

**Петар Јовановић,<sup>1</sup>**  
Мастер правник,  
Администратор за фармаковигиланцу

UDK: 342.738:[615.065:615.036

615.2.065

DOI: 10.5281/zenodo.12599390

Прегледни научни чланак

Примљен: 16. 10. 2023.

Прихваћен: 29. 01. 2024.

## **ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У ОБЛАСТИ ФАРМАКОВИГИЛАНЦЕ**

**Апстракт:** У овом раду аутор анализира заштиту података о личности у области фармаковигиланце као један од кључних механизма за функционисање ове области. Аутор даје преглед појма, значаја као и историјског утицаја на појаву фармаковигиланце, сам поступак такве заштите, правну регулативу која се примењује у области заштите података о личности у области фармаковигиланце, правних механизма у циљу заштите податка и личности као и утицаја лица за заштиту података о личности – DPO-а. Закључак који аутор изводи из целокупне анализе закона, доктрина, правилника, мишљења и праксе, јесте да су права грађана у вези са личним подацима у области фармаковигиланце једно од најважнијих средстава за очување приватности и заштите личних података. Са развојем технологије, развијају се у и могућности за све већу злоупотребу података. У циљу заштите личних података у области фармаковигиланце примењују се Општа уредба о заштити личних података – GDPR као и Закон о заштити личних података. Да би се лични подаци штитили постоји потреба да се грађанима прошири свест о потреби за заштитом њихових личних података као и начина на који се њихови подаци штите.

**Кључне речи:** Фармаковигиланца, заштита података о личности, Општа уредба о заштити личних података (GDPR), Закон о заштити личних података, Лице за заштиту података о личности.

### **1. Уводна разматрања**

Права грађана у вези са личним подацима представљају једно од најважнијих средстава за очување приватности и заштите личних

<sup>1</sup> peca.jovanovic7@gmail.com

података. У области фармаковигиланце, сигурност података пацијента представља један од кључних механизма функционисања ове области. У свакој фази испитивања лека, приликом пријава нежељених реакција од стране пацијента или за то овлашћеног лица, постоји потреба да се лични подаци пацијента сачувају, односно да се спречи свака злоупотреба таквих података од стране трећих лица. На таласу европске револуције у области заштите личних података и на територији Србије формирана је потреба за системским уређењем заштите података.

Потреба за заштитом личних података постоји кроз целокупан поступак испитивања лека, односно и кроз клиничку, и кроз постмаркетиншку фазу испитивања лека. Као најзначајнији прописи који се примењују у циљу заштите података у области фармаковигиланце јесте Општа уредба о заштити личних података – *GDPR*, као и Закон о заштити личних података. Улога ових прописа је велика, будући да су у њима препозната посебна људска права у вези са личним подацима у савременим околностима. Како подаци о здравственом стању пацијента предствљају посебну категорију личних података, тако су овим прописима установљени механизми правне заштите који обезбеђују пацијентима одређени степен сигурности у односу на њихове личне податке који обрађују друга лица.

Према дефиницији Светске здравствене организације фармаковигиланца је научна дисциплина која обухвата активности везане за откривање, разумевање, процену и превенцију нежељених дејстава лекова, као и других проблема везаних за њихову примену.<sup>2</sup> Информације добијене од пацијената и здравствених провајдера путем споразума о фармаковигиланци (ПВА - *Pharmacovigilance Agreements*), као и других извора као што је медицинска литература, играју кључну улогу у обезбеђивању података потребних за фармаковигиланцу. Наиме, да би се фармацеутски производ пласирао на тржиште или тестирао у већини земаља, подаци о штетним догађајима које добија власник лиценце (обично фармацеутска компанија) морају бити достављени локалном регулаторном телу за лекове (у Србији - *ALIMS* – *Агенција за лекове и медицинска средства Србије*).

Фармаковигиланца се бави идентификовањем опасности повезаних са фармацеутским производима и смањивањем ризика од било какве штетне последице које се могу јавити код пацијената. Фармацеутске

---

<sup>2</sup> Дефиниција фармаковигиланце Светске здравствене организације (WHO), <https://www.who.int/teams/regulation-prequalification/regulation-and-safety/pharmacovigilance>, приступљено 20.12.2022

компаније морају спровести свеобухватну ревизију сигурности лекова како би процениле своју усклађеност са светским законима, прописима и смерницама.

Заштита података о личности пацијената је есенцијална у области фармаковигиланце и потреба за њиховом заштитом је од круцијалне важности. Заштита података се примењује како у клиничком тако и у постмаркетиншком испитивању лека чиме се обезбеђује максимална заштита идентитета пацијената и спречава се злоупотреба од стране трећих лица. Наиме, у свакој фази испитивања лека, приликом пријава нежељених реакција од стране пацијента или за то овлашћеног лица, постоји потреба да се лични подаци пацијента сачувају, односно да се спречи свака могућа манипулација таквих података.

## **2. Правна регулатива у области фармаковигиланце**

Говорећи о заштити података о личности у области фармаковигиланце, као један од најзначајнијих прописа који се примењују у циљу заштите података пацијената, јесте **Општа уредба о заштити података, односно GDPR и Закон о заштити података о личности.**

### ***2.1. Општа уредба о заштити података (GDPR – General Data Protection Regulation)***

Општа уредба о заштити података грађана Европске уније (ЕУ) 2016/679 (GDPR) донета је на нивоу ЕУ 25. маја 2018. године и устављава највише могуће стандарде заштите личних података, као и строг систем санкција. Овај пропис се примењује на све појединце ЕУ и Европског економског савета (ЕЕА).

