На основу члана 15. став 1. и члана 63. став 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), Извршни одбор Народне банке Србије доноси

О Д Л У К У
О УСЛОВИМА И НАЧИНУ ПОВЕРАВАЊА АКТИВНОСТИ У ВЕЗИ СА ИНФОРМАЦИОНИМ СИСТЕМОМ ФИНАНСИЈСКЕ ИНСТИТУЦИЈЕ ТРЕЋИМ ЛИЦИМА

Уводне одредбе

1. Овом одлуком уређују се услови и начин поверавања активности у вези са информационим системом финансијске институције трећим лицима, као и начин управљања повереним активностима, у циљу стабилног и сигурног пословања које се односи на управљање информационим системима у банкама, друштвима за осигурање, даваоцима финансијског лизинга, друштвима за управљање добровољним пензијским фондовима, као и платним институцијама, институцијама електронског новца и јавном поштанском оператору у делу његовог пословања који се односи на пружање платних услуга и/или издавање електронског новца (у даљем тексту: финансијска институција).

Ова одлука примењује се на све финансијске институције из става 1. ове тачке, ако појединим њеним одредбама није друкчије утврђено.

2. Поједини појмови, у смислу ове одлуке, имају следеће значење:

1) *информациони систем*, *ресурси информационог система, софтверске компоненте, хардверске компоненте, информациона добра, ризик информационог система, инцидент, безбедност информационог система, поверљивост, интегритет* и *расположивост* имају значења утврђена одлуком којом се уређују минимални стандарди управљања информационим системом финансијске институције;

2) *критични/кључни пословни процеси* су пословни процеси или функције чије неадекватно функционисање може значајније угрозити стабилност и континуитет пословања финансијске институције или проузроковати изостанак пружања услуга финансијске институције утврђених законом;

3) *поверавање активности* означава скуп активности које предузима финансијска институција ради одабира пружаоца услуга и закључења уговора на основу ког тај пружалац услуга обавља активности/услуге у вези са информационим системом;

4) *пружалац услуга* је правно лице или предузетник коме је финансијска институција поверила обављање активности или дела активности у вези с њеним информационим системом;

5) *потповеравање активности* означава скуп активности које се предузимају ради закључења уговора између пружаоца услуга и потпружаоца услуга, на основу ког пружалац услуга даље поверава одређене активности у оквиру активности које је њему (пружаоцу услуге) поверила финансијска институција у вези с њеним информационим системом, при чему те активности обавезно укључују давање претходне сагласности финансијске институције на закључење тог уговора;

6) *потпружалац услуга* је правно лице или предузетник коме је пружалац услуга поверио активности или део активности у вези са информационим системом финансијске институције;

7) *клауд услуге (*енг. *cloud services)* су услуге код којих се на захтев омогућава широко распрострањен и погодан мрежни приступ заједничком скупу прилагодљивих ресурса информационог система (нпр. мреже, сервери, уређаји за складиштење података, апликације, услуге и др.), а које се могу лако обезбедити (енг. *provisioned*) и отказати (енг. *released*) уз минималну ангажованост пружаоца услуга.

Појам и обим поверавања активности у вези са информационим системом трећим лицима

3. Поверавање активности обавља се у складу с прописима којима се уређује пословање финансијских институција, ако овом одлуком није друкчије прописано.

4. Активности које финансијска институција може да повери пружаоцу услуга, а на које се примењују одредбе ове одлуке, нарочито обухватају следеће:

1) развој, одржавање и управљање ресурсима информационог система;

2) развој и одржавање пословних апликација које утичу на критичне/кључне пословне процесе;

3) обраду и/или чување података којима финансијска институција располаже а који се односе се на њено пословање и/или приступ тим подацима;

4) услуге провере безбедности информационог система (тестирања рањивости и слабости информационог система, пенетрационо тестирање и сл.);

5) послове обављања унутрашње ревизије информационог система.

