|  |  |  |
| --- | --- | --- |
| **Република Србија**Повереник за информацијеод јавног значаја и заштиту података о личности |  | Тел: +381 (0) 113408 900Фaкс:+381 (0) 11 3343 379Булевар краља Александра 1511000 Београдoffice@poverenik.rs[www.poverenik.rs](http://www.poverenik.org.rs) |

|  |
| --- |
|  |

Број: 072-04-3181/2018-07 Датум: 05.06.2018. године

Повереник за информације од јавног значаја и заштиту података о личности (у даљем тексту: Повереник), и то заменица Повереника, Станојла Мандић, по Одлуци Народне Скупштине Републике Србије број 17 од 08.04.2013. године о избору заменика Повереника, у поступку надзора над спровођењем и извршавањем Закона о заштити података о личности („Сл. гласник РС“, бр. 97/08,104/09 - др. закон, 68/2012 – одлука УС и 107/12 – у даљем тексту: ЗЗПЛ) од стране Министарства здравља Републике Србије, са седиштем у Београду, ул. Немањина бр. 22-26 и „Sorsix International“ д.о.о. Ниш, са седиштем у Нишу, ул. Мачванска број 1 , на основу члана 56. став 2. тачка 2. и члана 58. Закона о заштити података о личности, у вези са чланом 33. став 5. Закона о слободном приступу информацијама од јавног значаја („Сл. гласник РС“ бр. 120/04, 54/07, 104/09 и 36/10) и члана 16. став 1. и члана 136. став 2. Закона о општем управном поступку („Сл. гласник РС“, бр. 18/2016), доноси

**Р Е Ш Е Њ Е**

**I**

„Sorsix International“ д.о.о. Ниш забрањује се обрада података о личности путем апликације „Изабрани доктор“, која се обавља супротно одредбама члан 47. став 2. ЗЗПЛ, до отклањања неправилности у обради података.

**II**

Забрана обраде података ступа на снагу наредног дана од дана пријема овог решења.

**III**

О извршењу решења и предузетим мерама, „Sorsix International“ д.о.о. Ниш, писаним путем ће обавестити Повереника у року од 3 (три) дана од дана пријема овог решења, као и доставити доказ о извршењу наложеног из става I и II диспозитива Решења.

**О б р а з л о ж е њ е**

Повереник је, сходно овлашћењима из члана 54. став 1. и 2. ЗЗПЛ покренуо поступак надзора над спровођењем и извршавањем ЗЗПЛ од стране Министарства здравља Републике Србије и „Sorsix International“ д.о.о. Ниш, а по пријему представке грађанина од 25.05.2018. године, у којој, између осталог, подносилац наводи да је на „Google Play“ продавници преузео апликацију компаније Sorsix под називом „Изабрани доктор“ (<https://play.google.com/store/apps/details?id=com.sorsix.pingamdapp>), чијом је активацијом, након уношења свог личног броја осигураника (у даљем тексту: ЛБО) и броја мобилног телефона на који је примио СМС са кодом, добио приступ својим личним подацима. Такође, подносилац представке наводи да је апликацију затим угасио и да је приликом поновног покретања унео „насумичан“ ЛБО и свој број мобилног телефона ради активације, а затим је, након уношења новог кода могао да изврши увид у горе наведене податке за лице коме припада тај „насумични“ ЛБО.

Увидом у страницу „Google Play“ продавнице на којој је могуће преузети апликацију „Изабрани доктор“, дана 30.05.2018. године, у делу „Додатне информације“ утврђено је да исту нуди „Sorsix Internacional“, а посетом интернет презентацији на адреси <https://izabranidoktor.rs/>, којој се приступа кликом на „Посетите веб-сајт“, утврђено је да се на дну странице налази адреса електронске поште: izabranidoktor@sorsix.com која је означена за контакт, као и да је на мапи означена адреса Мачванска 1 у Нишу, без навођења других информација за контакт. У документу који садржи услове коришћења и политику приватности, који је истог дана био доступан на страници горе наведене апликације <https://izabranidoktor.rs/terms.html>, под тачком „1. Увод“ стајало је, између осталог, следеће: „Услови који следе представљају уговор између Вас и ИзабраниДоктор Апп д.о.о. (у даљем тексту: “ИзабраниДоктор Апп д.о.о.”, “ми”, или “нас”), руковаоца izabranidoktor.rs (“апликације”). Ови услови коришћења (“Услови коришћења”) одређују Ваше коришћење апликације, било као неформалан корисник или као регистровани корисник.“

Инсталацијом апликације на Android смарт уређај утврђено је да се на насловној страни/екрану, по покретању апликације, налази назив апликације, да је иста одобрена од стране Министарства здравља Републике Србије и лого „Sorsix Sva prava zadržana“, док следеће две стране/екрана садрже каратак опис намене и пријављивања у апликацију, уз додатне информације на тастеру „Помоћ“.

Уносом у апликацију валидног ЛБО за лице које нема изабраног лекара апликација указује на грешку и даје контакт телефон сервиса коме је потребно обратити се за помоћ. Уносом валидног ЛБО за лица које има изабраног лекара апликација даље омогућава унос произвољног броја мобилног телефона, на који се шаље код за верификацију, који се уноси на екрану/страници „Активација“ и где лице треба да потврди сагласност са правима и условима коришћења, након чега следи екран/страница за имаоца ЛБО са листом заказаних и обављених прегледа код изабраног лекара, уз могућност заказивања нових прегледа.

Увидом у интернет презентацију на адреси <https://sorsix.com/>, у делу „Contact us“ утврђено је да се, као једна од адреса за контакт, наводи и адреса седишта „Sorsix International“ д.о.о. Ниш.

