Врза 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:

ПРАВИЛНИК ЗА ОБЕЗБЕДУВАЊЕ НА БЕЗБЕДНОСТ И ИНТЕГРИТЕТ НА ЈАВНИТЕ ЕЛЕКТРОНСКИ КОМУНИКАЦИСKИ МРЕЖИ И УСЛУГИ И АКТИВНОСТИ КОИ ШТО ОПЕРАТОРИТЕ ТРЕБА ДА ГИ ПРЕВЗЕМАТ ПРИ НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ НА ПРЕТПЛАТНИЦИТЕ.

ПРЕДМЕТ

Член 1

Со овој правилник се пропишува:

* начинот на кој што операторите треба да ги обезбедуваат безбедноста и интегритетот на јавните електронски комуникациски мрежи и услуги,
* начинот на доставување на известувањето на операторите до Агенцијата за електронски комуникации во случај на нарушување на безбедноста или 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.

ДЕФИНИЦИИ

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 инциден: Напад на безбедноста или губиток на интегритетот што има значително влијание врз оперирањето на електронската комуникациска мрежа или сервис.
* 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.

ТЕХНИЧКИ И ОРГАНИЗАЦИОНИ МЕРКИ КОИ ШТО ОПЕРАТОРИТЕ ТРЕБА ДА ГИ ПРЕВЗЕМАТ ВО ОДНОС НА БЕЗБЕДНОСТ И ИНТЕГРИТЕТ НА ЈАВНИТЕ ЕЛЕКТРОНСКИ КОМУНИКАЦИСКИ МРЕЖИ И УСЛУГИ

Член 3

Операторите треба да превземаат соодветни технички и организациони мерки со цел соодветно да управуваат со ризиците за безбедноста на мрежите и услугите. Имајќи го предвид техничкиот напредок, овие мерки треба да обезбедат ниво на безбедност кое е соодветно на настанатиот ризик. Овие мерки особено треба да се преземаат за да се спречи и минимизира влијанието на безбедносните инциденти врз корисниците и меѓусебно поврзаните мрежи.

Операторите треба превземените технички и организациски мерки од ставот 1 на овој член да ги усогласат со прописите за заштита на личните податоци.

Член 4

Операторите на јавни електронски комуникациски мрежи треба да ги преземаат сите соодветни чекори за да го обезбедат интегритетот на нивните мрежи и истовремено, континуитетот на услугите кои ги обезбедуваат со тие мрежи.

Член 5

Заради спроведување на одредбите од членовите 3 и 4 операторите на јавни електронски комуникациски мрежи или јавни електронски комуникациски услуги треба да усвојат и имплементираат политика за безбедност со која ќе се утврди ранливоста на системот, надзорот и спроведување превентивни и корективни мерки, како и мерки за ублажување на инциденти по безбедноста и интегритетот на мрежите.

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,
* Заштита на итнерконектираните мрежи,
* Одржување на достапност на мрежата,
* Безбедност и интегритет на податоците.

ИЗВЕСТУВАЊА ЗА НАСТАНАТИ НАРУШУВАЊА НА БЕЗБЕДНОСТА ИЛИ 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 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 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.

Член 8

Агенцијата за електронски комуникации треба на Европската агенцијата за безбедност на мрежи и информации (ENISA) да и поднесе годишен збирен извештај за добиените известувања од страна на операторите, како и за преземените активности согласно член 7 на овој правилник. Начинот на кој што Агенцијата за електронски комуникации ќе го поднесува годишниот збирен извештај ќе ги следи насоките дефинирани од страна на Европската агенцијата за безбедност на мрежи и информации (ENISA).

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.

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 часa, и процентот на засегнати корисници е повеќе од 1 %

Член 11

Праговите од член 10 на овој правилник се однесуваат за секој од следните сервиси засебно:

* Фиксна телефонија
* Мобилна телефонија
* Фиксен интернет
* Мобилен интернет

Член 12

При известувањата за настанати нарушувања на безбедноста или 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.