Примена уредбе је обавезна за све организације које поседују и обрађују личне податке становника ЕУ, а односи се и на личне податке и посебне категорије личних података грађана ЕУ, без обзира где се они налазили. Ова уредба тиче се и држава које су кандидати за чланство у ЕУ, обзиром да имају обавезу усклађивања националног законодавства са правом ЕУ.<sup>3</sup>

У области фармаковигиланце, лични подаци пацијената као и они подаци који спадају под посебном категоријом, могу се обрађивати само у одређене сврхе, што значи да се они не могу користити и обрађивати у другачије сврхе од оних због које су првобитно прикупљени.

<sup>3</sup> GDPR, „Шта је GDPR?“. <https://mobes-quality.rs/services/gdpr-opsta-uredba-o-zastiti-podataka-o-licnosti> приступљено 15.01.2023

Општа уредба ЕУ даје одређење појма личних података. У њој се наводи да су подаци о личности „сви подаци који се односе на физичко лице чији је идентитет одређен или се може одредити; физичко лице чији се идентитет може одредити је лице које се може идентификовати посредно или непосредно, посебно помоћу идентификатора као што су име, идентификациони број, подаци о локацији, мрежни идентификатор или помоћу једног или више фактора својствених за физички, физиолошки, генетски, ментални, економски, културни или друштвени идентитет тог физичког лица“.<sup>4</sup>

*GDPR* се заснива на седам начела која морају бити испуњена када је обрада личних података у питању:

- Законитост, правичности и транспарентност
- Ограничење сврхе обраде
- Минимизација података
- Ограничење обраде
- Тачност података
- Интегритет и сигурност података
- Одговорност руковаоца

Општа уредба ЕУ такође познаје одређене категорије личних података који уживају посебну заштиту.<sup>5</sup> Они се односе на расно и етничко порекло, политичко опредељење, верска и филозофска убеђења, припадност синдикату, обраду генетских и биометријских података, сексуални живот, сексуалну оријентацију лица и здравствено стање лица.<sup>6</sup> Општа уредба даје нешто дужу листу „посебних категорија личних података“ у односу на „нарочито осетљиве податке“ у српском праву. За посебне категорије података сматра се да су „по својој природи посебно осетљиви у погледу основних права и слобода (које штите) и заслужују посебну заштиту, јер би у оквиру њихове обраде могло да дође до

---

<sup>4</sup> Члан 4, став 1, тачка 1, Опште уредбе EUGDPR (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

<sup>5</sup> Lambert 2018:112-115

<sup>6</sup> Чл. 9, Опште уредбе EUGDPR (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

значајних ризика за основна права и слободе“.<sup>7</sup> Државама чланицама је остављена могућност да својим унутрашњим прописима додатно уреде услове који се односе на обраду горе поменутих података.

Обрада посебних категорија података о личности у праву ЕУ је забрањена. Ипак, постоје одређене ситуације које оправдавају обраду оваквих података. Прва група ситуација када је могућа обрада јесте када постоји изричит пристанак њиховог имаоца на обраду, када је неопходно да се изврши обрада ради заштите основних животних интереса лица на које се подаци односе и када је такве податке очигледно објавило лице на које се подаци односе.

Друга група ситуација односе се на циљеве руковоца и обрађивача у области рада, приликом запошљавања, остваривања права из социјалног осигурања и социјалне заштите и приликом обрада које предузимају фондације и удружења. Трећа група ситуација која оправдава обраду посебних категорија личних података тиче се остваривања значајних јавних интереса. То су ситуације када суд обрађује посебне категорије података ради испитивања правних захтева, када је неопходно спровести у медицинске сврхе и сврхе јавног здравља, као и када обрадом треба да се оствари сврха научног, историјског или статистичког истраживања.<sup>8</sup> Руковалац и обрађивач података морају посветити посебну пажњу заштити људских права у вези са оваквим обрадама, при чему морају имати у виду право ЕУ и право држава чланице.

## **2.2. Закон о заштити података о личности**

У правном систему Србије, појам личних података не можемо пронаћи у Уставу, иако овај акт уређује питање заштите података о личности. Одређење личних података остављено је прописима ниже правне снаге, односно посебном закону. Тако је појам личних података одређен у Закону о заштити података о личности (2018).<sup>9</sup>

Закон о заштити података о личности („Службени гласник РС“, број 87/2018), који је на снази у Републици Србији, потпуно је усаглашен са одредбама *GDPR*-а и обавезује све организације које раде са опсежним

---

<sup>7</sup> Тач. 52 Преамбуле, Опште уредбе EUGDPR (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

<sup>8</sup> Андоновић, 2019: 124

<sup>9</sup> Андоновић, et al., 2019: 100

бројем личних података својих клијената да именују **Лице за заштиту података о личности** (*DPO – Data Protection Officer*).

Сваки правни систем и подсистем заснива се на начелима која представљају основне принципе, основне вредности и полазишне тачке у разумевању његових правила.<sup>10</sup> Закон о заштити података о личности познаје општа и посебна начела. Она општа начела која налазе примену у области заштите података јесу начело законистости, правичности и транспарентности. С друге стране, постоје посебна начела. То су начело коришћења најмањег обима података, начело ограничене сврхе обраде, начело тачности обраде, начело интегритета и поверљивости обраде и начело ограниченог броја разлога због којих се чувају подаци. Ова начела су уско повезана са општим начелима, те се кроз њихову примену остварује сврха општих начела и обрнуто.

