Даница Врањанин,[1]
Докторанд,
Правни факултет Универзитета у Нишу

UDK: 368.032:342.7

Прегледни научни чланак

СИСТЕМ ИНТЕРНИХ КОНТРОЛА У ОСИГУРАВАЈУЋИМ ДРУШТВИМА У ФУНКЦИЈИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ

Апстракт

Циљ рада је да укаже на важност добро постављеног и развијеног система интерних контрола, као једног од кључних предуслова за адекватан одговор на растућу потребу заштите података о личности у доба убрзаног развоја и све веће заступљености дигиталних технологија у пословању друштава за осигурање, где се као додатни изазов пред друштво ставља потреба за тзв. радом на даљину, односно, радом ван пословних просторија, условљена појавом пандемије COVID-19. У раду се анализира значај функције усклађености пословања (енг. compliance) као једне од кључних у систему интерних контрола у смислу заштите података о личности, врши се анализа оквира корпоративног управљања у друшвима за осигурање и анализа и компарација регулаторног оквира заштите података о личности у праву Европске уније и праву Републике Србије.

Кључне речи: *Заштита података о личности, осигурање, систем интерних конрола, управљање ризицима, контрола усклађености/законитости пословања, Закон о заштити података о личности (ЗЗПЛ), Општа уредба о заштити података (ГДПР).*

1. Увод

Право заштите података о личности није новина, представља људско право, које се издвојило из права на приватност, а уређено је највишим међународним[2] и домаћим актима[3]. Ипак, развој информационих техно-

[1] PhD Candidate at the University of Nis, Faculty of Law, e-mail: danicavranjanin@gmail.com

[2] Конвенција Савета Европе о заштити лица у односу на аутоматску обраду личних података од 28. 01. 1981. године, ратификована од стране Републике Србије.

[3] Устав Републике Србије у чл. 42. уређује заштиту података о личности.

логија, дигитализација живота и пословања, брзина протока информација учинили су да се број прикупљених, обрађиваних и складиштених података о личности увећава у огромном, скоро немерљивом обиму. Такође, подаци о личности су добили и своју велику вредност у тржишном смислу, толико да се називају и „нафтом 21. века", уколико су проверени, систематизовани, потпуни, односно, искористиви у исплативе сврхе. Управо ту су своју шансу за профит нашле многе компаније (такве „квалитетно обрађене податке" продају у сврхе политичке или маркетиншке кампање), али и хакери који кроз различите видове сајбер напада долазе до података које касније илегално могу уновчити. Неретко се догоди да подаци „исцуре" и простом непажњом или услед недовољне обучености у погледу безбедности података онога ко подацима рукује. Све горе наведено позиционирало је ризик од повреде података о личности високо на листи ризика пословања привредних друштава, а посебно друштава за осигурање, која теже да испрате све строжије захтеве регулативе у овој области и обезбеде заштиту од повреде података о личности.

2. Нови регулаторни оквир заштите података о личности

Потреба за савременијим, потпунијим и ригиднијим уређењем ове области препозната је у првом реду од стране Европске уније, чији је претходни правни оквир заштите података о личности постављен давне 1995. године[4]. Нови оквир за којим се трагало требало би да одговори на изазове савременог живота и да у ери глобалне дигитализације пружи правну сигурност и заштиту лицима чији се подаци у различите сврхе и на све бројније начине користе и обрађују. Након дуготрајних преговора[5] у оквиру ЕУ, нови пропис Општа уредба о заштити података[6] (у даљем тексту ГДПР), донет је 2016. године, а ступио је на снагу у мају 2018. ГДПР мења досадашње, али уводи и нове принципе, права и обавезе, те даје нове дефиниције кључних појмова на пољу заштите података. Осим у границама ЕУ, где за разлику од претходно постављеног правног оквира, има директну примену у државама чланицама, утицај овог прописа се осетио и на гло-

[4] Директива 95/46/ЕЗ донета је у време када је свега 1% грађана ЕУ користило интернет - https://www.paragraf.rs/dnevne-vesti/260219/260219-vest9.html приступљено 30. 04. 2021.

[5] Преговори о унапређењу области заштите података у Европској унији започети су 2012. године

[6] УРЕДБА (ЕУ) 2016/679 ЕВРОПСКОГ ПАРЛАМЕНТА И САВЕТА од 27. априла 2016. о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге (Општа уредба о заштити података).

балном нивоу[7]. Тако неке државе које нису чланице ЕУ, па и оне које ни не претендују то да буду, своје националне прописе су ускладиле са ГДПР-ом, односно, уредиле ову област по угледу[8] на ГДПР. Разлози за то леже у екстериторијалном деловању овог прописа, високо постављеним стандардима заштите података о личности, изузетно високим казнама[9] за прекршиоце његових одредби, али и страху од губитка тржишта какво је оно у оквиру ЕУ[10]. Покушај да наша земља, као земља са статусом кандидата за чланство у Унији, своје национално законодавство усклади са променама на нивоу ЕУ, учињен је 2018. године новим Законом о заштити података о личности („Сл. гласник РС", бр. 87/2018) (у даљем тексту ЗЗЛП), но како је оцењено у Студији[11] Европске комисије не у потпуности успешно. Према оцени Комисије ЗЗПЛ представља превод и компилацију ГДПР-а и Директиве (ЕУ) 2016/680 Европског парламента и Савета од 27. априла 2016. о заштити појединаца у погледу обраде личних података од стране надлежних органа у сврху спречавања, истраге, откривања или кривичног гоњења, кривична дела или извршење кривичних санкција којима се ставља ван снаге Оквирна одлука Савета 2008/977ПУП тзв. „Полицијске Директиве"[12], потпуно изостављајући преамбуле ових прописа што, ум-

[7] У теорији се могу наћи и мишљења да се утицај ГДПР-а ограничава превасходно на државе сличне правне традиције видети у Вучић М. (2020), Границе вантериторијалног дејства опште уредбе о заштити података Европске Уније, Европско законодавство, 73-74, 2020, 41-57.

