Република Србија
Повереник за информације
од јавног значаја и заштиту
података о личности
Служба Повереника
Сектор за надзор

Тел: +381 (0) 11 3408 900
Факс:+381 (0) 11 3343 379
Булевар краља Александра 15
11000 Београд
office@poverenik.rs
www.poverenik.rs

ЈКП "ИНФОРМАТИКА"
НОВИ САД

Примљено: 17. 03. 2020
Орг. јед. | Број | Прилог
6217-3/20

Број: 072-04-1015/2020-07

Датум: 11.03.2020. године

На основу члана 78. став 1. тачка 8. и став 2. Закона о заштити података о личности („Службени гласник РС“, бр. 87/2018), и члана 35. Закона о инспекцијском надзору („Службени гласник РС“, бр. 36/2015, 44/2018-др.закон и 95/2018), овлашћена лица Повереника за информације од јавног значаја и заштиту података о личности (у даљем тексту: Повереник), сачинила су

З А П И С Н И К
о извршеном инспекцијском надзору

1. Општи подаци о надзору и надзираном субјекту

Дана 11.03.2020. године, овлашћена лица Повереника за информације од јавног значаја и заштиту података о личности (у даљем тексту: Повереник), извршила су ванредан теренски надзор над спровођењем Закона о заштити података о личности од стране ЈКП „Информатика“ Нови Сад, Булевар цара Лазара 3 (у даљем тексту: Руковалац или Информатика).

Повереник је по службеној дужности покренуо поступак надзора над спровођењем Закона о заштити података о личности од стране Руковаоца, у циљу утврђивања чињеница и околности услед којих је дошло до повреде података о личности дана 01.03.2020. године, и то на тај начин што је злонамерни софтвер „закључао“ фајлове на 120 сервера и преко 2000 радних станица.

Надзор су извршила овлашћена лица Повереника Маријана Софиљ-Аћимовић, број службене легитимације 010 и Александра Лакићевић, број службене легитимације 013.

У погледу чињеница које се односе на статус, организацију и делатност Руковаоца, утврђено је следеће:

- Назив Руковаоца је: Јавно комунално предузеће „Информатика“ Нови Сад, Булевар цара Лазара 3;

- Матични број Руковаоца података је: 08023182, ПИБ 101651557.

Надзор је започет дана 11.03.2020. године у 11,00 часова, у просторијама седишта Руковаоца.

Надзирани субјекат је о предстојећем надзору обавештен телефонским путем дана 05.03.2020. године.

Присутним представницима Руковаоца уручен је налог за надзор.

Као представници надзираног субјекта, вршењу надзора присуствовали су:

- Ненад Барац, директор,
- Милан Краљевић, лице за заштиту података о личности,
- Бранислав Ђуричић, помоћник директора за обраду и опште регистре,
- Светлана Суџум, помоћница директора за правне послове,
- Маријана Захарија, помоћница директора за финансијско рачуноводствене послове и
- Биљана Јовчић, организатор послова система квалитета.

2. Предмет надзора

Повереник је дана 05.03.2020. године обавештен од стране Руковаоца, да је у недељу 01.03.2020. године око 05.00 часова дошло до компромитовања ИТ инфраструктуре Руковаоца. Такође, већ 02.03.2020. и у многим медијима се појавила вест о наведеном догађају.

Повереник је по службеној дужности покренуо поступак инспекцијског надзора – ванредни теренски надзор, над применом Закона о заштити података о личности, а у циљу непосредног утврђивања релевантних чињеница и околности везаних за догађај у коме је дошло до компромитовања ИТ инфраструктуре Руковаоца, односно да ли је и на који начин дошло до повреде података о личности.

3. Утврђено чињенично стање

На питање овлашћених лица Повереника на који начин је, како се у Обрасцу обавештења Повереника о повреди података о личности наводи, дошло до „компромитације ИТ инфраструктуре", надзору присутни представници Руковаоца су изјавили да је дана 01.03.2020. године око 19 часова помоћник директора за обраду и опште регистре, Бранислав Ђуричић, установио да је дошло до уласка „ransomwera" у систем, односно злонамерног софтвера који закључава сервере и рачунаре, тј. фајлове на њима.

Имајући у виду да се на успостављању система и „откључавању" података још увек ради, а да надлежне службе паралелно врше дигиталну форензику читавог догађаја, представници Руковаоца нису могли са сигурношћу да потврде на који начин је дошло до продора наведеног софтвера у рачунарски систем Руковаоца, али се претпоставља да је злонамерни софтвер „напао" мејл сервер Руковаоца, који је на Windows платформи, а који је потом, највероватније, ушао у систем отварањем електронске поште од стране неког од корисника 2000 радних станица, у чијем прилогу се налазио „заражени" фајл. Каснији развој догађаја је подразумевао уобичајено деловање овакве врсте „ransomwera" који врши закључавање датотека и онемогућава расположивост различите Windows услуге.