Поједине врсте личних података не уживају правну заштиту. Међутим, постоје и друге врсте личних података које уживају већи степен заштите у односу на ону која се уобичајено пружа. Јављају се посебне категорије личних података које се не смеју обрађивати. Ове категорије уживају посебну заштиту.<sup>11</sup> Актуелни Закон о заштити података о личности одређује ову врсту података као „посебну категорију“ личних података. У ову групу спадају: Расно и етничко порекло, политичко мишљење, верско и филозофско уверење, чланство у синдикату, генетске податке, биометријске податке, податке о здравственом стању и податке о сексуалном животу и сексуалној оријентацији лица.<sup>12</sup> Ипак, постоје одређене ситуације у којима је дозвољена њихова обрада. То су случајеви када постоји јавни интерес, ако постоји изричит пристанак лица за обраду таквих података, обрада од стране удружења и организација када се обрађују подаци њихових чланова, када је то потребно ради вођења судског поступка, ради заштите јавног здравља.

Како у фазама испитивања лека учествују пацијенти са различитим врстама обољења, и како ти пацијенти добровољно дају пристанак на употребу а самим тим и на испитивању лека против болести, свакако се може закључити да су дали и изричит пристанак на обраду „посебних категорија“ података, нарочито када је у питању њихово здравствено стање. Без увида у здравствено стање не би било могуће спровести истраживање лека. Заштита оваквих података је обавезна у свакој фази

<sup>10</sup> Андоновић, et. al., 2019: 146

<sup>11</sup> Андоновић, et. al., 2019: 120

<sup>12</sup> Чл. 17, ст. 1, Закона о заштити података о личности („Службени гласник РС“, бр. 97/2008, 104/2009, 68/2012 – одлука Уставног суда РС и 107/2012)

испитивања лека, па тако и приликом пријава нежељених реакција које лек производи.

### **2.3. Сличности и разлике између Опште уредбе о заштити података и Закона о заштити података о личности као и додатни механизми заштите**

Текст домаћег закона је у највећем делу адаптиран превод Опште уредбе о заштити личних података. Међутим, постоји доста недостатака домаћег закона, а тичу се нејасних одредби и нејасних механизма примене закона.

За примену *GDPR*-а довољно је да се обрађују подаци о личности лица која се, у моменту нуђења робе или услуга, налазе у територији једне од држава чланица ЕУ без обзира да ли су ова лица ту робу или услуге платила. Значи, већ сама обрада података у циљу нуђења робе или услуга, без крајње куповине ове робе, односно плаћања ових услуга, је довољна за примену ригорозних санкција прописаних *GDPR*-ом.

Наведени приступ прихватио је и српски законодавац. Закон о заштити података о личности се примењује на обраду података о личности коју врши руковалац, односно обрађивач који има седиште, односно пребивалиште или боравиште на територији Републике Србије, у оквиру активности које се врше на територији Републике Србије, без обзира да ли се радња обраде врши на територији Републике Србије. Тако се Закон о заштити података о личности примењује на обраду података о личности оних лица на која имају пребивалиште, или боравиште на територији Републике Србије и то од стране руковоаца, односно обрађивача који нема седиште, пребивалиште или боравиште на територији Републике Србије, ако су радње обраде везане за: понуду робе, односно услуге лицу на које се подаци односе на територији Републике Србије и праћење активности лица на које се подаци односе, ако се активности врше на територији Републике Србије.

Као једна од најважнијих разлика јесте висина казни, која према *GDPR*-у могу износити и до 20 милиона евра или 4% укупног оствареног годишњег прихода компаније, док према Закону о заштити података о личности максималне казне износе до 2 милиона динара за кршење неког начела.

Многе компаније су ускладиле своје пословање са *GDPR*-ом, односно Законом о заштити података о личности, односно израдили су или ревидирали постојеће акте. Поред тога, многе компаније су увеле



додатне механизме заштите, као што су енкрипција, заштита података на *Cloud*-у, едуковање запослених на свим нивоима и улагање у *Cyber*-сигурност. Енкрипција или криптографија представља аутоматско стављање садржаја компаније под шифру. Ради се о свим подацима унутар система компаније који се обрађују на било који начин. Без обзира о каквој врсти података је реч, потребно је онемогућити трећим лицима приступ таквим подацима. Криптографија представља вештину која проучава процесе чувања информација тако да они буду познати и читљиви само оним лицима којима су намењени. Појам криптографија потиче од грчких речи криптос (*κρυπτός*) – тајна и графеин (*γράφειν*), што значи писати.<sup>13</sup> *Cloud* је постао интегрално место дигитализацијских процеса. Како све више компанија пребацује податке на *Cloud*, јавља се све већи проблем дигиталне сигурности. Најбоља стратегија коју компаније могу преузети су шифровање осетљивих података пре преноса у *cloud*. Људски фактор често представља кључну рањивост у ланцу заштите податка. Било да је реч о незнању или немару, запослени могу свесно или несвесно нанети штету компанији и подацима које обрађују. Када је реч о најосетљивијим подацима, запосленима се дају директне и јасне смернице за поступање у ситуацијама у којима је могуће да дође до штете по сигурност податка. Ефикасан начин да се спречи губитак података може бити *software*, али битно је и едуковати запослене о поступцима заштите и мерама сигурности. *Cyber* сигурност је специфичан тип информацијске сигурности који се односи на начине на које организације штите дигиталне информације. Као претње по *Cyber* сигурност јесу вируси, *worms*, *phishing*, *rootkit*... Један од најпознатијих случајева крађе личних података пацијената јесте случај „*Community Health Systems*“.

