência») e o organismo responsável pela segurança da informação sobre a sua realocação prevista, pelo menos 30 dias antes da recolocação para fora da União Europeia.
- (3) Os serviços de apoio de terceiro nível para elementos fundamentais da rede são geralmente prestados na República da Eslovénia ou, tendo em conta todos os riscos de segurança e assegurando um elevado nível de medidas de segurança, e se tal não for especificado em contrário pelos regulamentos aplicáveis, na União Europeia. O operador deve notificar a Agência e o organismo responsável pela segurança da informação da realocação prevista dos seus serviços de apoio de terceiro nível, pelo menos 30 dias antes da recolocação para fora dos países da União Europeia.
- (4) A implementação de serviços de apoio de terceiro nível não deve comprometer a segurança ou o funcionamento dos serviços de entidades fundamentais ou a segurança nacional.

PROPOSTA

(5) O operador deve estabelecer e implementar regularmente o processo de identificação dos elementos fundamentais da rede. Tal deve ser realizado pelo menos uma vez por ano ou quando são adquiridos componentes de elementos fundamentais da rede.

(6) Se um componente individual representar apenas parcialmente um elemento fundamental de rede, deve ser considerado como parte de um elemento fundamental de rede.

(7) O operador deve manter atualizada uma lista de todos os componentes dos elementos fundamentais da rede, das suas funções, locais, administradores e gestores, dos seus prestadores de serviços de apoio de terceiro nível e dos seus fabricantes ou fornecedores. Mediante pedido, a lista é disponibilizada à Agência e a um organismo responsável pela segurança da informação.

Artigo 6.º

(Medidas de segurança para o fornecimento de componentes de elementos fundamentais da rede)

(1) O operador deve estar ciente de toda a cadeia de abastecimento e dos riscos que lhe estão associados, incluindo os subcontratantes de componentes individuais de elementos fundamentais da rede, que também incluem chaves de cifragem, UICC/eUICC e outros elementos de segurança, cuja utilização indevida possa comprometer a segurança das entidades fundamentais.

(2) O operador deve assegurar que os requisitos de segurança entre o operador e os fabricantes ou fornecedores de componentes de elementos fundamentais de rede ou os seus prestadores de serviços de apoio de terceiro nível são contratualmente acordados e documentados e exigem que os fabricantes ou fornecedores respeitem as medidas de segurança acordadas ao longo de toda a cadeia de abastecimento.

(3) A fim de impedir a exploração de vulnerabilidades por agentes maliciosos em tempo útil, o operador deve assegurar que o fabricante ou fornecedor de componentes de um elemento fundamental de rede se compromete contratualmente a informar imediatamente o operador da vulnerabilidade detetada e das medidas para reduzir os riscos e a aconselhar sobre as medidas de proteção ou reparação que o operador pode tomar em resposta à ameaça.

(4) O operador deve, pelo menos uma vez por ano, verificar a adequação dos direitos de acesso sobre elementos críticos da rede ou atualizá-los sem demora em conformidade com as alterações na organização ou no lado dos prestadores de serviços de apoio de terceiro nível.

(5) O operador deve impedir a sua dependência de um fornecedor individual ou de um prestador de serviços de terceiro nível (ou seja, «aprisionamento do fornecedor»), sempre que tal seja tecnicamente viável e economicamente sustentável, com o objetivo de reduzir a dependência e aumentar a resiliência em caso de vulnerabilidades críticas dos componentes, evitando também contratos a longo prazo com fabricantes ou fornecedores individuais ou prestadores de serviços de apoio de terceiro nível, ou tendo a opção de os

alterar com o objetivo de reduzir as perturbações na prestação de serviços a entidades críticas ao nível mais baixo possível.

Artigo 7.º

(Condições contratuais com fabricantes, fornecedores ou prestadores de serviços de apoio de terceiro nível)

A fim de garantir um elevado nível de segurança, o operador deve incluir, pelo menos, os seguintes elementos em novos termos contratuais com fabricantes, fornecedores ou prestadores de serviços de apoio de terceiro nível:

1. uma declaração do fabricante ou do fornecedor de que o componente ou as suas predefinições não têm portas traseiras não documentadas ou qualquer impacto negativo no funcionamento das entidades fundamentais;
2. o compromisso do fabricante, do fornecedor ou do prestador de serviços de terceiro nível de proteger os dados de que tenham conhecimento durante a prestação de serviços ou o acesso aos mesmos no âmbito da prestação do serviço de acesso;
3. o compromisso do fabricante, do fornecedor ou do prestador de serviços de terceiro nível de informar imediatamente o operador em caso de violações da proteção dos dados de comunicações ou de tráfego que afetem ou possam afetar o operador ou as entidades críticas referidas no artigo 1.º, ponto 1, da presente lei geral;
4. o compromisso do fabricante, do fornecedor ou do prestador de serviços de terceiro nível de notificar imediatamente o operador de quaisquer incidentes de segurança e vulnerabilidades que possam afetar a segurança da rede, dos serviços associados ou dos dados do operador;
5. o compromisso do fabricante, do fornecedor ou do prestador de serviços de terceiro nível de cumprir as normas e regras de segurança estabelecidas pelo operador e de tomar medidas de segurança adequadas para garantir a segurança dos sistemas e redes de informação, bem como dos dados do operador ou da entidade fundamental;
6. capacidade do operador para rever os ambientes, procedimentos, medidas de segurança e ferramentas utilizados pelo prestador de serviços de apoio de terceiro nível ao aceder em qualquer momento à rede e aos dados do operador;
7. responsabilidade do fabricante, do fornecedor ou do prestador de serviços de apoio de terceiro nível pelos danos que seriam causados por vulnerabilidades identificadas ou pela utilização indevida de componentes de elementos fundamentais de rede, a sua definição por defeito ou durante a prestação de serviços de apoio de terceiro nível que o fabricante ou o fornecedor ou o prestador de apoio de terceiro nível negligenciaram ou deliberadamente implementaram;
8. a obrigação de formar regularmente o pessoal do fabricante, do fornecedor ou do prestador de serviços de apoio de terceiro nível no domínio da segurança dos dados e dos sistemas e redes de informação.

Artigo 8.º

(Regras relativas ao acesso e utilização de elementos fundamentais da rede)

(1) Ao aceder física ou logicamente aos componentes dos elementos fundamentais da rede, às suas definições e aos dados do operador neles armazenados, tratados ou modificados, o operador deve assegurar que:

PROPOSTA

1. o acesso é estritamente limitado a pessoas que tenham sido previamente autorizadas;
2. todos os trabalhos sobre elementos fundamentais da rede realizados no local ou através de acesso remoto são controlados pelo operador;
3. a autenticação multifatores é efetuada para utilizadores aos quais são atribuídos os mais elevados privilégios de direitos para aceder a componentes individuais de elementos críticos da rede, às suas definições ou aos dados aí armazenados ou tratados;
4. cada pessoa autorizada a quem o acesso é concedido tem uma conta de utilizador e uma palavra-passe únicas;
5. apenas são utilizadas palavras-passe que sejam alteradas regularmente ou imediatamente em caso de utilização indevida detetada e que contenham pelo menos 15 caracteres e incluam letras maiúsculas e minúsculas, números e caracteres especiais, se o software o permitir;
6. o conceito de tolerância zero ou de confiança é aplicado no acesso, sempre que possível;
7. a segurança da ligação de comunicação do utilizador autorizado aos componentes individuais é protegida pela utilização de cifragem, tendo em conta os mais recentes desenvolvimentos tecnológicos e as melhores boas práticas industriais no domínio da segurança da informação, ou recomendada por instituições estabelecidas no domínio da segurança da informação;
8. é efetuado um registo indelével dos acessos e das tentativas de acesso, que é mantido durante, pelo menos, 6 meses, incluindo uma cópia de segurança, mas pode também ser por um período mais longo, quando a análise da gestão dos riscos e a avaliação do nível aceitável de riscos demonstrarem que os riscos devem ser geridos de forma adequada, mantendo os registos por um período mais longo;
9. o registo e a monitorização de todas as intervenções de software em componentes são realizados sempre que possível, incluindo alterações de configuração. Os registos, incluindo uma cópia de segurança destes dados, devem ser conservados durante o período indicado no ponto anterior;
10. o acesso a componentes individuais e aos dados neles armazenados ou tratados é limitado no tempo e aberto apenas durante o período de trabalho necessário.

(2) Em caso de acesso a componentes individuais de elementos fundamentais da rede por parte do pessoal ou dos funcionários de um prestador de serviços de apoio de terceiro nível, estes devem:

1. utilizar apenas um posto de trabalho específico intermédio seguro («servidor de salto»), que será sujeito a controlos de segurança regulares;
2. instalar numa estação de trabalho dedicada apenas as ferramentas, componentes e serviços ativos absolutamente necessários para aceder a outros recursos na rede que são absolutamente necessários e que devem ser atualizados com as correções de segurança mais recentes;
3. utilizar operações criptográficas seguras e chaves numa estação de trabalho específica, que devem estar localizadas na rede do operador e estão sob o seu controlo exclusivo;
4. cada acesso é aprovado e ativado pelo operador manualmente e apenas durante o período de acesso;
5. todos os acessos e atividades são fisicamente controlados e registados pelo operador;

PROPOSTA

6. utilizar autenticação de dois fatores e palavras-passe com pelo menos 15 caracteres e incluir letras maiúsculas e minúsculas, números e caracteres especiais, que devem ser alterados com base nos riscos avaliados.

