ОРГАНИЗАЦИЈА ЗА КОЛЕКТИВНО ОСТВАРИВАЊЕ ПРАВА ИНТЕРПРЕТАТОРА

ПРОЦЕДУРА

ЗА ПОСТУПАЊЕ ПРИЛИКОМ ПОВРЕДЕ ПОДАТАКА О ЛИЧНОСТИ

Садржај:

1. Сврха документа

Сврха овог документа је дефинисање упутстава за поступање Организације за колетивно остваривање права интерпретатора (у даљем тексту: „**Организација ПИ**“) у случају повреде података о личности у смислу Закона о заштити података о личности („Сл. гласник РС“ број 87/2018) (у даљем тексту „**Закон**“).

2. Ознаке, скраћенице и дефиниције

Руковалац	Физичко или правно лице које самостално или заједно са другима одређује сврху и начин обраде.
Обрађивач	Физичко или правно лице које обрађује податке о личности у име Руковаоца.
Лице на које се подаци односе	Физичко лице чији се подаци обрађују.
Повреда података о личности	Повреда безбедности података о личности која доводи до случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа подацима о личности који су пренесени, похрањени или на други начин обрађивани.

3. Подручје примене

Ова процедура се примењује на Организацију ПИ када обрађује податке о личности у својству руковаоца, односно у својству заједничког руковаоца, када је то примењиво.

4. Опис процедуре

4.1 Обавезност пријављивања неуобичајеног догађаја

Сва лица у оквиру Организације ПИ која приликом рада постану свесна било ког неуобичајеног догађаја који се односи на повреду података о личности дужна су да о томе одмах обавесте Лице за заштиту података о личности.

4.2 Анализа неоубичајеног догађаја

Лице за заштиту података о личности одмах по сазнању за неуобичајени догађај о томе прикупља све релевантне информације и укључује следећа лица: а) лице које је првобитно пријавило неуобичајен догађај, б) руководиоце сектора у оквиру Организације ПИ на које се неуобичајен догађај односи. Након тога, Лице за заштиту података о личности уз помоћ наведених лица врши процену да ли неоуобичајен догађај представља потенцијалну повреду података о личности или лажну узбуну (у ком случају се ова процедура прекида). Ако Лице за заштиту података о личности има било какве сумње са овим у вези, закључиће да неуобичајени догађај представља потенцијалну повреду података о личности.

Ако Лице за заштиту података о личности закључи да неуобичајени догађај представља потенцијалну повреду података о личности, он ће хитно иницирати спровођење свих неопходних мера како би се умањио утицај неоубичајеног догађаја.

4.3 План процене и поступања приликом повреде података о личности

Лице за заштиту података о личности покреће „План процене и поступања приликом повреде података о личности“.

Циљ овог плана је правилно поступање у случају повреде података о личности у складу са чланом 50, 52 и 53 Закона. У наставку су побројане и описане све активности поводом повреде података о личности.

1) Прикупљање свих неопходних доказа и информација

Лице за заштиту података о личности прикупља доказе и информације укључујући, уколико је потребно:

- све релевантне запослене у оквиру Организацији ПИ који могу пружити корисне информације и/или помоћ;
- екстерне пружаоце услуга Организација ПИ који могу пружити помоћ, предложити средства и мере за смањење ризика.

Лице за заштиту података о личности анализира све прикупљене податке заједно и узима их у обзир приликом израде Извештаја о повреди података о личности.

2) Класификација повреде података о личности

Лице за заштиту података о личности ће проценити потенцијалну повреду података о личности узимајући у обзир следеће критеријуме:

Тип догађаја:

- уобичајено хаковање;
- вируси;
- губитак или крађа пословних уређаја (ЦД-ова, УСБ флеш меморија, телефона, таблета сл.);
- губитак или крађа документације (укључујући и у папирном облику) који садрже податке о личности;
- природна непогода;
- случајно откривање имена/е-мејл адреса других примаоца е-мејла.
- итд.

Исход:

- незаконито уништење, приступ, губитак или измена података о личности;
- случајно уништење, приступ, губитак или измена података о личности;
- неовлашћено откривање, уништење, приступ или измена података о личности;
- крађа података о личности и сл.

Друге околности:

- да ли су посебне врсте података о личности погођене повредом;
- да ли су подаци о личности рањивих категорија лица на која се подаци односе погођени повредом података о личности;
- да ли радње обраде погођене повредом података о личности обухватају обраду података о личности у великом обиму;
- да ли радње обраде погођене повредом података о личности обухватају обраду великог броја лица на која се подаци односе;
- да ли ће неовлашћена лица лако идентификовати лица чији су подаци повређени.

Све напред наведене околности биће уредно евидентиране у Извештају о повреди података о личности.