Одредбе ове одлуке не примењују се на набавку и коришћење:

1) услуга глобалних сервиса за финансијску комуникацију (нпр. *SWIFT*) ако се кључни ресурси информационог система потребни за пружање те услуге налазе унутар финансијске институције;

2) услуга пружања информација о финансијским тржиштима (*Bloomberg, Reuters* и др.);

3) услуга глобалне мрежне инфраструктуре (*Visa, MasterCard* и др.) и телекомуникационих услуга;

4) софтвера који је као готово решење комерцијално доступан на тржишту и не захтева прилагођавања (енг. *customization*) тог решења (*off-the-shelf*);

5) других услуга сличних услугама из одредаба под 1) до 4) овог става ако је претходно о томе прибављено мишљење Народне банке Србије да се на коришћење тих услуга не примењују одредбе ове одлуке.

Финансијска институција не може пружаоцу услуга поверити процес управљања информационим системом који обухвата следеће:

1) процес доношења стратегије развоја информационог система;

2) успостављање политика и процедура за управљање информационим системом, као и за његово ревидирање и унапређење;

3) кључне контролне функције органа управљања у вези с њеним информационим системом.

Финансијска институција не може да пренесе овлашћења и одговорности својих органа управљања и надзора на пружаоца услуга.

5. Поверавање активности укључује сваког пружаоца услуга који има одвојени правни субјективитет у односу на финансијску институцију која поверава активности.

Поверавање активности из става 1. ове тачке укључује и лица повезана с финансијском институцијом имовинским и/или управљачким односима (лица са учешћем, чланице групе друштава којој та институција припада и др.) која послују у Републици Србији или у иностранству.

Одговорност за управљање повереним активностима

6. Финансијска институција је дужна да обезбеди да поверавање активности из тачке 4. став 1. ове одлуке не доводи до умањења одговорности надлежних органа управљања те институције, као ни запослених одговорних за управљање њеним информационим системом.

7. Надлежни орган управљања финансијске институције одговоран је за ефикасну примену ове одлуке, усклађеност и примену регулаторних

захтева, управљање ризицима повезаним са повереним активностима, као и за праћење поверених активности и надзор над њима.

8. Како би обезбедила примерено управљање повереним активностима, праћење тих активности и надзор над њима, финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационог система, обезбеди одговарајућу организациону структуру, с јасно утврђеном поделом послова и дужности запослених, ради стабилног и сигурног функционисања тог система.

Оквир за управљање повереним активностима

9. Финансијска институција је дужна да унутрашњим актима уреди поступак поверавања активности тако да обухвати:

1) процес одлучивања о поверавању активности који садржи линије одговорности у доношењу те одлуке;
2) критеријуме на основу којих се доноси одлука о поверавању активности;
3) критеријуме за одабир пружаоца услуга;
4) процену ризика концентрације изложености према једном пружаоцу услуга (зависност од једног пружаоца услуга) и утврђивање мера унутрашње контроле којима се смањује тај ризик;
5) процену очекиване користи и трошкова који произлазе из поступка поверавања појединачних активности;
6) начин укључивања поверених активности у процес управљања ризицима, нарочито ризиком информационог система, као и у систем интерног извештавања о ризицима;
7) начин на који се врши потповеравање активности потпружаоцу услуга;
8) начин на који финансијска институција обезбеђује континуитет обављања поверених активности и мере које предузима у случају раскида уговорног односа с пружаоцем услуга, као и у случају привременог застоја или престанка пружања тих услуга, односно могућност поновног самосталног обављања поверених активности у финансијској институцији или могућност преноса тих активности другом пружаоцу услуга („заменљивост пружаоца услуга“);
9) начин вођења евиденције поверених активности;
10) начин праћења примене уговора о поверавању активности, који обухвата и поступак обавештавања о променама уговора и поступак обнављања (продужења важења) уговора;
11) утицај поверених активности на критичне/кључне пословне процесе;

12) поступке у вези са заштитом података којима располаже финансијска институција а односе се на њено пословање (повреде поверљивости, интегритета и доступности података).

