На основу члана 10. став 1. и члана 63. став 4. Закона о дигиталној имовини („Службени гласник РС“, бр. 153/2020) и члана 18. став 1. тачка 3) Закона о Народној банци Србије („Службени гласник РС“, бр. 72/2003, 55/2004, 85/2005 – др. закон, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – одлука УС и 44/2018), гувернер Народне банке Србије доноси

О Д Л У К У
О УСЛОВИМА УПРАВЉАЊА ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМ СИСТЕМОМ ПРУЖАОЦА УСЛУГА ПОВЕЗАНИХ С ВИРТУЕЛНИМ ВАЛУТАМА

I. УВОДНЕ ОДРЕДБЕ

1. Овом одлуком утврђују се услови стабилног и сигурног пословања који се односе на управљање информационо-комуникационим системом пружаоца услуга повезаних с дигиталном имовином у делу пословања који се односи на виртуелне валуте (у даљем тексту: пружалац услуга).

Овом одлуком уређују се и минимални стандарди за управљање континуитетом пословања и опоравак активности у случају катастрофе код пружаоца услуга.

2. Поједини појмови, у смислу ове одлуке, имају следећа значења:

1) *корисник виртуелних валута* означава физичко лице, предузетника или правно лице које користи или је користило услугу повезану с виртуелним валутама или се пружаоцу услуга обратило ради коришћења те услуге;

2) *трансакција с виртуелним валутама* означава куповину, продају, прихватање или пренос виртуелне валуте или замену виртуелне валуте за другу виртуелну валуту и/или за другу дигиталну имовину;

3) *платформа за трговање виртуелним валутама* је мултилатерални систем који организује трговање виртуелним валутама, којим управља организатор платформе и који омогућава и олакшава спајање интереса трећих лица за куповину и/или продају виртуелне валуте и/или замену виртуелне валуте за другу виртуелну валуту и/или за другу дигиталну имовину, у складу са његовим обавезујућим правилима и на начин који доводи до закључења уговора;

4) *криптомат* јесте аутоматска машина преко које се обављају куповина и продаја виртуелних валута за новчана средства или замена виртуелне валуте за другу виртуелну валуту и/или за другу дигиталну имовину;

5) *информационо-комуникациони систем* је свеобухватни скуп технолошке инфраструктуре (хардверске и софтверске компоненте), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација;

6) *ресурси информационо-комуникационог система* обухватају софтверске компоненте, хардверске компоненте и информациона добра;

7) *софтверске компоненте* обухватају све типове системског и апликативног софтвера, софтверске развојне алате, као и остали софтвер;

8) *хардверске компоненте* обухватају рачунарску опрему, комуникациону опрему, медије за чување података, као и осталу техничку опрему која служи као подршка функционисању информационо-комуникационог система;

9) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и сл.;

10) *корисници информационо-комуникационог система* су сва лица која су овлашћена да користе информационо-комуникациони систем (запослени код пружаоца услуга, запослени у другим лицима који приступају информационо-комуникационом систему пружаоца услуга, корисници виртуелних валута који информационо-комуникационом систему пружаоца услуга приступају преко електронских интерактивних комуникационих канала и др.);

11) *ризик информационо-комуникационог система* је могућност настанка негативних ефеката на финансијски резултат и капитал, остваривање пословних циљева, пословање у складу с прописима и репутацију пружаоца услуга услед неадекватног управљања информационо-комуникационим системом или друге слабости у том систему која негативно утиче на његову функционалност или безбедност, односно угрожава континуитет пословања;

12) *контроле* су политике, процедуре, праксе, технологије и организационе структуре које се односе на информационо-комуникациони систем, утврђене да би се обезбедило разумно уверење да ће пословни циљеви код пружаоца услуга бити остварени и да ће нежељени догађаји бити спречени или откривени, а могу се разликовати према начину примене (управљачке, техничке и физичке) и намени (превентивне, детективне и корективне);

13) *управљачке контроле* обухватају доношење и примену политика, стандарда, планова, процедура и других унутрашњих аката, као и успостављање одговарајуће организационе структуре, а ради постизања и одржавања адекватног нивоа функционалности и безбедности информационо-комуникационог система;

14) *техничке контроле* су контроле примењене у хардверским и софтверским компонентама информационо-комуникационог система;

15) *физичке контроле* су контроле којима се ресурси информационо-комуникационог система штите од неовлашћеног физичког приступа, крађе, физичког оштећења или уништења;

16) *превентивне контроле* су контроле намењене спречавању настанка проблема и инцидената;

17) *детективне контроле* су контроле намењене откривању и препознавању проблема и инцидената и указивању на настале проблеме и инциденте;

18) *корективне контроле* су контроле намењене ограничавању и отклањању проблема и последица инцидената;

19) *инцидент* је сваки непланирани и нежељени догађај који може нарушити безбедност или функционалност информационо-комуникационог система;