На питање овлашћених лица Повереника, а везано за предметни догађај повреде података о личности, о којој врсти података о личности се у конкретној ситуацији ради, о ком броју лица се ради, као и који је број података о личности чија је безбедност повређена, представници Руковаоца су се изјаснили да не могу са сигурношћу да одговоре на наведена питања из разлога што је структура читавог система обраде података који је погођен нападом врло сложена, те је и улога Информатике у појединим обрадама података о личности различита. У том смислу, Информатика је Руковалац подацима о личности који се односе на њихове запослене, на грађане чије податке о личности Руковалац одрађује у оквиру поступка обједињене наплате, као и података који се обрађују у оквиру збирки података које су раније пријављене у Централни регистар који је Повереник водио на основу Закона о заштити података („Сл. гласник РС“, бр. бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012-пропис престао да важи), и то: Евиденција о корисницима комуналних услуга, Кадровска евиденција, Евиденција о присутности на послу, Евиденција о бројевима службених телефона и Евиденција о видео надзору.

Што се тиче података о личности чију обраду Информатика врши у својству руковаоца, представници Руковаоца су изјавили да сервер, на којем се налазе подаци о личности грађана који се обрађују у сврху издавања рачуна у оквиру обједињене наплате, није погођен наведеним злонамерним софтвером. Захваљујући томе што је на наведеном серверу инсталиран Линукс (Linux) оперативни систем, овај сервер и није био мета напада овог ransomwera, те су подаци о личности грађана остали у интегралном облику и њихова безбедност овом приликом није била угрожена. Чињеница је да су апликативни софтвери ИБС и ОРЕГ били обухваћени нападом и исти нису били у функцији од 01.03. до 06.03.2020. године, односно до 10.03.2020. године, али да је одмах након успостављања рада наведених софтвера извршена провера свих података, којом приликом је утврђено да подаци грађана нису били предмет напада. Као доказ наведеној тврдњи представници Руковаоца су овлашћеним лицима Повереника предали копију документа под називом „Извештај“ сачињен од стране Службе Општи регистри од 10.03.2020. године, као и копију документа под називом „Извештај о предузетим активностима Службе за обраду података и рекламација услед новонастале ситуације напада на информациони систем ЈКП“Информатика“ Нови Сад“ од 11.03.2020. године, који се налазе у прилогу овог Записника и чине његов саставни део.

С друге стране, део података о личности, који се односи на запослене код Руковаоца, односно подаци о личности запослених које Руковалац обрађује у складу са прописима којим се регулише област радних односа, налази се на опреми која је обухваћена предметним софтверским нападом, и наведени подаци су такође су били закључани. Ради се о подацима о личности за 232 (двестатридесетдва) запослена. Сви подаци су откључани и потпуно расположиви за све даље радње обраде.

У даљем поступку надзора, представници Руковаоца су изјавили да део опреме и података који су на њима смештени, није у надлежности Руковаоца, односно да Руковалац не располаже информацијама о томе да ли се и на којој опреми налазе подаци о личности. Руковалац је успоставио ИТ инфраструктуру коју пак даље користе различити руковаоци за своје сврхе из својих надлежности.

На питање овлашћених лица за које све врсте обраде података о личности је Информатика у својству обрађивача и ко су руковаоци у чије име и за чији рачун Информатика врши те обраде, представници Информатике су се изјаснили да се у систему налази опрема

различитих руковалаца, да је ту смештена опрема која је стара и преко 30 година и коју је Информатика затекла, тако да за многе од њих Информатика, по њиховом мишљењу, не представља обрађивача, већ је само пружен простор и инфраструктура помоћу које је сва та затечена опрема повезана на систем. Представници Руковаоца су даље навели да Информатика дужи низ година пружа услуге Hosting-а разним руковаоцима, као и да су те обраде углавном засноване на различитим одлукама, споразумима и другим актима којима нису посебно регулисана питања везана за обраду података о личности, тако да Информатика, бар до сада, није препознала своју улогу као обрађивача у наведеним ситуацијама.

С тим у вези, овлашћена лица Повереника су предочила надзору присутним представницима Руковаоца да је одредбама члана 4. тачка 8. Закона о заштити података о личности прописано да је руковалац физичко или правно лице, односно орган власти који самостално или заједно са другима одређује сврху и начин обраде, док је одредбама тачке 9. истог члана прописано да је обрађивач физичко или правно лице, односно орган власти који обрађује податке о личности у име руковаоца. Чланом 45. Закона прописано је да ако се обрада врши у име руковаоца, руковалац може да одреди као обрађивача само оно лице или орган власти који у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама овог закона и да се обезбеђује заштита права лица на које се подаци односе.

Такође, представницима Информатике је указано и на то да обрада од стране обрађивача мора бити уређена уговором или другим правно обавезујућим актом, који је закључен, односно усвојен у писменом облику, што обухвата и електронски облик, који обавезује обрађивача према руковаоцу и који уређује предмет и трајање обраде, природу и сврху обраде, врсту података о личности и врсту лица о којима се подаци обрађују, као и права и обавезе руковаоца.