[8] Као неки од значајних примера могу се навести Бразил, Америчка држава Калифорнија и Индија, која додуше још увек није званично усвојила нови пропис. Након доношења ГДПР-а свој правни оквир заштите података о личности ревидирале су државе: Нови Зеланд, Аустралија, Јапан, Кина, Чиле, Јужна Африка итд.

[9] Битне повреде података о личности санкционисане су казнама које могу износити и до 20 милиона евра или 4% укупног годишњег промета, у зависности од тога који износ је виши.

[10] Одредбама ГДПР-а штите се подаци о личности грађана ЕУ, без обзира на локацију обраде податаке, те се тако односи на све привредне субјекте који своје производе и/или услуге нуде и чине доступним грађанима ЕУ, без обзира где се налази њихово седиште, односно, да ли су и иначе субјекти права ЕУ, као и без обзира на чијој територији се затекну грађани ЕУ у моменту када се подаци учине доступним. Такође, пренос података о грађанима ЕУ у треће земље, према одредбама ГДПР-а, дозвољен је искључиво уколико Комисија процени да трећа држава има одговарајући степен заштите података о личности.

[11] У питању је студија Европске комисије чији је задатак био да оцени ниво усклађености нацрта ЗЗПЛ са регулативом ЕУ о заштити података о личности. Доступно на https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/engEKStudija.pdf приступљено 02. 05. 2021.

[12] Предмет Полицијске директиве прописује правила заштите података физичких лица приликом обраде коју врше надлежни органи у циљу спречавања, истраге,

ногоме отежава разумевање терминологије. Даље, нађено је да ЗЗПЛ садржи и велики број, дословно преписаних норми, које не одговарају типу нити нивоу прописа, те остављају велики простор тумачењу, а оцењено је да постоји и велики број изузетака, као и изостанак прописаних санкција за кршење одређених одредби од којих неке према ГДПР-у представљају битне повреде. Такође, важно је напоменути, да иако ЗЗПЛ, по угледу на ГДПР, прописује сопствену територијалну надлежност и за правна лица са статусом руковаоца или обрађивача чије седиште се налази ван Републике Србије, примена одредаба Закона није обезбеђена једнако строгим казнама[13], што се осећа приликом ,,борбе" са мултинационалним гигантима да испуне обавезу именовања свог представника у нашој земљи.[14]

3. Кључне новине и њихов утицај на осигуравајућа друшва

Неке од кључних промена које је донела Уредба, а последично и наш ЗЗПЛ, попут: права на приступ подацима, права на заборав, права на приговор/противљење профилисању, право на повлачење сагласности, право на преносивост, обавеза именовања лица за заштиту података (енг. *Data Protection Officer*, у даљем тексту ДПО), за делатност осигурања су наметнуле потребу за ревидирањем система корпоративног управљања у знатној мери. Екстериторијално деловање ГДПР-а је, такође, погодило већину водећих осигуравача и реосигуравача с обзиром да углавном послују у оквиру мултинационалних групација. С том чињеницом на уму, стиче се утисак, да две године, колико је остављено да се субјекти које адресира ГДПР припреме, није дуг временски период да осигуравајћа друштва ускладе своје пословање са захтевима Уредбе узимајући у обзир и природу делатности. Отежавајућу околност представља и комплексност посебног правног оквира који уређује њихово деловање, а који је у погледу одређених питања неусаглашен са ЗЗЛП и ГДПР-ом. Осигуравајућа друштва у свом раду на дневној бази прикупљају огроман број личних података и тзв. осетљивих података о личности, као што су подаци о здравственом стању неког лица. Оно што додатно компликује управљање подацима у области осигурања јесте чињеница да она неминовно сарађују са значајним бројем

откривања или гоњења учинилаца кривичних дела или извршења кривичних санкција. Драган П, Стефан А. (2018) Основи Права заштите података о личности, Институт за упоредно право.

[13] Највиша запређена новчана казна за прекршиоце норми ЗЗПЛ износи 100. 000 динара.

[14] Google је тек у мају 2020. именовао свог представника у Републици Србији. Саопштење доступно на https://www.poverenik.rs/sr-yu/saopstenja/3346, приступљено 05. 11. 2020.

партнерских организација, попут друштава за посредовање и заступање у осигурању, банака, медицинских установа, лизинг компанија итд. са којима морају делити одређене податаке постојећих и потенцијалних клијената. Нови правни оквир намеће нове обавезе друштвима за осигурање, како организационе, кадровске, технолошке, тако и финасијске, отвара нове ризике пословања, док корелативно осигураницима и потенцијалним осигураницима даје нова права и пружа већу контролу над подацима и већу правну сигурност (Тошић И, Новаковић О. 2020 : 102). У времену пре ГДПР-а и нових тенденција у регулисању заштите личних података, већина компанија које претрпе повреде података или сајбер нападе, нису имале обавезу да о томе обавесте надлежне органе нити лица о чијим подацима је реч. Самим тим такве ситуације су често пролазиле неопажено. Уколико томе додамо далеко мању освешћеност институција, компанија и физичких лица, изложеност репутационом и финансијском ризику је била врло ограничена. Данас, уколико се оствари ризик повреде података, осигуравајућа друштва осим велике финасијске штете, трпе репутациону штету, која на дуже стазе може значајније ослабити само друштво. Адекватна примена института корпоративног управљања несумњиво представља одговор на ризике са којима су осигуравајућа друштва суочена у погледу заштите података, где би централну улогу требало дати ситстему интерних контрола и у оквиру њега функцији усклађености пословања (енг. compliance).