ИЗВЕСТУВАЊА ЗА НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

Известување до Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци

Член 13

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.
2. Известувањето од ставот (1) на овој член треба да биде направено по електронски пат на следната електронска адреса incident@aec.mk за Агенцијата за електронски комуникации и на incident@privacy.mk за Дирекцијата за заштита на личните податоци. Електронскиот меил треба да биде електронски потпишан.
3. Известувањето треба да ги содржи информациите содржани во Прилог 2, кој е составен дел на овој правилник.
4. 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.
5. Доколку сите информации во Прилог 2 не се достапни и се потребни понатамошни истражувања во однос на нарушувањето на безбедноста на личните податоци, операторот може да направи иницијално известување предвидено во рок согласно став (1) на овој член. Во ова иницијално известување операторот треба да ги достави податоците предвидени во првиот дел на Прилог 2. Операторот треба да направи второ известување до Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци најбрзо што може но не подоцна од 3 дена по иницијалното известување. Второто известување треба да ги содржи податоците предвидени во вториот дел на Прилог 2 и доколку е потребно операторот може да направи надополнување на податодите кои што претходно ги доставил. Доколку операторот не е во можност да ги обезбеди сите информации во периодот од три ден по иницијалното известување, операторот треба да ја извести Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци со оние информации кои што ги поседува во оваа временска рамка и треба да поднесе разумно образложение за задоцнување на поднесување на останатите информации во врска со нарушувањето на безбедноста на личните податоци. Операторот треба да ја извести Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци со преостанатите информации во врска со инцидентот, и ако е неопходно да достави измена на претходно поднесените податоци најбрзо што може.

Известување до претплатникот или други физичко лице

Член 14

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.
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 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, 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.
1. 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 да ја искористи можноста да промовира и рекламира нови и дополнителни сервиси.
2. 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 или физичкото лице најбрзо што може.
3. Операторот треба да го извести претплатникот или физичкото лице 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.
4. 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.

Технички мерки за заштита

Член 15

1. Операторот не мора да го извести претплатникот или друго физичко лице 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.
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.

Член 16

Дирекцијата за заштита на личните податоци, независно од техничките мерки за заштита кои што ги има имплементирано операторот, може да бара од операторот за одредени безбедносни нарушувања на личните податоцида го извести претплатникот или другото физичко лице, земајќи ги предвид можните негативни ефекти од нарушувањето на безбедноста на личните податоци.

ДРУГ ОПЕРАТОР

Член 17

Доколку испорачувањето на електронската комуникциска услуга се реализира преку друг оператор кој што нема директен претплатнички договор со крајниот корисник, овој оператор треба веднаш да го извести операторот кој што има склучено претплатнички договор во случај на нарушување на безбедноста на личните податоци од корисникот.

ИМПЛЕМЕНТАЦИЈА НА ПРОВЕРКА НА МЕРКИТЕ КОИ ШТО ОПЕРАТОРИТЕ ГИ ПРАВАТ ЗА ОБЕЗБЕДУВАЊЕ НА БЕЗБЕДНОСТ И ИНТЕГРИТЕТ НА ЈАВНИТЕ ЕЛЕКТРОНСКИ КОМУНИКАЦИКСИ МРЕЖИ И УСЛУГИ

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 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.

Член 19

Агенцијата за електронски комуникации има право да ги испита случаите на неусогласеност и ефектите од истото врз безбедноста и интегритетот на мрежите.

РЕГИСТАР НА НАРУШУВАЊА НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 20

Операторите на јавни електронски комуникациски услуги треба да водат регистар на нарушувањата на безбедноста на личните податоци кој ги содржи:

* фактите и причините за нарушување на безбедноста на личните податоци,
* последиците предизвикани од таквото нарушување,
* преземените мерки за безбедност на личните податоци како и
* други информации согласно Прилог 2 и Прилог 3 што и овозможува на Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци да ја проверат усогласеноста на операторот со одредбите од овој правилник.

ЗАВРШНИ ОДРЕДБИ

Член 21

Овој правилник влегува во сила наредниот ден од денот на неговото објавувањето во „Службен весник на Република Македонија”.

По влегувањето во сила, овој правилник ќе биде објавен и на веб-страната на Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци.

Директор на Агенцијата за електронски комуникации

Роберт Орданоски

Директор на Дирекција за заштита на личните податоци

Димитар Ѓеорѓиевски

Прилог 1



Прилог 2

Прилог 3