3) Спровођење мера за смањење ризика

Примарни циљ и сврха Плана процене и поступања приликом повреде података о личности јесте благовремена идентификација и примена адекватних безбедносних мера прилагођених случају како би се избегле или умањиле последице по лица на која се подаци односе. У том смислу Лице за заштиту података о личности, константно сарађује током свих фаза ове процедуре у циљу идентификације, процене, примене и комуникације таквих мера. Такође, све спроведене активности и мере биће уредно евидентиране у Извештају о повреди података о личности.

4) Сазнање за повреду

Организација ПИ након утврђивања постојања повреде података о личности треба да буде свесна повреде и да правилно процени своје обавезе из члана 52 и 53 Закона. Након спровођења активности из тачке 1) и 2) сматра се да је Организација ПИ стекла разумни степен сазнања за повреду података о личности.

Након спровођења активности из тачки 1) до 3) Организација ПИ је дужна да без одлагања или у року од 72 сата обавести Повереника о повреди података о личности која може да произведе ризик по права и слободе физичких лица. Са друге стране, након спровођења активности из тачки 1) до 3) Организација ПИ је дужна да без непотребног одлагања о повреди обавести лице на које се подаци односе ако повреда података о личности може да произведе висок ризик по права и слободе физичких лица.

5) Процена вероватноће наступања и висине ризика

При вршењу процене, Лице за заштиту података о личности, узимајући у обзир постојеће безбедносне мере, процениће вероватноћу наступања последица по лица на која се подаци односе, али и по друга физичка лица, а нарочито следећих ризика:

- дискриминације;
- крађе идентитета или превара;
- финансијских губитака;
- угрожавања угледа;
- повреде поверљивих података о личности заштићених у виду професионалне тајне;
- неовлашћеног дешифровања псеудонимизованих података о личности;
- значајне економска или социјална штета;
- губитка или ограничавања права или слобода;
- смањења могућности за контролу података о личности од стране лица на које се подаци односе;
- физичког оштећења, материјалне или нематеријалне штете итд.

Лице за заштиту података о личности ће оценити вероватноћу наступања ризика по права и слободе физичких лица приликом повреде података о личности користећи доњу скалу са четири нивоа:

- немогуће;
- мало вероватно;
- вероватно;

- веома могуће.

На основу горњих елемената и процене, Лице за заштиту података о личности утврђује вероватноћу да је повреда података о личности проузроковала висок ризик за права и слободе физичких лица, користећи доњу скалу са четири нивоа, а узимајући у обзир постојеће безбедносне мере Организације ПИ:

- немогуће;
- мало вероватно;
- вероватно;
- веома могуће.

Све напред наведено биће уредно евидентирано у Извештају о повреди података о личности.

6) Обавештавање

-Обавештавање Повереника-

У складу са чланом 52 Закона, Организација ПИ је дужна да о повреди података о личности која може да произведе ризик по права и слободе физичких лица обавести Повереника без непотребног одлагања, или ако је то могуће, у року од 72 часа од сазнања за повреду.

Стога, Лице за заштиту података о личности најпре испитује и проверава сва документа и информације прикупљене током претходно описаних фаза. Након тога врши се обавештавање Повереника о повреди од стране Лица за заштиту података о личности.

Обавештење Поверенику садржи најмање следеће информације:

1) опис природе повреде података о личности, укључујући врсте података и приближан број лица на која се подаци односе, као и приближан број података о личности чија је безбедност повређена;
2) име и контакт податке лица за заштиту података о личности или информације о другом начину на који се могу добити подаци о повреди;
3) опис могућих последица повреде;
4) опис мера које је Организација ПИ предузела или чије је предузимање предложено у вези са повредом, укључујући мере које су предузете у циљу смањења штетних последица.

Уколико Организација ПИ није у могућности да све ове информације достави истовремено, може поступно достављати доступне информације, али без непотребног одлагања. Ово је посебно значајно у случају када се повреда података о личности десила код обрађивача Организације ПИ, те је прикупљање информација о повреди, из тог разлога отежано.

У сваком случају, све горе наведене информације Лице за заштиту података о личности евидентира у Дневнику повреда података о личности.

-Обавештавање лица на која се подаци односе-

Такође, Организација ПИ је дужна да о повреди података о личности која може да произведе висок ризик по права и слободе физичких лица без непотребног одлагања обавести лице на које се подаци односе, у складу са чланом 53 Закона. Ово обавештење се доставља након одлуке Лица за заштиту података о личности, и то по могућству на језику којим се користе лица на која се подаци односе. Такође је пожељно да се обавештење достави путем канала комуникације који је за лица на која се

подаци односе најприкладнији. Обавештење треба да буде јасно, потпуно, транспарентно и лако разумљиво.

У обавештењу упућеном лицу на које се подаци односе Организација ПИ је дужна да на јасан и разумљив начин опише природу повреде података и наведе најмање следеће информације: а) име и контакт податке лица за заштиту података о личности или информације о другом начину на који се могу добити подаци о повреди; б) опис могућих последица повреде; г) опис мера које је Организација ПИ предузела или чије је предузимање предложено у вези са повредом, укључујући мере које су предузете у циљу смањења штетних последица.