20) *безбедност информационо-комуникационог система* подразумева очување поверљивости, интегритета, расположивости, аутентичности, доказивости, непорецивости и поузданости у информационо-комуникационом систему;

21) *поверљивост* означава да подаци и информације нису откривени или доступни неовлашћеним лицима;

22) *интегритет* означава да су подаци, информације и процеси заштићени од неовлашћеног или непредвиђеног мењања, односно да евентуалне такве промене не остају неопажене;

23) *расположивост* означава да су подаци, информације и процеси доступни и употребљиви на захтев овлашћеног лица;

24) *аутентичност* означава да је идентитет лица заиста онај за који се тврди да јесте;

25) *доказивост* означава да свака активност у информационо-комуникационом систему може бити једнозначно праћена до њеног извора;

26) *непорецивост* означава немогућност порицања активности извршене у информационо-комуникационом систему или пријема информације;

27) *поузданост* означава да информационо-комуникациони систем доследно и очекивано врши предвиђене функције и пружа тачне информације;

28) *ауторизација* је процес доделе права приступа корисницима информационо-комуникационог система;

29) *идентификација* је процес представљања корисника информационо-комуникационог система приликом пријаве и у току извођења активности у том систему;

30) *аутентификација* је процес провере и потврде корисничког идентитета коришћењем једног од следећих елемената или њихове комбинације:

– нешто што само корисник зна (нпр. лозинка, лични идентификациони број и сл.),

– нешто што само корисник поседује (нпр. магнетна картица, чип картица, токен, криптографски кључ и сл.),

– нешто што само корисник јесте (биометријске карактеристике као што су отисак прста, очна дужица, глас, рукопис и сл.);

31) *повлашћени приступ информационо-комуникационом систему* је приступ ресурсима информационо-комуникационог система који овлашћеним корисницима (администратори системског софтвера, администратори мреже, администратори база података и сл.) омогућава заобилажење техничких контрола;

32) *удаљени приступ информационо-комуникационом систему* је приступ ресурсима информационо-комуникационог система са удаљене локације посредством телекомуникационе инфраструктуре над којом пружалац услуга нема потпуну контролу;

33) *оперативни и системски записи* означавају хронолошке записе о догађајима и активностима на ресурсима информационо--комуникационог система (записи оперативних система, апликативног софтвера, база података, мрежних уређаја и сл.);

34) *малициозни програмски кôд* је било који облик програмског кôда створен с намером да се неовлашћено оствари приступ ресурсима информационо-комуникационог система, прикупе информације, изазове неочекивано понашање или прекид у функционисању овог система, односно да се на други начин потенцијално наруши поверљивост, интегритет или расположивост тих ресурса (нпр. рачунарски вируси, тзв. црви, тројански коњи и др.);

35) *критични/кључни пословни процеси* су пословни процеси или функције чије неадекватно функционисање може значајно угрозити пословање пружаоца услуга ;

36) *најдужи прихватљив прекид* (енг. *MAO – Maximum Acceptable Outage*) означава најдужи прихватљив период нерасположивости пословног процеса, односно критично време за опоравак тог процеса;

37) *резервна копија података* представља копију најмање оних изворних података (софтверске компоненте и информациона добра) који су потребни за опоравак, односно за поновно успостављање пословних процеса;

38) *електронске услуге* су услуге повезане с виртуелним валутама из члана 3. став 1. Закона о дигиталној имовини које корисници виртуелних валута користе са удаљене локације, преко интернета, укључујући коришћење тих услуга помоћу криптомата, као и друге активности којима се приступа подацима у вези са услугама повезаним с

виртуелним валутама а који би могли бити предмет преварних радњи или других злоупотреба.

II. УПРАВЉАЊЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМ СИСТЕМОМ

3. Пружалац услуга дужан је да успостави адекватан информационо--комуникациони систем, који испуњава најмање следеће услове:

1) поседује функционалности, капацитете и перформансе који омогућавају пружање одговарајуће подршке пословним процесима у вези с пружањем услуга повезаних с виртуелним валутама;

2) обезбеђује благовремене, тачне и потпуне информације значајне за доношење пословних одлука, ефикасно обављање пословних активности и управљање ризицима, односно за сигурно и стабилно пословање;

3) пројектован је са одговарајућим контролама за валидацију података на улазу, у току процеса обраде, као и на излазу из тог система, ради спречавања нетачности и неконзистентности у подацима и информацијама;

4) поседује одговарајуће контроле како би се спречили инциденти који настају због сајбер напада, крађе или друге неисправности, као и како би се сачувала безбедност информационо-комуникационог система.

4. Пружалац услуга дужан је да унутрашњим општим актом, у складу са законом, утврди овлашћења и одговорности својих органа управљања и надзора који се односе на очување безбедности и функционалности информационо-комуникационог система.

Пружалац услуга дужан је да надзире, редовно ревидира и унапређује процес управљања информационо-комуникационим системом ради смањења изложености ризицима повезаним с тим системом.

5. Пружалац услуга дужан је да донесе стратегију развоја информационо-комуникационог система, која може бити саставни део његове пословне стратегије.