10. Финансијска институција је дужна да успостави континуирани надзор над обављањем поверених активности који укључује следеће:

1) утврђивање запослених који су одговорни за праћење нивоа и квалитета пружених услуга (енг. *service-level agreement – SLA*) и утврђивање да ли се услуге у потпуности пружају у складу са уговором;
2) анализу задовољства пруженим услугама, која, између осталог, узима у обзир прекиде у пружању услуга, редовност и садржајност извештаја пружаоца услуга о повереним активностима, као и одговоре на инциденте који су утицали на пословне процесе финансијске институције;
3) благовремено праћење и обавештавање надлежних органа финансијске институције о датуму истека уговора;
4) редовно тестирање планова континуитета пословања за критичне/кључне пословне процесе са пружаоцима услуга;
5) проверу усклађености поверених активности с прописима, добрим пословним обичајима и општеприхваћеним стандардима из одговарајуће области и др.

11. У случају поверавања активности лицима из тачке 5. став 2. ове одлуке, финансијска институција је дужна да посебно уреди начин вршења надзора над повереним активностима, као и да утврди врсте и динамику извештаја о повереним активностима које ће добијати од тих лица. Када надзор над повереним активностима за све чланице врши група којој финансијска институција припада (централизовано), финансијска институција је дужна да обезбеди да јој група редовно доставља извештаје о спроведеном надзору, као и да за критичне/кључне пословне процесе, без обзира на извршен надзор групе, обезбеди потпуно самосталан надзор над повереним активностима.

12. Банка која намерава да трећем лицу повери активности чије је извршење значајно за обезбеђивање континуитета њених критичних функција дужна је да обезбеди континуитет тих функција за случај примене инструмената и/или мера реструктурирања, и то на један од следећих начина:

1) обавезивањем тог трећег лица да обавља поверене активности у свим ситуацијама у којима је потребно обезбедити континуитет критичних функција банке у реструктурирању, односно банке за посебне намене;

2) уговором са алтернативним пружаоцем услуга који би могао да обезбеди континуитет обављања критичних функција банке у реструктурирању, односно банке за посебне намене;

3) детаљним планом обезбеђивања континуитета обављања критичних функција употребом интерно расположивих ресурса банке у реструктурирању, односно банке за посебне намене.

Управљање ризицима који произлазе из поверених активности

13. Финансијска институција је дужна да адекватно управља ризицима информационог система и другим ризицима који произлазе из поверених активности.

Финансијска институција је дужна да управљање ризицима који произлазе из поверених активности успостави као континуирани процес.

Финансијска институција је дужна да у оквиру процене ризика који произлазе из поверених активности идентификује ресурсе информационог система на које те активности утичу, потенцијалне претње безбедности информационог система и штете које би могле да настану ако би се те претње остариле, односно да идентификује, процени и прати ризике информационог система и да утврди и редовно преиспитује контроле којима би се ти ризици умањили.

Финансијска институција је дужна да приликом процене ризика узме у обзир очекиване користи и трошкове који произлазе из поступка поверавања конкретних активности, ризике који проистичу из поверавања активности пружаоцу услуга кога није једноставно заменити, ризике који су повезани с већим бројем уговора закључених са истим пружаоцем услуга или с њим повезаним лицима и ризике повезане са потповеравањем активности, као и да, с тим у вези, предузме мере у циљу управљања тим ризицима, односно њиховог смањења.

Поступак поверавања активности

14. Поверавање активности врши се на основу уговора закљученог између финансијске институције и пружаоца услуге, на основу ког пружалац услуга обавља одређене активности, односно пружа одређене услуге у вези са информационим системом финансијске институције, а које би у супротном обављала финансијска институција.

