КОМЕНТАРИ НА ВИП ОПЕРАТОР и ОДГОВОР НА КОМЕНТАРИТЕ по Предлог Правилник за обезбедување на безбедност и интегритет на јавните електронски комуникациски мрежи и услуги и активности кои што операторите треба да ги превземат при нарушување на безбедност на личните податоци на претплатници

Број на член	Член, став од Правилникот	ПРЕДЛОГ забелешка, измена и/или дополнување со Коментар/Прашање/Обрзложение
Почетен дел од Правилникот	Врз основа на член 166 и 167 од Законот за елктронски комуникации ("Службен весник на Република Македонија" бр 39/2014), Директорот на Агенцијата за електронски комуникации и Директорот на Дирекцијата за заштита на личните податоци на ден _____ го донесоа:	**Предлог измена:** Врз основа на член 166 и 167 од Законот за елктронски комуникации ("Службен весник на Република Македонија" бр 39/2014), Директорот на Агенцијата за електронски комуникации на ден _____ го донесе: **Генерален коментар и образложение:** Во врска со начинот на донесување на овој Предлог Правилник, ставот на Вип оператор е дека донесување на подзаконски акт од страна на два органи е непознато дејство во правен систем во Република Македонија. Согласно член став (7) од член 167 од ЗЕК, Агенцијата во согласност со Дирекцијата за заштита на личните податоци ќе донесе подзаконски акт со кој ќе го пропише начинот во кој операторите се должни да ги спроведат одредбите од овој член, преку задолжителни инструкции, формата, содржината и начинот на доставување на известувањата утврдени со овој член и членот 167 од овој закон, како и формата и содржината на регистарот на нарушувањата на безбедноста на личните податоци и начинот на

		неговото водење од членот 167 став (6) од овој закон. На основа на тоа, овој Правилник го донесува Агенцијата, по претходно прибавена согласност од Дирекцијата за заштита на личните податоци односно Правилникот не треба да го донесуваат двата органи истовремено. Следствено, а во врска со начинот на кој Правилникот е донесен предлагаме корекција на текстот во целиот Правилник каде е потребно. АЕК и ДЗЛП ОДГОВОР: Во член 166 став 7 од Законот за електронски комуникации (Сл. весник 39/2014 и 188/2014) стои дека Агенцијата во согласност со Дирекцијата за заштита на личните податоци ќе го донесе овој подзаконски акт, што значи дека директорите на двете институции го донесуваат овој подзаконски акт.
Член 7	Операторите треба веднаш, но не подоцна од 13:00 часот од следниот работен ден од моментот на нарушување на безбедноста или губење на интегритетот кое имало значително влијание врз функционирањето на мрежите или услугите, да достават известување до Агенцијата за електронски комуникации по електронски пат на следната електронска адреса incident@aec.mk. Електронскиот меил со кој што операторот ќе ја извести Агенцијата за електронски комуникации треба да биде електронски потпишан. Доколку е тоа соодветно Агенцијата за електронски	**Предлог измена:** Операторите треба веднаш, но не подоцна од 24 часа од моментот на утврдување на нарушувањето на безбедноста или губење на интегритетот кое имало значително влијание врз функционирањето на мрежите или услугите, да достават известување до Агенцијата за електронски комуникации по електронски пат на следната електронска адреса incident@aec.mk. Електронскиот меил со кој што операторот ќе ја извести Агенцијата за електронски комуникации треба да биде електронски потпишан. Доколку е тоа соодветно Агенцијата за електронски комуникации за истото може да ги извести националните регулаторни тела од други