Пружалац услуга дужан је да, по потреби, мења стратегију развоја информационо-комуникационог система, и то нарочито ако то захтевају одговарајуће измене и/или допуне стратегије пословања.

6. Пружалац услуга дужан је да, ради адекватног управљања информационо-комуникационим системом, обезбеди одговарајућу организациону структуру, с јасно утврђеном поделом послова и дужности

запослених, односно са утврђеним унутрашњим контролама којима се спречава сукоб интереса.

Пружалац услуга је у оквиру поделе послова и дужности из става 1. ове тачке нарочито дужан да јасно утврди послове и дужности запослених који су у непосредној вези са ефикасним и одговарајућим управљањем безбедношћу информационо-комуникационог система.

7. Пружалац услуга дужан је да обезбеди примену свих унутрашњих општих аката и процедура у вези са информационо-комуникационим системом, као и да обезбеди да сви корисници тог система буду упознати са садржајем тих аката и процедура, у складу с њиховим овлашћењима, одговорностима и потребама.

8. Пружалац услуга дужан је да утврди критеријуме, начин и поступке извештавања свог надлежног органа о релевантним чињеницама у вези с функционалношћу и безбедношћу информационо-комуникационог система.

III. УПРАВЉАЊЕ РИЗИКОМ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

9. Пружалац услуга дужан је да, у оквиру свеобухватног система управљања ризицима, успостави процес управљања ризиком информационо-комуникационог система који обухвата идентификовање и мерење, односно процену тог ризика, као и његово ублажавање, праћење и контролу.

Пружалац услуга дужан је да редовно прати и оцењује адекватност примењених контрола за ублажавање идентификованих ризика информационо-комуникационог система.

10. Пружалац услуга дужан је да ризиком информационо-комуникационог система управља тако да омогући несметано управљање безбедношћу овог система и управљање континуитетом свог пословања.

Управљање ризиком информационо-комуникационог система мора да обухвати целокупан информационо-комуникациони систем пружаоца услуга и да буде интегрисано у све фазе развоја тог система.

11. Пружалац услуга дужан је да адекватно управља ризицима који произлазе из уговорних односа с правним и физичким лицима чије се активности односе на његов информационо-комуникациони систем.

Пружалац услуга дужан је да континуирано надзире начин и квалитет обављања уговорених активности из става 1. ове тачке.

12. Одредбе прописа којима се уређују општи услови и начин управљања ризицима у пословању пружаоца услуга примењују се и на управљање ризиком информационо-комуникационог система.

IV. УНУТРАШЊА РЕВИЗИЈА ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

13. Пружалац услуга дужан је да методологијом рада унутрашње ревизије обухвати критеријуме, начин и поступке унутрашње ревизије информационо-комуникационог система засноване на резултатима процене ризика.

14. Унутрашња ревизија информационо-комуникационог система обавља се у складу с прописима којима се уређује пословање пружаоца услуга.

V. БЕЗБЕДНОСТ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

15. Пружалац услуга дужан је да донесе унутрашњи општи акт којим ће се успоставити оквир за управљање безбедношћу информационо-комуникационог система (у даљем тексту: политика безбедности).

Политиком безбедности нарочито се уређују принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система, као и овлашћења и одговорности у вези са овом безбедношћу и ресурсима тог система.

Пружалац услуга дужан је да политику безбедности усклађује с променама у окружењу и у самом информационо-комуникационом систему.

16. Пружалац услуга дужан је да процес управљања безбедношћу информационо-комуникационог система успостави као континуирани процес идентификовања потреба за овом безбедношћу и постизања и одржавања адекватног нивоа те безбедности, и то најмање на основу резултата процене ризика тог система и обавеза које произлазе из прописа, унутрашњих општих аката, уговорних односа и сл.

17. Пружалац услуга дужан је да, ради постизања и одржавања адекватног нивоа безбедности информационо-комуникационог система, успостави одговарајуће контроле.

18. Пружалац услуга дужан је да спроводи одговарајућу контролу приступа ресурсима информационо-комуникационог система, као и да с тим у вези успостави адекватан систем управљања корисничким правима приступа.

Системом управљања корисничким правима приступа нарочито се обухватају процеси евидентирања корисника информационо--комуникационог система, ауторизације, идентификације и аутентификације, као и надзор над корисничким правима приступа.

Пружалац услуга дужан је да обезбеди да се ауторизација корисника информационо-комуникационог система заснива на принципу доделе најмањих могућих права приступа ресурсима тог система која омогућују ефикасно обављање послова.

Пружалац услуга дужан је да периодично и по потреби, а најмање једном годишње, ревидира корисничка права приступа.

При управљању корисничким правима приступа, пружалац услуга је дужан да посебно уреди повлашћени и удаљени приступ информационо-комуникационом систему.

