

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 ИЗМЕНАМА И ДОПУНАМА ОДЛУКЕ О МИНИМАЛНИМ
СТАНДАРДИМА УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМОМ
ФИНАНСИЈСКЕ ИНСТИТУЦИЈЕ

1. У Одлуци о минималним стандардима управљања информационим системом финансијске институције („Службени гласник РС“, бр. 23/2013, 113/2013 и 2/2017), у тачки 5. после става 1. додаје се нови став 2, који гласи:

„У складу са стратегијом развоја информационог система, финансијска институција дужна је да донесе одговарајуће стратегијске и оперативне планове.“.

Досадашњи став 2. постаје став 3.

После досадашњег става 2, који постаје став 3, додаје се став 4, који гласи:

„Финансијска институција је дужна да о свакој измени и/или допуни стратегије развоја информационог система обавести Народну банку Србије у року од 15 дана од дана њеног усвајања.“.

2. У тачки 6. после става 1. додаје се став 2, који гласи:

„Финансијска институција је у оквиру поделе послова и дужности из става 1. ове тачке нарочито дужна да јасно утврди послове и дужности запослених који су у непосредној вези са ефикасним и одговарајућим управљањем безбедношћу информационог система.“.

3. У тачки 17. после става 1. додаје се нови став 2, који гласи:

„Финансијска институција је дужна да, у складу с природом, обимом и сложеностју пословања, као и сложеностју информационог система:

1) поделу послова у вези са безбедношћу тог система изврши тако да се у унутрашњим актима којима се уређује организација њеног

пословања јасно могу утврдити послови и дужности запослених у вези с том безбедношћу;

2) одреди кључне запослене задужене за безбедност информационог система водећи рачуна о томе да њихова позиција има значајан утицај на активности и доношење одлука у вези с том безбедношћу;

3) у управљање безбедношћу информационог система укључи довољан број запослених који имају одговарајућу стручност и професионално искуство.“.

Досадашњи став 2. постаје став 3.

4. У тачки 29. став 2. мења се и гласи:

„Финансијска институција је дужна да Народну банку Србије обавести у случају инцидента који је озбиљно угрозио или нарушио њено пословање, односно који би могао озбиљно угрозити или нарушити њено пословање, и то:

1) ако је настао услед нарушавања функционалности ресурса информационог система – одмах по утврђивању околности о настанку тог инцидента;

2) ако је настао као последица нарушавања безбедности информационог система – одмах по сазнању о том инциденту;

3) ако је настао код пружаоца услуге, а имао је или је могао имати значајан утицај на информациони систем финансијске институције – одмах по утврђивању околности о настанку тог инцидента, односно сазнању о том инциденту.“.

После става 2. додају се ст. 3. и 4, који гласе:

„Након обавештења из става 2. ове тачке, ако је инцидент и даље у току, финансијска институција је дужна да Народну банку Србије континуирано обавештава о битним догађајима и другим релевантним информацијама у вези са инцидентом (статус инцидента), као и о активностима предузетим ради ублажавања инцидента и његовим последицама. Ово обавештење садржи и детаљан опис инцидента, информације о процени броја корисника на које је инцидент утицао, оквирно време потребно да се инцидент реши, потенцијални утицај на друге финансијске институције, 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).

Финансијска институција је дужна да Народној банци Србије достави завршни извештај о насталом инциденту у року од 15 дана од дана престанка инцидента, односно од дана када процени да су успостављени редовно пословање финансијске институције и стабилан рад информационог система. Овај извештај садржи коначне информације о инциденту – датум почетка и датум окончања инцидента, дужина трајања инцидента, врста инцидента (недоступност хардверских компоненти, проблеми у раду софтверских компоненти или безбедносни инцидент), опис инцидента, узроци настанка и последице инцидента, активности које је финансијска институција спроводила током инцидента, план активности којима ће превентивно деловати и спречити поновне појаве истог инцидента, број корисника на које је инцидент утицао, настали финансијски трошкови повезани са инцидентом, утицај на друге финансијске институције и, по потреби, друге релевантне информације.“.

5. После тачке 29. додаје се тачка 29а, која гласи:

„29а. Финансијска институција је дужна да тромесечно извештава Народну банку Србије о инцидентима који су повезани са злоупотребом осетљивих података корисника финансијских услуга, неодобреним платним трансакцијама, злоупотребом, крађом или губитком платних инструмената, укључујући коришћење техничких манипулација на банкоматима (АТМ), преварним радњама и злоупотребима корисника финансијских услуга, злоупотребима фактора аутентификације и система за аутентификацију и сл. а који нису имали директан утицај на њен информациони систем.

