



## ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

### РЕЗИМЕ ОБЈЕДИЊЕНОГ ИЗВЕШТАЈА О РЕВИЗИЈАМА СВРСИСХОДНОСТИ ПОСЛОВАЊА

„Информациони системи у јавном градском превозу”

19. фебруар 2024. године

Државна ревизорска институција је спровела четири ревизије сврсисходности „Информациони системи у јавном градском превозу“ (у Нишу, Крагујевцу, Новом Саду и Београду).

Ревизија информационог система градског превоза подразумева преглед и анализу постојећег система ради идентификације недостатака и предлога за побољшања. Ревизија се обично врши како би се осигурала ефикасност и поузданост система, као и како би се идентификовале могућности за унапређење.

У конкретним случајевима, ревизија обухвата ревизијске поступке над оба подсистема: контролу наплате карата (ticketing) и контролу пружених услуга од стране превозника како би се плаћање вршило у складу са квалитетом и квантитетом пружених услуга- (monitoring).

Информациони системи у градском превозу користе се за побољшање ефикасности, као и за пружање информација путницима.

Информациони системи у локалним самоуправама који се односе на јавни градски превоз треба да имају две основне функционалности: контролу наплате карата и контролу пружених услуга од стране превозника како би се плаћање вршило у складу са квалитетом и квантитетом пружених услуга.

Базе података у овим системима садрже осетљиве личне податке (за месечне карте прикупљају се подаци из личне карте) и изискују примену одређених мера заштите. Проблематику заштите податка осигураника предвиђају више законских прописа из области здравственог осигурања, а посебно Закон о заштити података о личности и Закон о информационој безбедности, који са својим уредбама уређује обавезне мере заштите, које даље, треба примењивати са циљем очувања интегритета, поверљивости и расположивости података.

Циљ ревизије би био да се оцени ефективност и ефикасност информационих система у локалним самоуправама који се односе на јавни градски превоз односно у којој мери су примењене мере испуниле неопходне циљеве када је у питању управљање

системима, поузданост информационих система и управљање подацима корисника-грађана, и у којој мери је систем омогућава ефикасност контроле наплате и плаћања услуга превоза. Поузданост електронских података и информационих система подразумева интегритет, комплетност, тачност, конзистентност и очување података, безбедност информационог система и континуитет пословања, имајући у виду сврху за коју се ти подаци и системи користе.

У Нишу, услугу градског превоза пружа ЈКП Дирекција за јавни превоз Града Ниша. Пружалац услуге када је информациони систем у питању је Bus Logic DOO Пожаревац. Систем је имплементиран 2020. године и у досадашњем периоду није спроведена ни интерна ни екстерна ревизија овог система. Систем се за сада користи за евиденцију пружених услуга од стране превозника, док се не користи и за евиденцију персонализованих картице, јер не постоје електронске персонализоване карте.

У Крагујевцу, услугу градског превоза пружа ЈКП Шумадија Крагујевац. Пружалац услуге када је информациони систем у питању је фирма Kentkart Southeast Europe DOO Београд. Систем је имплементиран 2019. године и у досадашњем периоду није спроведена ни интерна ни екстерна ревизија овог система. Систем се за сада користи и за продају карата и за евиденцију-контролу пружених услуга од стране превозника. ЈКП Шумадија Крагујевац врши обраду података о личности и то: запослених лица, радно ангажованих, као и лица којима се пружају комуналне услуге а коју обраду прикупљања, бележења, разврставања и раздвајања, обезбеђивања и коришћења (приступ) података, стављање на увид и чување и брисање врши у аутоматизованом облику кроз програме и у неаутоматизованом (папирном) облику.

У Новом Саду, услугу градског превоза пружа Јавно градско саобраћајно предузеће "Нови Сад". Пружалац услуге када је информациони систем у питању је фирма Bus Logic DOO Пожаревац. Систем је имплементиран 2019. године и у досадашњем периоду није спроведена ни интерна ни екстерна ревизија овог система. Систем се за сада користи и за продају карата и за евиденцију-контролу пружених услуга од стране превозника.

У Београду, за пружање услуга градског превоза задужен је Секретаријат за јавни превоз, као део градске управе града Београда. Пружалац услуге када је информациони систем у питању је фирма Kentkart Southeast Europe DOO Београд. Систем је имплементиран 2010. године и у досадашњем периоду није спроведена ни интерна ни екстерна ревизија овог система. Систем се за сада користи и за продају карата и за евиденцију-контролу пружених услуга од стране превозника.

Ревизијом би били обухваћени наведени системи у ова четири града.

У току ревизије је анализирана достављена документација, обављен је један број интервјуа са одговорним лицима у субјектима ревизије, и коришћени су јавно доступни подаци. Након спроведених ревизија утврдили смо:

Потребна је сарадња градских управа и градских предузећа које врше услугу јавног градског превоза у Републици Србији, у циљу покретања заједничке иницијативе ка стандардизацији информационих система у јавном градском превозу, што је кључни корак ка пружању бољих и свеобухватнијих услуга грађанима и успостављању неопходне поузданости система.

