ПРЕДЛОГ ИЗМЕНИ И КОМЕНТАРИ НА ПРАВИЛНИКОТ 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 БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ НА ПРЕТПЛАТНИЦИТЕ

Табела со предлог измени, дополни, коментари и образложенија на понапред наведениот Правилник:

Реден број на членот	**Предлог измени на Македонски Телеком и Т-Мобиле Македонија**	**Коментари и образложенија**
Член 1	Со овој правилник се пропишува: • начинот на кој што операторите треба да ги обезбедуваат безбедноста и интегритетот на јавните електронски комуникациски мрежи што има значително влијание врз функционирањето на електронската комуникациска мрежа или услуги, • начинот на доставување на известувањето на операторите до Агенцијата за електронски комуникации во случај на нарушување на безбедноста кој предизвикал губење на интегритетот кое имало значително влијание врз функционирањето на мрежите или услугите, • начинот на кој што Агенцијата за електронски комуникации ќе известува за нарушувањата на безбедноста на мрежите на операторите до Европската агенција за безбедност на мрежи и информации (ENISA), • активностите кои што операторите треба да ги превземат при нарушување на безбедноста на личните податоци на претплатниците, како и • формата и содржината на регистарот на нарушувањата на безбедноста на личните податоци и начинот на неговото водење.	Предлагаме допрецизирање на термините безбедност и интегритет на јавните комуникациски мрежи во насока на дефинирање на нарушувањето. Имено, сите оператори секојдневно се соочуваат со проблеми поврзани со безбедноста и интегритетот на нивните мрежи (кои успешно ги надминуваат) затоа сметаме дека од значење за овој Правилник би требало да бидат само оние нарушувања кои имаат значително влијание врз функционирањето на електронската комуникациска мрежа и кои предизвикуваат губење на интегритетот на јавните комуникациски мрежи, следствено обврската за известување на Агенцијата за електронски комуникации (во

		понатамошниот текст: АЕК) да се однесува само за нив. АЕК и ДЗЛП: Предлогот не се прифаќа. Одредбите на овој член се согласно Законот за електронски комуникации. Безбедност и интегритет на јавни електронски комуникациски мрежи се два различни поими дефинирани во член 2 на овој правилник иако според овие дефиниции нарушувањето на интегритетот значи нарушување и на безбедноста на јавните електронски комуникациски мрежи.
Член 2	Во овој правилник покрај дефинициите од Законот за електронски комуникации и Закон за заштита на личните податоци се користат и следните дефиниции: • Компјутерски инцидент: Напад на безбедноста кој предизвикал губење на интегритетот што има значително влијание врз оперирањето на електронската комуникациска мрежа или услуга. • Интегритет на јавните електронски комуникациски мрежи: Можност на системот да ги зачува специфичните карактеристики во однос на перформансите и функционалностите. Најчесто интегритетот на мрежите се смета за достапност или континуитет на сите информациски безбедносни системи. • Безбедност на јавните електронски комуникациски мрежи: зачувавање на доверливоста, интегритетот и достапноста на мрежите.	Предлагаме допрецизирање на нарушувањето согласно погоре наведеното објаснување. Дополнително, губиток на интегритет на комуникациска мрежа може да настане и поради други причини, (на пр. прекин во напојување на уредите, или прекин на опремата поради поплава на внатрешна водоводна инсталација и сл.). Дали овие инциденти влегуваат тука? Ако влегуваат, тогаш терминот “Компјутерски“ инцидент не е најсоодветен, бидејќи асоцира исклучиво на компјутери. (Истата терминологија е и во Прилог 1).

