Државна ревизорска институција

Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у Републичком фонду за здравствено осигурање (РФЗО)

- Матичну евиденцију јединствено за територију Републике Србије устројава и организује Републички фонд за здравствено осигурање (РФЗО).
- Матичну евиденцију чине подаци о:
  1) осигураницима;
  2) члановима породице осигураника;
  3) обвезницима плаћања доприноса;
  4) коришћењу права из обавезног здравственог осигурања.
- Подаци о коришћењу права из обавезног здравственог осигурања воде се одвојено од других података и тим подацима рукује за то овлашћено лице Републичког фонда за здравствено осигурање (РФЗО).
- Информациони систем МЕОП је кључна апликација за пословање РФЗО.

ДРИ је у претходним годинама уочила проблеме у функционисању информационих система РФЗО у више области:

- **X** стратегијски приступ;
- **X** поузданост информационих система;
- **X** начин пријаве осигураника и приступа картону осигураника;
- **X** синхронизације података са здравственим установама.

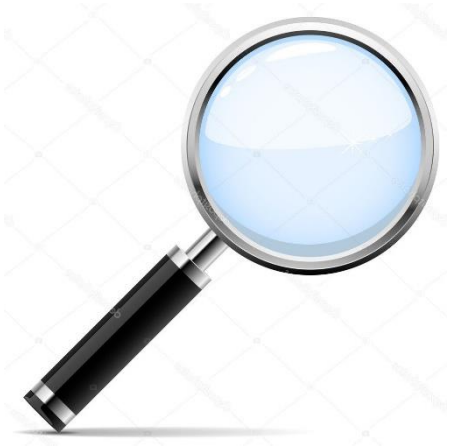
Циљ ревизије је да се оцени ефективност информационог система МЕОП у Републичком фонду за здравствено осигурање (РФЗО).

Ревизорска питања

1. Да ли је успостављено ефективно ИТ управљање у РФЗО?

2. У којој мери успостављене мере безбедности података у информационом систему МЕОП обезбеђују поверљивост, заштиту и интегритет података (поузданост ИС)?

3. У којој мери је уговорни однос са пружаоцем услуге одржавања и МЕОП обезбедио испуњење пословних циљева и неопходни ниво поузданости ИС?



Републички фонд за здравствено осигурање (РФЗО)

Извори информација – Републички фонд за здравствено осигурање (РФЗО), филијале РФЗО и здравствене установе различитих нивоа здравствене заштите.

Период обухваћен ревизијом је од 1. јануара 2020. године до 31. децембра 2022. године.

1.

РФЗО није у потпуности успоставио ефективно ИТ управљање због недостатка кадровских капацитета, непрепознавања могућих ИТ ризика и управљања подацима из матичне евиденције осигураника

НАЛАЗИ

1.1 РФО није донео ИТ стратегију за период 2022–2024. године.

1.2 ИТ управљање није успостављено на адекватан начин због непрепознавања свих ИТ ризика и недовољних кадровских капацитета.

1.3 РФЗО није успоставио правила управљања подацима из матичне евиденције осигураника, којима би онемогућио приступ личним подацима осигураника и без њиховог физичког присуства.

РФЗО није донео ИТ стратегију за период 2022–2024. године

Стратегија се по правилу усваја за период од пет до седам година, а остваривање њених циљева планира се и прати посредством акционог плана за спровођење стратегије.

РФЗО је усвојио ИТ стратегију за период 2019–2021. године.
РФЗО није израдио ИТ стратегију за период 2022–2024. године и пратећи акциони план ради спровођења мера из ИТ стратегије.

РФЗО наводи да због пандемије вируса COVID 19 и додатних послова и задатака није усвојио нову стратегију, за период 2022–2024. године.

Користи од усвајања ИТ стратегије и акционог плана јесу олакшано планирање развоја ИТ, сврсисходно коришћење расположивих финансијских средстава и унапређено ИТ управљање и тиме остваривање пословних циљева.

ИТ управљање није успостављено на адекватан начин због непрепознавања свих ИТ ризика и недовољних кадровских капацитета

Управљање ризицима обухвата идентификацију, процену и контролу потенцијалних догађаја и ситуација које могу утицати на остваривање циљева корисника јавних средстава обезбеђујући да ће ти циљеви бити остварени (члан 7 став 1 Правилника о заједничким критеријумима и стандардима за за успостављање, функционисање и извештавање о систему ФУК у јавном сектору).

РФЗО није идентификовао све ИТ ризике, а последично ни планове и мере за умањење ризика.
РФЗО је усвојио Стратегију управљања ризицима, а за период ревизије 2020–2022. године утврдио три ИТ ризика која се понављају сваке године.

У Сектору за развој и ИТ у Дирекцији РФЗО у Београду на 34 систематизована радна места, запослено је 15 лица. У 29 филијала РФЗО, попуњеност радних места на ИТ пословима је 63%.