Наведено заснивамо на закључцима и налазима који су изложени у наставку текста:

1. Информациона безбедност није успостављена на свеобухватан начин јер нису усвојене и примењене мере заштите које обухватају управљање ИТ ризицима и ИТ инцидентима, успостављање адекватне организационе ИТ структуре, усвајање, ажурирање и примену одговарајућих правилника, политика и процедура у области информационе безбедности, управљање приступом системима и управљање процесом континуитета пословања, што је неопходно како би била осигурана поузданост система.

Због недостатка довољно стручног знања и недостатка кадровских капацитета, организација ИТ безбедности није успостављена тако да обухвата примену адекватних докумената која уређују ову област, управљање инцидентима и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система.

Није успостављен процес приступа систему на задовољавајући начин, због тога што нису усвојене процедуре које уређују овај процес и није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података.

Нису у потпуности усвојена и имплементирана правила и процедуре за континуитет пословања у ванредним околностима, због недовољно финансијских средстава, недовољно хардверских ресурса, недовољно искуства и стручног знања и обученог ИТ кадра, што може за последицу имати нефункционисање система у неодређеном временском периоду, па самим тим и отежано пружање услуга.

Субјекти нису успоставили управљање ИТ ризицима, што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера. Нарочито када се документација налази у електронском облику.

2. Није успостављен ефективан механизам сарадње са пружаоцима услуга, зато што нису усвојена и имплементирана правила и процедуре када је у питању ова област, није обезбеђен континуитет пословања у случају раскида сарадње и није процес обраде података о личности уређен на начин прописан законом

Код већине субјеката, сарадња са пружаоцем услуга није у потпуности уређена процедурама и другим актима, што за последицу има већи степен рањивости информационог система.

Сарадњу са пружаоцем услуга није у потпуности уређена када је у питању заштита и обрада података, у смислу успостављања механизма којим се осигурава да је пружалац услуге усвојио услове за заштиту и безбедност података и да ли их спроводи, начина на који се прати реализација извршења уговора и на начин прописан Законом о информационој безбедности и Законом о заштити података о личности што за последицу има смањени степен поузданости система.

Не постоје планови континуитета пословања у случају раскида сарадње са пружаоцем услуга што за последицу може имати отежану наплату, онемогућено

праћење ГПС сигнала возила, отежан обрачун за плаћање услуга превозницима и онемогућено пружање услуга грађанима у дужем временском периоду.

3. Већина субјеката није успоставила свеобухватан механизам употребе апликативних контрола у циљу боље контроле тачности података, али и свеобухватнијих услуга грађанима пре свега у смислу бољег информисања и интеграције са другим информационим системима.

Субјекти ревизије нису у потпуности процедурама и другим актима уредила процес наплате карата и механизам контроле тог процеса, што за последицу може имати неусклађеност података о броју продатих карата које приказује апликација са подацима превозника, који врше продају карата.

Субјекти нису у потпуности процедурама и другим актима уредили контролу пружених услуга од стране ангажованих превозника, што за последицу може имати плаћање услуга у износу вишем од износа који је заснован на стварно реализованим услугама.

Државна ревизорска институција, након спроведене ревизије „Информациони системи у јавном градском превозу“, даје следеће препоруке:

да успоставе организацију информационе безбедности која обухвата усвајање, ажурирање и имплементацију аката која уређују ову област – акта (правилника) о информационој безбедности, процедура које се односе на ИТ безбедност, управљање инцидентима, и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података; уреде процес приступа систему, што подразумева усвајање/ажурирање процедура које уређују овај процес и контролу тог процеса, а односи се на логички приступ, рад на даљину и физичку заштиту система; успоставе свеобухватан план континуитета пословања у ванредним околностима, што подразумева усвајање/ажурирање постојећег Правилника (Акта) о безбедности ИКТ система, усвајање процедуре за континуитет пословања у ванредним околностима и управљање резервним копијама података; успоставе управљање ИТ ризицима, што подразумева евидентирање, анализу, класификацију ИТ ризика и дефинисање стратегије за смањивање/отклањање ризика; усвоје/ажурирају и имплементирају правила и процедуре за безбедност података када је у питању сарадња са пружаоцима услуга што подразумева обавезну примену мера заштите података, и успостављање механизма за праћење примене тих мера; уреде сарадњу са пружаоцем услуга када је у питању заштита и обрада података, на начин прописан Законом о информационој безбедности и Законом о заштити података о личности; успоставе план континуитета пословања у случају раскида сарадње са пружаоцима услуга; ЈКП Дирекција за јавни превоз града Ниша и ЈКП Шумадија Крагујевац процедурама и другим актима уреди процес наплате карата и механизам контроле тог процеса, Градска управа града Београда, Секретаријат за јавни превоз упути иницијативу Јавном комуналном предузећу Наплата превозне услуге Београд да процедурама и другим актима уреди процес наплате карата и механизам контроле тог процеса; ЈКП Дирекција за јавни превоз града Ниша и ЈКП Шумадија Крагујевац процедурама и другим актима уреди контролу пружених услуга од стране ангажованих превозника, Градској управи града Београда, Секретаријату за јавни превоз да током увођења система, постојеће процедуре прилагоди новом систему.

