

На основу члана 35. став 4. Закона о Централном регистру обавезног социјалног осигурања („Службени гласник РС”, број 95/18),

Министар финансија доноси

ПРАВИЛНИК

о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања

"Службени гласник РС", број 48 од 5. јула 2019.

Садржина Правилника

Члан 1.

Овим правилником уређују се процедуре чувања, заштите и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања (у даљем тексту: информациони систем Централног регистра).

Циљеви заштите информационог система

Члан 2.

Циљеви заштите информационог система Централног регистра су:

- 1) очување поверљивости података, чиме се онемогућава неауторизован увид и коришћење података из информационог система Централног регистра;
- 2) заштита интегритета података, чиме се онемогућава измена података и гарантује аутентичност података;
- 3) очување расположивости података, чиме се омогућава реконструкција података у случају њиховог намерног или ненамерног оштећења.

Заштита из става 1. овог члана обезбеђује се кроз заштиту приступа рачунарској опреми и мрежи, која се реализује на мрежном нивоу кроз специјализоване хардверске компоненте и уз употребу протокола заштите, као и кроз заштиту приступа подацима.

Чување, заштита и сигурност података Централног регистра

Члан 3.

Централни регистар је одговоран за чување, заштиту и сигурност података у оквиру информационог система Централног регистра, што подразумева:

- 1) заштиту од неовлашћеног приступа ресурсима који су предмет заштите, њихово неовлашћено коришћење или манипулације базом података информационог система од стране интерних и екстерних корисника;
- 2) заштиту интегритета података, њихову расположивост и неовлашћени увид у поверљиве податке;

- 3) заштиту базе података од вируса и осталих облика малициозних кодова;
- 4) осигурање преноса података из Јединствене базе интерним и екстерним корисницима;
- 5) чување података и управљање сигурносним копијама базе података у оквиру информационог система;
- 6) политику преносних рачунара у погледу приступа бази података Јединствене базе и чувања података у јединственој бази;
- 7) осигурање континуитета активности у случају пожара, поплаве, земљотреса или друге непогоде која се сматра резултатом више силе и која доводи до неуобичајеног прекида у раду информационог система;
- 8) повраћај сачуваних података у случају губитка, оштећења или уништења рачунарске опреме информационог система;
- 9) тестирање јединствене базе података ради откривања сигурносних проблема на редовној основи и након инсталирања нових верзија Јединствене базе података;
- 10) инсталирање софтверске надоградње ради уклањања сигурносних проблема који се установе на Јединственој бази у оквиру информационог система или на повезаном софтверу;
- 11) праћење сигурносних инцидената у бази података информационог система ради предузимања корективних мера;
- 12) управљање сигурносним инцидентима, едукација и обука свих овлашћених лица ради стицања потребних знања о чувању и сигурности података;
- 13) физички приступ и заштита базе података у оквиру информационог система и рачунарске опреме;
- 14) одржавање рачунарске опреме информационог система.

Мере заштите приступа информационом систему

Члан 4.

Мере заштите приступа информационом систему Централног регистра су:

- 1) аутентификација – која представља процес утврђивања идентитета лица које жели да приступи информационом систему Централног регистра;
- 2) ауторизација – која представља право приступа и дозвољених операција за аутентификовано лице;
- 3) заштита тајности – што подразумева шифровање података у циљу спречавања неовлашћеног увида;

4) непорицање одговорности – што подразумева обезбеђење доказа да је неко извршио одређену радњу, односно трансакцију.

Реализација система заштите информационог система Централног регистра подразумева обавезну примену квалификованих електронских сертификата за приступ преко Портала и аутентификацију трансакција, као и за аутентификацију приступа Веб сервисима.

Аутентификација приступа сервисима од стране државних органа и организација, са којима Централни регистар врши размену података подразумева и обавезну примену серверских сертификата.

Изузетно, осигураници и осигурана лица, који имају право увида у личне податке који се односе на осигурање, могу приступити информационим систему Централног регистра на основу јединственог броја и лозинке, које додељује Централни регистар.

Приступ информационом систему Централног регистра

Члан 5.

Централни регистар управља корисничким налозима, правима приступа и корисничким лозинкама за интерне и екстерне кориснике јединствене базе Централног регистра.

Централни регистар дужан је да обезбеди приступ подацима у оквиру информационог система само од стране овлашћених лица.

Сваки приступ информационом систему мора бити аутоматски забележен јединственим идентификатором лица у бази података јединственог система, са тачним временом приступа.

О сазнањима у вези са покушајима неовлашћеног приступа информационом систему Централног регистра, администратори Јединствене базе података дужни су да обавесте овлашћено лице.

Физичка заштита података информационог система и чување безбедносних копија

Члан 6.

Ради обезбеђења непрекидног функционисања информационог система, Централни регистар обезбеђује физичку заштиту података примарног информационог система, формирањем секундарне базе података и секундарног рачунарског система.

Секундарна база података и секундарни рачунарски систем морају бити удаљени од места на коме се налази примарни информациони систем.

Локације из ст. 1. и 2. овог члана морају бити на адекватан начин заштићене од пожара и поплава, као и имати 24-сатни безбедносни систем.

Приступ локацијама на којима се налазе базе података информационог система и чувају безбедносне копије имају само овлашћена лица.

Одржавање, поправка и повлачење из употребе опреме за информациони систем

Члан 7.

Централни регистар обезбеђује одржавање рачунарске опреме за информациони систем а, у случају поправки, претходно спрема безбедносне копије података, како би се спречио губитак података.

Одржавање и поправка рачунарске опреме, врши се искључиво под надзором овлашћених запослених у Централном регистру.

У случају повлачења рачунарске опреме из информационог система, сви подаци претходно морају бити трајно и сигурно избрисани.

Престанак важења ранијег прописа

Члан 8.

Даном ступања на снагу овог правилника престаје да важи Правилник о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања („Службени гласник РС”, број 29/13)

Ступање на снагу

Члан 9.

Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

Број 110-00-00375/2019-03

У Београду, 26. јуна 2019. године.

Министар,

др **Синиша Мали**, с.р.