4. Ризик повреде података о личности у пословању осигуравајућих друштава

Теорија даје различита шира или ужа одређења појма „податак о личности"[15]. За потребе овог рада ослонићемо се на она која су дата у ГДПР-у и ЗЗПЛ. ГДПР дефинише у члану 4. податак о личности као „било који податак који се односи на физичко лице чији је идентитет одређен или одредив (лице на које се подаци односе)", док у истом члану физичко лице чији је идентитет одредив дефинише као „лице која се може идентификовати посредно или непосредно, посебно помоћу идентификатора као што су име, идентификациони број, подаци о локацији, мрежни идентификатор или помоћу једног или више фактора својствених за физички, физиолошки, генетски, ментални, економски, културни или друштвени идентитет тог физичког лица". У нашем праву податак о личности је дефинисан на готово идентичан начин у члану 4. ЗЗПЛ. На основу дефини-

[15] Више о теоријском одређењу појма „податак о личности" видети у Драган П. Стефан А. (2018), "Основи заштите података о личности", Институт за упоредно парво Београд, стр. 15-32.

ција података о личности можемо видети да је скоро сваки податак који осигуравајућа друштва прикупе у обављању своје делатности и у односу са својим клијентима/потенцијалним клијентима „податак о личности", од којих неки потпадају под категорију „осетљивих података о личности". Пођимо од тога да приликом закључења уговора о осигурању или давања понуде за закључење уговора о осигурању, осим основних индентификационих личних података, попут личног имена, јединственог матичног броја, броја личне карте и слично, осигуравајућа друштва често морају имати информације о занимању, старости, здравственом стању, приходима, како би могла да процене ризик остварења осигураног случаја и висину премије, а у крајњем случају и спремност за пружање услуге осигурања одређеном лицу. Такође, друштва за осигурање често у процесу обављања делатности деле прикупљене податке са партнерским огранизацијама (реосигуравачима, друштвима за заступање и посредовање у осигурању, медицинским установама, банкама, лизинг компанијама, а приликом мењања или одржавања система информационих технологија подаци буду доступни и спољним ИТ компанијама) што додатно повећава изложеност друштава ризику повреде података о личности, а тиме и оперативном ризику, ризику усклађености пословања, ризику информационе безбедности и репутационом ризику[16]. Осим тога, осигуравајућа друштва, као и сва друга привредна друштва, располажу и значајним бројем података о личности запослених, као и подацима лица која учествују на конкурсима за запослење у друштву. У процесу обављања делатности осигуравајућа друштва користе велике базе података које су системски повезане и умрежене у циљу лакшег управљања и коришћења, анализе, преноса, дељења тзв. „биг дата"[17] и друге различите алате информационих технологија. Како произилази из одредбе члана 4. ГДПР-а, ризик повреде података о личности се остварује у ситуацији када неко лице неовлашћено, намерно или нехотице, дође у посед података о личности појединаца или их обелодани, као и када дође до уништења, губитка или неовлашћене измене података.[18] Дуго је важила претпоставка да највећа претња по безбедност података о личности лежи у потенцијалним хакерским нападима који користе различите техничке рањивости софтвера, као и да је пре свега потребно уложити

[16] Мисли се на ризик у смислу вероватноће настанка неповољних последица по пословање, финансије и углед друштва.

[17] Више о појму „биг дата" видети у Драган П. Стефан А. (2018), "Основи заштите података о личности", Институт за упоредно парво Београд, стр. 31-32.

[18] УРЕДБА (ЕУ) 2016/679 ЕВРОПСКОГ ПАРЛАМЕНТА И САВЕТА од 27. априла 2016. о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге (Општа уредба о заштити података), члан 4, тачка 12.

највише ресурса у различита, најнапреднија технолошка решења како би се исти превенирали, те да би одговорност за евентуалну повреду података требло превасходно да сноси ИТ сектор друштва. Неретко су припадници ИТ сектора компаније, управо из наведеног разлога, именовани за лица за заштиту података тј. ДПО. Међутим, ова претпоставка, иако није у потпуности неутемељена, није ни у потпуности тачна. Наиме, уочено је у пракси далеко чешће узрок повреде лежи у „социјалном инжењерингу", мањкавости у едукацији и пажњи у области руковања личним подацима и заштите личних података код запослених у осигуравајућем друштву или партенрским огранизацијама, али и неадекватно постављених организационих и техничких мера заштите података.

Најчешће коришћена техника социјалног инжењеринга, која може довести до остварења ризика повреде података у осигуравајућим друштвима је фишинг[19] (енг. Phishing) који у основном подразумева преварну радњу код које се очекује да мета одрегује брзо, емотивно и да без претераног размишљања учини податке доступним неком лицу, као на пример ситуација у којој запослени одговара на мејл који је наводно послат од стране претпостављеног или партнерске организације где се хитно траже одређени подаци. Слична техника би била и „спер фишинг" (енг. *spear phishing*) где се циља тачно одређена особа у тачно одређеној компанији, чије податке треба прибавити, те након истраживања које хакери спроведу у циљу упознавања жртве шаљу врло персонализовану поруку са малициозним линком путем кога долазе до рачунара мете и комплетне мреже компаније. Треба имати на уму да технике социјалног инжењеринга које се користе у сврху неовлашћеног приступа подацима о личности не морају увек да подразумевају интернет окружење, нити долазити од стране хакера. Пример технике која подраземва коришћење телефона је „вишинг" (енг. Vishing) где лице које тежи неовлашћеном прикупљању података зове службеника осигуравајуће компаније (најчешћа мета су запослени у колцентру друштва) и, представљајући се као колега или запослени партнерске организације, на основу односа поверења са метом преваре долази до жељених података.