	комуникации за истото може да ги извести националните регулаторни тела од други земји, како и Европската агенцијата за безбедност на мрежи и информации (ENISA). Доколку истото е во интерес на јавноста, Агенцијата за електронски комуникации може да ја извести јавноста или да побара од операторот да го стори тоа. Исто така, доколку е тоа соодветно и во зависност од степенот на нарушување на безбедноста или интегритетот на мрежите или услугите, Агенцијата за електронски комуникации за истото ќе го извести и телото надлежно за справување со компјутерски инциденти во Република Македонија	земји, како и Европската агенцијата за безбедност на мрежи и информации (ENISA). Доколку истото е во интерес на јавноста, Агенцијата за електронски комуникации може да ја извести јавноста или да побара од операторот да го стори тоа. Исто така, доколку е тоа соодветно и во зависност од степенот на нарушување на безбедноста или интегритетот на мрежите или услугите, Агенцијата за електронски комуникации за истото ќе го извести и телото надлежно за справување со компјутерски инциденти во Република Македонија. **Образложение:** Вип оператор смета дека периодот за известување за нарушувањето на безбедноста или губење на интегритетот кое имало значително влијание врз функционирањето на мрежите или услугите во рок не подоцна од 13:00 часот од следниот работен ден е прекраток, поради што Вип оператор ја предлага погоренаведената измена. Дополнително, имајќи во предвид дека постои можност операторот да не биде свесен за нарушувањето на безбедноста или губење на интегритетот во реално време, предлагаме известувањето да се испраќа од моментот на утврдување на односното нарушување. Од друга страна, а на основа на точка 3.4 од "Technical Guideline on Incident Reporting"на "ENISA" од јануари 2013 година, Агенцијата треба да утврди што се подразбира под терминот "значително влијание".

		"Note that it is at the discretion of the NRA to determine what is significant. This ultimately depends on national circumstances. For example, a security incident affecting just a small number of users in a specific area could already be considered significant by an NRA." На основа на тоа, Вип оператор предлага Агенцијата да наведе конкретни примери или дефиниција за терминот "значително влијание", со цел операторите да имаат јасна слика во кои случаи е потребно да испраќаат известување. Исто така, за Вип оператор не е јасен терминот "соодветно" односно под кои критериуми ќе се утврдува соодветноста за Агенцијата за електронски комуникации да ги извести националните регулаторни тела од други земји, како и Европската агенцијата за безбедност на мрежи и информации (ENISA и телото надлежно за справување со компјутерски инциденти во Република Македонија. Имено, во оваа одредба, согласно овој субјективен критериум се наведени три начини на постапување на Агенцијата. Ставот на Вип оператор е дека соодветноста треба да се постави во корелација со некој објективен критериум со цел истото да не биде на целосна дискреција од страна на Агенцијата. АЕК и ДЗЛП ОДГОВОР: Член 166 став 4 стои дека Операторите се должни веднаш, но не подоцна од 24 часа од моментот на нарушување на безбедноста или губење на интегритетот кое имало значително влијание

		врз функционирањето на мрежите или услугите, по електронски пат на Агенцијата да и достават известување за истото. Рокот за известувањето во правилникот ќе биде променет согласно рокот дефиниран во Законот за електронски комуникации. Во член 10 од правилникот наведени се праговите според кои Операторите треба да ја известуваат Агенцијата за електронски комуникации за нарушувањата на безбедноста или губењето на интегритетот на мрежите. Тоа значи дека ова се праговите кои што се оденсуваат на Член 7 од правилникот. Овие прагови се дефинирани согласно точка 6.4.1 од Technical Guideline on Incident Reporting"на ENISA верзија 2.1 од октомври 2014 година. Направени се измени на правилникот во делот на известување до други земји по однос на нарушувањата на безбедноста на мрежите– "Доколку нарушувањето на безбедноста може негативно да влијае на корисниците од други земји Агенцијата за електронски комуникации за истото нарушување може да ги извести националните регулаторни тела од засегнатите други земји. Агенцијата ќе направи процена дали ќе го извести телото надлежно за справување со компјутерски инциденти во Република Македонија по однос на нарушувањето на безбедноста или губење на интегритетот кое имало значително влијание врз функционирањето на мрежите или услугите на операторите.