#### **2.4. Добра пракса фармаковигиланце - *Good Pharmacovigilance Practices (GVP)***

Један од најзначајнијих докумената у области фармаковигиланце јесте Добра пракса фармаковигиланце – *Good Pharmacovigilance Practices (GVP)*, (у даљем тексту ГВП), издата од стране Европске агенције за лекове (ЕМА). Овај документ представља сет мера сачињених да би се олакшало обављање надзора безбедности лекова у Европској унији. Донет је 2012. године и заменила је дотадашње мере из књиге 9А правила која регулишу лекове у ЕУ - *Volume 9A of the Rules Governing Medicinal Products in the EU*. ГВП се примењује на носиоце одобрења за стављање лека у промет, Европску Агенцију за лекове и регулаторна тела за лекове у

<sup>13</sup> Куљански 2010: 65



државама чланицама ЕУ. Овај документ се односи на све лекове који су одобрени од стране Агенције, као и лекове који су одобрени на националним нивоима.

Смерница о Доброј пракси фармаковигиланце је подељена у две категорије: Модули који покривају главни процес фармаковигиланце и посебна разматрања производа или популације.<sup>14</sup> Свако поглавље развијао је тим који се састоји од стручњака из Европске агенције за лекове и из земаља чланица ЕУ. Постоји 12 модула означених од I до XVI, који покривају главне процесе фармаковигиланце (модули XI, XII, XIII и XIV су ништави јер је су обрађени у другим документима од стране ЕМА). Сваки од модула има своју улогу у циљу заштите пацијента.

Правни оквир за фармаковигиланцу и медицинске производе за људску употребу у ЕУ дати су у Уредби (ЕС) бр. 726/2004 и Директиви 2001/83/ЕС који се односи на медицинске производе за људску употребу.

### **2.5. Уредба (ЕС) 726/2004 - Regulation (EC) No. 726/2004**

Уредба (ЕС) 726/2004 - *Regulation (EC) No. 726/2004* односи се на утврђивање поступака одобравања примене и поступка надзора над применом лекова које се користе у људској и ветеринарској медицини у Европској Унији. Ова Уредба примењује се и на клиничка испитивања у погледу таквих медицинских производа који се производе у Унији. Донета је 31. марта 2004. године од стране Европског парламента.

Уредбом се жели постићи висок стандард квалитета и безбедности лекова у ЕУ и укључује мере за подстицање иновација и конкурентности.<sup>15</sup> Да би се лек ставио у промет, он мора бити у складу са Уредбом.

### **2.6. Директива 2001/83/ЕС - Directive 2001/83/EC**

Директива 2001/83/ЕС - *Directive 2001/83/EC* односи се на прописе Заједнице о лековима за људску употребу. Донета је 2001. године од стране Европског парламента. Основни циљ свих правила која регулишу производњу, дистрибуцију и употребу медицинских производа мора бити заштита јавног здравља. Сви лекови који се нуде на продају у ЕУ морају имати претходно одобрење било националног органа или

---

<sup>14</sup> Смернице добре праксе фармаковигиланце, <https://www.ema.europa.eu/en/human-regulatory/post-authorisation/pharmacovigilance/good-pharmacovigilance-practices> приступљено 08.05.2023.,

<sup>15</sup> Резиме Уредбе 726/2004, <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32004R0726> приступљено 08.05.2023.

*ЕМА*. Да би добили дозволу, произвођачи морају да обезбеде низ детаљних терапијских информација о производу, укључујући све могуће нежељене ефекте.

Глава IX члан 101. Директиве посвећена је области фармаковигиланце. Према Директиви, државе чланице ће предузети све неопходне мере да подстакну лекаре и друге здравствене раднике да пријаве сумњиве нежељене ефекте лекова надлежним органима. Државе чланице могу наметнути посебне услове лекарима и другим здравственим радницима у вези са пријављивањем сумњивих озбиљних или неочекиваних нежељених ефеката, посебно када је такво пријављивање услов за стављање у промет лека.<sup>16</sup> У циљу обезбеђивања доношења одговарајућих одлука о лековима одобреним у Заједници, узимајући у обзир добијене информације о нежељеним ефектима лекова у уобичајеним условима медицинске употребе, државе чланице треба да успоставе систем фармаковигиланце. Овај систем се користи за прикупљање корисних информација за праћење лекова, са посебним освртом на нежељене ефекте код људи, и за научну процену таквих информација.

### ***2.7. Међународно веће за усклађивање техничких услова за лекове за људску употребу - International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH)***

Међународно веће за усклађивање техничких услова за лекове за људску употребу (ICH) јединствен је по томе што окупља регулаторна тела и фармацеутску индустрију како би разговарали о научним и техничким аспектима регистрације лекова. Од свог оснивања 1990. године, ICH се постепено развија како би одговорио на све већи глобални развој лекова. Мисија ICH-а је постизање веће усклађености широм света како би се осигурало да се безбедни, ефикасни и висококвалитетни лекови развијају и региструју на најефикаснији начин. Од најаве организационих промена у октобру 2015. године, ICH је порастао као организација и тренутно укључује 16 чланова и 32 посматрача.

### **3. Поступак заштите података о личности у области фармаковигиланце**

Лични подаци означавају сваку информацију која се односи на одређено или одредиво лице. Треба имати у виду да постоји разлика између

<sup>16</sup> Глава IX, члан 101, став 2 Директиве 2001/83/EC (Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use)

општих личних података и личних података које обухватају посебне категорије. Посебна категорија личних података су здравствени подаци пацијената, који се сматрају осетљивим, и код којих се примењује начело ограничене сврхе обраде података. Начело ограничене сврхе обраде података подразумева да се подаци могу обрађивати само у односу на одређене, изричите или оправдане сврхе. Прикупљање података без одређене сврхе је протиправно.