О учешћу техничких и организационих мера у превенцији ризика повреде података говори недавни случај кажњавања осигуравајућег друштва од стране Пољског органа за заштиту података о личности (УОДО).[20] Агент

[19] Изрази на енглеском језику којима се означавају наведене технике социјалног инжењеринга се користе и у српском, услед недостатка акдекватног превода на српском језик.

[20] Доступно на https://edpb.europa.eu/news/national-news/2021/polish-dpa-warta-failure-notify-personal-data-breach-without-undue-delay_en, приступљено 04. 05. 2021.

осигурања овог Друштва (делујући у својству обрађивача података) послао је мејл који је садржао полису осигурања, на погрешну мејл адресу, чиме је учинио податке доступним неовлашћеном лицу. Управо то неовлашћено лице које је примило мејл је и обавестило УОДО о повреди података о личности. Након спроведеног поступка истраге и надзора, утврђено је да је погрешну адресу дао сам клијент, али и да ни након захтева за појашњење упућеног од стране УОДО, Друштво није обавестило лица на која се подаци односе о насталој повреди. Тек након покретања управног поступка, лица на која се подаци односе су обавештена о инциденту, односно, чак пет месеци након настанка повреде[21]. Даље, УОДО је нашао да без обзира што је погрешна мејл адреса прибављена од самог лица на које се подаци односе, не ослобађа само Друштво одговорности. Наиме, успостављајући праксу слања Полиса (које садрже значајан број личних и потенцијално осетљивих личних података) путем мејла, Друштво је морало имати на уму ризик повреде података какав таква пракса носи и морало је успоставити адекватне мере заштите, попут верификације мејл адреса или енкрипције докумената. Наведена повреда података резултирала је казном у износу од 20 хиљада евра као и јавним обавштењем о повреди на страници УОДО и Европског одбора за заштиту података о личности (EDPB).

Велики допринос изложености ризику повреде података даје коришћење приватних мобилних телефона, рачунара у службене сврхе, коришћење УСБ-ова, екстерних хард-дискова и других носача података. Посебно треба истаћи изазове које пред заштиту података ставља све распрострањенији рад ван пословних просторија друштва, који је условљен панедемијом COVID-19, у ком случају је заштита јавног здравља отворила низ нових проблема у заштити података, где осим коришћења приватних уређаја долази и до коришћења необезбеђених интернет мрежа, рада у присуству лица која нису ни на који начин део компаније, а посебно ризик представља изношење папирне документације ван канцеларије. Папирна документација је посебно осетљива у погледу повреда података попут губитка, уништења и стављања на увид неовлашћеним лицима.

Међутим, иако чине можда и најрањивију карику у ланцу заштите по-

[21] Према члану 33. ГДПР-а1рок за обавештење надлежног органа о повреди података о личности износи 72 сата од сазнања за повреду, осим уколико није вероватно да ће повредом безбедности података о личности бити угрожена права и слободе физичких лица. У случају да обавештење изостане у року од 72 сата, руковалац мора оправдати кашњење. Члан 34. прописује да лица на која се подаци односе морају бити обавештена о повреди без одлагања од тренутка сазнања за поведу, када је вероватно да ће повреда безбедности података о личности проузроковати велики ризик за права и слободе физичких лица. Такође, у члану 34. у ставу 3. саводе се ситуације у којима такво обавештење може изостати.

датака у свакодневном раду друштва и сносе одговорност за своје поступке, политика рада, организација посла, стратешко и системско решавање проблема, управљање ризицима уопште, а самим тим и ризиком заштите података није у надлежности запослених оперативаца, већ припада домену корпоративног управљања, односно, улази обухват рада менаџмента, где се мисли на топ менаџмент и на средњи менаџмент[22]. Успостављање система корпоративног управљања је препознато као одговор на кључне изазове и ризике пословања друштава за осигурање. Наведено потврђује чињеница да важећа европска и национална регулатива намеће обавезу успостављања система корпоративног управљња и прописује његов оквир[23], а његов интегрални део чини управљање ризицима[24] и механизми за идентификацију и превазилажење ризика који се остварују кроз систем интерних контрола[25].

5. Систем интерних контрола у осигуравајућин друштвима у функцији заштите података о личности

Систем интерних контрола према одредбама Директиве Солвентност II и Закона о осигурају РС[26], подразумева успостављање одговарајућих

[22] Више о улози менаџмента у систему корпоративог управљања видети у Јовановић Zattila M. (2016), „Контролни механизми корпоративног управљања". Зборник радова Правног факултета у Нишу, 74/2016, 189-202.

[23] Директива *EU Solventost II*, поглавље *IV* (*Directive 2009/138/EC of the European Parliament and of the Council of 25. November 2009. on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)*), Закон о Осигурању (Сл. Гласник РС, бр. 139/2014) глава ВИ, Одлука Народне банке Србије о систему управљања у друштву за осигурање/реосигурање, Службени гласник РС, бр. 51/2015 и 29/2018.

[24] Више о организацији управљања ризиком видети у Мркшић Д. Петровић З. Иванчевић К. (2014), Право осигурања, Беодград, Прави факултет Универзитета Унион у Београду, Службени гласник. стр. 95-96.

[25] Више о дефинисању управљања ризицима са правног апсекта као једнмом од чинилаца корпоративног управљања видети у Љиљана С. (2013), Правни аспекти управљања ризиком и систем интерних контрола као интегрални део корпоративног управљања у друштву за осигурање. Европска ревија за право осигурања, 3-2013, 46-53.