19. Пружалац услуга дужан је да, на основу резултата процене ризика информационо-комуникационог система, успостави адекватан систем надгледања тог система и генерисања оперативних и системских записа, и да обезбеди одговарајућу заштиту тих записа, као и да утврди време чувања, те учесталост, опсег и начин праћења тих записа.

Записи из става 1. ове тачке морају садржати довољну количину информација за идентификовање проблема, реконструисање догађаја и откривање неовлашћених приступа и активности на ресурсима информационо-комуникационог система, као и за утврђивање одговорности с тим у вези.

20. Пружалац услуга дужан је да, применом одговарајућих контрола, ресурсе информационо-комуникационог система и друге системе који су подршка функционисању информационо-комуникационог система заштити од неовлашћеног физичког приступа, од крађе, као и од физичког оштећења или уништења изазваног људским или природним фактором.

У случају да изнајми рачунарски центар, пружалац услуга дужан је да утврди да су примењене одговарајуће контроле из става 1. ове тачке.

21. Пружалац услуга је нарочито дужан да обезбеди интегритет података о трансакцијама с виртуелним валутама које се извршавају на основу налога корисника виртуелних валута, као и при њиховој обради, чувању и предузимању свих других радњи у вези с тим подацима.

22. Пружалац услуга дужан је да, применом одговарајућих контрола и техничких решења, ресурсе информационо-комуникационог система заштити од злонамерног софтвера и сајбер напада.

VI. КОНТИНУИТЕТ ПОСЛОВАЊА И ОПОРАВАК АКТИВНОСТИ У СЛУЧАЈУ КАТАСТРОФЕ

23. Пружалац услуга дужан је да, ради обезбеђивања несметаног и континуираног функционисања свих својих значајних система и процеса, као и ограничавања губитака у ванредним ситуацијама, успостави процес управљања континуитетом пословања.

24. Пружалац услуга дужан је да обезбеди да управљање континуитетом пословања буде засновано на анализи утицаја на пословање и на процени ризика.

Анализа утицаја на пословање нарочито обухвата:

1) утврђивање ресурса и система потребних за одвијање појединачних пословних процеса, као и њихове међузависности и повезаности;
2) процену ризика у вези с појединачним пословним процесима, укључујући и вероватноћу настанка нежељених догађаја и њихов потенцијални утицај на континуитет пословања, финансијско стање и репутацију пружаоца услуга;
3) утврђивање прихватљивих нивоа ризика и техника за ублажавање идентификованих ризика;
4) утврђивање критичних/кључних пословних процеса и активности;
5) утврђивање најдужег прихватљивог прекида (*MAO*) појединачних пословних процеса.

25. Надлежни орган пружаоца услуга дужан је да, на основу активности спроведених у складу с тачком 24. ове одлуке, донесе план континуитета пословања (енг. *Business Continuity Plan*), као и план опоравка активности у случају катастрофе (енг. *Disaster Recovery Plan*)

којим се превасходно уређује стварање услова за опоравак и расположивост ресурса информационо-комуникационог система потребних за одвијање критичних/кључних пословних процеса.

План континуитета пословања нарочито садржи:

1) опис процедура у случају прекида пословања;
2) ажуран списак свих ресурса неопходних за поновно успостављање континуитета пословања;
3) податке о тимовима који ће бити одговорни за поновно успостављање пословања у случају настанка непредвиђених догађаја и о именованим члановима тих тимова, укључујући и њихове јасно утврђене дужности и одговорности, као и план унутрашњих и спољних линија комуникације;
4) резервну локацију – у случају прекида пословања и немогућности поновног успостављања пословних процеса на примарној локацији.

План опоравка активности у случају катастрофе нарочито садржи:

1) процедуре за опоравак информационо-комуникационог система кад наступе катастрофални догађаји;
2) приоритете опоравка ресурса информационо-комуникационог система;
3) податке о тимовима који ће бити одговорни за опоравак информационо-комуникационог система и о именованим члановима тих тимова, укључујући и њихове јасно утврђене дужности и одговорности;
4) резервну локацију за опоравак информационо-комуникационог система, односно локацију резервног рачунарског центра.

Пружалац услуга дужан је да, ради ефикасног спровођења планова из става 1. ове тачке, обезбеди да сви запослени буду упознати са својим улогама и одговорностима у случају наступања ванредних ситуација.

Пружалац услуга дужан је да предузима све неопходне активности ради усклађивања планова из става 1. ове тачке с пословним променама, укључујући и промене у производима, активностима, процесима и системима, с променама у окружењу, као и с пословном политиком и стратегијом пословања.

Пружалац услуга дужан је да периодично и после настанка значајних промена, а најмање једном годишње, тестира планове из става

1. ове тачке, као и да документује резултате тих тестирања и обезбеди њихово укључивање у извештавање надлежног органа пружаоца услуга.

За спровођење планова из става 1. ове тачке одговоран је надлежни орган пружаоца услуга.

26. Пружалац услуга дужан је да, при управљању континуитетом пословања, узме у обзир и активности поверене трећим лицима и зависност од услуга тих лица.

