И З В Е Ш Т А Ј

О ИЗВРШЕНОМ НАДЗОРУ НАД СПРОВОЂЕЊЕМ И ИЗВРШАВАЊЕМ ЗАКОНА О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ ОД СТРАНЕ ОПЕРАТОРА МОБИЛНЕ И ФИКСНЕ ТЕЛЕФОНИЈЕ У РЕПУБЛИЦИ СРБИЈИ

У в о д

Поступак надзора над спровођењем и извршавањем Закона о заштити података о личности од стране оператора фиксне и мобилне телефоније у Републици Србији, у делу који се односи на достављање државним органима задржаних података из члана 129. Закон о електронским комуникацијама ("Сл. гласник Републике Србије", бр. 44/2010), започет је дана 22.03.2012. године - достављањем дописа Друштву за телекомуникације ОРИОН ТЕЛЕКОМ д.о.о, са седиштем у Новом Београду, Гандијева 76а, Привредном друштву са ограниченом одговорношћу ТЕЛЕНОР, са седиштем у Новом Београду, Омладинских бригада 90, VIP MOBILE DOO Београд, са седиштем у Новом Београду, Омладинских бригада 21 и ТЕЛЕКОМ СРБИЈА, са седиштем у Београду, Таковска 2.

У дописима су на једнобразан начин тражена изјашњења и то, да у року од 8 дана од дана пријема дописа, за период од 12 месеци уназад, доставе следеће податке:

1. Укупан број примљених захтева државних органа за достављање задржаних података из члана 129. Закона о електронским комуникацијама.

2. За сваки од појединачних захтева:

   а) пун назив подносиоца захтева,

   б) ознаку, деловодни број и време поднетог захтева (датум и тачно време подношења),

   ц) одредбе закона на основу којих државни орган захтева достављање задржаних података (уколико нису наведене, користити формулацију „без навођења правног основа“),

   д) да ли је захтев одговорено и на који начин (писаним путем, електронском поштом, усмено у непосредном контакту, телефонским путем и сл.),

   е) ознака, деловодни број и време одговора оператора (датум и тачно време слања одговора), са назнаком да ли је дат позитиван или негативан одговор,

   ф) у случају позитивног одговора, да опишу начин достављања задржаних података (непосредним приступом просторијама, електронској комуникационој мрежи, припадајућим средствима или електронској комуникационој опреми оператора од стране представника државног органа - са навођењем датума и времена приступа, путем електронске поште, препоручене поштанске пошиљке, лица регистрованих за обављање послова достављања, лица запосленог у државном органу које је упутило захтев, лица запосленог код оператера и др.),

г) врсту носача информација на којем су достављени задржани подаци (папир, оптички диск, USB flash stick, External Hard Drives и сл.).

Достављање наведених података захтевано је у односу на све примљене захтеве, без обзира да ли се тичу задржаних података насталих у оквиру јавне фиксне телекомуникационе мреже, јавне мобилне телекомуникационе мреже, или јавне фиксне бежичне телекомуникационе мреже (Орион Телеком).

На дописе Повереника, оператори мобилне и фиксне телефоније су се изјаснили, и то:

1. ТЕЛЕНОР ДОО, дописом број 203/94/12 од 03.04.2012. године у којем је доставио одговоре на питања из дописа Повереника, а за сваки појединачни захтев државних органа - податке садржане у Excel табелама под називом "Писмени_захтеви" и "e-mail_захтеви", приложивши их на компакт диску, као прилог дописа.

2. ОРИОН ТЕЛЕКОМ, дописом број 1206/12 од 04.04.2012. године, у којем се наводи да у назначеном периоду нису примили, цитирамо "*званичан* захтев за достављање задржаних података из члана 129. Закона о електронским комуникацијама, који су настали у јавној фиксној и бежичној телекомуникационој мрежи (Fixed Wireless Access – FWA) ...".

   С обзиром на изречену тврдњу, дана 06.04.2012. године ОРИОН ТЕЛЕКОМУ је упућен нов допис са захтевом за достављањем података поводом *незванично* примљених захтева државних органа за достављање задржаних података.

   Дописом 1206/12 од 04.04.2012. године, на преформулисани захтев Повереника, ОрионТелеком је одговорио да "од државних органа није примао конкретне захтеве за достављање задржаних података о личности, нити званичне нити незваничне природе".

3. VIP MOBILE DOO Београд, дописом од 12.04.2012. године, уз који је доставио две табеле са траженим подацима, и то: 1) табелу у којој су подносиоци захтева за приступ задржаним подацима а) Управа криминалистичке полиције – Служба за специјалне истражне методе и б) БИА и 2) табелу у којој су подносиоци захтева остали државни органи.

4. ТЕЛЕКОМ СРБИЈА, дописом број 430/1-12 од 04.04.2012. године, уз који је доставио Извештај о решеним захтевима надлежних државних органа за задржаним подацима о оствареним електронским комуникацијама.

Имајући у виду садржину наведених одговора оператора, као и количину и врсту података којима државни органи приступају, било непосредним приступом задржаним подацима у базама података оператора, било кроз захтеве за приступ подацима о оствареним електронским комуникацијама, Повереник је наставио поступак непосредним надзором код сваког од наведена четири оператора.

Надзор су вршила овлашћена лица Повереника, Маријана Софиљ - Аћимовић, Радоје Гвозденовић и Аца Стојев.

Надзор код Орион Телеком, Теленор, и Вип Мобиле извршен је у периоду 24.04. - 25.05.2012. године, док је надзор у Телеком Србија, који је започет 12.06.2012. године, још увек у току.

Задржани подаци у смислу одредби члана 129. ЗЕК, чија је обрада од стране оператора и државних органа предмет вршења надзора, јесу:

1. *Праћење и утврђивање извора комуникације* (тач. 1. чл. 129. ЗЕК) односи се на број мобилног телефона, или IMEI број телефона који је иницирао телефонски саобраћај, што подразумева листинг оствареног одлазно – долазног саобраћаја са тих бројева који се тарифира у Теленоровој мрежи.

2. *Утврђивање одредишта комуникације* (тач. 2. чл. 129. ЗЕК) односи се на број мобилног телефона, или IMEI број телефона који је позван у оквиру већ иницираног телефонског саобраћаја, који се тарифира у Теленоровој мрежи.

3. *Утврђивање почетка, трајања и завршетка комуникације* (тач. 3. чл. 129. ЗЕК) односи се на време комуникације, односно датум, време отпочињања и трајања комуникације.

4. *Утврђивање врсте комуникације* (тач. 4. чл. 129. ЗЕК) односи се на врсту услужног сервиса, односно да ли је у питању телефонски позив, или SMS, MMS, или GPRS.

5. *Идентификација терминалне опреме корисника* (тач. 5. чл. 129. ЗЕК) односи се на IMEI број позиваоца и позиваног.

6. *Утврђивање локације мобилне терминалне опреме корисника* (тач. 6. чл. 129. ЗЕК) односи се на утврђивање адресе базне станице (БСА) са које је иницира саобраћај терминалном опремом корисника (телефон, таблет, лап-топ), при чему овај податак не пружа могућност утврђивања приближније локације са које је саобраћај иницира.