[26] Треба напоменути да Солвентност II и Закон о осигурању врло штуро уређују питање система интерних контрола, односно, постављају захтев за његовим успостављањем и кратко дају опис његове минималне садржине и улоге. Директива то чини само у члану 46, док Закон о Осигурању РС овом питању посвећује чланове 151-153. Детаљнији оквир Система интерних контрола, посебно у погледу управљања ризицима, на нивоу ЕУ даје Делегирана уредба Комисије (ЕУ) 2015/35 од 10. октобра 2014. године о допуни Директиве 2009/138 / ЕЦ, док у РС то чини Одлука НБС о систему управљања у друштвима за осигурање/реосигурање (Службени гласник РС, бр. 51/2015 и 29/2018)

административних и рачуноводствених процедура, оквир интерне контроле, начине извештавања на свим нивоима друштва, а посебно функцију усклађености пословања. Успостављање система интерних контрола је у надлежности надзорног одбора друштва, док је извршни одбор одговоран за спровођење система у складу са одлукама надзорног одбора.

Као једна од четири кључне функције интегралног система управљања друштвом за осигурање, који уз остале три (управљање ризицима, интерна ревизија и актуарство), има улогу да обезбеди заштиту капитала друштва (како би оно могло дугорочно да одговори на обавезе према корисницима осигурања) кроз адекватно постваљену контролу правилности пословања и тзв. систем три нивоа контроле, односно, одбране друштва од понтецијалних опасности, односно, ризика.

Суштински линијска контрола поставља основе система интерне контроле душтва, обезбеђујући кроз своје континуирано деловање на свим нивоима, у сваком организационом делу, да сваки запослени буде укључен и освешћен по питању културе система интерне контроле. Систем контроле првог нивоа спроводи се кроз мере и радње **ex-ante** (она која се састоји од првентивних радњи у циљу блокирања нерегуларности које доводе до остварења ризика у пословању друштва) и ex-post контроле, организационе и оперативне контроле, као и контроле у вези са пословима повереним трећим лицима. Кровну улогу на овом нивоу контроле има Сектор организација. У надлежности овог сектора је успостављање организационе структуре друштва, као и подела рада и одговорности унутар организационих целина (на начин да делују синергично), креирање и континурано унапређење процедуре за спровођење задатака у сваком од сектора и старање о успешној имплементацији истих, утврђивање система извештавања између функција у друштву. Важно је истаћи и улогу овог сектора у имплентацији ISO стандарда, који у сваком сегменту пословања друштва постављају одређене захтеве, па тако и у сфери заштите података кроз ISO 27701 и 27001. Даље, превенцији повреде података значајно доприноси усвајање принципа „Интегрисане заштите података о личности" (енг. *Privacy by design*) и „Приватност као подразумевано подешавање" (енг. *Privacy by default*) у политикама и процедурама друштва, а да ови принципи не би остали само „мртво слово на папиру" потребно је имплементирати их у пракси, што се постиже пре свега коришћењем инжењерских техника заштите безбедности података[27]. Дакле, на линијском нивоу контроле значајно место заузима ИТ сектор, пре свега у погледу *ex*

[27] Више о улози инжењерских техника у имплементацији поменутих принципа видети у публикацији Европске агенције за безбедност мрежа и података (ЕНИСА) из 2015. године *„Privacy and Data Protection by Design – from policy to engineering"*

ante мера заштите података о личности које су саставни део ИТ процедура. Најчешће коришћене технолошке мере, односно технике су: псеудонимизација (као основна мера у имплементацији принципа Privacy by design), енкрипција, анонимизација, двострука ауторизација и аутентификација, аутоматско ограничење у погледу приступа одређеним подацима само на оне запослене којим је то неопходно у обављању радних задатака[28], креирање система мрежне безбедности уз обавезно коришћење „Фајервол" (енг. Firewall) уређаја нове генерације (NGFW)[29], старање о безбедности уређаја који се користе у раду (компјутера, мобилних телефона), старање о редовном ажурирању оперативних система, периодична провера јачине и ефикасности лозинки које се користе за приступ уређајима, серверима, клаудима (енг. Cloud) итд. Свака од поменутих техника и мера ИТ сектора тешко би функионисала уколико не би постојала адекватна едукација запослених у циљу разумевања важности коришћења поменутих техника, али и шта тачно подразумевају оне технике за које се очекује да буду коришћене у свакодневном раду запослених. За организацију такве едукације запослених одговара Сектор за управљање људским ресурсима (у даљем тексту ХР сектор). Међутим, посебно запослени у овом сектору морају и сами у обављању и других послова из своје надлежности користити горе описане технолошке превентивне мере заштите, с обзиром да обрађују велики број података о личности од тренутка исказивања интересовања за запослење до тренутка окончања радног односа (Перачек, 2021 : 449*)*, а неке радње обраде се настављају и након тог момента (нпр. архивирање). Ограничење приступа подацима, кроз техничке и организационе мере је од посебне важности за рад ХР сектора. Опште је познато да досијеи запослених садрже прегршт личних података те ни у ком случају не смеју бити лако доступни неовлашћеним трећим лицима и у сектору и ван сектора. На пример, не смеју се чувати у ходницима пословних просторија друштва, у необезбеђеним ормарићима (а и уколико су ормарићи закључани мора постојати ограничење ко може доћи у посед кључева), оригинални примерци уговора о раду и други документи не смеју ноншалантно бити остављени на радном столу запослених, нацрти докумената или копије докумената који садрже личне податке бачени у корпу за отпатке поред радних столова, често и непоцепани. Осим тога, ХР служба

[28] Примера ради непотребно је да лице које обавља послове актуара у друштву за осигурање има приступ подацима о кандидатима који су се пријавили за конкурс за посао у друштву.