Значајно ограничење у развоју ИКТ система је недовољан број запослених у Сектору за развој и ИТ и смањена могућност запошљавања нових кадрова, што последично утиче и на спровођење мера за умањење ИТ ризика.

Последице непрепознавања ИТ ризика могу бити непотребно велики трошкови у случају настанка нежељеног догађаја (који се могао спречити) или велики нефинансијски губици (у првом реду података) због немогућности благовременог предузимања мера.

РФЗО није успоставио правила управљања подацима из матичне евиденције осигураника, којима би онемогућио приступ личним подацима осигураника и без њиховог физичког присуства

Исправа о осигурању је КЗО и потврда о здравственом осигурању (члан 25 и 26 Закона о здравственом осигурању).

РФЗО синхронизацију података на контактном микроконтролору (ЧИП) КЗО не врши електронским путем, већ је потребна физичка синхронизација података на ЧИП-у.

Картица здравственог осигурања (КЗО) се не користи у свим ЗУ на идентичан начин, јер се подацима матичне евиденције може приступити без идентификације корисника (учитавањем КЗО или коришћењем минимум два податка – ЈМБГ и ЛБО/број здравствене исправе).

РФЗО није обезбедио да ЗУ приступају подацима матичне евиденције осигураника на јединствен начин, који би обезбедио већу поузданост и заштиту личних података осигураника.

КЗО су почеле да се користе 2013. године и за претходних десет година је технолија израде картица значајно напредовала. У пракси ЗУ КЗО користи као „обичну“ књижицу и само један податак (ЛБО или број ЗИ), а не минимум два ради идентификације осигураника.

Последице приступа матичној евиденцији осигураника без уноса минимум два податка (или учитавањем КЗО) оставља могућност да се од стране корисника система оствари увид у личне податке осигураника и у случајевима када он није присутан, идентификован на други начин или када то уопште није потребно.

2.

РФЗО није у потпуности успоставио управљање информационом безбедношћу ИС МЕОП јер није попунио радна места у Сектору за информациону безбедност и заштиту података и не прати и не контролише додељена права приступа ИС МЕОП, што може довести до неовлашћеног приступа подацима осигураника и остварeним правима у здравственој заштити

НАЛАЗИ

2.1 РФЗО није у потпуности успоставио логички приступ ИС МЕОП који обезбеђује поузданост информационог система (контролу права приступа).

2.2 РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података.

2.3 РФЗО није у потпуности успоставио процес праћења и контроле приступа ИС МЕОП од стране ЗУ и запослених у РФЗО.

РФЗО није у потпуности успоставио логички приступ ИС МЕОП који обезбеђује поузданост информационог система (контролу права приступа)

Оператер ИКТ система је у обавези да предвиди процедуру за одобравање и укидање овлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа, тако што предвиђа услове за одобравање и укидање овлашћеног приступа, проверу адекватности одобреног нивоа приступа и доделу јединствене идентификационе ознаке лицу којем се одобрава приступ (члан 10 став 1 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

Додела и коришћење администраторских права приступа треба да буде ограничена и контролисана (члан 10 став 4 Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја).

РФЗО додељивање привилегованих (администраторских) права на приступ врши на основу одлуке Сектора за развој и информационе технологије (члан 14 Акта о безбедности ИКТ система РФЗО).

РФЗО није успоставио контролне механизме да:

- *додела и коришћење администраторских права приступа буде ограничена и контролисана и*
- *креирање, додељивање, измена и деактивирања корисничких имена (корисничких идентификатора) у ИС МЕОП буде у складу са одредбама Акта о безбедности ИКТ система.*

Након издавања Нацрта извештаја РФЗО је доставио доказе да је извршио анализу матрице привилегија администаторских и корисничких налога у ИС МЕОП (додељених права приступа) и ускладио права приступа ИС МЕОП у складу са прописима и интерним актима.

РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података

Мере заштите ИКТ система односе се на успостављање организационе структуре са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система (члан 7 став 3 тачка 1 Закона о информационој безбедности).

Оператор ИКТ система дужан је да у оквиру организационе структуре, у складу са природом, обимом и сложеношћу пословања, утврди послове и одговорности запослених, у циљу управљања информационом безбедношћу (члан 2 став 1 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја).

РФЗО је успоставио организациону структуру са утврђеним пословима и одговорностима запослених за ИТ безбедност. Међутим, РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података, иако је Правилником о организацији и систематизацији послова систематизовано 12 радних места.

Поједини запослени на ИТ пословима у опису послова имају задужење везано за информациону безбедност, а да им то није примарни радни задатак. Запослени на ИТ пословима су учествовали на две обуке за ИТ безбедност у периоду ревизије (2020–2022. година).

Управљање информационом безбедношћу је изузетно важна област и захтева одговарајућу организацију и запослене који могу заштитити ресурсе РФЗО, како опреме тако и информационог система од неовлашћеног упада и приступа подацима.