Член 9	Во случај на значителен ризик од повреда на безбедноста на мрежата, операторот на јавни електронски комуникациски услуги треба да ги информира претплатниците за таквиот ризик и доколку истиот е надвор од опсегот на мерки кои ги презема операторот, да ги информира и за можните решенија за отстранување на ризикот како и за можните трошоци за таквите решенија. Информирањето до претплатниците операторот може да го стори на еден од следните начини: •Преку неговата веб страна, •Преку сопствен телевизиски канал на операторот, •Преку електронска порака, •Преку СМС порака, •Преку останатите медиуми за јавно информирање.	**Предлог измена:** Во случај на значителен ризик од повреда на безбедноста на мрежата, операторот на јавни електронски комуникациски услуги треба да ги информира претплатниците за таквиот ризик и доколку истиот е надвор од опсегот на мерки кои ги презема операторот, да ги информира и за можните решенија за отстранување на ризикот како и за можните трошоци за таквите решенија, веднаш, но не подоцна од 24 часа по утврдување на значителен ризик од повреда на безбедноста на мрежата. Информирањето до претплатниците операторот може да го стори на еден од следните начини: •Преку неговата веб страна, •Преку сопствен телевизиски канал на операторот, •Преку електронска порака, •Преку СМС порака, •Преку останатите медиуми за јавно информирање. **Образложение:** На основа на погоренаведениот коментар, Вип оператор смета дека и во овој случај е потребно Агенцијата да специфицира и дефинира што се подразбира под терминот "значителен ризик". Имено, доколку нема конректна дефиниција за овој термин, постои можност секој оператор различно да квалификува одреден инцидент односно инцидент со низок ризик, додека пак Агенцијата истиот да го квалификува за инцидент со значителен ризик.

		Дополнително, со цел обврската за известување да произлезе по утврдувањето на значителниот ризик од повреда на безбедноста на мрежата, Вип оператор го предлага погоренаведеното дополнување, како реален период во кој известувањето треба да се реализира. АЕК и ДЗЛП ОДГОВОР: Предлогот за воведувањето на рокот во овој член се смета за прифатлив и ќе се направат соодветни измени на правилникот. Членот 9 од правилникот кој што се однесува на информирањето на претплатниците во случај на "значителен ризик од повреда на безбедноста на мрежата", ќе се преформулира на следниот начин: "Во случај на значителен ризик од повреда на безбедноста на мрежата, веднаш но не подоцна од 24 часа од моментот на утврдување на значителен ризик од повреда на безбедноста на мрежата, доколку операторот смета дека е од јавен интерес претплатниците да бидат запознати со ризикот треба да ги информира претплатниците за таквиот ризик и доколку истиот е надвор од опсегот на мерки кои ги презема операторот, да ги информира и за можните решенија за отстранување на ризикот како и за можните трошоци за таквите решенија. Информирањето до претплатниците операторот може да го стори на еден од следните начини преку: - неговата веб страна, - сопствен телевизиски канал на операторот, - електронска порака, - СМС порака, - други медиуми за јавно информирање."