П р а в н и о к в и р

Право на неповредивост тајности писама и других средстава комуницирања и право на заштиту података о личности гарантовани су Уставом Републике Србије као основна људска права и слободе. Одступања од начела неповредивости тајности електронских комуникација дозвољена су само на одређено време и на основу одлуке суда, ако су неопходна ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом (Устав РС, члан 41). Такође, забрањена је и кажњива употреба података о личности изван сврхе за коју су прикупљени у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом (Устав РС, члан 42).

Када говоримо о електронским комуникацијама, треба подсетити да је Међународни суд за људска права у Стразбуру (ECHR), у случају *Copland vs. the United Kingdom* 2007. године пресудио да информације везане за време и дужину телефонског разговора, а посебно изабрани бројеви саговорника, представљају „интегрални део телефонске комуникације". С обзиром на то да су пресуде ECHR обавезујуће за Републику Србију, јасно је да начело неповредивости тајности електронских комуникација и у Републици Србији треба примењивати подједнако на садржај и податке о обављеним електронским комуникацијама, што потврђује и одлука Уставног суда .....

Приватност и заштита личних података у законима земаља ЕУ темељи се, као уосталом и у Србији, на конвенцији Савета Европе о заштити лица у односу на аутоматску обраду података. У складу са Конвенцијом, ЕУ је донела оквирну Директиву 95/46/ЕЦ о заштити података о личности. Уважавајући специфичности сектора електронских комуникација, Европски парламент и Савет 2002. године доносе посебну директиву која утврђује оквире заштите приватности, података о личности и интегритета јавних мрежа електронских комуникација, већ поменуту директиву 2002/58. Након бомбашких напада у Мадриду и Лондону, под притиском безбедносног сектора, ова директива је 2006. године допуњена директивом 2006/24, која уређује оквир за задржавање података о саобраћају за потребе борбе против тзв. озбиљног криминала, у смислу врсте података и рока чувања од 6 месеци до 2 године. Државе чланице су за примену добиле рок до 15.09.2007. године, односно продужен је рок до 15.03.2009. године за Интернет приступ, електронску пошту и Интернет телефонију. Директива је наишла на велики отпор јавности и телекомуникационе индустрије, уз главне примедбе да је мера задржавања непропорционална претњи, неефикасна, нарочито у домену Интернета, да намеће велико финансијско оптерећење операторима смањујући њихову конкурентност, превише флексибилна у погледу обавезног рока чувања података и да на мала врата уводи принцип презумпције кривице за све кориснике услуга. По устаљеној логици модела управљања, ЕТСИ је 2007. донео техничку спецификацију за имплементацију Директиве. Суочена са великим проблемима у пракси, Европска комисија је 25.03.2008. године донела одлуку о формирању групе експерата, као сталног консултативног тела Комисије и земаља чланица за питања задржавања података о телекомуникационом саобраћају.

Интересантно је да закон у Републици Србији не препознаје позиционирање телекомуникационог терминала у реалном времену као меру органа гоњења за откривање и доказивање кривичних дела, иако спада у озбиљно задирање у приватност, као и да се осетљиво питање задржавања и обраде података о комуникацијама или избегава или решава на дискутабилан начин.

Тако на пример, ЗКП му најближе прилази у члану 504.љ, као аутоматском рачунарском претраживању личних и других са њима повезаних података, и захтева да ову меру наређује истражни судија на предлог тужиоца, а извршавају органи унутрашњих послова, БИА и ВБА.

Члан 128. Закона о електронским комуникацијама ("Сл. гласник РС", бр. 44/2010), (даље ЗЕК), говори о обавезама оператора да задржи податке из члана 129. став 1. ЗЕК који су потребни за праћење и утврђивање извора комуникације, утврђивање одредишта комуникације, утврђивање почетка, трајања и завршетка комуникације, утврђивање врсте комуникације, идентификацију терминалне опреме корисника и утврђивање локације мобилне терминалне опреме корисника.

Ови подаци се задржавају за потребе спровођења истраге, откривања кривичних дела и вођења кривичног поступка, у складу са законом којим се уређује кривични поступак, као и за потребе заштите националне и јавне безбедности Републике Србије, у складу са законима којима се уређује рад служби безбедности Републике Србије и рад органа унутрашњих послова, а оператор је дужан да задржи податке 12 месеци од дана обављене комуникације.

Надлежни државни орган који остварује приступ, односно коме се достављају задржани подаци, дужан је да води евиденцију о приступу, односно достављању задржаних података, која нарочито садржи: одређење акта који представља правни основ за приступ, односно

достављање задржаних података, датум и време приступања, односно достављања задржаних података, као и да ову евиденцију чува као тајну, у складу са законом којим се уређује тајност података.

Када надлежни државни орган није у могућности да оствари приступ задржаним подацима без приступа просторијама, електронској комуникационој мрежи, припадајућим средствима или електронској комуникационој опреми оператора, оператор из је дужан да о примљеним захтевима за приступ, односно достављање задржаних података, води евиденцију, која нарочито садржи идентификацију овлашћеног лица које је приступило задржаним подацима, односно коме су достављени задржани подаци, одређење акта који представља правни основ за приступ, односно достављање задржаних података, датум и време приступања, односно достављања задржаних података, као и да ову евиденцију чува као тајну, у складу са законом којим се уређује тајност података.

У члану 129. ЗЕК се поред навођења врсте задржаних података у ставу 1, наводи и обавеза о задржавању података о успостављеним позивима на које није одговорено, али не и података о позивима чије успостављање није успело и да је забрањено задржавање података који откривају садржај комуникације.

У члану 130. ЗЕК који говори о заштити задржаних података, наводи се да је оператор дужан да, у погледу заштите задржаних података, поред осталог нарочито обезбеди:

- да су задржани подаци заштићени од случајног или недопуштеног уништења, случајног губитка или измене, неовлашћеног или незаконитог чувања, обраде, приступа или откривања, у складу са законом којим се уређује заштита података о личности, односно законом којим се уређује заштита тајних података када се ради о подацима који су сачувани и достављени у складу са чланом 128. став 5. овог закона, да се приступ задржаним подацима ограничи само на овлашћена лица органа који остварују приступ задржаним подацима и да се задржани подаци униште по истеку рока од 12 месеци од дана обављене комуникације, осим података који су сачувани и достављени надлежним државним органима;

Надзор над извршењем обавеза оператора врши орган надлежан за заштиту података о личности, а када су подаци достављени надлежном државном органу и орган надлежан за надзор над спровођењем закона који регулише заштиту тајности података.

Такође су још на снази, између осталих, и Технички услови за подсистеме, уређаје, опрему и инсталације мобилне телекомуникационе мреже и Технички услови за подсистеме, уређаје, опрему и инсталације фиксне телекомуникационе мреже, који се могу наћи на страници РАТЕЛ www.ratel.rs/uputstva_i_obrasci/tehnicki_uslovi.52.html.

Наведени технички услови су донети у периоду март – јули 2008. године, на основу члана 55. став 3. Закона о телекомуникацијама („Сл. гласник РС“, бр. 44/03 и 36/06), који је престао да важи даном ступања на снагу Закона о електронским комуникацијама ("Сл. гласник РС", бр. 44/2010), односно 08.07.2010. године, осим члана 6. став 1. тачка 4, чл. 36, 37. и 39, који су престали да важе 31.12.2011. године, при чему до данашњег дана нису донети нови технички услови у складу са новим законом.