		Сметаме дека поимите „интегритет на јавни електронска комуникациски мрежи“ и „безбедност на јавните електронски комуникациски мрежи“ содржат многу сличности односно преклопувања во предложените дефиниции. Сметаме дека е корисно да се избегне вакво нешто. Предлагаме втората реченица од поимот интегритет на мрежи целосно да се избрише, или да гласи: „Под интегритет на мрежите најчесто се подразбира достапност или континуитет на сите информациски безбедносни системи“, но во вториов случај би постоела сличност со дефиницијата за „безбедност на јавните електронски комуникациски мрежи“ АЕК и ДЗЛП: Предлогот делумно се прифаќа. Терминот компјутерски инцидент ќе биде преименуван во безбедносен инцидент. Дефиницијата за безбедносен инцидент ќе биде дефинирана согласно договорената дефиниција на јавната расправа: Безбедносен инциден: Нарушување на безбедноста што има значително влијание врз оперирањето на електронската комуникациска мрежа или

		услуга. Дефиницијата за безбедност на јавни електронски комуникациски мрежи ќе биде оставена бидејќи има пошироко значење од дефиницијата за интегритет на јавните електронски комуникациски мрежи.
Член 6	Политиките за безбедност кои што треба да ги усвојат операторите согласно член 5 треба да го опфатат минимум следните подрачја: • Менаџирање со генералните безбедносни ризици, • Заштита на крајните корисници, • Одржување на достапност на мрежата, • Безбедност и интегритет на податоците.	Доколку ова се однесува на мрежите на другите оператори со кои имаме интерконекција, оваа точка би требало да се избрише бидејќи секој оператор е одговорен за заштита на сопствената мрежата. Сметаме дека е потребно дефинирање на терминот интегритет на податоци. АЕК и ДЗЛП: Предлогот делумно се прифаќа. “Заштита на интерконектирани мрежи” ќе се избрише. Под интегритет на податоците се подразбира зачувување на точноста и конзистентност на податоци. Дополнително “Безбедност и интегритет на податоци” ќе биде преформулиран во “Безбедност и интегритет на личните податоци”

Четврто поглавје	ИЗВЕСТУВАЊА ЗА НАСТАНАТИ НАРУШУВАЊА НА БЕЗБЕДНОСТА И ГУБЕЊЕ НА ИНТЕГРИТЕТОТ НА МРЕЖИТЕ НА ОПЕРАТОРИТЕ	
Член 7	Операторите треба веднаш, но не подоцна од 13:00 часот од следниот работен ден од моментот на нарушување на безбедноста кој предизвикал 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 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 и 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.	Предлагаме допрецизирање на нарушувањето согласно погоре наведеното објаснување. Агенцијата да ја појасни процедурата за електронско потпишување на е-маил. Дали се очекува електронската пошта да биде потпишана од законскиот застапник на операторот или од лице овластено од законскиот застапник. Ве молиме за посочување на релевантен документ во кој е дефинирано во кои случаи односно за какви инциденти АЕК би информирала други национални регулаторни тела и ENISA. Сметаме дека проблематиката третирана во овој Правилник упатува на тоа дека тој е во надлежност на „телото надлежно за справување со компјутерски инциденти во Република Македонија“ т.е. посебната организациона единица MKD-CIRT која е во фаза на формирање во склоп на АЕК. Но, наведеното во последната реченица од член 7 укажува дека некој друг во АЕК е надлежен за ова, па оттаму ве молиме за појаснување кој сектор во АЕК ќе е надлежен за e-mail адресата incident@aec.mk и кои се неговите

		ингеренции, а кои на MKD-CIRT. АЕК и ДЗЛП: Предлогот делумно се прифаќа. На дискусијата беше појаснето дека електронската пошта треба да биде потпишана од одговорното лице на операторот. Потпишувањето треба да биде направено со сертификат добиен од овластен СА во МК. Безбедност и интегритет на јавни електронски комуникациски мрежи се два различни поими дефинирани во член 2 на овој правилник иако според овие дефиниции нарушувањето на интегритетот значи нарушување и на безбедноста на јавните електронски комуникациски мрежи.
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.	Што се подразбира под поимот значителен ризик? Сметаме дека е потребно дефинирање на поимот значителен ризик во смисла на овој Правилник. АЕК:Предлогот е делумно прифатлив. Членот ќе биде променет како што следи-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 кој предизвикал губење на интегритетот кое имало значително влијание врз функционирањето на мрежите согласно следните прагови: • Нарушувањето трае повеќе од 1 час, и процентот на засегнати корисници е повеќе од 15 % од вкупниот број на корисници на операторот; • Нарушувањето трае повеќе од 2 часа, и процентот на засегнати корисници е повеќе од 10 % од вкупниот број на корисници на операторот; • Нарушувањето трае повеќе од 4 часа, и процентот на засегнати корисници е повеќе од 5 % од вкупниот број на корисници на операторот; • Нарушувањето трае повеќе од 6 часа, и процентот на засегнати корисници е повеќе од 2% од вкупниот број на корисници на операторот, или ако • Нарушувањето трае повеќе од 8 часа, и процентот на засегнати корисници е повеќе од 1 % од вкупниот број на корисници на операторот.	Предлагаме прецизирање на процентот на засегнати корисници, со дополнување на одредбите со зборовите “од вкупниот број на корисници на операторот”. АЕК и ДЗЛП:Предлогот е делумно прифатлив. Првата забелешка не е прифатлива бидејќи безбедност и интегритет на јавни електронски комуникациски мрежи се два различни поими дефинирани во член