[29] Више о потреби коришћења фајервола нове генерације ради заштите података у *K. Neupane, R. Haddad and L. Chen, "Next Generation Firewall for Network Security: A Survey," SoutheastCon 2018, 2018, pp. 1-6*, доступно на https://ieeexplore.ieee.org приступљено 09. 05. 2021.

мора, као и остале службе, водити рачуна поштовању основних начела обраде података, попут начела „законитости", „ограничење на сврху обраде", „тачности", „ограничења чувања", „минимизације података"[30].

Други ниво контроле чине функције управљања ризицима и функција усклађености пословања. Функцију управљања ризицима врши посебан огранизациони део друштва. Сектор за управљање ризицима своју улогу у систему интерних контрола обавља кроз индентификацију и квантификацију ризика којима је друштво изложено или би могло бити изложено, односно, кроз процену адекватности мера и процедура које се примењују на првом нивоу контроле са циљем заштите од ризика по пословање друшва, самим тим и ризика повреде о личности. Сектор управљања ризицима не врши специфичне контроле над радом осталих сектора, већ је у питању однос сарадње. Сектор усклађености пословања представља посебну, додатну и независну контролу у оквиру система интерних контрола, а делокруг овог сектора обухвата контролу пословања у складу са прописима, као и извештавање о томе, процену утицаја промене прописа на рад друштва као и идентификовање у процену правног ризика. О раду, улози и важности функције за делатност друштва и заштиту података о личности, коју обавља овај сектор биће више речи у посебном поглављу рада.

Трећи ниво контроле је у надлежности интерне ревизије. Обавеза интерне ревизије је да самостално и независно процени ефикасност и ефективност система интерних контрола друштва. Сва документа друштва морају бити доступна интерној ревизији, а надзор над радом друштва мора да буде без ограничења. Међутим, током свог развоја, интерна ревизија је добила и улогу саветовања менаџмента о потенцијалним ризицима у смислу постављања оквира и надзора над системом интерних контрола који има за циљ њихово успешно умањење. Интерна ревизија доприноси унапређењу корпоративног управљања управо кроз поменуту саветодавну улогу, унапређење система интерних контрола и управљања ризицима (Јовановић Zattila, 2016 : 198).

С обзиром да повреда података свакако представља ризик са растућим потенцијалом наношења штете и угрожавања пословања друштва, очекује се да систем интерне контроле као механизам за превазилажење ризика пружи одговарајући одговор. Како би очекивани одговор био адекватан и у пракси, односно, да би оквир постављен важећим прописима, односно, интерном регулативом друштва (општим актима, стратегијама, политикама и процедурама) дао резултате потребно је да постоји и фактичка, редовна и двосмерна сарадња, у првој линији између топ менаџмента и

[30] Начела заштите података о личности дефинисана су у чл. 5. ГДПР и као и у чл. 5. ЗЗПЛ.

носилаца контролних функција, а онда и између носилаца контролних функција и директора осталих сектора друштва са сваким од запослених.

Пример добре праксе би био формирање Комитета за информациону безбедност, који би чинили носиоци кључних функција и директори горе описаних сектора. Ово тело би се састајало на редовној бази, али и ad hoc уколико има потребе, са циљем да се континуирано усавршава систем интерних контрола у функцији заштите података. На тај начин би се благовремено испратила динамика развоја нових технологија, појава нових и све креативнијих начина угрожавања безбедности података, развој и промене у регулативи, чиме би друштво испунило и једну од основних обавеза – усклађеност пословања.

6. Улога функције усклађености пословања у остварењу заштите података о личности

Основни задатак функције усклађености пословања јесте праћење регулативе која адресира осигуравајућа друштва, регулише или директно, односно, индиректно утиче на њихово пословање, као и старање да друштво свој рад усклади са релевантном регулативом. Осим наведеног ова функција подразумева информисање, али и саветовање надзорног, односно, управног одбора у вези са питањима која се тичу усклађености пословања (Лабудовић Станковић 2013 : 49), али и пружање помоћи у разумевању прописа, начинима примене и важности ускађености на свим нивоима у друштву. Анализа, сагледавања најбољих начина имплементације, као и специфична контрола надзора над имплементацијом промена које је донео нови правни оквир на пољу заштите података о личности налазе се у надлежности сектора усклађености пословања. Сам сектор је, у многим осигуравајућим друштвима, у организационом смислу претрпео значајну промену, увођењем функције лица за заштиту података о личности (у даљем тексту ДПО) чије успостављање за осигуравајућа друштва представља обавезу прописану ГДПР-ом, али и ЗЗПЛ. ГДПР опису функције ДПО, именовању, положају, одговорности посвећује одредбе садржане у члановима од 37. до 39, док ЗЗПЛ то чини члановима 56. до 58. Из одредаба оба прописа следи да осигуравајућа друштва, с обзиром да су друштва која у склопу своје редовне делатности обрађују податке у великом обиму, а због природе делатности и посебне категорије података, такође у великом обиму, увек морају именовати ДПО.[31] Даље ГДПР и ЗЗПЛ постављају

[31] Чл. 37. ст. 1 тачка цц ГДПР-а гласи у слободном преводу ,,Руковалац и обрађивач именују овлашћено лице за заштиту података увек када: са основне делатности руковаоца или обрађивача се састоје из масовне обраде посебних категорија података на основу члана 9. и података о личности који се односе на кривичну и прекршајну

захтев да ДПО буде именован на основу стручних квалификација, посебно знања у области заштите података о личности како кроз познавање прописа тако и кроз познавање праксе, као и способности да обавља задатке дефинисане овим прописима[32]. Иако ГДПР, нити било који други пропис, не намеће обавезу да се ДПО именује у оквиру сектора усклађености пословања, овакво решење за осигуравајућа друштва[33] би требало сматрати добром праксом, из више разлога:

У опису посла сектора усклађености пословања је праћење и познавање релевантних прописа, самим тим и оних који се тичу заштите података о личности, али ако се сагледају и друге активности у надлежности сектора јасно је да лице на челу овог сектора или које је само запослено у сектору би требало да успешно одговори на задатке дефинисане као минимум описа посла ГДПР-ом у чл. 39. и ЗЗПЛ-ом у чл. 58, али и више од тога. Наиме према наведеним одредбама ДПО у друштву је задужен за информисање и саветовање управе друштва и запослених који обрађују податке о њиховим и у погледу њихових обавеза, а права лица чије податке обрађују. Затим, стара се о усклађености заштите података о личности у друштву са овим прописима, као и са политикама друштва које се односе на заштиту података о личности, што укључује и праћење поделе одговорности, подизање свести и оспособљавања запослених који учествује у радњама обраде, као и с тим повезане ревизије. Такође, ДПО спроводи Процену утицаја у вези са заштитом података и консултације у вези са тим, те прати спровођење процене. ДПО је надлежан и за сарадњу са Надлежним органом, односно, Повереником и има комуникацију са њим испред друштва приликом обавештавања, али и о свим питањима која се тичу обраде података, претходних консултација, односно, тражења мишљења итд. У складу са горе наведеним одредбама од ДПО се очекује да посебно, приликом обављања својих задатака води рачуна о ризицима везаним за радње обраде и узима у обзир природу, обим, околности и сврхе обраде. Према водичу радне групе 29 (WП29)[34] о Лицу за заштиту података о личности, како би ДПО успешно обављао задатке потребно је да буде посматран као партнер у дискусијама у Друштву које се тичу питања заштите података, као и да редовно присуствује састанцима топ и средњег менаџмента. Мишљењу ДПО-а увек се мора придати одговарајућа тежина. У случају неслагања, Во-

осуђиваност из члана 10".

[32] Чл. 37. ст. 5. ГДПР-а, чл. 56. ст. 8. ЗЗПЛ

[33] Када су у питању друштва која обављају делатности ван финансијског сектора, постојање одељења за праћење усклађености пословања се не подразумева, те се тако ова тврдња на њих не односи.

[34] WП 29 заменио је ЕДПБ који је на првој пленарној седници усвојио овај Водич WП29.

дич препоручује, као добру праксу, да друштво документује разлоге непоштовања савета ДПО-а. ДПО се мора без одлагања консултовати када дође до повреде података или другог инцидента, а тамо где је то прикладно, друштво може развити смернице за заштиту података или програм који одређују када се ДПО мора консултовати.[35]

Сектор у обављају својих послова сарађује са осталим секторима, а нарочито сектором управљања ризицима, ИТ сектором и ХР сектором, а као део другог нивоа контроле има прилику да стекне ширу слику о потребама друштва када је у питању заштита података;

Једно од основних обележја функције пословања јесте независност, која се постиже кроз одвојеност од оперативних функција и других контролних функција друштва, адекватности ресурса посматрано са аспекта стручности запослених у овом сектору, слободан приступ свим активностима и релевантним информацијама за контролу и обезбеђивање усклађености пословања друштва и кроз чињеницу да одговара директно Надзорном одбору. Према одредбама ГДПР-а и ЗЗПЛ, ДПО мора бити независтан у свом раду, а руковалац, односно друштво, је у обавези да му омогући несметани рад, средства за рад, као и приступ свим информацијама које се тичу података о личности, свим подацима о личности и поступцима обраде, те да ДПО мора да одговара непосредно највишем руководству друштва;

Одредбама ГДПР-а и ЗЗПЛ дозвољено је да ДПО обавља и друге задатке и дужности код руковаоца, односно друштва, уколико не постоји сукоб интереса.[36]

7. Закључак

Друштва за осигурање су посебно изложена ризику повреде податка о личности, а самим тим су и посебно погођења променама насталим у правном оквиру који регулише заштиту података о личности, превасходно из разлога који произилазе из природе делатности, комплексности корпоративног управљања, обима обраде података, као и учесталости и обима обраде посебних категорија података. Ризик повреде података у модерном систему пословања, насталом на темељу брзог развоја и доступности модерних технологија, представља ризик са растућим потенцијалом наношења штете и угрожавања пословања друштва, а утиче на остварења и других кључних ризика пословања друштава за осигурање, попут оперативног, репутационог и ризика усклађености пословања. Одговарајући

[35] *Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)* стр. 13, доступно на https://ec.europa.eu/newsroom/article29/items/612048 , приступљено 09. 05. 2021.

[36] Чл. 38 ГДПР-а регулише положај ДПО, исто чини ЗЗПЛ у члану 57.

систем интерних контрола од пресудне је важности за заштиту података о личности, али и самог друштва од ризика повреде података, јер омогућава да сваки од учесника у пословању друштва, од менаџмента, носилаца кључних функција, преко запослених и спољних сарадника, у свом домену, учествује у превенцији и санирању последица евентуалне повреде. Централну улогу међу секторима друштва, овде би требало да припадне сектору организације, усклађености пословања, управљања ризицима, ИТ сектору, сектору управљања људским ресурсима (ХР сектор). Посебно се истиче важност Сектора усклађености пословања и прихватања праксе именовања Лица за заштиту података (ДПО) управо у оквиру овог сектора, из разлога сродности стручних квалификација и задатака који улазе у опис посла обе функције, а који су претежно задати важећим правним оквиром.

Литература

Вучић, М. (2020), Границе вантериторијалног дејства опште уредбе о заштити података Европске Уније, *Европско законодавство*, 73-74, 2020, 41-57.

Јовановић Zattila, М. (2016), Контролни механизми корпоративног управљања, *Зборник радова Правног факултета у Нишу*, 74/2016, 189-202.