Претрагом података Агенције за привредне регистре (АПР) за правна лица, на адреси: <http://pretraga2.apr.gov.rs/ObjedinjenePretrage/Search/Search>, утврђено је да ИзабраниДоктор Апп д.о.о. није регистрован као правно лице код те агенције. Такође, истом претрагом утврђено је да није регистровано ни привредно друштво под називом „Sorsix Internacional“, али да је регистровано привредно друштво под називом „Sorsix International“ д.о.о. Ниш, са адресом у Нишу, улица Милорада Вељковића – Шпаје број 1/М3.

Дана 31.05.2018. године, на истој веб адреси „Google Play“ продавнице <https://play.google.com/store/apps/details?id=com.sorsix.pingamdapp> , утврђено је да је документ који садржи услове коришћења и политику приватности накнадно измењен, те да је у истом уместо „ИзабраниДоктор Апп д.о.о.“ наведено „Sorsix International д.о.о.“ Истог дана овај документ је, накнадно, у потпуности уклоњен са ове интернет странице, на којој се не налази ни на дан доношења овог решења.

Увидом у интернет страницу АПР утврђено је да је „Sorsix International“ д.о.о. Ниш 31.05.2018. године променио адресу седишта, те да је иста у Нишу, улица Мачванска број 1.

Члан 47. став 2. ЗЗПЛ прописује да су руковалац и обрађивач дужни да предузму техничке, кадровске и организационе мере заштите података, у складу са утврђеним стандардима и поступцима, а које су потребне да би се подаци заштитили од губитка, уништења, недопуштеног приступа, промене, објављивања и сваке друге злоупотребе, као и да утврде обавезу лица која су запослена на обради, да чувају тајност података.

Поред чињенице да су услови коришћења и политике приватности првобитно упућивали на непостојеће правно лице („ИзабраниДоктор Апп д.о.о.“), затим били измењени тако да упућују на постојеће правно лице, без прецизирања седишта и адресе истог („Sorsix International д.о.о.“), да би коначно били у потпуности уклоњени и недоступни корисницима апликације, Повереник је, на основу расположивих чињеница, утврдио озбиљне пропусте у техничким мерама заштите података који се прикупљају и даље обрађују путем предметне апликације.

Овлашћена лица Повереника су непосредно утврдила да се уносом исправног ЛБО у апликацију, по добијању верификационог кода, путем СМС поруке на произвољни број мобилног телефона, повратно добијају информације о лицу на које се ЛБО односи, и то: име и презиме, статус здравственог осигурања, податке о здравственој установи и изабраном лекару опште праксе, гинекологу, педијатру и стоматологу, датуму и термину обављених лекарских прегледа и шифри лекарских прегледа, као и могућност заказивања нових лекарских прегледа.

Обрада података употребом апликације подразумева ризик да неовлашћено лице употребом туђег ЛБО неовлашћено приступи свим наведеним подацима.

Подацима о ЛБО, поред самих лица, располажу и њихови послодавци и остали корисници Централног регистра обавезног социјалног осигурања. Повереник је у више наврата констатовао масовно прикупљање ЛБО грађана од стране пословних банака, у виду фотокопија или преписа здравствених књижица. Такође, овим подацима располажу и правна лица која се баве добровољним осигурањем.

Овлашћена лица Повереника утврдила су да се валидни ЛБО могу, такође, пронаћи и једноставном интернет претрагом (нпр. у Google претраживачу је довољно унети речи „*здравствена књижица*“, те извршити претрагу слика):

* <https://bit.ly/2Jcoky7>
* <https://bit.ly/2sDrFw3>
* <https://bit.ly/2xH5tWs>
* <https://bit.ly/2JdOvV6> ...

Коначно, валидација исправних ЛБО врши се употребом „Луновог алгоритма“, као стандардизованог средства које користи контролну суму за потврду разних идентификационих бројева, као што су бројеви здравственог осигурања, платних картица, ИМЕИ бројева и сл. „Лунов алгоритам“ је [јавно власништво](https://sr.wikipedia.org/wiki/%D0%88%D0%B0%D0%B2%D0%BD%D0%BE_%D0%B2%D0%BB%D0%B0%D1%81%D0%BD%D0%B8%D1%88%D1%82%D0%B2%D0%BE) и данас је у широкој употреби. Овај алгоритам верификује исправност броја који се проверава помоћу контролне цифре која је укључена у сам број и која се обично надовезује на непотпун број, чиме се добије потпун број.

На интернету су доступни разни алати за декодирање, односно за проверу валидних бројева према Луновом алгоритму, а чијом употребом неовлашћена лица могу доћи до неограниченог броја валидних ЛБО.

Из напред наведених разлога, Повереник је утврдио да обрада података у апликацији „Изабрани доктор“ представља специфичан ризик за право грађана на заштиту података о личности, гарантовано чланом 42. Устава Републике Србије, па је одлучио као у диспозитиву.

ПОУКА О ПРАВНОМ ЛЕКУ:

Против овог решења није допуштена жалба, већ се може покренути управни спор тужбом Управном суду, у року од 30 дана од дана пријема решења (чл. 56. ст. 3. ЗЗПЛ).

У складу са Законом о судским таксама („Сл. гласник РС“, бр. 28/94, 53/95, 16/97, 34/2001 – др. закон, 9/2002, 29/2004, 61/2005, 116/2008 – др. закон, 31/2009, 101/2011, 93/2012, 93/2014 и 106/2015) за тужбу против управног акта којом се покреће управни спор плаћа се 390 динара (Тарифни број 28).

 **ЗАМЕНИЦА ПОВЕРЕНИКА**

 Станојла Мандић ср.