		2 на овој правилник иако според овие дефиниции нарушувањето на интегритетот значи нарушување и на безбедноста на јавните електронски комуникациски мрежи. Забелешката дека процентот треба да се однесува на вкупниот број на корисници на операторот е прифатлива.
Член 12	При известувањата за настанати нарушувања на безбедноста кои предизвикале губење на интегритетот на мрежите на операторите, согласно член 7 од овој правилник, истите треба да го користат образецот дефиниран во Прилог 1, кој е составен дел на овој правилник.	Предлагаме допрецизирање на нарушувањето согласно погоре наведеното објаснување. АЕК и ДЗЛП: Предлогот не се прифаќа. Безбедност и интегритет на јавни електронски комуникациски мрежи се два различни поими дефинирани во член 2 на овој правилник иако според овие дефиниции нарушувањето на интегритетот значи нарушување и на безбедноста на јавните електронски комуникациски мрежи.
Член 13 став 1, став 4	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. 4. Се смета дека операторот го детектирал нарушувањето на безбедноста на личните податоци во моментот кога операторот ќе стекне доволно знаење дека е	Што се подразбира под поимот безбедност на лични податоци? Сметаме дека е потребно дефинирање на терминот безбедност на лични податоци во смисла на овој Правилник. Поимот компромитација не е доволно јасен, Ве молиме за прецизирање на истиот.

	настанат безбедносен инцидент кој што води до компромитација на личните податоци на претплатниците.	АЕК и ДЗЛП: Коментарите делумно се прифаќаат. Дефиницијата за нарушување на безбедност на лични податоци е формулирана во ЗЕК. дефиниција- Нарушување на безбедност на личните податоци е нарушување што доведува до случајно или незаконско уништување, губење, промена, неовластено откривање или пристап до лични податоци кои се пренесуваат, чуваат или на друг начин се обработуваат во врска со обезбедувањето на јавни електронски комуникациски услуги; Ставот ќе биде сменет во - Се смета дека операторот го открил нарушувањето на безбедноста на личните податоци во моментот кога операторот ќе стекне доволно знаење дека е настанат безбедносен инцидент кој што довел до случајно или незаконско уништување, губење, промена, неовластено откривање или пристап до личните податоци на претплатникот или на друго физичко лице.
Член 14	1. Ако нарушувањето на безбедноста на личните податоци може негативно да влијае на личните податоци или приватноста на претплатникот, операторот на	Сметаме дека терминот или друго физичко лице треба да се избрише,

	јавни електронски комуникациски услуги е должен дополнително на известувањето од член 13 на овој правилник да го извести односниот претплатник. 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. 3. Се смета дека операторот го детектирал нарушувањето на безбедноста на личните податоци во моментот кога операторот ќе стекне доволно знаење дека е настанат безбедносен инцидент кој што води до компромитација на личните податоци на претплатниците. 4. Операторот треба да направи процена дали нарушувањето на безбедноста на личните податоци може негативно да влијае на личните податоци или приватноста на претплатникот, при што особено треба да ги земе во предвид следните околности: - Природата и содржината на личните податоци кои што се засегнати со безбедносниот инцидент дали истите се од финансиска природа, податоци за локацијата на претплатникот, 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, 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 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. 5. Известувањето до претплатникот треба да ги содржи информациите од Прилог 3, што е составен дел на овој правилник. Известувањето до претплатникот треба да биде изразена на јасен и лесно разбирлив јазик. При известувањето операторот не треба да ја искористи можноста да промовира и	бидејќи операторот располага со личните податоци само на сопствените претплатници. Одговорноста на операторот да се ограничи само на безбедноста на податоците на неговите претплатниците. АЕК и ДЗЛП:: Коментарот не се прифаќа Во “COMMISSION REGULATION (EU) 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” се употребуваат термините: subscriber or individual