Член 10	Операторите треба да ја известуваат Агенцијата за електронски комуникации за нарушувањата на безбедноста или губењето на интегритетот на мрежите согласно следните прагови: •Нарушувањето трае повеќе од 1 час, и процентот на засегнати корисници е повеќе од 15 %; •Нарушувањето трае повеќе од 2 часа, и процентот на засегнати корисници е повеќе од 10; •Нарушувањето трае повеќе од 4 часа, и процентот на засегнати корисници е повеќе од 5 %; •Нарушувањето трае повеќе од 6 часа, и процентот на засегнати корисници е повеќе од 2%, или ако •Нарушувањето трае повеќе од 8 часа, и процентот на засегнати корисници е повеќе од 1 %	Операторите треба да ја известуваат Агенцијата за електронски комуникации за нарушувањата на безбедноста или губењето на интегритетот на мрежите согласно следните прагови: •Нарушувањето трае повеќе од 1 час, и процентот на засегнати корисници е повеќе од 15 %; •Нарушувањето трае повеќе од 2 часа, и процентот на засегнати корисници е повеќе од 10; •Нарушувањето трае повеќе од 4 часа, и процентот на засегнати корисници е повеќе од 5 %; **Образложение:** Вип оператор смета дека е потребно прецизно да биде наведено дали праговите утврдени во овој член се однесуваат на терминитe "значително влијание" од член 7 и "значителен ризик" од член 9. Дополнително, Вип оператор смета дека последните 2 прага дефинираат премногу детална категоризација, особено ако станува збор за интегритет на мрежи, поради што предлагаме да се избришат. Така, истото во пракса би значело дека и при најмали испади, ќе биде потребно да се испраќа известување. Од друга страна, сметаме дека е потребно во случајот за мобилна телефонија да се наведе дали е потребно сметањето да се реализира по технологија или пак сумарно, особено што е невозможно да се утврди точен број или уште повеќе листа на афектирани претплатници, кога има

		испад на само една технологија. АЕК ОДГОВОР: Коментарот не се прифаќа бидејќи овие прагови се дефинирани согласно точка 6.4.1 од Technical Guideline on Incident Reporting"на ENISA верзија 2.1 од октомври 2014 година.
Член 13, точка 1	Во случај на нарушување на безбедноста на личните податоци, операторот на јавни електронски комуникациски услуги, е должен веднаш, но не подоцна од 13:00 часот од следниот работен ден од моментот на утврдување на нарушувањето на безбедноста на личните податоци, да достави до Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци известување за нарушување на безбедноста на личните податоци	**Предлог измена:** Во случај на нарушување на безбедноста на личните податоци, операторот на јавни електронски комуникациски услуги, е должен веднаш, но не подоцна од 24 часа од моментот на утврдување на нарушувањето на безбедноста на личните податоци, да достави до Дирекцијата за заштита на личните податоциизвестување за нарушување на безбедноста на личните податоци **Образложение:** На основа на наведеното во рамки на точка 2 од член 2 од "COMMISSION REGULATION (EU) No 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications" од 24.06.2013 година, Вип оператор ја предлага погоренаведената измена. *"2. The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible."* Вип оператор смета дека најефикасен начин за

		известување е доколку известувањето се насочи кон една точка за контакт со цел да се избегнат грешки при практична имплементација. Така, аналогно на начинот на известување при нарушување на безбедност и интегритет на мрежи каде се известува само Агенциајата, за сите случаи за нарушување на безбедност на лични податоци треба да се известува само и единствено Дирекцијата за заштита на личните податоци, имајќи во предвид дека тоа тело е надлежно за овој тип на податоци. АЕК ОДГОВОР: Предлогот за рокот на известување е прифатлив и соодветно ќе биде направена измана на правилникот. Согласно Член 167 став 1 известувањето треба да биде направено до двете институции – така до вториот предлог не е прифатлив.
Член 14, точка 1	1. Ако нарушувањето на безбедноста на личните податоци може негативно да влијае на личните податоци или приватноста на претплатникот или на друго физичко лице, операторот на јавни електронски комуникациски услуги е должен дополнително на известувањето од член 13 на овој правилник да го извести односниот претплатник или физичкото лице.	**Коментар:** Во врска со наведеното во овој член би сакале да посочиме дека операторот, не може со сигурност да знае дали нарушувањето на безбедноста на личните податоци може негативно да влијае на личните податоци или приватноста на претплатникот или на друго физичко лице односно сметаме дека оваа обврска е неприменлива во пракса, односно истото е надвор од контрола на операторот. Често и при нарушување на интегритетот и при нарушување на безбедноста на јавните мобилни комуникациски мрежи, операторот нема можност да обезбеди точен податок конкретно кои претплатници и во која мерка се афектирани од инцидентот, а уште помалку да има информација дали тоа негативно влијае на личните