Извештај из става 1. ове тачке доставља се најкасније 10. у првом месецу тромесечја, а Народна банка Србије може ближе уредити начин достављања овог извештаја.“.

6. У тачки 37. став 1. после речи: „главних пословних апликација (*core business application*)“ додају се речи: „или у други рачунарски центар, односно која врши промену локације рачунарског центра,“.

У ставу 2. одредба под 4) после речи: „пре миграције података“ додају се запета и речи: „који укључује динамику тог враћања и опис активности, као и критеријуме за доношење одлуке за примену овог плана“.

У ставу 3. после речи: „с подацима из става 2. те тачке“ додају се запета и речи: „а банка је дужна да достави и захтев за омогућавање функционисања привременог рачуна правног следбеника (у даљем тексту: захтев за привремени рачун) који мора потписати законски

заступник правног следбеника – ради поступања Народне банке Србије по том захтеву у случају из става 5. ове тачке“.

После става 3. додају се ст. 4. до 8, који гласе:

„Привремени рачун правног следбеника представља рачун банке која престаје да постоји због статусне промене који је отворен у Народној банци Србије у складу с прописима, односно правилима рада платног система у којем та банка учествује а који због статусне промене преузима правни следбеник, ради његовог привременог функционисања у року утврђеном овом одлуком.

Финансијска институција која донесе одлуку о примени плана враћања на стање пре миграције података дужна је да о томе без одлагања обавести Народну банку Србије.

Ако донесе одлуку о примени плана враћања на стање пре миграције података због статусне промене, банка је дужна да о томе обавести Народну банку Србије најкасније наредног радног дана од дана када је започела миграцију података, и то најкасније један сат пре почетка периода утврђеног Дневним терминским планом рада RTGS платног система Народне банке Србије (у даљем тексту: RTGS НБС систем) за извршавање налога за пренос у том систему.

Финансијска институција је дужна да поступак миграције података због статусне промене спроведе најкасније у року од десет радних дана од дана почетка примене плана из става 5. ове тачке.

Привремени рачун правног следбеника из става 4. ове тачке, као и поступање Народне банке Србије у складу са захтевом за привремени рачун ближе се уређују правилима рада RTGS НБС система.“.

7. У тачки 41. после става 1. додаје се став 2, који гласи:

„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, на један од следећих начина:

1) обавезивањем тог 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 добављачем 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.“.

8. У тачки 43. после става 1. додаје се нови став 2, који гласи:

„Финансијска институција је дужна да обезбеди да сваки уговор закључен с пружаоцем услуга садржи одредбу којом се пружалац услуга обавезује да испуни обавезу из става 1. ове тачке, као и одредбу која финансијској институцији омогућава да једнострано раскине овај уговор ако то наложи Народна банка Србије и у складу с тим налогом.“.

Досадашњи став 2. постаје став 3.

9. У тачки 45. став 2. мења се и гласи:

„Ако се мења уговор из става 1. ове тачке а да се при томе не мења поверена активност, односно пружалац услуга или се не утиче на резултате анализе из тачке 42. став 1. одредба под 1) ове одлуке, односно на резултате процене из тачке 42. став 2. те одлуке – финансијска институција је дужна да најкасније 15 дана пре закључења анекса тог уговора о томе обавести Народну банку Србије и достави јој нацрт тог анекса.“.

После става 3. додаје се став 4, који гласи:

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

10. Тачка 46. брише се.

11. У тачки 47. став 1. речи: „и тачке 46.“ бришу се.

После става 3. додаје се став 4, који гласи:

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

12. У тачки 48. после става 1. додаје се нови став 2, који гласи:

„Финансијска институција је дужна да континуирано врши надзор над пруженим услугама, као и проверу квалитета пружених услуга у вези с повереним активностима.“.

Досадашњи став 2. постаје став 3.

13. После тачке 48. додаје се тачка 48а, која гласи:

„48а. Финансијска институција је дужна да Народној банци Србије достави уговор из тачке 40. 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, финансијска институција о томе без одлагања обавештава Народну банку Србије.“.

14. Финансијске институције су дужне да своје пословање ускладе са одредбама ове одлуке до дана почетка њене примене.

15. Ова одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије“, а примењује се од 12. марта 2020. године.

ИО НБС бр. 73
12. децембра 2019. године
Београд

Председавајући
Извршног одбора Народне банке Србије
на седници одржаној
12. децембра 2019. године
Вицегувернер
Народне банке Србије

Др Жељко Јовић, с.р.