На питање овлашћених лица Повереника да ли Информатика, у својству обрађивача, на наведени начин уредила питања везана за обраду података са другим руковаоцима, представници Информатике су се изјаснили одрично. Такође, на питање овлашћених лица Повереника да ли Руковалац води евиденције радњи обраде из члана 47. Закона о заштити података о личности, представници Руковаоца су се изјаснили да Информатика не води евиденцију о радњама обраде података о личности, али да ће без одлагања приступити успостављању исте.

На питање овлашћених лица Повереника да ли је Информатика испоштовала обавезе прописане одредбама члана 52. Закона о заштити података о личности, односно да ли је по сазнању за повреду података о личности обавестила остале руковаоце података чија је опрема део система обухваћеног нападом злонамерног софтвера, представници Руковаоца су се изјаснили да је Информатика дана 03.03.2020. године упутила допис број 6235/20 на преко 170 адреса институција, установа, фирми и др. на који начин су исти обавештени да је дана 01.03.2020. године извршена компромитација ИТ инфраструктуре Информатике. Овлашћеним лицима Повереника је предата копија наведог дописа као и списак интитуција којима је исти достављен. Наведени допис и списак налазе се у прилогу овог Записника и чине његов саставни део.

Руковалац је, у складу са одредбама члана 53. Закона о заштити података о личности, путем саопштења у средствима јавног информисања, као и у електронским медијима (shorturl.at/izST7, shorturl.at/vBI46 и др.), обавестио лица на која се подаци односе-грађане о нападу злонамерног софтвера на информациони систем Руковаоца.

На питање овлашћених лица Повереника да ли су наведеним софтвером „заражени" и системски бекапови (backup) предметног рачунарског система, представници Руковаоца су одговорили потврдно, односно да су бекапови такође обухваћем овим нападом, да су подаци у њима били закључани, али да су захваљујући обучености особља које је запослено код Руковаоца, као и помоћи многих колега из струке (стручњаци БИА, приватне ИТ куће и др...), готово сви подаци, па и бекапови, откључани као и да се још увек ради на успостављању расположивости свих потребних сервиса.

На питање овлашћених лица Повереника које је Руковалац мере предузео, а у вези са предметном повредом података, представници Руковаоца су се изјаснили да је пре свега цео информациони систем изолован од спољног утицаја, тј. интернета. Стручни тим Руковаоца је у сарадњи са колегама ИТ стручњацима, одмах приступио изградњи нове софтверско-хардверске архитектуре информационог система, а у циљу спречавања оваквог или сличног поновног покушаја продора у информациони систем Руковаоца.

Представници Руковаоца података су навели да је Информатика увела ИСО стандард 27001-систем менаџмента безбедношћу информација, те да је последња контрола имплементације наведеног стандарда била у месецу јуну 2019. године. С тим у вези, Руковалац података ће кроз поступак ревизије акта о процени ризика, а у оквиру страндардизованог процеса управљања ризицима из ИСО стандарда 27001, предузети све неопходне мере.

4. Мере за отклањање незаконитости

У складу са чланом 79. став 1. тачка 2. Закона о заштити података о личности и члана 27. став 1-4. Закона о инспекцијском надзору, овлашћена лица Повереника су, пошто су у поступку надзора утврдила незаконитости у поступању Руковаоца, Руковаоцу предложила, односно наложила мере за отклањање утврђених незаконитости.

Мере за отклањање незаконитости:

Налаже се:

1. Руковаоцу да, сагласно члану 47. Закона о заштити података о личности, успостави и води евиденцију о свим радњама обраде података о личности за које је одговоран, а за које није успостављена евиденција о радњама обраде, и то за све радње обраде које врши било да је у улози руковаоца или обрађивача података о личности.

2. Руковаоцу да, сагласно члану 52. став 4. тачка 4. Закона о заштити података о личности, достави опис мера које је Руковалац предузео или чије предузимање је планирано у вези са повредом, укључујући и мере које су предузете у циљу умањења штетних последица напада злонамерног софтвера .

О поступању по изреченим мерама за отклањање незаконитости надзирани субјекат је дужан да обавести овлашћена лица Повереника у року од 30 дана од дана пријема овог записника. Уз обавештење, Руковалац је дужан да приложи и документацију, односно други материјал из кога је видљиво да су утврђени незаконитости отклоњене, а прописане обавезе испуњене.

Ако надзирани субјекат у остављеном року не поступи по изреченим мерама за отклањање незаконитости, односно не отклони незаконитост и не испуни прописане обавезе, Повереник ће донети решење којим изриче мере за отклањање незаконитости и испуњавање прописаних обавеза.

Надзор је завршен дана 11.03.2020. године у 14,00 часова.

4. Примедбе на записник

Записник је сачињен у три истоветна примерка, од којих се један примерак доставља Руковаоцу података, а два примерка су за потребе Повереника.

ПРЕДСТАВНИЦИ РУКОВАОЦА

Нонад Бараћ

Милан Краљевић

Бранислав Буричић

Светлана Суџум

Маријана Захарија

Биљана Јовчић

ОВЛАШЋЕНА ЛИЦА ПОВЕРЕНИКА

Маријана Софиљ-Аћимовић

Александра Лакићевић