1. У *Техничким условима за подсистеме, уређаје, опрему и инсталације мобилне телекомуникационе мреже*, у тачки 3. наводи се да јавни телекомуникациони оператор мора обезбедити надлежним државним органима апсолутна администраторска права, што подразумева потпуно аутономно увођење и укидање мера, добијање података о комуникацијама за које су уведене мере и преусмеравање садржаја комуникације на сервер надлежних државних органа, да се приступ надлежних државних органа ка централама јавног телекомуникационог оператора остварује на директан начин, преко сопственог порта на централи без преусмеравања.

У тачки 4. напред наведених Техничких услова, наводи се да је јавни телекомуникациони оператор дужан да надлежним државним органима омогући преузимање свих билинг података и то аплоудовањем на задату адресу или омогућавањем даунлоуда, да билинг подаци морају садржавати CDR за услуге које се наплаћују и за бесплатне услуге.

У тачки 5. напред наведених Техничких услова наводи се да је јавни телекомуникациони оператор дужан да надлежним државним органима омогући непрекидан терминалски приступ подсистему за позиционирање терминалног мобилног уређаја.

2. У *Техничким условима за подсистеме, уређаје, опрему и инсталације фиксне телекомуникационе мреже*, у тачки 3. наводи се да јавни телекомуникациони оператор мора обезбедити надлежним државним органима апсолутна администраторска права, што подразумева потпуно аутономно увођење и укидање мера, добијање података о комуникацијама за које су уведене мере и преусмеравање садржаја комуникације на сервер надлежних државних органа, да се приступ надлежних државних органа ка централама јавног телекомуникационог оператора остварује на директан начин, преко сопственог порта на централи без преусмеравања или путем мониторинг функције које су интегралног софттвера централе.

У тачки 4. напред наведених Техничких услова, наводи се да је јавни телекомуникациони оператор дужан да надлежним државним органима омогући преузимање свих билинг података и то аплоудовањем на задату адресу или омогућавањем даунлоуда, да билинг подаци морају садржавати CDR за услуге које се наплаћују и за бесплатне услуге, као и да омогући приступ билинг подацима за јавне говорнице и употребљене телефонске картице.

Што се тиче Законика о кривичном поступку ("Сл. гласник РС", бр. 72/2011 и 101/2011), нови ЗКП је ступио на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Србије", а примењује се од 15.01.2013. године, изузев у поступцима за кривична дела за која је посебним законом одређено да поступа јавно тужилаштво посебне надлежности, у ком случају се примењује од 15.01.2012. године.

У Законика о кривичном поступку ("Сл. лист СРЈ", бр. 70/2001 и 68/2002 и "Сл. гласник РС", бр. 58/2004, 85/2005, 115/2005, 85/2005 - др. закон, 49/2007, 20/2009 - др. закон, 72/2009 и 76/2010), који примењују тужилаштва опште надлежности, за прибављање задржаних података, користи се члан 235. став 2. ЗКП, у којем се поред осталог наводи да јавни тужилац може сам или посредством других органа, прикупити потребна обавештења, а ако није у могућности да то предузме сам, јавни тужилац ће захтевати од органа унутрашњих послова да прикупе потребна обавештења и да предузму друге мере ради откривања кривичног дела и учиниоца.

Пре ступања на снагу новог ЗКП, одредбе чл. 504.а до 504.ћ, садржале су поједина посебна правила поступка за кривична дела организованог криминала, корупције и друга изузетно тешка кривична дела, а у члану 504.а је наведено шта се подразумева под организованим криминалом, организованом криминалном групом и побројана су кривична дела на која се примењују ови чланови закона.

У члану 504љ, који се односи на аутоматско рачунарско претраживање личних и других са њима повезаних података наводи се:

- да се аутоматско рачунарско претраживање личних и других са њима повезаних података и њихова електронска обрада може се предузети ако постоје основи сумње да је учињено кривично дело из члана 504.а овог законика, ако се на други начин не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано и да се мера изузетно може одредити и ако постоје основи сумње да се припрема неко од кривичних дела из члана 504.а овог законика, а околности случаја указују да се на други начин дело не би могло открити, спречити или доказати, или би то изазвало несразмерне тешкоће или велику опасност.

- да се мера из става 1. овог члана се састоји у аутоматском претраживању већ похрањених личних и других, са њима непосредно повезаних података и у њиховом аутоматском поређењу са подацима који се односе на кривично дело из става 1. овог члана и на осумњиченог, да би се као могући осумњичени искључила лица у погледу којих не постоји вероватноћа да су повезана са кривичним делом.

- да меру из става 1. овог члана наређује истражни судија, на предлог јавног тужиоца, а она садржи: законски назив кривичног дела из става 1. овог члана, опис података које је потребно аутоматски прикупити и проследити, означење државног органа који је дужан да аутоматски прикупља тражене податке и доставља их јавном тужиоцу и органу унутрашњих послова, обим посебне доказне радње и време њеног трајања, да мера може трајати највише шест месеци, а из важних разлога њено трајање се може продужити за још три месеца.

- да меру из става 1. овог члана спроводе органи унутрашњих послова, БИА, ВБА, органи царинске службе или други државни органи, односно друга правна лица која на основу закона врше одређена јавна овлашћења.

У ЗКП, који од 15.01.2012. године примењују јавна тужилаштва посебне надлежности, од чл. 161. до 187. ЗКП наведене су одредбе које се односе на посебне доказне радње које се примењују према лицу за које постоје основи сумње да је учинило неко од кривичних дела наведених у члану 162. овог законика, а за која се на други начин не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано.

Чланови од 178. до 180. ЗКП, говоре о рачунарском претраживању података, па се тако:

1. у члану 178. ЗКП се наводи да на образложени предлог јавног тужиоца, суд може одредити рачунарско претраживање већ обрађених личних и других података и њихово поређење са подацима који се односе на осумњиченог и кривично дело;

2. у члану 179. став 1. ЗКП наводи се да посебну доказну радњу из члана 178. овог законика одређује судија за претходни поступак образложеном наредбом, да наредба треба да садржи податке о осумњиченом, законски назив кривичног дела, опис података које је потребно рачунарски претражити и обрадити, означење државног органа који је дужан да спроведе претрагу тражених података, обим и време трајања посебне доказне радње, а да рачунарско претраживање података може трајати највише три месеца, а због неопходности даљег прикупљања доказа може се изузетно продужити још највише два пута у трајању од по три месеца.

3. у члану 180. став 1. ЗКП наводи се да наредбу из члана 179. став 1. овог законика извршава полиција, БИА, ВБА, царинске, пореске или друге службе или други државни орган, односно правно лице које на основу закона врши јавна овлашћења, да се по завршетку рачунарског претраживања података државни орган, односно правно лице из става 1. овог члана доставља судији за претходни поступак извештај који садржи: податке о времену почетка и завршетка рачунарског претраживања података, податке који су претражени и обрађени, податке о службеном лицу које је спровело посебну доказну радњу, опис примењених техничких средстава, податке о обухваћеним лицима и резултатима примењеног рачунарског претраживања података, а да судија за претходни поступак извештај доставља јавном тужиоцу.