	рекламира нови и дополнителни сервиси. 6. Во исклучителни околности, кога известувањето до претплатникот или физичкото лице може да ја стави во ризик правилната истрага во однос на нарушувањето на безбедноста на личните податоци, оперторот по добиена согласност од Агенцијата за електронски комуникации или Дирекцијата за заштита на личните податоци може да го одложи известувањето до претплатникот. По завршувањето на оваа истрага операторот треба да го извести претплатникот најбрзо што може. 7. Операторот треба да го извести претплатникот за настанатото нарушување на безбедноста на личните податоци преку комуникација која обезбедува брз прием на информациите од страна на претплатникот или физичкото лице и која комуникација е соодветно безбедна. Информациите треба да се однесуваат само за нарушувањето на безбедноста на личните податоци. 8. Доколку операторот што има директни договорни односи со крајните корисници, во временската рамка дефинирана во став 1 од овој член не може успешно да ги идентификува сите лица кои што имаат негативни ефекти од нарушувањето на безбедноста на личните податоци , тогаш операторот треба да ги извести овие лица преку некој национален или регионален медиум во истата временската рамка дефинирана во став 1 од овој член. Ова известување до медиумите треба да ги содржи информациите од Прилог 3 на овој правилник или информаците може да бидат објавени во скратена форма доколку тоа е потребно. Во овој случај, операторот треба најбрзо што може да ги направи сите напори за да ги идентификува лицата на кои им е нарушена безбедноста на лични податоци и да ги извести со информациите согласно Прилог 3.	
Член 15	1. Операторот не мора да го извести претплатникот за нарушувањето на безбедноста на личните податоци согласно член 14 на овој правилник, доколку операторот покаже пред Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци дека има имплементирано соодветни технички заштитни мерки и дека овие мерки се применети на податоците чија безбедност е нарушена. Ваквите технички заштитни мерки треба ги направат податоците нереазбирливи и нејасни на било кое лице кое што нема авторизиран пристап до истите.	Сметаме дека терминот или друго физичко лице треба да се избрише, бидејќи операторот располага со личните податоци само на сопствените претплатници. Одговорноста на операторот да се ограничи само на безбедноста на податоците на неговите претплатниците

	2. Податоците се смета дека се неразбирливи и нејасни за било кое лице кое што нема авторизиран пристап до истите доколку: - Истите се безбедносно енкриптирани со стандарден алгоритам, и безбедносните клучеви за декриптирање не се копмромитирани преку некој безбедносен пробив, како и тоа дека клучот за декриптирање на податоците е генериран на начин за да не може да биде дознаен преку расположливите технички алатки од било кое лице кое што не е авторизиран за пристап до клучот, - Се заменети со нивна хеширана (eng. hash) вредност генерирана со стандардна криптографска функција со клучеви, клучевите кои што се користат за да се хешираат(eng. hash) податодите не се копмромитирани преку некој безбедносен пробив, како и тоа дека клучот кој што се користи за хеширање(eng. hash) на податодите е генериран на начин за да не може да биде дознаен преку расположливите технички алатки од било кое лице кое што не е авторизиран за пристап до клучот.	АЕК и ДЗЛП: Коментарот не се прифаќа
Член 17	(1) Доколку испорачувањето на електронската комуникциска услуга се реализира преку друг оператор кој што нема директен претплатнички договор со крајниот корисник, одговорноста за отстранување на нарушувањето на безбедноста на личните податоци од корисникот е на страната на овој оператор кој треба веднаш да преземе соодветни мерки за истражување и решавање на проблемот,како и да го извести операторот кој што има склучено претплатнички договор со претплатникот за преземените мерки. (2) Квалитетот на испорачаната електронската комуникациска услуга од оригинирачката претплатничка пристапна точка од која потекнува повикот до Пристапната точка за интерконекција каде што терминира повикот, е одговорност на страната од каде што потекнува повикот (без оглед дали причината за нарушување на квалитетот се наоѓа во неговата мрежа или пак во мрежа на некоја трета страна инволвирана во преносот на сообраќајот).	Предлагаме допрецизирање на одредбата во насока на тоа одговорноста за отстранување на нарушувањето на безбедноста на личните податоци на корисникот да биде на страната на операторот кој ја испорачува електронската комуникациска услуга бидејќи услугата која ја пренесува операторот доаѓа од трета страна со која задолжително треба да ги уреди односите како страна со која има склучено директен договор.. Операторот кој ја испорачува електронска комуникациска услуга е должена да ги преземе сите расположливи мерки за истражување и решавање на настанатиот проблем и за