Финансијска институција која поверава активности лицима из тачке 5. став 2. ове одлуке дужна је да обезбеди да су закључени уговори из

става 1. ове тачке усклађени са законима и другим прописима Републике Србије.

15. Пре доношења одлуке о сваком појединачном поверавању активности, односно о промени пружаоца услуга – финансијска институција је дужна да:

1) истражи тржиште предметних услуга и прикупи понуде више потенцијалних пружалаца услуга;

2) изврши детаљну упоредну анализу свих потенцијалних пружалаца услуга која се односи на квалитет њихових услуга, цену пружања услуга, њихову способност обављања тих активности, адекватне ресурсе информационог система који могу подржати поверене активности, довољан број запослених опредељених за обављање поверене активности, финансијско стање и пословну репутацију;

3) процени да ли прекиди у пружању или неодговарајући ниво пружене услуге могу имати негативан утицај на континуитет пословања финансијске институције и услуге које она пружа, односно да ли активност коју поверава утиче на критични/кључни пословни процес;

4) утврди да ли постоји зависност од једног пружаоца услуга;

5) утврди да ли прописи државе или држава у којима потенцијални пружалац услуга послује омогућују Народној банци Србије несметано вршење непосредне контроле тог пословања у делу који се односи на обављање поверених активности или је у вези с тим активностима;

6) процени могуће потешкоће и време потребно за избор другог пружаоца услуга или могућност наставка обављања тих активности унутар финансијске институције у случају престанка пружања уговорених услуга, као и да, с тим у вези, утврди одговарајућу излазну стратегију;

7) када је то могуће, изврши анализу успешности претходне сарадње са одређеним пружаоцем услуга.

При доношењу одлуке из става 1. ове тачке или приликом битне измене поверене активности (нпр. додавање/укидање сервиса, апликативних решења и др.) финансијска институција нарочито процењује утицај поверавања активности на:

1) континуитет пословања и репутацију финансијске институције;

2) трошкове, финансијски резултат, ликвидност и солвентност финансијске институције;

3) ризични профил финансијске институције;

4) ризик информационог система финансијске институције;

5) квалитет услуга које финансијска институција пружа клијентима.

16. Приликом поверавања активности лицима из тачке 5. став 2. ове одлуке финансијска институција је дужна да цену услуга утврди по тржишним условима, као и да узме у обзир да на цену услуге утиче околност да се иста услуга обавља за више институција повезаних имовинским и/или управљачким односима.

17. Финансијска институција је дужна да, у складу с тачком 15. став 1. одредба под 6) ове одлуке, донесе излазну стратегију у случају престанка пружања уговорених услуга, која нарочито садржи:

1) критеријуме на основу којих се доноси одлука за спровођење ове стратегије;
2) одговорност надлежних органа финансијске институције за спровођење те стратегије;
3) списак мера и активности које је потребно предузети од тренутка престанка пружања уговорених услуга до избора другог пружаоца услуга или потпуног успостављања процеса обављања тих активности унутар финансијске институције, као и динамику њиховог спровођења;
4) анализу финансијских и људских ресурса потребних за спровођења ове стратегије, укључујући и обављање активности унутар финансијске институције;
5) обезбеђење услова да обављање поверених активности настави други пружалац услуга или сама финансијска институција (набавка софтверских компоненти, хардверских компоненти, лиценце и др.).