27. Пружалац услуга дужан је да, у случају настанка околности које захтевају примену плана континуитета пословања и плана опоравка активности у случају катастрофе, обавести о томе Народну банку Србије, и то најкасније наредног дана од дана настанка тих околности. Народна банка Србије може захтевати додатну документацију у вези с релевантним чињеницама о овим околностима и одредити рок за достављање те документације.

28. Пружалац услуга дужан је да успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности ресурса информационо-комуникационог система.

Пружалац услуга дужан је да Народну банку Србије обавести о инциденту који је озбиљно угрозио или нарушио његово пословање, односно који би могао озбиљно угрозити или нарушити његово пословање, и то:

1) ако је настао услед нарушавања функционалности ресурса информационо-комуникационог система – одмах по утврђивању околности о настанку тог инцидента;
2) ако је настао као последица нарушавања безбедности информационо-комуникационог система – одмах по сазнању о том инциденту;
3) ако је настао код трећег лица у смислу тачке 37. став 5. ове одлуке а имао је или је могао имати значајан утицај на информационо--комуникациони систем пружаоца услуга – одмах по утврђивању околности о настанку тог инцидента, односно сазнању о том инциденту.

Након обавештења из става 2. ове тачке, ако је инцидент и даље у току, пружалац услуга је дужан да Народну банку Србије континуирано обавештава о битним догађајима и другим релевантним информацијама у вези са инцидентом из тог става (статус инцидента), као и о активностима предузетим ради ублажавања тог инцидента и о његовим

последицама. Ово обавештење садржи и детаљан опис инцидента, информације о процени броја корисника виртуелних валута на које је инцидент утицао, оквирно време потребно да се инцидент реши, потенцијални утицај на друге пружаоце услуга, као и битне догађаје и друге релевантне информације од настанка инцидента (нпр. информације о томе да ли је инцидент ескалирао, да ли су откривени нови узроци и о ефикасности примењених активности).

Пружалац услуга дужан је да Народној банци Србије достави завршни извештај о насталом инциденту из става 2. ове тачке у року од 15 дана од дана престанка тог инцидента, односно од дана када процени да су успостављени његово редовно пословање и стабилан рад информационо-комуникационог система. Овај извештај садржи коначне информације о инциденту – датум почетка и датум окончања инцидента, дужину трајања инцидента, врсту инцидента (недоступност хардверских компоненти, проблеми у раду софтверских компоненти или безбедносни инцидент), опис инцидента, узроке настанка и последице инцидента, активности које је спроводио током инцидента, план активности којима ће превентивно деловати и спречити поновне појаве истог инцидента, број корисника виртуелних валута на које је инцидент утицао, финансијске трошкове настале у вези са инцидентом, утицај на друге пружаоце услуга и, по потреби, друге релевантне информације.

Пружалац услуга дужан је да у складу са ст. 1. и 2. ове тачке извештава Народну банку Србије о инцидентима који су повезани са злоупотребом осетљивих података корисника виртуелних валута, неодобреним трансакцијама с виртуелним валутама, техничким манипулацијама на криптоматима, преварним радњама и злоупотребама корисника виртуелних валута, злоупотребама фактора аутентификације и система за аутентификацију и сл. а који нису имали директан утицај на његов информационо-комуникациони систем.

Народна банка Србије може захтевати додатну документацију у вези с релевантним чињеницама о околностима и последицама насталог инцидента и одредити рок за достављање те документације.

29. Пружалац услуга дужан је да успостави процес управљања резервним копијама података, те да у ту сврху утврди детаљне процедуре и одговорности.

Управљање резервним копијама података мора да обухвати поступке израде, чувања и тестирања ових копија, као и опоравка података и софтверских компонената, како би се омогућило поновно успостављање пословних процеса.

Пружалац услуга дужан је да обезбеди да су резервне копије података ажурне и адекватно заштићене, а поступци опоравка тестирани и успешни.

Најмање једна ажурна и комплетна резервна копија података мора бити адекватно ускладиштена на удаљеној и безбедној локацији.

VII. РАЗВОЈ И ОДРЖАВАЊЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА

30. Пружалац услуга дужан је да процес развоја информационо--комуникационог система спроводи у складу са стратегијом развоја информационо-комуникационог система, узимајући у обзир функционалне захтеве и потребе за безбедношћу.

Пружалац услуга дужан је да, током самосталног развоја информационо-комуникационог система, успостави и документује процес тог развоја, који обухвата анализу и пројектовање, програмирање, тестирање и увођење у продукцију.

Пружалац услуга дужан је да успостави и на одговарајући начин раздвоји тестно и продукционо окружење.

У случају самосталног развоја информационо-комуникационог система, пружалац услуга дужан је да, поред окружења из става 3. ове тачке, успостави и развојно окружење.

31. Пружалац услуга дужан је да успостави процес управљања хардверским и софтверским компонентама у свим фазама њиховог животног циклуса – од набавке или развоја до повлачења из употребе.