Мимо наведених чланова ЗКП, у члану 286. ЗКП са називом овлашћења полиције наводи се да је у случају постојања основа сумње да је извршено кривично дело за које се гони по службеној дужности, полиција дужна да предузме потребне мере да се пронађе учинилац кривичног дела, да се учинилац или саучесник не сакрије или не побегне, да се открију и обезбеде трагови кривичног дела и предмети који могу послужити као доказ, као и да прикупи сва обавештења која би могла бити од користи за успешно вођење кривичног поступка.

У ставу 2. истог члана, наведене су радње полиције, па између осталог да може да оствари увид у документацију правних лица и да је по потреби одузме, а да се о предметима који су пронађени или одузети, саставља записник или службена белешка, што се користи да би се прибавили задржани подаци, мимо наредбе истражног судије.

Такође, по налогу јавног тужиоца полиција може у циљу испуњења дужности из става 1. овог члана прибавити евиденцију остварене телефонске комуникације, коришћених базних станица или извршити лоцирање места са којег се обавља комуникација, а о предузимању мера и радњи из ст. 2. и 3. овог члана полиција одмах, а најкасније у року од 24 часа након предузимања, обавештава јавног тужиоца, при чему лице, према коме је примењена нека од мера и радњи ст. 2. и 3. овог члана има право да поднесе притужбу надлежном јавном тужиоцу.

Дакле, очигледно је да заштита приватности корисника и безбедност информационих и комуникационих технологија нису искључиво проблем загарантованих права и слобода човека, већ представљају озбиљно друштвено - економско, политичко и безбедносно питање за сваку земљу. Такође је јасно да заштита приватности корисника и безбедност електронских комуникационих мрежа и услуга нису искључиво проблем технологије, већ отварају и друга комплексна питања као што су законски и регулаторни оквир, модел и имплементација управљања од националног до микро нивоа, државна и јавна безбедност, развој институционалних капацитета, процес европских интеграција Србије, понашање, култура и освешћеност корисника и слично. Стално увођење нових комуникационих технологија и

услуга додатно отежава већ ионако сложен проблем, поготово ако се у обзир узму драматичне промене у простору потенцијалних претњи и нови, до сада непознати ризици по безбедност. Јасно је стога да решавање питања приватности и безбедности у електронским комуникацијама захтева свеобухватан приступ, укључивање широког круга заинтересованих и усаглашавање многих, често различитих потреба и интереса. Европска унија и земље чланице, као уосталом и све западне демократије које теже увођењу информационог друштва као следећег степена развоја цивилизације, велику пажњу посвећују овим питањима.

Н А Л А З

1) ОРГАНИЗАЦИЈА ПОСЛОВА У ВЕЗИ СА РЕШАВАЊЕМ ЗАХТЕВА ДРЖАВНИХ ОРГАНА ЗА ДОСТАВЉАЊЕ ЗАДРЖАНИХ ПОДАТАКА:

- **ТЕЛЕНОР**

  Стручна служба којој су поверени послови асистенције државним органима при Одељењу за корпоративну безбедност које је између осталог задужено и за физичку и техничку заштиту људи и имовине, безбедност информација, заштиту података о личности, превенцију и откривање превара у коришћењу телекомуникационих услуга, управљање безбедносним ризицима и решавање безбедносних инцидента. Захтеве оперативно обрађује троје лица запослених у Одељењу, уз укључивање вође тима којег представља руководилац Одсека за сузбијање телекомуникационих превара Одељења корпоративне безбедности, и самог директора Одељења, по потреби.

- **ОРИОН ТЕЛЕКОМ**

  Стручна служба за Data Processing (служба од три запослена) је задужена за сарадњу како са државним органима, тако и са корисницима - власницима претплатничког броја фиксне телефоније. На основу писаног захтева државних органа, уз проверу идентитета подносиоца, захтев се обрађује и одговор на исти се потом прослеђује подносиоцу.

- **ВИП МОБИЛЕ**

  Код Руковаоца података не постоји посебна служба која се бави сарадњом са државним органим. Три запослена у ВИП мобиле су, поред обављања редовних послова, добили и дужности да сарађују са надлежним државним органима.

  Стручна служба за безбедност података је задужена за сарадњу са БИА, ВБА и МУП, док је једно лице из правне службе задужено за сарадњу са судовима и тужилаштвом.

- **ТЕЛЕКОМ**

  Правилником о организацији Предузећа за телекомуникације "Телеком Србија" а.д. као посебна организациона целина на нивоу Руковаоца података, за сарадњу са државним органима (судови, тужилаштва, МУП РС, БИА, ВБА, Финансијска полиција и др.) и

решавање њихових захтева, одређен је - Сектор за безбедност и заштиту у Функцији за логистичке и опште послове.

2) НАЧИН НА КОЈИ СЕ ОПЕРАТОРИМА ДОСТАВЉАЈУ ЗАХТЕВИ ДРЖАВНИХ ОРГАНА ЗА ДОСТАВЉАЊЕ ЗАДРЖАНИХ ПОДАТАКА:

- **ТЕЛЕНОР**

Писаним путем, факсом и електронском поштом, уз накнадно достављање оригинала докумената захтева.

Прелиминарни упити и појашњења већ пристиглих захтева, понекад се обављају и телефонским путем међутим, по захтевима који су упућени телефонским путем - Теленор никада не поступа.

Сви запослени у компанији обавезани су да захтеве државних органа за давање података о преплатницима и њиховим комуникацијама усмере или проследе Одељењу за корпоративну безбедност у седишту Компаније.

- **ОРИОН ТЕЛЕКОМ**

На постављено питање овлашћених лица Повереника, да ли је ОРИОН ТЕЛЕКОМ у периоду од 12 месеци уназад имао примљених захтева од стране државних органа за достављање задржаних података из члана 129. Закона о електронским комуникацијама, представници Руковаоца података су изјавили да у наведеном периоду нису имали таквих захтева од стране државних органа.

- **ВИП МОБИЛЕ**

Писаним путем, факсом и електронском поштом, уз накнадно достављање оригинала докумената захтева.

- **ТЕЛЕКОМ**

Писаним путем, факсом, електронском поштом и усмено (непосредно или телефоном).

3) ЗАВОЂЕЊЕ И ЧУВАЊЕ ПРИМЉЕНИХ ПИСАНИХ ЗАХТЕВА ДРЖАВНИХ ОРГАНА ЗА ДОСТАВЉАЊЕ ЗАДРЖАНИХ ПОДАТАКА:

- **ТЕЛЕНОР**

У апликацији *Поверљиви деловодник* заводе се и у електронској форми чувају сви писмени захтеви судова и других државних органа за достављање задржаних података, као и одговори Теленора, док се достављени подаци чувају у посебно заштићеној електронској архиви.

Копија писаних захтева чува се у поверљивој архиви, у папирном, скенираном и у облику електронског документа.

У папирном облику документи се чувају у закључаним орманима Стручне службе, до њиховог слања у Централну архиву.

- **ОРИОН ТЕЛЕКОМ**

Како није било примљених захтева за достављање задржаних података, евиденција о истим се и не води.

- **ВИП МОБИЛЕ**

Сви примљени захтеви за достављање задржаних података, ако и одговори на исте, у папирној форми, смештају се у архиву над којом су примењене све техничке и организационе мере заштите, у смислу да је архива смештена у простор под кључем и којој може приступити ограничени број овлашћених лица (о чему се води евиденција). Такође, архиви у електронској форми може да приступи само овлашћено лице.