У личне податке пацијената спадају: име, презиме пацијента, адреса становања, *e-mail* адреса, број телефона, подаци о здравственом стању итд. Наведени подаци биће предмет разних активности обраде као што су прикупљање, евидентирање, складиштење, преношење итд. Заштита података о личности пацијената у области фармаковигиланце праћена је најпре пријављивањем сумње на нежељене реакције које лек производи. Правилником је тачно одређено који подаци о личности требају да буду садржани у самој пријави. О свим сумњама на нежељене реакције лека, пацијенти треба да обавесте здравственог радника који им пружа услугу (нпр. лекар, стоматолог, фармацеут). Пацијенти о свим сумњама на нежељене реакције лека који се налазе у промету у Републици Србији могу писмено да обавесте регионални центар за фармаковигиланцу или Агенцију за лекове и медицинска средства Србије (АЛИМС) или носиоца дозволе за лек. У случајевима када је пацијент радно неспособан, лице са душевном сметњом или малолетно лице, нежељену реакцију може пријавити родитељ, законски заступник, односно старатељ пацијента.

Пријава пацијента треба да садржи податке о: 1) Лицу које пријављује (углавном иницијале); 2) Пацијенту којег је могуће идентификовати (иницијали, година рођења и пол); 3) Називу лека за који се сумња да је узроковао нежељену реакцију; 4) Нежељеној реакцији на лек.<sup>17</sup> Такви подаци се сматрају посебно осетљивим и потреба за њиховом заштитом је предвиђена Законом о заштити података о личности чија обрада није дозвољена осим под одређеним условима.<sup>18</sup> У случају нежељене реакције лека, пацијент подноси пријаву попуњавањем *CIOMS-I* обрасца. На овом обрасцу пацијент од личних података попуњава своје иницијале, пол, датум рођења, односно године и земљу рођења. Ови подаци смеју да буду познати искључиво лекару, Агенцији за лекове и медицинска

---

<sup>17</sup> Члан 11 Правилника о начину пријављивања, прикупљања и праћења нежељених реакција на лекове: 64/2011-30, 75/2017-20, 82/2017-84

<sup>18</sup> За више о условима допуштености обраде посебних категорија података о личности („Службени гласник РС“, бр. 97/2008, 104/2009, 68/2012 – одлука Уставног суда РС и 107/2012)

средства Србије, носиоцу дозволе за лек као и компанијама које се баве пословима фармаковигиланце. Они су у обавези поступати у складу са *GDPR*-ом, односно Законом о заштити података о личности, као и другим прописима и правилницима везаних за заштиту личних података.

Поред пацијента који пријављује нежељену реакцију лека, постоји и одговорно лице за фармаковигиланцу које је одговорно за успостављање, одржавање и управљање системом фармаковигиланце. У складу са законом, ово лице прати безбедоносни профил и сва безбедоносна питања у вези са свим лековима за које носилац дозволе за лек има дозволу у Републици Србији. Такође је и контакт особа за Агенцију, као и за инспекцију у области фармаковигиланце.<sup>19</sup>*CIOMS* - Јобразац је стандардизовани међународни образац за пријаву *ICSR* издат 1990. године од стране *CIOMS I* радне групе Већа интернационалних организација за медицинске науке (*The Council for International Organizations of Medical Sciences - CIOMS*). У наведеном обрасцу, као и у случају када пријаву доставља пацијент, попуњавају се исти подаци болесника.

У ранијим фазама испитивања лека, у оквиру клиничког испитивања, спонзор је одговоран за благовремено обавештавање Агенције за лекове и медицинска средства Србије у случају озбиљне и неочекиване реакције у току спровођења клиничког испитивања лека.<sup>20</sup> Спонзор клиничког испитивања је појединац или правно лице које преузима одговорност за започињање, спровођење, односно финансирање клиничког испитивања.<sup>21</sup> Здравствени радник који учествује у клиничком испитивању у својству истраживача, обавезан је да све озбиљне нежељене догађаје одмах пријави спонзору, осим оних за које се то не захтева протоколом испитивања или брошуром за истраживаче.<sup>22</sup> Извештавање Агенције о озбиљним, неочекиваним нежељеним реакцијама на лек, спонзор обавља достављањем стандардизованог међународног обрасца за пријаву, на *CIOMS – I* обрасцу.

---

<sup>19</sup> Члан 16, став 1, тачка 1,2,3,4 Правилника о начину пријављивања, прикупљања и праћења нежељених реакција на лекове: 64/2011-30, 75/2017-20, 82/2017-84

<sup>20</sup> Члан 43, став 1, Правилника о начину пријављивања, прикупљања и праћења нежељених реакција на лекове: 64/2011-30, 75/2017-20, 82/2017-84

<sup>21</sup> Члан 2, став 1, тачка 20 Закона о лековима и медицинским средствима. („Службени гласник РС“ бр. 30/2010, 107/2012, 113/2017 – др. закон и 105/2017 – др. закон)

<sup>22</sup> Члан 43, став 2, Правилника о начину пријављивања, прикупљања и праћења нежељених реакција на лекове: 64/2011-30, 75/2017-20, 82/2017-84

За ефикасну анализу безбедносних података потребни су старост/старосна група пацијента, пол, тежина, висина, етничка припадност, медицинска историја и здравствени статус. Иницијали пацијента (не рачунајућ клиничка испитивања), број медицинског картона и клиничке студије и/или датум/година рођења (пун датум рођења не важи за клиничка испитивања) такође су важни за идентификацију. С друге стране репортер (лекар, стоматолог, фармацеут...), од личних података је у обавези доставити своје име, медицинску квалификацију, адресу и контакт податке (е-mail адреса, број телефона) како би се осигурало прикупљање потпуних и тачних података пацијента. Поред тога, ти подаци су неопходни за континуитет пословања и одрживост и не постоји очекивање приватности репортера приликом обраде овог опсега личних података. Сви остали подаци репортера су неважни за обраду. У клиничким испитивањима, подаци пацијента (иницијали, пун датум рођења) у свим документима морају бити обрисани (осим године рођења).