18. Финансијска институција је дужна да обезбеди да сваки уговор закључен с пружаоцем услуга нарочито садржи одредбе којима се:

1) детаљно и прецизно описује поверена активност која је предмет уговора;
2) утврђују обавезе пружаоца услуга из тачке 19. ст. 2. и 4. ове одлуке;
3) омогућава да финансијска институција једнострано раскине уговор ако то наложи Народна банка Србије;
4) уређује могућност потповеравања активности уз навођење неопходних услова за потповеравање;
5) одређује рок на који се уговор закључује, односно завршетак пружања услуга;
6) утврђују локације на којима ће се обављати поверена активност и локације на којима ће се обрађивати и чувати подаци финансијске институције у вези с повереном активношћу, као и обавеза пружаоца услуга да обавести финансијску институцију о промени тих локација;

7) уређује начин приступа информационом систему финансијске институције, односно начин управљања правима приступа када је то неопходно за пружање услуге;

8) уређује начин на који ће финансијска институција континуирано пратити квалитет и ниво пружених услуга (квантитативни и квалитативни), као и врсте и динамика извештаја које ће финансијска институција добијати од пружаоца услуга;

9) дефинише управљање инцидентима тако да се утврде поступци и улоге за решавање инцидента, као и начин извештавања о насталом инциденту и његовим последицама по финансијску институцију у складу са одредбама одлуке којом се уређују минимални стандарди управљања информационим системом финансијске институције;

10) уређује начин сарадње с пружаоцем услуга у вези са захтевима за промене хардверских/софтверских компоненти, за отклањање уочених недостатака или за хитне интервенције у случају инцидента;

11) утврђују услови на основу којих може доћи до престанка уговора;

12) утврђује обавеза пружаоца услуге из тачке 31. ст. 1. и 2. ове одлуке;

13) утврђује обавеза пружаоца услуга да при пружању услуга у потпуности поступа у складу са прописима Републике Србије.

19. Финансијска институција је дужна да обезбеди да се поверавањем активности не угрози безбедност или функционалност њеног информационог система, као и да подаци финансијске институције остану у њеном поседу, односно под њеном контролом.

Финансијска институција је дужна да обезбеди да пружалац услуга поверене активности обавља у складу с политиком безбедности информационог система и другим актима финансијске институције којима се уређује безбедност њеног информационог система.

Финансијска институција је дужна да обезбеди одржавање и редовно тестирање својих планова континуитета пословања с пружаоцима услуга за све поверене критичне/кључне пословне процесе.

Финансијска институција и пружалац услуга дужни су да при поверавању активности, односно током обављања 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 финансијских институција.

20. Финансијска институција може одређене активности да повери и закључи уговор о поверавању активности, да битно измени уговор о поверавању активности (додавањем/укидањем поверених активности) и

да промени пружаоца услуга, односно изабере новог пружаоца услуга – само ако о томе обавести Народну банку Србије најкасније 30 дана пре закључења уговора о поверавању активности или анекса тог уговора, и то на обрасцу из Прилога 1, који је одштампан уз ову одлуку и њен је саставни део.

Уз обавештење из става 1. ове тачке, финансијска институција доставља:

1) одлуку надлежног органа управљања финансијском институцијом о поверавању активности, битној измени уговора о поверавању активности или промени пружаоца услуга, односно избору новог пружаоца услуга;

2) нацрт уговора о поверавању активности у складу с тачком 18. ове одлуке, односно нацрт анекса тог уговора, укључујући све пратеће уговоре (нпр. који се односе на ниво пружених услуга и заштиту података);

3) детаљну анализу пружаоца услуга, услове које треба да испуни и критеријуме на основу којих је одабран;

4) резултате процене из тачке 15. став 2. ове одлуке;

5) излазну стратегију из тачке 17. ове одлуке;

6) доказ о томе да прописи државе, односно држава у којима пружалац услуга 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 пружалац услуга има седиште изван Републике Србије или је уговорено да поверене активности обавља изван Републике Србије.

Ако на основу обавештења, документације и доказа из става 2. ове тачке није могуће утврдити све чињенице значајне за поступање по том обавештењу, Народна банка Србије може од финансијске институције тражити да јој достави и другу документацију за коју оцени да јој је потребна.

Ако се уговор из става 1. ове тачке мења тако да се измене односе на трајање тог уговора, финансијске услове (цена услуга) или на измене одредаба које не утичу на обављање поверених активности – финансијска институција је дужна да најкасније 15 дана пре закључења анекса тог уговора о томе обавести Народну банку Србије на обрасцу који је утврђен у Прилогу 1 и достави јој нацрт тог анекса.