- **ТЕЛЕКОМ**

Нису дати подаци, надзор у току. Питање је делимично обрађено у Упутству Руковаоца података.

4) ЗАВОЂЕЊЕ И ЧУВАЊЕ ПРИМЉЕНИХ ЗАХТЕВА ДРЖАВНИХ ОРГАНА ЗА ДОСТАВЉАЊЕ ЗАДРЖАНИХ ПОДАТАКА ДОСТАВЉЕНИХ ПУТЕМ ЕЛЕКТРОНСКЕ ПОШТЕ :

- **ТЕЛЕНОР**

Пријем захтева МУП РС (не и других државних органа) за достављање задржаних података путем електронске поште, врши се са две предефинисане адресе: [redacted]@mup.gov.rs и [redacted]@ptt.rs.

Пријем захтева и слање одговора са прилозима врши се кроз посебну апликацију.

Овако пристигли захтеви чувају се у наменском „сандучету“ у наведене апликације.

- **ОРИОН ТЕЛЕКОМ**

Како није било примљених захтева за достављање задржаних података, евиденција о истим се и не води.

- **ВИП МОБИЛЕ**

Управа криминалистичке полиције - Служба за специјалне истражне методе (не и други државни органи) захтеве за достављање задржаних података шаље путем електронске поште. На такве захтеве оператор одговара по правилу мејлом, са адресе једног лица – стручњака за системе за пословну подршку.

- **ТЕЛЕКОМ**

Не постоји посебна евиденција.

5) ПОДНОСИОЦИ ЗАХТЕВА ЗА ДОСТАВЉАЊЕ ЗАДРЖАНИХ ПОДАТАКА:

- **ТЕЛЕНОР**

Судови, тужилаштва, Министарство унутрашњих послова Републике Србије (даље: МУП РС), Војно – безбедносна агенција (даље:ВБА) и Безбедносно – информативна агенција (даље: БИА), као и царина, пореска управе, инспекцијски органи, судски вештаци и адвокати.

1. У дефинисаном периоду у трајању од годину дана, од укупно **513** *писмених* захтева:

- ТУЖИЛАШТВА су поднела **31** захтев и у свим случајевима дат им је негативан одговор,

- СУДОВИ су поднели **446** захтева, на које је у 30 случајева негативно одговорено, а у 416 дат је позитиван одговор.

  Од наведеног броја захтева ПРЕКРШАЈНИ судови су се обратили **5** пута (3 негативна и 2 позитивна одговора), ПРИВРЕДНИ само **1** (позитиван одговор)

- МУП РС је поднео писмене захтеве **29** пута (18 позитивних и 11 негативних одговора).

  НАПОМЕНА: С обзиром на број захтева достављених електронском поштом (**1.559**) укупан број свих захтева од МУП РС износио би **1.588**

- ВБА је поднео **3** захтева на које је позитивно одговорено.
- СУДСКИ ВЕШТАЦИ су послали **2** захтева на које је позитивно одговорено.
- ВОЈСКА СРБИЈЕ је поднела **1** захтев на који је позитивно одговорено.

2. У дефинисаном периоду у трајању од годину дана, од укупно **1.559** захтева упућених *путем електронске поште од стране МУП РС*:

- Служба за специјалне истражне методе са адресе [redacted]@mup.gov.rs упутила је **905** захтева за достављање задржаних података,
- док је са другог налога [redacted]@ptt.rs упућено **654** захтева.

На СВЕ захтеве је ПОЗИТИВНО одговорено.

- **ОРИОН ТЕЛЕКОМ**

Нема поднетих захтева.

- **ВИП МОБИЛЕ**

Представници Руковаоца података су изјавили да су се ВИП Мобиле обраћали са захтевом за достављање задржаних података поред МУП, БИА и ВБА и други државни органи, као што су основни и виши судови, парнични и прекршајни судови, судски вештаци на основу налога суда, тужилаштва.

У дефинисаном периоду у трајању од годину дана, од укупно **459** захтева:

- ТУЖИЛАШТВА су поднела **28** захтева и у 15 случајева дат је позитиван одговор, док је у 13 случајева одговор био негативан,
- СУДОВИ су поднели **248** захтева, на које је у 118 случајева негативно одговорено, а у 130 дат је позитиван одговор.
- МУП РС је поднео **176** захтева (писменим путем и електронском поштом) од ког броја је дато 50 негативна одговора и 126 позитивних.
- ОСТАЛИ су поднели **7** захтева од тога БИА **2**, а ВБА **1**.

- **ТЕЛЕКОМ**

Подносиоци захтева су према наводима Руковаоца података: судови, тужилаштва, МУП РС "и други државни органи".

У дефинисаном периоду у трајању од годину дана, од укупно **1.851** захтева:

- ТУЖИЛАШТВА су поднела **65** захтев и у 56 случајева дат је позитиван одговор, док је у 9 случајева одговор био негативан,
- СУДОВИ су поднели **868** захтева, на које је у 56 случајева негативно одговорено, а у 812 дат је позитиван одговор.

  Од наведеног броја захтева ПРЕКРШАЈНИ судови су се обратили 11 пута (2 негативна и 9 позитивних одговора), ПРИВРЕДНИ само 1 (позитиван одговор)
- МУП РС је поднео **803** захтева (писменим путем и електронском поштом) од ког броја је дато 42 негативна одговора и 761 позитиван.
- СУДСКИ ВЕШТАЦИ су послали **14** захтева на које је у само 1 случају негативно одговорено.
- АДВОКАТИ су послали **3** захтева (2 позитивна и 1 негативан одговор).

Мањи број захтева поднет је од стране других државних органа, као што су: Градске управе (3 позитивна одговора), Министарство правде РС (1 негативан), Министарство

културе, информисања и информационог друштва РС (1 позитиван одговор), Покрајински фонд за ПИО (1 негативан одговор), Предшколска установа (1 негативан одговор), Градски штаб за ванредне ситуације (1 позитиван одговор), Детективска агенција из Црне Горе (1 негативан одговор), Дирекције које послују у оквиру Руковаоцас података (4 позитивна одговора), физичко лице Тодоровић Славољуб по ЗИКС (1 позитиван одговор).

6) УКУПАН БРОЈ ПРИМЉЕНИХ ЗАХТЕВА ЗА ДОСТАВЉАЊЕ ЗАДРЖАНИХ ПОДАТАКА

- **ТЕЛЕНОР**

  Укупно **2.072** (двехиљадеседамдесетидва), од тога

  - 513 (петстотинатринаест) *у писаној форми,*
  - 1.559 (хиљадупетстотинапедестидевет) *путем електронске поште.*

- **ОРИОН ТЕЛЕКОМ**

  Нема примљених захтева.

- **ВИП МОБИЛЕ**

  Укупно **459** захтева, од тога:

  - 344 *у писаној форми,*
  - 115 *путем електронске поште.*

- **ТЕЛЕКОМ**

  Укупан број захтева према подацима Руковаоца података је **1.959** међутим, њиховим пребројавањем у оквиру достављених Excel тебела, дошло се до бројке од **1.851** захтева који нису сви у форми писмених захтева.

  Анализом садржаја достављених Excel тебела утврђује се да су захтеви у мањем броју случајева достављани и путем електронске поште, факсом и усменим, односно телефонским путем, што је у супротности са Упутством Руковаоца од 07.03.2011. године и става изреченог у његовом допису од 05.04.2012. године, да се достављање задржаних података врши искључиво на писане захтеве државних органа.