Носиоци дозволе за лек обрађују податке о личности, тако да те информације могу омогућити идентификацију пацијента директно или индиректно. Ти подаци представљају личне податке који су заштићени законима о заштити личних података.

Како би такви подаци могли бити предмет обраде, мора постојати изричита сагласност пацијента. Постоје различите ситуације када је потребно добити пристанак пацијента:

- Када је потребно истражити нежељени догађај;
- Како би носилац дозволе за лек могао да добије додатне информације пацијента о нежељеном догађају;
- Ради упоређивања информације о нежељеном догађају са другим информацијама о нежељеним догађајима како би се анализирао безбедност лека;
- Како би носилац дозволе за лек могао пружити информацију у случајевима упита од стране пацијента, који је корисник њиховог лека, о неком медицинском питању;
- Како би се обезбедио извештај националним и/или регионалним надлежним регулаторним телима, како би се анализирао безбедност лека (*EMA, MHRA* итд.).

Када је у питању трансфер личних података пацијента у оквиру државе, носилац дозволе за лек и прималац таквих података, морају водити

рачуна о примени свих законских прописа везаних за заштиту података у оквиру земље у којој се врши трансфер. Са друге стране, постоје случајеви када су такви подаци предмет трансфера у друге земље. Овде можемо говорити о два случаја: када се такви подаци шаљу између земаља које су потписнице *GDPR*-а и када се подаци шаљу у земље који су означене као „небезбедне“, односно не подлежу прописима *GDPR*-а. Примена Опште уредбе, када се трансфер врши између земаља Европске Уније, је обавезна за све организације које поседују и обрађују личне податке становника ЕУ, а односи се и на личне податке и посебне категорије личних података грађана ЕУ, без обзира где се оне налазиле.

У случају трансфера података у земље које не подлежу прописима *GDPR*-а, они могу бити заштићени на различите начине. Као најчешћи пример јесте закључивање уговора носиоца дозволе за лек са примаоцем таквих података о заштити личних података, којим се обезбеђује безбедност да такви подаци не буду предмет злоупотребе. Трансфер је могућ само у случајевима када постоје адекватни нивои заштите личних података код земаља које нису део *GDPR*-а. Пренос податка може бити заснован на различитим правним основама нпр. када је то потребно ради заштите јавног интереса (члан 49, став 1, Опште уредбе о заштити података).

Као најзначајнија техничка мера заштите личних података пацијента, јесте обрада података у псеудонимизованом облику. Псеудонимизација представља техничку меру обраде података чијом применом се лични подаци више не могу приписати одређеном лицу без употребе додатних информација, уз услов да се додатне информације чувају одвојено и да се на њих примењују мере које спречавају да се податак може приписати одређеном или одредивом лицу.<sup>23</sup> У клиничком испитивању стандардна је пракса да се псеудонимизирају прикупљени подаци у обрасцима за пријаву случаја. На пример, уколико је потребно пријавити нежељену реакцију неког лека, у наведеном обрасцу стајаће идентификациони број субјекта (пацијента) клиничког испитивања (нпр. *SRB006-301*), чиме се смањује могућност сазнања псеудонимизираних података. Међутим, организације треба да имају у виду да се псеудонимизовани подаци и даље морају третирати пажљиво и да се са применом псеудонимизације не завршава брига о праву корисника на приватност. Чак и у случају да дође до цурења псеудонимизованих података изван организације, оне су у обавези да о томе обавесте особе, на које се подаци односе.

<sup>23</sup> Члан 4, став 1, тачка б, Закона о заштити података о личности („Службени гласник РС“, бр. 97/2008, 104/2009, 68/2012 – одлука Уставног суда РС и 107/2012)

#### **4. Механизми правне заштите личних података у Републици Србији**

У праву Србије можемо одредити три врсте правних механизма заштите личних података. То су механизам заштите који се остварује пред независним контролним телом, механизам судске заштите и механизам овлашћеног лица за заштиту података о личности.

У правном систему Републике Србије постоји инокосно независно тело које контролише стање и штити права грађана у области личних података. Ову улогу обавља Повереник за информације у области личних података. Чисто правни послови Повереника односе се на решавање о притужбама грађана на рад организација у вези са прикуљањем и обрадом личних података. Уколико постоји повреда личних података у области фармаковигиланце, свако физичко лице чији су подаци повређени, може поднети притужбу Поверенику против одговорног лица, односно организације. Повереник може вршити инспекцијски надзор који се разлику у зависности од предмета контроле, па се контрола може вршити прегледом докумената, просторија, непосредним опажањем предмета, испитивањем лица или на друге адекватне начине.

Устав гарантује заштиту података о личности. У случају повреде или злоупотребе личних права, грађанима је уставом загарантовано право на судску заштиту личних података, која се ближе уређује законом. Физичко лице на које се подаци односе има право на судску заштиту ако сматра да је неко од његових посебних права повређено обрадом података или неком другом радњом. Тужба се може поднети вишем суду у месту пребивалишта, боравишта или седишта руковооца или обрађивача података или пребивалишта, односно боравишта лица на које се подаци односе. Свако ко је претрпео неки облик материјалне (нпр. спречавање увећања имовине због објављеног личног податка) или нематеријале (повреда части, угледа, наношење психичког бола и сл.) штете има право да пред судом тражи накнаду од руковооца или обрађивача.