32. Пружалац услуга дужан је да обезбеди адекватно одржавање хардверских и софтверских компонената информационо-комуникационог система према препорукама произвођача и да чува записе о том одржавању, као и да се стара о томе да се притом не угрози безбедност или функционалност овог система.

Пружалац услуга дужан је да у складу са ставом 1. ове тачке адекватно надзире поверене активности у вези са одржавањем хардверских и софтверских компонената информационо-комуникационог система.

33. Пружалац услуга дужан је да успостави процес управљања променама хардверских и софтверских компонената информационо-комуникационог система, како би се избегло да оне доведу до неочекиваног и нежељеног понашања овог система, односно да наруше његову безбедност или функционалност.

Пружалац услуга дужан је да обезбеди да све промене хардверских и софтверских компонената, укључујући и нове компоненте и системе, буду тестиране и одобрене пре пуштања у продукцијски рад, као и да утврди план враћања на претходно стање.

Пружалац услуга дужан је да унутрашњим општим актом уреди процес управљања хитним променама хардверских и софтверских компонената информационо-комуникационог система.

34. Пружалац услуга који планира миграцију података на нову платформу за трговање виртуелним валутама, увођење нове платформе за трговање виртуелним валутама или миграцију података у други рачунарски центар, односно који врши промену локације рачунарског центра – дужан је да о томе обавести Народну банку Србије најкасније 30 дана пре почетка тестирања планираног у вези с том миграцијом.

Обавештење из става 1. ове тачке нарочито садржи:

1) детаљне описе система између којих се подаци преносе, односно опис нове платформе за трговање виртуелним валутама;
2) план, динамику и опис активности у вези с преласком на нову платформу за трговање виртуелним валутама, или у вези с преласком у други рачунарски центар;
3) резултате процене ризика и опис контрола које ће се применити током миграције података с циљем очувања поверљивости, интегритета и расположивости података;
4) план враћања на стање пре миграције података, који укључује динамику тог враћања и опис активности, као и критеријуме за доношење одлуке за примену тог плана.

Изузетно од става 1. ове тачке, пружалац услуга који планира миграцију података због статусне промене за коју је дужан да прибави сагласност, односно дозволу Народне банке Србије – дужан је да, истовремено са захтевом за давање те сагласности, односно дозволе, Народној банци Србије достави и обавештење с подацима из става 2. ове тачке.

Народна банка Србије може захтевати додатну документацију у вези с релевантним чињеницама о околностима миграције из ст. 1. и 3. ове тачке.

35. Пружалац услуга дужан је да обезбеди израду, чување и редовно одржавање документације која се односи на информационо-комуникациони систем, како би та документација у сваком тренутку била тачна, потпуна и ажурна.

Пружалац услуга дужан је да свим корисницима информационо-комуникационог система обезбеди приступ одговарајућим документима у складу с потребама посла.

36. Пружалац услуга дужан је да обезбеди адекватно и континуирано стручно оспособљавање и обучавање запослених за коришћење информационо-комуникационог система и очување његове безбедности и функционалности.

VIII. ПОВЕРАВАЊЕ АКТИВНОСТИ У ВЕЗИ СА ИНФОРМАЦИОНО-КОМУНИКАЦИОНИМ СИСТЕМОМ ТРЕЋИМ ЛИЦИМА

37. Поверавање активности у вези са информационо-комуникационим системом пружаоца услуга трећим лицима (у даљем тексту: поверавање активности) обавља се у складу с прописима којима се уређује пословање пружалаца услуга и овом одлуком.

Активностима из става 1. ове тачке сматрају се све активности које обухватају обраду, чување и/или приступ подацима којима располаже пружалац услуга а односе се на његово пословање, као и активности развоја и/или одржавања главних пословних апликација и платформи за трговање виртуелним валутама.

Поверавање активности укључује и поверавање активности лицима повезаним с пружаоцем услуга имовинским и управљачким односима (лица са учешћем, чланови групе друштава којој тај пружалац услуга припада и др.) која послују у Републици Србији или у иностранству.

Поверавањем активности не сматра се коришћење стандардизованих сервиса или телекомуникационих услуга, као ни набавка софтвера који је као готово решење комерцијално доступан на тржишту (енг. *off-the-shelf*) и сл.

Поверавање активности врши се на основу уговора закљученог између пружаоца услуга и лица коме се те активности поверавају (у даљем тексту: треће лице).

Поверавање активности у смислу ове одлуке не односи се на активности пружаоца услуга које се непосредно односе на пружање услуга повезаних с виртуелним валутама из члана 3. став 1. Закона о дигиталној имовини.

38. Пружалац услуга који намерава да повери одређене активности дужан је да уреди:

1) процес одлучивања о поверавању активности и критеријуме за доношење те одлуке;
2) начин укључивања тих активности у процес управљања ризицима и у систем интерног извештавања о ризицима;
3) начин на који обезбеђује континуитет обављања активности које је поверио и мере које предузима у случају раскида уговорног односа с трећим лицима, као и у случају привременог застоја или престанка пружања услуга трећих лица;
4) начин вршења надзора над обављањем активности које је поверио, укључујући и надзор над усклађеношћу тих активности с прописима, добрим пословним обичајима и општеприхваћеним стандардима из одговарајуће области.