  Према томе, од укупног броја, **1.851** захтева:

  - **1.724** *је у писаној форми,*
  - **127** *је достављено путем електронске поште, иако Упутством Руковаоца овакав начин достављања није предвиђен.*

7) ВРСТА ЗАДРЖАНИХ ПОДАТАКА КОЈИ СУ ПРЕДМЕТ ЗАХТЕВА ДРЖАВНИХ ОРГАНА ЗА ДОСТАВЉАЊЕ ЗАДРЖАНИХ ПОДАТАКА:

- **ТЕЛЕНОР**

1. Идентификација и уговорни подаци корисника,
2. Подаци о комуникацијама индивидуалних корисника,
3. Подаци о саобраћају базних станица,
4. Подаци о покривености сигналом и присутности мобилних апарата у сервисној области одређене базне станице,
5. Подаци о вези између коришћених SIM (енг. Subscriber Identity Module) картица и мобилних уређаја,
6. Подаци о вези између преплатничког броја у мобилној мрежи MSISDN (енг. The Mobile station ISDN Number) и IP (енг. Internet Protocol) адресе у јавној интернет мрежи, за одређену Интернет сесију,
7. SMS (енгл. Short Message Service) поруке које су евентуално задржане у Систему за надзор мрежене сигнализације - SS7 (енг. Signalling System No. 7).

Фактички, када наведени државни органи, са додељеним правима приступа не могу да преузму све потребне податке преко Инфо апликације која им је учињена доступном, обраћају се формалним захтевима Руковаоцу података који их заприма и обрађује у оквиру своје Стручне службе.

Стручна служба за потребе давања одговора државним органима по захтевима за достављање задржаних података, користи другу апликацију која садржи далеко више информација (IMEI, BS), која државним органима није доступна, и у оквиру које радници Стручне службе могу да врше следеће упите:

1. По броју телефона (припејд, постпејд),
2. По IMEI броју (припејд, постпејд),
3. За базне станице односно, саобраћај преко БС у задатом периоду (припејд, постпејд),
4. Утврђивање различитих IMEI бројева, на основу броја телефона MSISDN (енг. mobile subscriber ISDN),
5. Утврђивање свих бројева MSISDN, на основу IMEI броја,

6. Утврђивање различитих БС – базних станица, по броју телефона MSISDN,

7. Утврђивање различитих БС – базних станица, по IMEI броју.

- **ОРИОН ТЕЛЕКОМ**

Нема захтева.

- **ВИП МОБИЛЕ**

Захтеви за достављање задржаних података се најчешће односе на:

1. Листиг долазно-одлазног саобраћаја,
2. Садржину SMS (енг. *Short Message Service*) порука,
3. Идентификацију корисника (напомена: Руковалац података нема формиран телефонски именик својих корисника),
4. Достављање корисничких уговора,
5. Адресе базних станица,
6. Податке о SIM (енг. *Subscriber Identity Module*) картицама и
7. Податке о MSISDN (енг. *Mobile Subscriber ISDN*), тј. интернационални ISDN број мобилног корисника.

- **ТЕЛЕКОМ**

8) ПОСЛОВНА ПОЛИТИКА И КРИТЕРИЈУМИ ОПЕРАТОРА ПРИЛИКОМ ОДЛУЧИВАЊА У ПОГЛЕДУ ДАВАЊА ОДГОВОРА НА ДОСТАВЉЕНЕ ЗАХТЕВЕ:

- **ТЕЛЕНОР**

По захтевима који су упућени телефонским путем - Теленор никада не поступа.

Не удовољава се захтевима за достављање задржаних података за период дужи од 12 месеци од дана обављене комуникације, што је супротно чл.128. став 4. ЗЕК.

Захтеви тужалаштава, полиције, царине, пореске управе, инспекцијских органа, судских вештака и адвоката који нису подржани одговарајућом наредбом суда - одбијају се, без изузетка.

Захтеви привредних, парничних и судова за прекршаје, за достављање задржаних података, начелно се одбијају, иако у пракси има и изузетака. Оваква одступања појављују се искључиво у погледу захтева упућених од стране судова редовне надлежности.

Захтевима судова који поступају по одредбама Законика о кривичном поступку Руковалац података удовољава и у оним случајевима када правни основ, у виду цитирања одређеног члана ЗКП није наведен, или пак није одговарајући у односу на садржај захтева који се доставља.

Навођење правног основа у писменим захтевима

Од укупног броја *свих захтева,* у укупно **2.027** захтева НИЈЕ НАВЕДЕН ПРАВНИ ОСНОВ у виду цитирања одредби закона. На све овакве захтеве дати су позитивни одговори. Највећи број тих захтева чине захтеви МУП РС достављени електронском поштом (1.559).

Од укупног броја (513) *поднетих писмених захтева* свих државних органа, у **468** случајева позитивно је одговорено на захтев иако у истима није наведен правни основ у виду цитирања одређених одредби Закона.

У **40** писмених захтева као правни основ наведене су одредбе Законика о кривичном поступку - ЗКП, и то: 131. став 1. ЗКП, 235. став 2. ЗКП, 85. став 1 ЗКП, чл.235 ст.2 ЗКП, 239 став 1. ЗКП, 225. став 1. ЗКП, 260. ЗКП и чл. 82. ст.3 ЗКП, чл. 241 ЗКП, чл.114 ст. 1 ЗКП, чл. 114 ЗКП, чл. 260 у вези чл. 240 ЗКП, чл. 78 ЗКП, чл. 504 љ ЗКП у вези одредбе члана 504 а. став 1. и 63. ЗКП, чл. 114. став 1. ЗКП, чл. 220. ЗКП, чл. 260. ЗКП и 82. ст.3 ЗКП, члан 113. и 114. у вези члана 240. ЗКП), док су у **3** случаја наведене одредбе Закона о јавним тужилаштвима - ЗООЈТ и то одредбе члана 8, или 9. ЗООЈТ и у 1 случају, одредбе Закона о парничном поступку (чл. 181. у вези са 234. и 235. ЗПП?).

На све захтеве достављене електронском поштом (МУП РС) дат је позитиван одговор, иако у њима није навођен правни основ.

- **ОРИОН ТЕЛЕКОМ**

Нема захтева.

- **ВИП МОБИЛЕ**

ВИП мобиле по правилу не одговара позитивно на захтеве за достављање задржаних података, који не испуњавају услове предвиђене законом, а посебно истичу да су негативне одговоре слали судовима и тужилаштву, уколико би се захтев односио на период за који ВИП мобиле не може да врши претрагу података или на информације којима оператер не располаже.

Такође, било је и захтева за достављање задржаних података, али за период дужи од законског рока чувања, којом приликом је ВИП мобиле на овакве захтеве одговарао негативно, јер ВИП мобиле, у складу са Законом о електронским комуникацијама, задржане податке, након утврђеног рока, брише. Руковалац података је негативне одговоре давао и на захтеве државних органа за достављање садржаја SMS прука конкретног корисника, из разлога што се такви подаци код Руковаоца података не бележе и не чувају.

Од укупног броја *свих захтева,* у укупно **216** захтева НИЈЕ НАВЕДЕН ПРАВНИ ОСНОВ у виду цитирања одредби закона. Од наведеног броја, на 30 је дат позитиван одговор.