Једна од најзначајнијих новина које доноси нови Закон о заштити података о личности јесте увођење посебног механизма заштите у облику овлашћеног лица задуженог за заштиту података. Ангажовање лица задуженог за заштиту личних података, односно *DPO*-а, обавезно је у ситуацијама уколико се основна делатност руковооца или обрађивача састоји из радњи обраде података која подразумева редовно и масовно праћење лица на која се ти подаци односе или уколико се



њихова основна делатност састоји из масовне обраде посебних категорија података попут података о здравственом стању лица.

## 5. Лице за заштиту података о личности – Data Protection Officer

Лице за заштиту података о личности (у даљем тексту: лице) је лице које је овлашћено и именовано од стране послодавца, ради руковођења подацима о личности. Закон о заштити података о личности, ослањајући се на *GDPR*, чланом 56 предвиђа могућност да послодавац одреди лице за заштиту података о личности.

Међутим, обавеза да одредите лице за заштиту података о личности постоји у случају да:

- сте орган власти
- је основна активност ваше компаније обрада података о личности
- основна активност представља обраду посебно осетљивих података о личности, који су прописани законом (нпр. подаци о здравственом стању, политичком опредељењу, подаци о казним евиденцијама итд), уз додатни услов, да се обрада наведена у овој тачки врши у великом обиму. Шта представља велики обим, закон није детаљно регулисао, али се може закључити да би нпр. компаније које имају преко 250 запослених требало да одределице за заштиту података.

Лице за заштиту података о личности може бити било лице које је запослено код послодавца (компаније, предузећа, институције и сл.), или било које лице ван компаније на основу посебног Уговора. Након што се такво лице одреди, неопходно је објавити контакт податке лица, најбоље већ у политици приватности послодавца, и доставити их Пове-ренику који води евиденцију лица. Неодређивање лица за заштиту личних података од стране оних правних лица који су на то обавезани законом, представља прекршај за које се може изрећи казна од 5.000,00 до 2.000.000,00 динара.<sup>24</sup> Чак и када то није обавеза послодавца, свакако постоји препорука да се именује такво лице, нарочито ако поседује стручна знања и искуства у области заштите података. Да би лице могло бити одређено за овлашћено лице за заштиту података, оно мора

---

<sup>24</sup> Денис Тул “Лице за заштиту података о личности – Data protection officer”, <https://lawit.rs/2019/11/17/lice-za-zastitu-podataka-o-licnosti-data-protection-officer-dpo-2/> приступљено 25.01.2023

поседовати стручна знања и професионалне способности који се односе на област заштите података.<sup>25</sup>

Лице које поседује стручна знања, превасходно надзире усклађеност пословања са Законом о заштити података о личности и дужно је старати се о томе да компанија обрађује податке у складу са Законом. Улога Лица је информативног и саветодавног карактера и не постоји могућност да обавезе на неко чињење, већ да укаже на евентуалне пропусте, мере побољашња пословања у усклађивања са законом. Лице је контакт особа за односе са Повереником, саветује се са њим у вези са питањима која се односе на обраду, укључујући и обавештавање и прибављање мишљења у вези са извршеним проценама утицаја на заштиту података о личности намераваних радњи обраде. Такође, може континуирано сарађивати и са лицима задуженим за имплементацију техничко-безбедносних мера ради заштите података, као и ради имплементације самоих законских решења на самим веб сајтовима исл.

Послодавац је дужан да осигура да лице за заштиту података о личности може да квалитетно обавља свој посао. Пре свега је дужан да обезбеди адекватна софтверска решења која омогућују ефикасно праћење начина обраде података и разумевање тих процеса. Повереник за информације од јавног значаја и заштиту података о личности је у обавези водити евиденцију лица за заштиту података о личности. Евиденција садржи податке о руковооцу, односно обрађивачу (име, презиме и адресу, односно назив и седиште) и податке о лицу за заштиту података о личности (име, презиме, адресу, имејл и број телефона).<sup>26</sup>

## 6. Закључак

Права грађана у вези са личним подацима представљају једно од најважнијих средстава за очување приватности и заштите личних података. У области фармаковигиланце, сигурност података пацијента представља један од кључних механизма функционисања ове области. Наиме, у свакој фази испитивања лека, приликом пријава нежељених реакција од стране пацијента или за то овлашћеног лица, постоји потреба да се лични подаци пацијента сачувају, односно да се спречи свака злоупотреба таквих података од стране трећих лица. На таласу европске револуције у области заштите личних података и на територији Србије формирана је потреба за системским уређењем заштите података.

<sup>25</sup> Мразница, 2017: 172

<sup>26</sup> Члан 2, став 2, Правилника о обрасцу и начину вођења евиденције лица за заштиту података о личности ("Службени гласник РС", број 40/2019)

Као најзначајнији пропис који се примењује у области фармаковигиланце јесте Општа уредба о заштити личних података – *GDPR*, као и Закон о заштити личних података из 2018. године. Улога ових прописа је велика, будући да су у њима препозната посебна људска права у вези са личним подацима у савременим околностима. Како подаци о здравственом стању пацијента предствљају посебну категорију личних података, тако су овим прописима установљени механизми правне заштите који обезбеђују пацијентима одређени степен сигурности у односу на њихове личне податке који обрађују друга лица. Поред несумњивог напретка у области заштите података о личности у односу на период пре доношења Закона о заштити података о личности 2018. године, дошли смо до закључка да систем заштите података ипак садржи одређене недостатке које је неопходно исправити, како би се остварила сврха заштите личних података. Дигитализација у пословању, комуникација електронским путем представљају нове начине „трговине“ информацијама, те је такве информације, нарочито личне податке физичких лица, потребно заштитити.