Рокови из ст. 1. и 4. ове тачке рачунају се од дана достављања уредне документације из ове тачке.

21. Народна банка Србије посебно цени да ли поверавање активности пружаоцу услуга може довести до концентрације учесника на тржишту

услуга информационих технологија које се пружају финансијским институцијама или до доминантног положаја пружаоца услуга на том тржишту, који би се могао негативно одразити на ово тржиште или на несметано функционисање платног система или на стабилност финансијског система.

Народна банка Србије оцену из става 1. ове тачке може дати након достављања обавештења са уредном документацијом из тачке 20. ове одлуке, и то пре или након поверавања активности у било ком тренутку.

Ако оцени да поверавање активности пружаоцу услуга може довести до концентрације учесника на тржишту услуга информационих технологија које се пружају финансијским институцијама или до доминантног положаја пружаоца услуга на том тржишту, који би се могао негативно одразити на ово тржиште или на несметано функционисање платног система или на стабилност финансијског система – Народна банка Србије о томе обавештава финансијску институцију, на основу чега та институција не може поверити активности пружаоцу услуга из става 1. ове тачке. Ако је обавештење из овог става примила након поверавања активности – финансијска институција је дужна да уговор о поверавању активности раскине у року који је утврдила Народна банка Србије, а који не може бити краћи од три месеца од дана пријема тог обавештења.

22. Финансијска институција је дужна да Народној банци Србије достави уговор из тачке 20. став 1. ове одлуке, укључујући и анексе тог уговора – у року од 15 дана од дана закључења тог уговора, односно анекса. У случају да се закључени уговор разликује од нацрта уговора који је финансијска институција доставила уз обавештење из тачке 20. став 1. ове одлуке, неопходно је да се при достављању уговора из ове тачке назначи у којем делу су извршене измене.

У случају раскида уговора из става 1. ове тачке, финансијска институција је дужна да о томе без одлагања обавести Народну банку Србије.

Поступак потповеравања активности

23. Пружалац услуга може потпружаоцу услуга поверити активности које је финансијска институција поверила њему или друге послове који су у вези с тим активностима – само уз претходну сагласност финансијске институције, коју она даје у сваком појединачном случају.

У случају критичних/кључних пословних процеса, финансијска институција дужна је да пре давања сагласности из става 1. ове тачке процени ризике повезане с потповеравањем активности и ризике који

могу настати када један пружалац услуга за реализацију поверених активности ангажује више потпружалаца услуга (сложени ланци поверавања активности).

24. Финансијска институција је дужна да обезбеди да сваки уговор закључен с потпружаоцем услуга нарочито садржи одредбе којима се:

1) детаљно и прецизно описују потповерене активности које су предмет уговора;

2) утврђују обавезе за потпружаоца услуга из тачке 19. ст. 2. и 4. ове одлуке;

3) пружалац услуга обавезује да врши надзор над квалитетом, квантитетом и континуитетом обављања поверених активности;

4) финансијској институцији омогућава право приговора на квалитет и ниво пружених услуга, као и евентуални раскид уговора с пружаоцем услуга или право да од пружаоца услуга захтева да раскине уговор с потпружаоцем услуга;

5) дефинишу локације на којима ће се обављати потповерене активности и локације на којима ће се обрађивати и чувати подаци;

6) уређује начин приступа информационом систему финансијске институције, односно начин управљања правима приступа када је то неопходно за пружање услуге;

7) утврђује обавеза потпружаоца услуга да при пружању услуга у потпуности поступа у складу с прописима Републике Србије.

25. Финансијска институција може дати сагласност из тачке 23. став 1. ове одлуке само ако је најкасније 30 дана пре давања те сагласности обавестила Народну банку Србије о намераваном потповеравању активности на обрасцу који је утврђен у Прилогу 1.