- **ТЕЛЕКОМ**

Према наводима Руковаоца података, достављање задржаних података државним органима обавља се на основу посебног "Упутства Друштва за за поступање по захтевима надлежних државних органа за подацима о електронским комуникацијама", број: 70749/1 од 07.03.2011. године. У наведеном Упутству је прописано да се истим дефинише поступање по писаним захтевима државних органа међутим, надзором је утврђено да Руковалац података поступа и по захтевима који нису достављени искључиво писаним путем.

Организацију послова на нивоу Руковаоца података спроводи Функција за логистичке и опште послове преко:

- Сектора за безбедност и заштиту, Службе за нормативно правне послове и осигурање имовине,
- Службе за логистичке и опште послове, Одељења за безбедност и заштиту,
- Одељења за логистичке и опште послове извршне јединице, реферата за безбедност и заштиту извршне јединице/радног центра (ИЈ/РЦ):

Сви организациони делови Руковаоца података, одмах по пријему захтева испитују да ли је захтев поднет од стране надлежног државног органа "у складу са законом".

Као надлежни државни органи у Упутству су набројани: судови, јавна тужилаштва, органи МУП у предкривичном и кривичном поступку који поступају по налогу суда, БИА и ВБА, РАТЕЛ и "други државни органи" који могу "на основу закона" тражити "податке из области електронских комуникација".

Упутство разрађује и питање достављања података судском вештаку приликом решавања захтева који су пропраћени наредбом или решењем суда о одређивању вештачења.

Функција за правне послове, на захтев Сектора за безбедност и заштиту, уколико постоји потреба, даје правно мишљење о основаности решавања појединих захтева надлежних државних органа.

Навођење правног основа у писменим захтевима

Од укупног броја поднетих захтева (1851) свих државних органа у **704** случаја НИЈЕ НАВЕДЕН ПРАВНИ ОСНОВ у виду цитирања одређених одредби Закона и од тог укупног броја у **63** случаја негативно је одговорено, односно у **641** позитивно.

У 366 писмених захтева као правни основ наведене су одредбе Законика о кривичном поступку - ЗКП, док се одредбе Кривичног законика као правни основ цитиран у захтевима наводе у 715 случајева.

9) ОСТВАРИВАЊЕ НЕПОСРЕДНОГ, САМОСТАЛНОГ ПРИСТУПА ЗАДРЖАНИМ ПОДАЦИМА ОПЕРАТОРА И ЊИХОВО ПРЕУЗИМАЊЕ ОД СТРАНЕ ДРЖАВНИХ ОРГАНА:

- **ТЕЛЕНОР**

  - *Ко може да приступа*

МУП РС, ВБА и БИА преко Инфо систем апликације могу самостално да приступају ИТ системима Теленора и преузимају задржане податке.

Сваки овакав приступ подацима о комуникацијама бележи се у системским дневницима Теленора, са подацима: датум/време упита, телефонски број, период за који су подаци тражени и кориснички налог са кога је упит упућен.

За сваки од појединачних упита постоје логови у бази Теленора из којих се може видети ко је приступио, односно: корисничко име, да ли су скидани листинзи позиваоца или и позиваних бројева, или мешовито, период који је обухваћен, датум и време упита, подаци о базним станицама и IMEI броју.

Теленор д.о.о. нема увид и не бележи правни основ по ком се ови приступи врше.

  - *Број и структура датих корисничких налога за приступ апликацији:*

БИА, МУП РС и ВБА, имају укупно **75** корисничких налога преко којих неутврђен број службених лица остварује приступ подацима о листинзима и базним станицама са које је разговор започет.

МУП РС има **44** корисничка налога, БИА **24**, а ВБА **6**, плус **1** којим се контролише приступ претходних шест. Од укупног броја налога, сви се не користе.

  - *Број приступа:*

У периоду од 27.03.2011. до 27.03.2012. године, наведени државни органи остварили су непосредан приступ задржаним подацима у базама података Теленор још укупно **272.327** пута - што је *130 пута више* од броја поднетих захтева у наведеном периоду.

  - *Врста задржаних података у које је на овај начин могуће извршити увид и њихово преузимање:*

Приликом самосталног приступа могу да виде код ПРИПЕЈД бројева:

a) број позиваоца - број А,
b) његов IMEI број,
c) број позиваног - број Б,
d) податке базне станице са које је иницран саобраћај,
e) као и врсту сервиса, односно да ли је у питању позив, SMS, MMS, или GPRS.

Код ПОСТПЕЈД корисника, доступни су:

a) датум и време успостављања везе,
b) време трајања разговора или количина података,
c) позивани број
d) и услуга,

при чему се и за позивани број може вршити претрага уколико је у питању претплатник Теленора. Дакле, у том случају, упит/претрага може да се изврши и по Б (позиваном) броју, где ће резултат бити остварен долазни соабраћај са Теленор постпејд бројева.

Код постпејд корисника се у листингу позива *не могу видети IMEI бројеви, ни базне станице са којих су иницирани позиви*, односно за постпејд саобраћај је доступан искључиво комерцијални листинг.

С обзиром на ограничен број података којем се може приступити, на посебан упит, односно захтев за достављање задржаних података из члана 129. ЗЕК, тражиоци од оператора могу да добију већи број података ЗА ПОСТПЕЈД И РОМИНГ кориснике, и то: податке о власнику броја позиваоца и позиваног броја, уколико је претплатник Теленора; адресе базних станица; списак свих SIM картица које су биле у телефону годину дана уназад и др.

- *Структура остварених упита по субјекту и броју извршених упита :*

- МУП РС - **267.976** пута,
- ВБА - **2.872** пута,
- БИА - **1.479** пута.

- *Структура остварених упита по врсти задржаних података:*

- **178.230** индивидуалних упита за 59.000 различитих бројева,
- **3.600** упита за укупан саобраћај 1.870 различитих базних станица за периоде од 1 (једног) до 30 (тридест) дана, при чему Теленор нема евидентирано колико података о комуникацијама и колико различитих бројева је захваћено овим упитима,
- **90.496** упита за 28.100 различитих IMEI бројева, при чему Теленор нема евидентирано колико различитих бројева је захваћено овим упитима.

- **ОРИОН ТЕЛЕКОМ**

Војно-безбедносној агенцији је 30.11.2011. године омогућен приступ задржаним подацима, али без могућности да ВБА изврши увид у садржај комуникације. Конкретни упити ВБА нису евидентирани. Корисничко име и лозинка за приступ одговарајућој

бази података су усмено саопштениц овлашћеном представнику ВБА, који се том приликом легитимисао. Име представника ВБА, које је забележено у документацији Орион Телекома је Александар Митић.

МУП – УКП је у току новембра месеца 2011. године, омогућен приступ задржаним подацима о личности, без могућности да МУП изврши увид у садржај комуникације. Конкретни упити МУП-а нису евидентирани. Корисничко име и лозинку за приступ одговарајућој бази података су усмено саопштени овлашћеном представнику МУП-а, који се том приликом легитимисао. Име представника МУП-а, које је забележено у документацији Орион Телекома је Владимир Грујанић.

Ниједном од наведених органа није технички омогућено да врши непосредан увид у базу података о корисницима (телефонски именик).