Обавештавање лица на које се подаци односе није неопходно уколико су испуњени следећи услови:

- Организација ПИ је предузела одговарајуће техничке, организационе и кадровске мере заштите у односу на податке о личности чија је безбедност повређена, а посебно криптозаштиту или друге мере којима је онемогућио разумљивост података свим неовлашћеним лицима;
- Организација ПИ је накнадно предузела мере којима је обезбедио да повреда података о личности са виским ризиком за права и слободе лица на које се подаци односе више не може да произведе последице за то лице;
- ако би обавештавање лица на које се подаци односе представљало несразмеран утрошак времена и средстава, у ком случају је Организација ПИ дужна да путем јавног обавештавања или на други делотворан начин обезбеди пружање обавештења лицу на које се подаци односе.

Са друге стране, ако Ораганизација ПИ није обавестила лице на која се подаци односе о повреди података о личности, Повереник може узимајући у обзир могућност да повреда произведе висок ризик, да наложи Организацији ПИ да то учини или може да утврди да су испуњени горе наведени услови.

Све горе наведене чињенице, укључујући и то да ли је обавештење достављено лицима или не, као и вид комуникације (нпр. непосредно лицу на које се подаци односе или путем јавног обавештавања) Лице за заштиту података о личности евидентира у Дневнику повреда података о личности.

7) Израда Извештаја о повреди података о личности и укључивање управитеља

Лице за заштиту података о личности је одговорно за израду Извештаја о повреди података о личности - основног оперативног извештаја који предочава поступање Организације ПИ у случају повреде. Извештај садржи следеће информације:

- класификацију догађаја и последице потенцијалне повреде података;
- процену вероватноће наступања и висине ризика;
- предузете мере за смањење или отклањање последица повреде;
- преостали ризик;
- да ли је неопходно обавештавање Повереника и/или лица на која се подаци односе.

Лице за заштиту података о личности израђује Извештај о повреди података о личности у најкраћем могућем року.

Узимајући у обзир значај повреде података о личности за пословање Организације ПИ, Лице за заштиту података о личности ће одмах путем е-мејла или на други прикладан начин обавестити

директора Организације ПИ о повреди уз достављање Извештаја о повреди приликом обавештавања. Директор може у било ком тренутку давати упутства и предлоге Лицу за заштиту података о личности у вези са управљањем повредом података о личности.

4.4 Анализа након догађаја

Током ове фазе врши се анализа у циљу провере успешности и ефикасности примењених безбедносних мера које би требало да спрече повреду података о личности, као и радњи предузетих током управљања неуобичајеним догађајем. Ова анализа би требало да идентификује одређене аспекте које би требало унапредити. Приликом отклањања уочених слабости треба посебно узети следеће чињенице у обзир, а у циљу спречавања сличних појава у будућности:

- адекватност постојећих техничких, организационих и кадровских мера и потреба за надоградњом истих (нпр. усвајање ефикаснијег система за праћење неуобичајених догађаја);
- потребу за додатном обуком запослених и других лица у оквиру Организације ПИ;
- потребу за додатним/учесталијим ревизијама и контролама.

Све ове активности ће спроводити Лице за заштиту података о личности, уз помоћ руководиоца сектора у оквиру Организације ПИ. Резултати анализе након догађаја и свих спроведених активности (нпр. одржаних обука и семинара, унапређења упустава и процедура) биће такође евидентирани у Дневнику повреда од стране Лица за заштиту података о личности.

4.5 Дневник повреда

Дневник повреда података о личности је документ који укратко предочава одговорност за поступање Организације ПИ и чија сврха је вођење евиденције о: а) свим неуобичајеним догађајима и повредама података о личности, б) активностима које је Организација ПИ спровела ради смањења њиховог утицаја, в) мерама које је Организација ПИ спровела ради избегавања сличних догађаја у будућности и г) активностима обавештавања, уколико их је било.

Лице за заштиту података о личности документује активности и догађаје у Дневник повреда, укључујући потенцијалне и стварне повреде података о личности, који садржи следеће информације:

- врсту догађаја према Извештају о повреди података о личности;
- да ли су предузете мере за смањење или отклањање последица повреде;
- да ли је неопходно обавештавање Повереника и/или лица на која се подаци односе;
- повратне информације од Повереника и/или лица на која се подаци односе;
- резултате анализе извршене након догађаја.

Заједно са Дневником повреда чувају се копије свих документа који се односе на пријављене инциденте, а посебно Контролне листе повреде и Извештаји о повреди података о личности.

Сврха Дневника повреда података о личности је да омогући Поверенику да изврши увид и проверу усклађености Организације ПИ са обавезама обавештавања о повреди података о личности.

ЗА ОРГАНИЗАЦИЈУ ПИ:

_____

Живорад Ајдачић,
председник Управног одбора