39. Пружалац услуга дужан је да обезбеди да треће лице њему, спољном ревизору и Народној банци Србије омогући благовремен и неограничен приступ документацији и подацима у вези с повереним активностима.

Пружалац услуга дужан је да обезбеди да сваки уговор закључен с трећим лицем садржи одредбу којом се треће лице обавезује да испуни обавезу из става 1. ове тачке, као и одредбу која пружаоцу услуга омогућава да тај уговор једнострано раскине ако то наложи Народна банка Србије и у складу с тим налогом.

Пружалац услуга дужан је да Народној банци Србије омогући и несметано вршење непосредне контроле обављања поверених активности у просторијама трећег лица, односно на локацији на којој се поверене активности обављају.

40. Пружалац услуга дужан је да обезбеди да се поверавањем активности не угрози безбедност или функционалност информационо-комуникационог система, као и да подаци остану у његовом поседу.

Пружалац услуга дужан је да обезбеди да треће лице поверене активности обавља у складу с политиком безбедности пружаоца услуга, као и актима и професионалним стандардима којима се уређује безбедност његовог информационо-комуникационог система.

Пружалац услуга и треће лице дужни су да при поверавању активности, односно обављању поверених активности поступају у складу са законом којим се уређује заштита података о личности, као и другим прописима којима се уређује чување тајне настале у пословању пружаоца услуга.

41. Пружалац услуга може одређене активности да повери, односно треће лице да промени само ако о томе обавести Народну банку Србије најкасније 30 дана пре закључења уговора о поверавању активности.

Ако се уговор из става 1. ове тачке мења а да се притом не мења поверена активност, односно опсег поверених активности (додавање нових функционалности, модула и сл.) или се не мења треће лице – пружалац услуга дужан је да најкасније 15 дана пре закључења анекса тог уговора о томе обавести Народну банку Србије и достави јој нацрт тог анекса.

Обавештење из става 1. ове тачке нарочито садржи:

1) одлуку надлежног органа пружаоца услуга о поверавању активности, односно о промени трећег лица;

2) опис активности које пружалац услуга намерава да повери, обавезе и услове које је треће лице дужно да испуни, као и рок на који ће активности бити поверене;

3) основне податке о трећем лицу (пословно име, седиште, матични број и ПИБ, односно други одговарајући подаци за страно лице);

4) нацрт уговора о поверавању активности;

5) резултате анализе потенцијалног трећег лица која се односи на његову способност пружања услуга, финансијско стање и пословну репутацију;

6) излазну стратегију којом је пружалац услуга проценио могуће потешкоће и време потребно за избор новог трећег лица или могућност наставка самосталног обављања тих активности у случају престанка пружања уговорених услуга, која мора да садржи списак мера и активности које је потребно предузети, као и динамику њиховог спровођења од тренутка престанка пружања уговорених услуга до избора новог трећег лица или потпуног успостављања самосталног процеса обављања тих активности;

7) резултате процене утицаја поверавања активности на континуитет пословања, репутацију, трошкове, финансијски резултат и ризични профил пружаоца услуга;

8) доказ о томе да прописи државе, односно држава у којима треће лице послује омогућавају Народној банци Србије да несметано врши непосредну контролу пословања у делу који се односи на обављање поверених активности или је у вези с њима – ако треће лице има седиште изван Републике Србије или је уговорено да поверене активности обавља изван Републике Србије.

Рок из става 1. ове тачке рачуна се од дана достављања уредне документације из ове тачке.

42. Треће лице може другом лицу поверити активности које је пружалац услуга поверио њему или друге послове који су у вези с тим активностима, и то само уз претходну сагласност пружаоца услуга, коју он даје у сваком појединачном случају, уз сходну примену одредаба тач. 38. до 40. ове одлуке.

Пружалац услуга може сагласност из става 1. ове тачке дати само ако је најкасније 30 дана пре тога обавестио Народну банку Србије о намераваном поверавању активности или послова из тог става.

Обавештење из става 2. ове тачке нарочито садржи:

1) нацрт одлуке надлежног органа управљања пружаоца услуга о давању сагласности из става 1. ове тачке;

2) опис активности које треће лице намерава да повери, као и обавеза и услова које је друго лице из става 1. ове тачке дужно да испуни;

3) основне податке о другом лицу из става 1. ове тачке (пословно име, седиште, матични број и ПИБ, односно други одговарајући подаци за страно лице);

4) нацрт уговора између трећег лица и другог лица из става 1. ове тачке о поверавању активности из тог става;

5) резултате анализе потенцијалног другог лица из става 1. ове тачке која се односи на његову способност пружања услуга, финансијско стање и пословну репутацију;

6) ревидирану излазну стратегију којом је пружалац услуга обухватио и друго лице из става 1. ове тачке;

7) резултате процене утицаја поверавања активности из става 1. ове тачке на континуитет пословања, репутацију, трошкове, финансијски резултат и ризични профил пружаоца услуга;

8) доказ о томе да прописи државе, односно држава у којима друго лице из става 1. ове тачке послује омогућавају Народној банци Србије

несметано вршење непосредне контроле пословања у делу који се односи на обављање поверених активности или је у вези с њима – ако то лице има седиште изван Републике Србије или је уговорено да поверене активности обавља изван Републике Србије.