Након приступа Web порталу овлашћена лица у ВБА и МУП имају могућност увида у време позива, позив са броја, позивани број, време трајања разговора и call-ID.

На постављено питање овлашћених лица Повереника, да ли државни органи имају непосредан приступ електронској пошти и њеном садржају, представници Руковаоца података су изјавили да надлежни државни органи имају непосредан приступ листингу електронске поште, и то само оној која иде преко сервера ОРИОН-а, док немају приступ оној пошти која се обавља путем *web* мејла и сл.

- **ВИП МОБИЛЕ**

  - *Ко може да приступа:*

У складу са захтевима надлежних државних органа, ВИП мобиле је корисницима (МУП, ВБА и БИА) издао ID картице са чипом (на постављено питање колико картица је издато ком државном органу, Руковалац података није дао прецизан одговор, јер не води тачну евиденцију), којима се аутентификују на систем, те на тај начин добијају могућност приступа серверу ВИП мобиле на коме се налазе апликације. Коришћењем ових картица не може се утврдити број службених лица која остварују приступ подацима о оствареном саобраћају.

  - *Број приступа:*

ВИП мобиле не води евиденцију о томе колико пута су до сада државни органи извршили непосредан приступ задржаним подацима, тј. да не контролише непосредан приступ државних органа задржаним подацима, иако систем генерише тзв. *log* фајлове који садрже податке о извршеним претрагама, и то: корисничко име, време приступа, критеријуме претраге, тип претраге и време трајања сесије.

  - *Врста задржаних података у које је на овај начин могуће извршити увид и њихово преузимање:*

Наведене апликације овлашћеним корисницима омогућавају непосредан приступ следећим подацима:

- претрага података корисника према MSISDN броју и SIM картици (име и презиме, MSISDN, SIM, PUK, IMSI, IMEI, модел телефона и произвођач, ЈМБГ, адреса корисника, додатни контакт телефон),

- лоцирање корисника према MSISDN броју ,

- листинг према броју (позивајући број, позивајући IMEI, позивајућа ћелија, позивани број, позивани IMEI, позивана ћелија, датум, време, тип саобраћаја (разговор, SMS. MMS...)
- листинг по ћелији (позивајући број, позивајући IMEI, позивајућа ћелија, позивани број, позивани IMEI, позивана ћелија, датум, време, тип саобраћаја (разговор, SMS. MMS...) .

- **ТЕЛЕКОМ**

Нису дати подаци, надзор је још увек у току. Начелно, дато нам је до знања да овакви приступи постоје.

  - *Ко може да приступа?*
  - *Број и структура датих корисничких налога за приступ апликацији:*
  - *Број приступа:*
  - *Врста задржаних података у које је на овај начин могуће извршити увид и њихово преузимање:*
  - *Структура остварених упита по субјекту и броју извршених упита :*
  - *Структура остварених упита по врсти задржаних података:*

10) ГЕОГРАФСКО ЛОЦИРАЊЕ МОБИЛНИХ КОРИСНИКА У РЕАЛНОМ ВРЕМЕНУ БЕЗ ПРЕДУСЛОВА ДА СЕ СА ТЕРМИНАЛНЕ ОПРЕМЕ У ТОМ ТРЕНУТКУ ВРШИ КОМУНИКАЦИЈА:

- **ТЕЛЕНОР**

Врши се преко наменских мобилних телефона (све службе) и преко директне ИТ везе (БИА).

Ово лоцирање не представља утврђивање локације мобилне терминалне опреме корисника из тач. 6. чл. 129. ЗЕК, већ географско лоцирање мобилних корисника *у реалном времену* којима су телефони активни и видљиви у мрежи иако не остварују саобраћај, односно иако не позивају, нити су позивани.

Теленор не врши географско лоцирање мобилних корисника за потребе државних органа, али га омогућава на тај начин што у процедури добијања ове функционалности

за наменски телефон, по захтеву МУП РС, БИА, или ВБА, генерални директор Теленора одлучује по захтеву и прослеђује одлуку надлежној служби која се, уколико је позитивна, реализује у техници Теленора која за дати телефон омогућава тражену функционалност.

Сва лоцирања преко наменских мобилних телефона бележе се у системским дневницима Теленора.

- **ОРИОН ТЕЛЕКОМ**

Ову могућност овај оператор нема из разлога што је он искључиво оператор за фисну мобилну телефонију.

- **ВИП МОБИЛЕ**

ВИП Мобиле не врши географско лоцирање мобилних корисника за потребе државних органа.

- **ТЕЛЕКОМ**

Нису се још изјаснили, надзор је у току.

11) ПОСЕБНЕ МОГУЋНОСТИ БЕЗБЕДНОСНО ИНФОРМАТИВНЕ АГЕНЦИЈЕ У САМОСТАЛНОМ ПРИСТУПУ И ПРЕУЗИМАЊУ ЗАДРЖАНИХ ПОДАТАКА:

- **ТЕЛЕНОР**

Подаци о свим комуникацијама оствареним у мрежи Теленор д.о.о, CDR (енгл. call detail record), дневно се достављају БИА и исти представљају копију података о комплетном саобраћају. Подаци о свим комуникацијама (CDR) обављеним преко MSC (енгл. Mobile Switching Center), односно мобилних комутационих централа Теленора, упућују се на BGW (Billing Gateway), одакле се БИА на дневној основи, кроз аутоматизован процес, достављају сви подаци о оствареном саобраћају.

- **ОРИОН ТЕЛЕКОМ**

РАТЕЛ је дана 27.10.2009. године доставио оператеру упутство о начину постављања опреме неопходне државним органима за њихов законит мониторинг, која упутства су заснована на техничким правилницима РАТЕЛ-а, донетим за конкретне системе комуникација, са шематским приказима и техничком спецификацијом опреме. Орион Телеком је поступио према налозима РАТЕЛ-а и у том смислу обезбедио је два PS сервера, као и посебну инфраструктуру (физичке водове), која обезбеђује да сви линкови буду остварени кроз заштићене комуникационе канале (употребом IPSec протокола). [redacted] Након

инсталације наведене ИТ опреме Орион Телеком је исту предао БИА на даљу употребу и одржавање.

БИА је у току октобра месеца 2010. године инсталирала телекомуникациони систем за надзор над електронским комуникацијама у просторије Орион Телекома. Путем инсталиране опреме БИА има могућност да без посебних приступних података (корисничког имена и шифре) остварује увид у задржане податке, као и у садржај телефонске комуникације. Представници Руковаоца података даље наводе да се контакт са представницима БИА у вези наведеног обављао искључиво лично и телефонским путем, тако да не поседују писане трагове о идентификационим подацима нити о садржајима комуникације представника Орион Телекома са представницима БИА-е. Реализовани технички систем не омогућава да се евидентирају конкретни упити, тј. да се утврди који подаци су били предмет увида, те у које време и од стране представника БИА-е.

- **ВИП МОБИЛЕ**

ВИП мобиле је обезбедио опрему за законито пресретање електронских комуникација чиме је омогућено да искључиво БИА може да врши пресретање сардржаја електронских комуникација. Успостављена је веза сервера БИА, преко оптичких каблова са ВИП мобиле системом, одакле се необрађени подаци преузимају од стране софтвера које користи БИА.

- **ТЕЛЕКОМ**

Нису се још изјаснили, надзор је у току.