		податоци и приватноста. На основа на тоа, предлагаме експлицитно да се наведе дека оваа обврска не важи односно не е применлива за јавна мобилна комуникациска мрежа. АЕК ОДГОВОР: Предлогот не е прифатлив, одредбата во правилникот е согласно Член 167 став 2 од ЗЕК. Оценката дали нарушувањето на безбедноста на личните податоци може негативно да влијае на личните податоци или приватноста на претплатникот или на друго физичко лице е образложена во член 14 став 4. Член 14 е во согласност со Article 3 на COMMISSION REGULATION (EU) No 611/2013 of 24 June 2013 - on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications
Член 14, став 2	2. Операторот треба известувањето од став (1) на овој член да го направи веднаш, но не подоцна од 13:00 часот од следниот работен ден од моментот на утврдување на нарушувањето на безбедноста на личните податоци.	**Предлог измена:** 2. Операторот треба известувањето од став (1) на овој член да го направи веднаш, но не подоцна од 24 часа од моментот на утврдување на нарушувањето на безбедноста на личните податоци. **Образложение:** На основа на наведеното во став 3 од член 3 од "COMMISSION REGULATION (EU) No 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications" од 24.06.2013 година, Вип оператор ја

		предлага наведената измена. *"3. The notification to the subscriber or individual shall be made without undue delay after the detection of the personal data breach, as set out in the third subparagraph of Article 2(2). That shall not be dependent on the notification of the personal data breach to the competent national authority, referred to in Article 2."* *2. The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible.* АЕК ОДГОВОР: Забелешката се прифаќа.
Член 14, точка 4	4. Операторот треба да направи процена дали нарушувањето на безбедноста на личните податоци може негативно да влијае на личните податоци или приватноста на претплатникот или на друго физичко лице, при што особено треба да ги земе во предвид следните околности: - Природата и содржината на личните податоци кои што се засегнати со безбедносниот инцидент се од финансиска природа, податоци за локацијата на претплатникот или физичкото лице, фајлови за интернет записи (eng. log), историја на веб прелистувач, податоци за електронски пораки, детални сметки за повиците како и специјални категории на податоци како што се од расно или етничко потекло, политички мислења,	**Предлог измена:** 4. Операторот треба да направи процена дали нарушувањето на безбедноста на личните податоци може негативно да влијае на личните податоци или приватноста на претплатникот или на друго физичко лице, при што особено треба да ги земе во предвид следните околности: - Природата и содржината на личните податоци кои што се засегнати со безбедносниот инцидент се од финансиска природа, податоци за локацијата на претплатникот или физичкото лице, фајлови за интернет записи (eng. log), историја на веб прелистувач, податоци за електронски пораки, детални сметки за повиците, - Последиците од нарушувањето на безбедноста на личните податоци по претплатникот или физичкото лице може да доведат до злоупотреба на идентитетот

	религиозни и филозофски верувања, како и податоци кои што се однесуваат на здравјето и сексуалниот живот, - Последиците од нарушувањето на безбедноста на личните податоци по претплатникот или физичкото лице може да доведат до злоупотреба на идентитетот (eng. identity theft) или измама, физичка штета, психолошка болка, понижување или штета на угледот и, - Услови во кои што нарушувањето на безбедноста на личните податоци доведува податоците да бидат украдени или операторот знае за трето лице кои што ги поседува овие податоци на неавторизиран начин.	(eng. identity theft) или измама, физичка штета, психолошка болка, понижување или штета на угледот и, - Услови во кои што нарушувањето на безбедноста на личните податоци доведува податоците да бидат украдени или операторот знае за трето лице кои што ги поседува овие податоци на неавторизиран начин. **Образложение:** Во врска со оваа обврска би сакале да посочиме дека операторот нема можност секогаш точно да процени за што ќе може да се искористатат компромитираните/украдените податоци, често и што е точно компромитирано и конкретно за кои претплатници. Дополнително, а на основа на дефинираното во рамки на точка а) од став 3 од член 3 од "COMMISSION REGULATION (EU) No 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications" од 24.06.2013 година, Вип оператор предлага бришење на дополнителните околности кои треба да бидат земени во предвид а кои се наведени во алинеја 1 од овој став. *"(a) the nature and content of the personal data concerned, in particular where the data concerns financial information, special categories of data referred to in Article 8(1) of Directive 95/46/EC, as well as location data, internet log files, web browsing histories, e-mail data, and itemised call*