Лице за заштиту података о личности је позиција настала на основу ступања на снагу *GDPR*-а. Оно је задужено за надзор имплементације стратегије заштите података код послодавца како би се осигурало усклађивање са *GDPR*-ом и другим примењивим законима о заштити података. Ангажовање лица за заштиту података о личности је према Општој уредби обавезно у случајевима уколико се основна делатност руковоаца или обрађивача састоји из радњи обраде података која подразумева редовно и масовно праћење лица на која се ти подаци односе или уколико се њихова основна делатност састоји из масовне обраде посебних категорија података као што су, између осталих, и подаци о здравственом стању лица. Самим тим улога лица за заштиту података о личности је веома важна у циљу заштите личних података, нарочито када су предмет обраде подаци који се односе на здравствено стање пацијента.

## Литература

Андоновић, С. Н. (2019) „Заштита података у електронској јавној управи у Републици Србији – Правни аспекти, Докторска дисертација, Правни факултет, Београд; стр. 100-146,

Lambert, P. (2018) „*Understanding the New European Data Protection Rules*“, Auerbach Publications, New York;

Куљански, С. (2010). Алгоритам и његова практична примена, *Војно-технички гласник* бр. 3/10, Министарство одбране Републике Србије, Београд;

Мразница, Е. (2017), *GDPR – Нови изазов заштите података о личности*, Удружење банака Србије, Београд;

### *Прописи*

General Data Protection Regulation/ Општа уредба ЕУ – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation/GDPR)

Директива 2001/83/EC/Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use

Закон о заштити података о личности, *Службени гласник РС*, бр. 97/2008, 104/2009, 68/2012–одлука Уставног суда РС и 107/2012

Закон о лековима и медицинским средствима Републике Србије, *Службени гласник РС*, бр. 30/2010, 107/2012, 113/2017– др. закон и 105/2017– др. закон)

Правилник о начину пријављивања, прикупљања и праћења нежељених реакција на лекове: *Службени гласник РС*, бр. 64/2011-30, 75/2017-20, 82/2017-84.

Правилник о обрасцу и начину вођења евиденције лица за заштиту података о личности, *Службени гласник РС*, бр. 40/2019.

### *Интернет извори*

Светска здравствене организација/World Health Organization (2022). *What is Pharmacovigilance?*, <https://www.who.int/teams/regulation-prequalification/regulation-and-safety/pharmacovigilance>, приступљено 20.12.2022

ЕМА/European Medicines Agency (2023). Good pharmacovigilance practices (Смернице добре праксе фармаковигиланце) <https://www.ema.europa.eu/en/human-regulatory/post-authorisation/pharmacovigilance/good-pharmacovigilance-practices>, приступљено 08.05.2023

EUR-LEX (2011). *Safe medicines for Europeans* — European Medicines Agency (Резиме Уредбе 726/2004), Summary of Regulations EC

No726/2004- procedures for the authorisation and supervision of medicinal products for human and veterinarz use , and establishing a European Medicines Agency, <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32004R0726>, приступљено 08.05.2023

Mobes-Quality (2023). *Šta je GDPR?*, <https://mobes-quality.rs/services/gdpr-opsta-uredba-o-zastiti-podataka-o-licnosti/> , приступљено 15.01.2023.

LawIT/Denis Tul (2019). *Lice za zaštitu podataka o ličnosti (Data Protection Officer/DPO)*, <https://lawit.rs/2019/11/17/lice-za-zastitu-podataka-o-licnosti-data-protection-officer-dpo-2/>, приступљено 25.01.2023

***Petar Jovanovic, LL.M.,***

*Data protection administrator for pharmacovigilance*

## ***PERSONAL DATA PROTECTION IN THE FIELD OF PHARMACOVIGILANCE***

### ***Summary***

In this paper, the author analyzes the protection of personal data in the field of pharmacovigilance as one of the key mechanisms for the functioning of this area. The author provides an overview of the concept of pharmacovigilance, the procedure of such protection, the legal regulations applicable in the field of personal data protection in the field of pharmacovigilance, legal mechanisms aimed at protecting data and personal data, as well as the role of Data Protection Officers as person in charge of personal data protection.

The need for personal data protection is increasingly prominent in the modern world. The EU General Data Protection Regulation (GDPR), as well as the Serbian Personal Data Protection Act (2018) are the most important documents for the protection of personal data in the field of pharmacovigilance. The Medicinal Products and Medical Devices Agency of the Republic of Serbia, licenseholders, doctors, and companies involved in pharmacovigilance activities are obliged to act in accordance with the aforesaid regulations and to prevent any possible misuse of personal data. In case of personal data breach, a natural person whose rights have been violated is entitled to initiate legal mechanisms for data protection.

Based on the overall analysis of laws, doctrines, regulations, opinions and practices, the author concludes that citizens' rights in relation to personal data in the field of pharmacovigilance are one of the most important means of preserving privacy and protecting personal data. The development of technology increased the opportunities for data misuse and abuse. The applicable law for the protection of personal data in the field of pharmacovigilance are the General Data Protection Regulation (GDPR) and the Serbian Personal Data Protection Act. In order to protect personal data, there is a need to raise citizens' awareness of the need to protect their personal data and how their data are protected.

***Keywords:*** Pharmacovigilance, personal data protection, General Data Protection Regulation (GDPR), Personal Data Protection Act, Data Protection Officer (DPO).