Уз обавештење из става 1. ове тачке, финансијска институција доставља:

1) нацрт одлуке надлежног органа управљања финансијском институцијом о давању сагласности из тачке 23. став 1. ове одлуке;

2) нацрт уговора о потповеравању активности у складу с тачком 24. ове одлуке;

3) резултате процене ризика из тачке 23. став 2. ове одлуке;

4) резултате ревидиране процене из тачке 15. став 2. ове одлуке;

5) ревидирану излазну стратегију из тачке 17. ове одлуке;

6) доказ о томе да прописи државе, односно држава у којима потпружалац услуга 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

потпружалац услуга 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.

Поверавање активности коришћењем клауд услуга

26. Поверавање активности коришћењем клауд услуга врши се у складу са одредбама ове одлуке.

27. У случају поверавања активности из тачке 26. ове одлуке, финансијска институција дужна је да додатно утврди:

1) јасне улоге и одговорност за информациону безбедност пружаоца клауд услуга према финансијској институцији;
2) одговорности за одржавање хардверских и софтверских компоненти према захтевима произвођача, тестирања и примене безбедносних закрпа (енг. „*patch*“);
3) начин управљања инцидентима тако да се утврде поступци и улоге за решавање инцидента, као и начин извештавања о насталом инциденту и његовим последицама по финансијску институцију;
4) безбедан механизам аутентификације, односно контролу приступа подацима и сервисима коришћењем вишеструке аутентификације;
5) поступке којима се обезбеђује адекватна енкрипција података у преносу, при складиштењу и прил изради резервних копија података.

28. Финансијска институција која намерава да повери активности коришћењем клауд услуга дужна је да приликом процене ризика тог поверавања додатно узме у обзир следеће:

1) модел имплементације клауд услуга (јавни, приватни, заједнички, хибридни и др.);
2) тип клауд услуга (инфраструктура као услуга – IaaS, платформа као услуга – PaaS и софтвер као услуга – SaaS и др.);
3) утицај миграције податка и имплементације ресурса у изабрани тип клауд услуга;
4) капацитете мреже за једноставан и безбедан пренос података (преносивост података);
5) заштиту података при преносу и чувању у клауду.

29. Код поверавања активности коришћењем клауд услуга финансијска институција је дужна да, у складу с тачком 17. ове одлуке, изради адекватну излазну стратегију у случају престанка пружања тих

услуга, која додатно укључује поступке којима се уређују укидање и поновно успостављање клауд услуга или њихово преношење на другог пружаоца услуга или на ту финансијску институцију, као и детаљне планове за миграцију података и/или ресурса информационих система у зависности од типа клауд услуга.

30. Финансијска институција је дужна да обезбеди да сваки уговор којим се поверавају активности коришћењем клауд услуга, поред одредаба из тачке 18. ове одлуке, садржи и одредбе којима се уређују власништво над подацима, начин приступа подацима и сервисима, као и преузимање података финансијске институције у читљивом облику након престанка пружања те услуге и њихово адекватно брисање код пружаоца услуга.

Надзор над повереним активностима

31. Финансијска институција је дужна да обезбеди да пружалац услуга њој, спољном ревизору и Народној банци Србије омогући благовремен и неограничен приступ документацији и подацима у вези с повереним активностима.

Финансијска институција је дужна да Народној банци Србије омогући и несметано вршење непосредне контроле обављања поверених активности у просторијама пружаоца или потпружаоца услуга, односно на локацији на којој се поверене активности обављају.

Ако у поступку контроле, односно надзора утврди да финансијска институција, због пропуста у раду пружаоца услуга или потпружаоца услуга, не поступа у складу са овом одлуком и другим прописима – Народна банка Србије може финансијској институцији наложити да раскине уговор о поверавању активности закључен с пружаоцем услуга.