(3) Antes de transferir o serviço de gestão, manutenção ou atualização de elementos fundamentais da rede ou dos seus componentes individuais para terceiros, o operador deve verificar e assegurar que dispõe, pelo menos, dos mesmos ou melhores mecanismos de segurança e processos de gestão da segurança em comparação com os seus mecanismos e processos. Deve informar imediatamente a entidade crítica em causa, a Agência e o organismo responsável pela segurança da informação sobre a intenção de transferência.

(4) O operador deve verificar o estado real dos processos de segurança antes do início da prestação do serviço e, posteriormente, pelo menos uma vez por ano. O operador deve manter registos das revisões e controlos internos da prestação de serviços de apoio a terceiros e mantê-los durante o período de prestação dos serviços e durante um ano após a sua cessação, mas não superior a cinco anos.

DISPOSIÇÃO TRANSITÓRIA E FINAL

Artigo 9.º **(Disposições transitórias)**

(1) O operador deve notificar a Agência e o organismo responsável pela segurança da informação das localizações existentes dos elementos críticos da rede no prazo de 30 dias a contar da data de entrada em vigor da presente lei geral.

(2) O operador deve notificar a Agência e o organismo responsável pela segurança da informação das localizações existentes dos serviços de apoio de terceiro nível para elementos fundamentais da rede no prazo de 30 dias a contar da data de entrada em vigor da presente lei geral.

(3) A Agência publica pela primeira vez os documentos referidos no n.º 2 do artigo 3.º da presente lei geral a partir da data da sua entrada em vigor.

Artigo 10.º
(Entrada em vigor)

A presente lei geral entra em vigor no trigésimo dia após a sua publicação no *Jornal Oficial da República da Eslovénia*, nos termos do qual os operadores podem utilizar o equipamento e manter a prestação de serviços de apoio de terceiro nível até ao termo dos prazos especificados no artigo 312.º, n.ºs 2 e 3, da Lei.

Não _____

Mišmaš

Ljubljana, em _____

EVA 2023-3150-0034

mag. Marko

diretor

PROPOSTA

Anexo

Lista de elementos fundamentais da rede e sistemas de informação associados:

Elementos fundamentais da rede	Funcionalidades da rede e dos sistemas de informação
Gestão de assinantes e mecanismos de encriptação	<ul style="list-style-type: none">- Gestão da sessão (voz e dados),- autenticação de utilizadores e equipamentos com a rede,- gestão e armazenamento de chaves para autorização de assinantes e componentes de rede (UICC/eUICC, certificados digitais/HSM),- funções de autenticação segura, proteção da integridade da comunicação (encriptação) e armazenamento de chaves de utilizador, componentes de rede e de gestão,- gestão dos direitos de acesso.
Interligação	<ul style="list-style-type: none">- Alojamento de funcionalidades e interfaces com outras redes e serviços.
Serviços de rede geridos	<ul style="list-style-type: none">- Registo e autorização de serviços de rede,- armazenamento e tratamento dos dados de comunicação, localização e tráfego,- exposição das funções da rede e da rede a aplicações e serviços externos.
Gestão e orquestração de funções de rede virtualizadas (NFV) e orquestração de redes (MANO), incluindo infraestruturas de virtualização	<ul style="list-style-type: none">- Funções de gestão da orquestração e configuração de NFV, independentemente do tipo de implementação (VM, contentor, micro-serviços),- funções de virtualização para a implementação e utilização de NFV,- Função de Seleção de Cortes de Rede (NSSF)
Rede de acesso rádio	<ul style="list-style-type: none">- Estações de base que suportam tecnologia 5G ou superior.
Sistemas de gestão e outros sistemas de apoio	<ul style="list-style-type: none">- Monitorizar o funcionamento e a gestão da rede de comunicações móveis, incluindo a parte relativa ao acesso (RAN/O-RAN),- sistemas de deteção de incidentes de segurança, anomalias, ameaças e respetiva gestão (funções de segurança, incluindo SIEM/SOAR).
Interceção legal	<ul style="list-style-type: none">- Funções de acesso ao conteúdo da comunicação e aos dados sobre o tráfego dos utilizadores pela autoridade competente.