Лабудовић Станковић, Ј. (2011), Интегрисани концепт управљања ризицима компанија за осигурање као начин корпоративног управљања, *Ревија за право осигурања*, 3-2011, 9-16.

Лековић, В. (2018), Систем управљања у друштву за осигурање према Директиви Солвентност II, *Страни Правни живот*, 62(1), 137-152.

Neupane, K, Haddad R, Chen L (2018), Next Generation Firewall for Network Security: Survey, *SoutheastCon* 2018, (pp.1-6), https://ieeexplore.ieee.org/document/8478973, приступљено 09. 05. 2021.

Мркшић, Д, Петровић З, Иванчевић К. (2014), Право осигурања, Прави факултет Универзитета Унион у Београду, Службени гласник, Београд

Peráček, T. (2021), GDPR in terms of data protection in the field of HRM, доступно на https://www.researchgate.net/publication/350447767_GDPR_IN_TERMS_OF_DATA_PROTECTION_IN_THE_FIELD_OF_HRM, приступљено 09. 05. 2021.

Прља, Д, Андоновић, С. (2018), Основи Права заштите података о личности, Институт за упоредно право, Београд

Стојковић, Љ. (2020), Управљање ризицима и систем контроле у друштву за осигурање: теоријско-правна анализа. *Европска ревија за право осигурања*, 4-2019, 26-33.

Стојковић, Љ. (2013), Правни аспекти управљања ризиком и систем интерних контрола као интегрални део корпоративног управљања у друштву за осигурање. *Европска ревија за право осигурања*, 3-2013, 46-53.

Тошић, И, Новаковић, О. (2020), Утицај нове регулације у области заштите података о личности на рад осигуравајућих друштава, *Зборник Института за упоредно право* 2020, Београд, 93-104.

Хаусер, П. (2014), Растући значај функције законитости пословања на примеру аустријске економије осигурања. *Европска ревија за право осигурања*, 2-2014, 7-15.

Нормативни акти:

European Comission (2016), Guidelines on Data Protection Officers *('DPOs') (wp243rev.01)* доступно на https://ec.europa.eu/newsroom/article29/items/612048, приступ 09. 05. 2021.

Commission Delegated Regulation (EU) 2015/35 of 10. October 2014. supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)

Directive 2009/138/EC of the European parliament and of the Council of 25. November 2009. on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), Official Journal of the European Union, L 335.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27. April 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119, corrected by Corrigendum, OJ L 127, 23. 05. 2018, p. 2 ((EU) 2016/679)

Закон о осигурању, *Службени гласник РС*, бр. 139/2014

Закон о заштити података о личности, *Службени гласник РС*, бр. 87/2018

Одлука Народне банке Србије о систему управљања у друштву за осигурање/реосигурање, *Службени гласник РС,* бр. 51/2015 и 29/2018

Одлука Народне банке Србије о минималним стандардима управљања информационим системом финансијске институције *Службени гласник РС,* бр. 23/2013, 113/2013, 2/2017 и 88/2019

Резиме

Развој информационих технологија, дигитализација живота и пословања, брзина протока информација учинили су да се број прикупљених, обрађиваних и складиштених података о личности увећава у огромном, скоро немерљивом обиму. Такође, подаци о личности су добили и своју велику вредност у тржишном смислу, где су своју шансу видели хакери који „нафту 21. века" продају на црном тржишту, чиме су друштва која рукују подацима постала атрактивне мете. Ризик повреде података у савременом систему пословања, представља ризик са растућим потенцијалом наношења штете и угрожавања осигуравајућих друштава, а утиче на остварења и других кључних ризика, попут оперативног, репутационог и ризика усклађености пословања. Успостављање одговарајућег система интерних контрола наметнуло се као централно питање на пољу заштите личних података, будући да је пракса недвосмислено показала да виши ниво развијености истог у друштву значајно доприноси ублажављању вероватноће остварења ризика повреде података, оперативног ризика, ризика усклађености пословања и репутационог ризика по друштво. Одговарајући систем интерних контрола омогућава да сваки од учесника у пословању друштва, од менаџмента, носилаца кључних функција, преко запослених и спољних сарадника, у свом домену, учествује у превенцији и санирању последица евентуалне повреде личних података. Централна улога овде би требало да припадне секторима огранизације, усклађености пословање, управљања ризицима, ИТ, као и сектору управљања људским ресурсима.

Danica Vranjanin,
PhD student,
Faculty of Law, University of Niš

THE ROLE OF INSURANCE COMPANIES' INTERNAL CONTROL SYSTEMS IN PERSONAL DATA PROTECTION

Summary

Due to the development of Information Technologies, digitalization of life and business, and the speed of information flow, the volume of collected, processed, and stored personal data has been increasing to massive, almost immeasurable, extents. In that context, personal data have gained enormous value on the market, which has created an opportunity for hackers to sell this "21st century oil" on the black market. Thus, data managing/processing companies have become attractive targets. In the contemporary business system, the risk of data breaches has a growing potential to cause damage and jeopardize the opreration of insurance companies. It also increases some other major risks, such as operational, reputational and compliance risks. Establishing the appropriate system of internal control is a central issue in the field of personal data protection. Practice has unambiguously shown that a higher level of development of company internal control systems significantly contributes to mitigating the risk of data breaches, as well as operational, reputational and compliance risks. An appropriate system of internal controls enables each of the participants in the company activities, including the company management, holders of key offices, employees and external partners, to participate (within their domain) in the prevention and remediation of possible personal data breaches. In this regard, the central role should be played by the organization, compliance, risk management, IT, and HR sectors.

Keywords*: personal data protection, insurance, internal control system, risk management, control of compliance/legality of business, Personal Data Protection Act, General Data Protection Regulation (GDPR).*