		истото да го извести операторот со кој крајниот корисник има директен претплатнички договор. АЕК и ДЗЛП: Коментарот не се прифаќа. COMMISSION REGULATION (EU) 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 Article 5 Use of another provider Where another provider is contracted to deliver part of the electronic communications service without having a direct contractual relationship with subscribers, this other provider shall immediately inform the contracting provider in the case of a personal data breach.
Прилог1, 2 и 3		Општа забелешка е дека во самите прилози треба да е наведено кој прилог до кој орган се праќа. incident@aec.mk, и/или incident@privacy.mk. Во однос на Прилог 3 не е јасно како надлежните ќе имаат контрола и евиденција дали и што операторот пратил до претплатникот. АЕК и ДЗЛП – Забелешките делумно се

		прифаќаат. Прилозите ќе бидаат соодветно променети за да се знае до која институција кој прилог се испраќа. Контролата и евиденцијата дали и што операторот пратил до претплатникот ќе се прави при стручниот надзор.
Прилог 1: Образец за известување е компјутерски инциденти		Предлагаме во Прилог 1 да бидат наведени e-mail адресите на кои треба да се испрати истиот. Сметаме дека последното поле во образецот со назив „Научени лекции“ е несоодветно и предлагаме истото треба да се избрише. АЕК и ДЗЛП – Забелешките делумно се прифаќаат. Прилозите ќе бидаат соодветно променети за да се знае до која институција кој прилог се испраќа. Научените лекции се обврски согласно регулативата COMMISSION REGULATION (EU) 611/2013 - 24 June 2013.
Прилог 2. Содржина на известувањето за нарушувањето на безбедноста на личните		Предлагаме во Прилог 2 да бидат наведени e-mail адресите на кои треба да се испрати истиот. АЕК и ДЗЛП – Забелешките се прифаќаат. Прилозите ќе бидаат соодветно променети за да се знае до која институција кој прилог се испраќа.

податоци што операторот и доставува до националните регулаторни тела		
Прилог 3. Содржина на известувањето за нарушување на безбедноста на личните податоци што операторот го доставува до претплатникот или физичкото лице		Предлагаме во Прилог 3 да бидат наведени e-mail адресите на кои треба да се испрати истиот Сметаме дека референцирањето на член 13 став 2 во полето со назив „Природа и содржина на засегнатите лични податоци“ е погрешно, бидејќи во него е предвидено известување до АЕК и ДЗЛП, а овој Прилог се однесува на известување до претплатник. Бараме да биде референцирана соодветна одредба што според наше мислење е член 14 став 5. Сметаме дека полето со назив „Применети технички и организациони мерки (или што ќе се применат) од операторот во однос на засегнатите лични податоци“ е несоодветно за овој образец, бидејќи не ја гледаме вредноста од ваквата информација за претплатникот.

		Сметаме дека полето „Мерки што операторот ги предлага крајниот на корисник со цел да се намалат негативните ефекти од овој инцидент“ е несоодветно формулирано. АЕК и ДЗЛП – Забелешките се прифаќаат. Референцирањето во предлог правилникот е погрешно и истото треба да биде на член 14 став 4. Полето со назив „Применети технички и организациони мерки (или што ќе се применат) од операторот во однос на засегнатите лични податоци“ ќе биде преименувано во “Применети мерки (или што ќе се применат) од операторот во однос на засегнатите лични податоци“