Неадекватно управљање информационом безбедношћу може имати дугорочни утицај на циљеве организације, а у ИТ делу рањивост информационог система и могућност злоупотреба података из ИС МЕОП.

РФЗО није у потпуности успоставио процес праћења и контроле приступа ИС МЕОП од стране ЗУ и запослених у РФЗО

Оператор ИКТ система треба да обезбеди да се у ИКТ систему формирају записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати (члан 18 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја и члан 22 Акта о безбедности ИКТ система РФЗО).

РФЗО бележи приступ ИС МЕОП (од стране запослених у РФЗО-у и ЗУ) путем записа о догађајима (лог фајлова).

РФЗО нема успостављена правила и процедуре редовног праћења и контроле записа о догађајима (лог фајлова) у одређеном периоду, већ се зависно од случаја до случаја ради проверу записа о догађајима (лог фајлова).

Записи о догађајима (лог фајлови) су веома обимни и захтевају редовно праћење и контролу.

Користи од праћења и редовне контроле записа о догађајима (лог фајлова) су брже откривање/реаговање на инциденте/нежељене догађаје а тиме и мања могућност злоупотреба података из ИС МЕОП.

3.

РФЗО није у потпуности успоставио ефективан механизам сарадње, односно није у потпуности уредио правилима и процедурама однос са пружаоцем услуге одржавања ИС МЕОП и мере којима обезбеђује континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП

НАЛАЗИ

3.1 РФЗО није успоставио (уредио) однос са пружаоцем услуга одржавања ИС МЕОП у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.

3.2 РФЗО је обезбедио заштиту осетљивих података о осигураницима тако да врши псеудонимизацију података базе МЕОП.

3.3 РФЗО није предвидео мере које обезбеђују континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

РФЗО није успоставио (уредио) однос са пружаоцем услуга одржавања ИС МЕОП у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом

РФЗО је дужан да споразумом регулише обавезе пружаоца услуге у вези са информацијама и средствима која су доступна пружаоцима услуге (члан 26 Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја).

РФЗО није дефинисао правила и процедуре којима се уређује сарадња са пружаоцем услуге одржавања ИС МЕОП, у делу нивоа доступности и врсте информација којима може да приступи пружалац услуге, начине приступа информацијама и средствима и надзора над приступом.

Регулисање односа са пружаоцем услуга одржавања ИС МЕОП у овом делу подразумева управљање информационом безбедношћу за шта је потребно јачати кадровске капацитете и стручна знања.

Као што смо навели, информациона безбедност није кадровски успостављена у РФЗО, што може имати утицаја на реализацију уговора о одржавању ИС МЕОП, квалитет извршених услуга, контролу приступа ИС, надзор над извршењем уговорних обавеза и заштиту података.

РФЗО није предвидео мере које обезбеђују континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП

Оператор ИКТ система одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мере заштите ИКТ система односе се и на континуитет пословања у ванредним околностима (члан 7 Закона о информационој безбедности).

Такође, одредбама члана 29 Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја, прописане су мере које обезбеђују континуитет обављања посла у ванредним околностима.

РФЗО је знатно зависан од добављача, тј. пружаоца услуге развоја и одржавања ИС МЕОП и у случају раскида/отказа уговора, РФЗО у дужем временском периоду неће бити у стању да врши неопходне измене ИС МЕОП. Такође, у уговору о одржавању ИС МЕОП није дефинисан миграција података у случају да РФЗО промени пружаоца услуга развоја ИС.

План континуитета пословања пружа одговор на ризике који постоје у вези са губитком података и треба да буде успостављен и периодично тестиран. Ризик је већи када је у питању раскид сарадње са пружаоцима услуга одржавања информационог система, јер у том случају недостаје неопходно знање потребно за наставак одржавања и развоја, а нарочито у случају потенцијалног преласка на нови систем и неопходну миграцију података.

Неопходно је да РФЗО унапреди ИТ управљање, обезбеди виши ниво информационе безбедности и обезбеди континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП

ДРИ је **Републичком фонду за здравствено осигурање (РФЗО)** дала девет препорука, од којих су најважније:

- да у циљу успостављања организационе структуре за ИТ управљање, предузме мере за јачање кадровских капацитета кроз повећање броја и/или стручних знања запослених;
- да предузме мере на кадровском јачању Сектора за информациону безбедност и заштиту података;
- да успостави правила управљања подацима матичне евиденције осигураника којима би се, уз обавезно физичко присуство осигураника, омогућио приступ личним подацима осигураника;
- да предузме активности у циљу континуиране едукације запослених који обављају ИТ послове;
- да успостави правила и процедуре за редовну контролу и праћење приступа ИС МЕОП;
- да предузме активности у циљу успостављања континуитета пословања у делу измена/доградње информационог система МЕОП и евентуалне миграције података, у случају прекида сарадње са пружаоцем услуге.

Хвала на пажњи!

kancelarija@dri.rs

www.dri.rs