32. Финансијска институција одговара у целини за активности које је поверила пружаоцима услуга.

33. Финансијска институција је дужна да предузме одговарајуће мере, укључујући и раскид уговора, ако пружалац услуга или потпружалац услуга не поступа у складу са уговором, прописима или професионалним стандардима или ако су утврђени значајни пропусти у вези са очувањем поверљивости, интегритета, расположивости, аутентичности, доказивости, непорецивости и поузданости у информационом систему.

34. Финансијска институција је дужна да редовно врши надзор над пруженим услугама, односно да најмање једном годишње изврши:

1) детаљну анализу сваког пружаоца услуга која се односи на његову способност пружања услуга, могућност његовог информационог система да подржи поверене активности, број запослених код пружаоца услуга опредељених за обављање поверене активности, финансијско стање, пословну репутацију и др.;

2) процену ризика информационог система у односу на поверене активности;

3) процену да ли прекиди у пружању услуге или неодговарајући ниво пружене услуге могу имати негативан утицај на континуитет пословања финансијске институције и услуге које она пружа, односно да ли активност коју поверава утиче на критичан/кључни пословни процес;

4) анализу успешности претходне сарадње са одређеним пружаоцем услуга и могућност његове замене.

Евиденција поверених активности

35. Финансијска институција је дужна да води ажурну евиденцију о повереним активностима у вези са информационим системом која садржи:

1) број уговора о поверавању активности;

2) датуме закључења, евентуалне измене и престанка важења уговора;

3) податке о пружаоцу услуга – пословно име, седиште пружаоца услуга, матични број и друге релевантне податке;

4) информацију о томе да ли је пружалац услуга повезан с финансијском институцијом имовинским и/или управљачким односима;

5) класификацију поверене активности која треба да олакша њену идентификацију (нпр. одржавање хардверске опреме, имплементација софтверских компоненти, пенетрационо тестирање, одржавање главне пословне апликације и др.);

6) кратак опис активности која се поверава;

7) опис података којима пружалац услуга има приступ или се код њега налазе, односно информацију о томе да ли је дошло до преноса података на другог пружаоца услуга;

8) информацију о томе да ли је поверена активност критична/кључна или утиче на критичне/кључне пословне процесе;

9) назив државе или држава у којима се обавља поверена активност и државе или држава у којима се налазе подаци;

10) информацију о моделу и типу клауд услуге;

11) датум последње процене нивоа пружене услуге и процене ризика информационог система у вези с повереним активностима;

12) информације о потповереним услугама (кратак опис услуге, основне податке о потпружаоцу услуга и др.).

Банка је дужна да извод из евиденције који садржи преглед свих поверених активности доставља Народној банци Србије у складу са одлуком којом се уређује поверавање активности банке трећем лицу.

Прелазне и завршне одредбе

36. Финансијска институција је дужна да своје унутрашње акте усклади са одредбама ове одлуке у року од шест месеци од дана њеног ступања на снагу.

37. Финансијска институција је дужна да постојеће уговоре о поверавању активности који су закључени у складу са Одлуком о минималним стандардима управљања информационим системом финансијске институције („Службени гласник РС“, бр. 23/2013, 113/2013, 2/2017, 88/2019 и 37/2021) усклади са одредбама ове одлуке при првој измени уговора, а најкасније 31. децембра 2024. године.

38. Даном почетка примене ове одлуке престају да важе тач. 40. до 48а. Одлуке о минималним стандардима управљања информационим системом финансијске институције („Службени гласник РС“, бр. 23/2013, 113/2013, 2/2017, 88/2019 и 37/2021).

39. Ова одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије“, а примењује се од 1. марта 2024. године.

ИО НБС бр. 83
9. новембра 2023. године
Б е о г р а д

Председавајућа
Извршног одбора Народне банке Србије
Г у в е р н е р
Народне банке Србије

Др Јоргованка Табаковић, с.р.