		lists;" *АЕК ОДГОВОР: Забелешката не се прифаќа.* *Article 3(2), point a of COMMISSION REGULATION (EU) No 611/2013 of 24 June 2013 - on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.* *"the nature and content of the personal data concerned, in particular where the data concerns financial information, special categories of data referred to in Article 8(1) of Directive 95/46/EC, as well as location data, internet log files, web browsing histories, e-mail data, and itemised call lists;"* *Article 8(1) of Directive 95/46/EC-* *1 . Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life .*
Член 14, став 5	5. Известувањето до претплатникот или физичкото лице треба да ги содржи информациите од Прилог 3, што е составен дел на овој правилник. Известувањето до претплатникот или физичкото лице треба да биде изразена на јасен и лесно разбирлив јазик. При известувањето операторот не треба	**Предлог измена:** 5. Известувањето до претплатникот или физичкото лице треба да ги содржи информациите од Прилог 3, што е составен дел на овој правилник. Известувањето до претплатникот или физичкото лице треба да биде изразена на јасен и лесно разбирлив јазик. При известувањето операторот треба да ја искористи

	да ја искористи можноста да промовира и рекламира нови и дополнителни сервиси.	можноста да промовира и рекламира нови и дополнителни сервиси, доколку истите овозможат зголемување на безбедноста. **Образложение:** Вип оператор смета дека промовирањето на нови и дополнителни сервиси ќе придонесе до зголемување на нивото на безбедност, поради што го предлагаме погоренаведеното дополнување како неопходно. АЕК И ДЗЛП ОДГОВОР:: Забелешката не се прифаќа. COMMISSION REGULATION (EU) No 611/2013 – Art 3(4) - The provider shall include in its notification to the subscriber or individual the information set out in Annex II. The notification to the subscriber or individual shall be expressed in a clear and easily understandable language. The provider shall not use the notification as an opportunity to promote or advertise new or additional services.
Член 18	Агенцијата за електронски комуникации може да направи проверка на мерките кои што операторите ги прават за обезбедување на безбедност и интегритет на јавните електронски комуникациски мрежи и услуги, така што од операторите може да бара: а) да и достават потребни информации за процена на безбедноста и/или интегритетот на нивните услуги и мрежи, вклучително и усвоените политики за безбедност и б) да обезбедат безбедносна ревизија која ја	**Коментар:** Вип оператор смета дека е нејасна обврската операторот да се изложува на овој тип на трошок. Доколку Агенцијата смета дека е потребна ревизија на мерките кои што операторите ги превземаат за цели на обезбедување на безбедност и интегритет на јавните електронски комуникациски мрежи и услуги, сметаме дека товарот треба да падне на страна на Агенцијата. Имено, ваков тип на ревизија може да се прави неколку пати годишно или пак на месечна основа, поради што ставот на Вип оператор е дека овој тип на

	врши квалификувано независно тело или надлежен државен орган и резултатите од истата да ги направат достапни за Агенцијата за електронски комуникации. Трошоците за ревизијата ги плаќа операторот.	трошок е непотребно оптоварување на страна на операторите, покрај трошоците кои веќе се реализирани за цели на донесување на мерките за безбедност и интегритет на јавните електронски комуникациски мрежи и услуги. Дополнително, предлагаме да се утврди и разумен период за спроведување на ревизијата на секои две години. АЕК И ДЗЛП ОДГОВОР: Забелешката не се прифаќа. Согласно ЗЕК Член 166(8) трошоците за ревизија ги плаќа операторот.