Рок из става 2. ове тачке рачуна се од дана достављања уредне документације из ове тачке.

43. Пружалац услуга одговара у целини за активности које је поверио трећим лицима.

Пружалац услуга дужан је да континуирано врши надзор над пруженим услугама, као и проверу квалитета пружених услуга у вези с повереним активностима, нарочито у делу који се односи на безбедност информационо-комуникационог система.

Ако у поступку контроле, односно надзора утврди да пружалац услуга, због пропуста у раду трећег лица или другог лица из тачке 42. ове одлуке, не поступа у складу са овом одлуком и другим прописима – Народна банка Србије може пружаоцу услуга наложити да раскине уговор о поверавању активности закључен с трећим лицем и предузети друге мере у поступку надзора над пословањем пружаоца услуга.

44. Пружалац услуга дужан је да Народној банци Србије достави уговор из тачке 37. став 5. ове одлуке, укључујући и анексе тог уговора – у року од 15 дана од дана закључења тог уговора, односно анекса.

У случају раскида уговора из става 1. ове тачке, пружалац услуга дужан је да о томе без одлагања обавести Народну банку Србије.

IX. ЕЛЕКТРОНСКЕ УСЛУГЕ

45. Пружалац услуга који пружа електронске услуге (у даљем тексту: пружалац електронских услуга) дужан је да, као саставни део управљања ризиком информационо-комуникационог система, успостави процес управљања ризицима који произлазе из пружања електронских услуга.

46. Пружалац електронских услуга дужан је да при пружању електронских услуга примени безбедне и ефикасне методе за проверу и потврду идентитета и овлашћења лица, процеса и система.

Пружалац електронских услуга дужан је да корисницима виртуелних валута при коришћењу електронских услуга обезбеди

аутентификацију која укључује комбинацију најмање два међусобно независна елемента за потврђивање корисничког идентитета.

Изузетно од става 2. ове тачке, пружалац електронских услуга може применити аутентификацију корисника виртуелних валута која се врши коришћењем једног елемента за потврђивање корисничког идентитета, у случају услуга које су на основу анализе ризика процењене као нискоризичне.

Пружалац електронских услуга може да примени аутентификацију корисника виртуелних валута из става 3. ове тачке само ако је најмање 30 дана пре дана почетка пружања услуге из тог става о томе обавестио Народну банку Србије и уз то обавештење доставио свеобухватну и детаљну анализу ризика и начина управљања ризицима.

Рок из става 4. ове тачке рачуна се од дана достављања уредне документације из тог става.

47. Пружалац електронских услуга дужан је да усвоји и примени правила којима се на одговарајући начин, у складу с проценом ризика и прихваћеним стандардима, ограничава број покушаја пријаве на систем за пружање електронских услуга, односно покушаја аутентификације, да одреди најдуже време без активности корисника виртуелних валута након пријаве на тај систем, као и да утврди рокове важења параметара аутентификације.

При коришћењу једнократних лозинки ради аутентификације (нпр. *One Time Password – OTP*), пружалац електронских услуга дужан је да обезбеди да временско важење те лозинке буде ограничено на период који је потребан за обављање аутентификације.

Пружалац електронских услуга дужан је да утврди највећи могући број неуспешних покушаја пријаве на систем за пружање електронских услуга након којих ће тај систем бити трајно или привремено блокиран, као и да успостави процедуре за безбедно поновно активирање овог система.

Пружалац електронских услуга дужан је да утврди најдуже могуће време без активности корисника виртуелних валута на систему за пружање електронских услуга по пријављивању у тај систем након којег долази до аутоматског одјављивања корисника из овог система (тзв. завршетак сесије).

Пружалац електронских услуга дужан је да обезбеди одговарајућу потврду свог идентитета на дистрибутивном каналу за пружање електронских услуга, како би корисници могли да провере пружаоца електронских услуга.

Пружалац електронских услуга дужан је да обезбеди постојање оперативних и системских записа како би се у одговарајућој мери обезбедила непорецивост и доказивост радњи у вези с пружањем електронских услуга.

X. ЗАВРШНА ОДРЕДБА

48. Ова одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије“, а примењује се од 29. јуна 2021. године.

О. бр. 12
13. маја 2021. године
Б е о г р а д

Г у в е р н е р
Народне банке Србије

Др Јоргованка Табаковић, с.р.