ОБРАБОТВАНЕТО НА ЗДРАВНИ ДАННИ СЪГЛАСНО ОБЩИЯ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ (ЕС) 2016/679

И. Иванова

1. Въведение

Темата за защитата на здравните данни е изключително важна, доколкото потенциална загуба или по друг начин нарушение на сигурността на тази информация може сериозно да увреди интересите на пациента и неговите права и свободи, като дори застраши здравето или живота му. Тази изключителна важност е и причина защитата на здравните данни да върви ръка за ръка с редица специални задължения за лечебните заведения и практикуващите лекари, включително задължението за спазване на лекарска тайна, което произхожда още от времето на Хипократ (4 век п.н.е.) и е скрепено и днес в Кодекса за професионалната етика на лекарите (чл. 51-53 от [1]).

Въпреки, че изискването за защита на здравната информация е уредено на хартия в Закона за здравето, (чл. 28, ал. 3 от [2]) за съжаление в българските условия то досега често не се спазва в практиката без особени последствия за допуснатите нарушения. Чувствителни здравни данни се събират редовно в присъствието на други лица и се обсъждат нерядко без наложителна необходимост между медицинския персонал. Грешки в медицинската документация стават причина за грешна диагноза, а оттам и грешно лечение. Информациите от медицинските документи е като цяло недостатъчно добре защитена от нерегламентиран достъп както на хартия, така и в информационните системи и онлайн бази-дани, които с новите технологии поставят много по-големи заплахи пред информационната сигурност. Предизвикателство за пациентите понякога представлява и получаването на достъп до медицинската им документация.

Дали обаче това положение може да се промени и то по причини, независещи толкова от българското законодателство и стандарти в медицинското обслужване, колкото поради наложена от Европа необходимост за по-добра защита на личните данни, включително и здравните такива?

Смятано от 25 май т. г. Общият регламент за защита на личните данни (ЕС) 2016/679 [3], наричан от мнозина с английското му съкращение „GDPR“ или на български „ОРЗД“ вече е приложимо право в България, както и в целия Европейски съюз. Едва ли досега е имало друга такава европейска регулация, която да засегне в такъв мащаб всички сфери на обществения, социалния и икономическия живот, доколкото Регламентът се прилага спрямо всички публично и частно-правни субекти, обработващи лични данни, в това число лечебните и здравните заведения, Министерството на здравеопазването, регионалните здравни инспекции, общопрактикуващите лекари, лекарите по дентална медицина, фармацевтите, лабораториите и всякакви други юридически и физически лица, обработващи лични данни за професионални цели. Новите засилени мерки за защита на данните ще имат пряко отношение към отговорността и задълженията на всички тези лица, като неспазването им може да доведе до сериозни санкции в размер до 20 млн. евро или 4% от годишния оборот на лечебното заведение или практикуващия лекар.

Поради тези страховити глоби прилагането на Регламента от 25 май т.г. предизвика бурни реакции и всеобща паника, а наред с това и някои неразбирания и грешни интерпретации относно приложението му на практика при обработването на личните данни. Хаосът засегна всички сфери на обществения живот, включително и здравеопазването. Граждани бяха засипвани от и-мейли с искания за подновяване

на съгласията си. Аптеки изискваха всеки, който си купува лекарства, заплатени напълно или частично от здравната каса, да попълва декларации-съгласие за всяко закупено лекарство [4]. Болници изискваха съгласие от пациентите си при регистрация, някои лични лекари изтриваха или отказваха да съхраняват медицинска документация на пациентите си от страх да не им бъде наложена глоба. Както председателят на Сдружението на общопрактикуващите лекари доц. Любомир Киров обобщава: „На председателя на Комисията за защита на личните данни може да са му ясни нещата, но на всички останали не са.“ [5]

Днес повече от два месеца след влизането в сила на Регламента, можем да кажем, че паниката по привидното съответствие с неговите изисквания изчезна, но със сигурност неразбирането остава. Много лечебни заведения и общопрактикуващи лекари едва ли могат изцяло да докажат спазване на всички изисквания за защита на личните данни в дейността си, а видно от описаното по-горе вероятно има и такива, които макар да са заплатили скъпите консултантски услуги, са получили недостатъчно пълен или компетентен съвет по темата.

Именно с цел да допринесе за по-пълното изясняване на задълженията по новия Регламент и да подпомогне лечебните заведения и практикуващите лекари, тази статия ще анализира изискванията на новия режим за защита на личните данни и ще ги съотнесе към действащото национално законодателство в сферата на здравеопазването, което регулира защитата на здравните данни. Ще бъдат разгледани конкретно задълженията на лечебните заведения и общопрактикуващите лекари и основанията, които се прилагат към обработката на здравни и други лични данни, както и изключенията от нововъведените правила, които са специфични за сферата на здравеопазване.

2. Взаимодействие между Регламента и българското законодателство за защита на здравните данни

Както бе споменато в началото, защитата на здравните данни в България и досега имаше стабилна законова основа, макар да не се спазваше винаги на практика. До влизане в сила на Регламента, тази материя се уреждаше в Закона за защита на личните данни и Закона за здравето, които регламентират разкриването на здравни данни, достъпа до тях от пациенти и изискванията за защитата им. Законът за здравето се явява *lex specialis* или специален закон, който има предимство пред общия Закон за защита на личните данни, който се прилага на общо основание винаги, когато се обработват лични данни. Всъщност основните принципи за защита на данните (разгледани в т. 4 по-долу от анализа), а също и много от изискванията на Регламента съществуват и при досега действащия режим по Закона за защита на личните данни, който обаче не беше достатъчно добре прилаган, като една от целите на Регламента е именно да засили контрола и да завиши занапред санкциите при неспазването му.

Регламентът на практика заменя голяма част от разпоредбите на българския Закон за защита на личните данни, като въвежда единни хармонизирани европейски правила за защита на личните данни, които са пряко приложими във всички държави членки и са задължителни за всички, обработващи лични данни. Все пак, на националния законодател е оставено право на преценка относно някои предвидени

изключения, които в България ще бъдат отразени със Закона за изменение и допълнение на Закона за защита на личните данни [6], който обаче се забави и предстои да бъде гласуван едва наесен от Народното събрание. Забавянето на приемането на този закон също допринася за объркването около прилагането на Регламента, затова е важно да се каже, че Регламентът няма нужда от националния закон, за да се прилага. Макар към момента надзорният орган, който е Комисията за защита на личните данни (КЗЛД) да проявява толеранс към обработващите лични данни, като не прави проверки, въведените с Регламента нови правила за защита на личните данни вече са в сила и следва да се спазват от всички. Заедно с тях, специалните разпоредби на Закона за здравето и други нормативни актове в областта на здравеопазването също продължават да действат, като поставят допълнителни изисквания, които трябва да се спазват от лечебните заведения и практикуващите лекари при обработката на здравните данни.

3. Основни определения

Следващ важен въпрос, който трябва да се изясни още от самото начало, е свързан с някои основни дефиниции на използвани понятия, доколкото чрез тях се определя обхватът на приложение на Регламента.

Отговорни за спазването на Регламента са всички „Администратори на данни“, които включват всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни, както и „обработващи лични данни“, които обработват лични данни от името на администратора въз основа на писмен договор (напр. доставчици на информационни услуги, охрана, счетоводни услуги и други подизпълнители). Тоест, както бе казано по-горе, Регламентът се прилага както към държавни органи, агенции, държавни и общински болници, така и към частни лица като лечебни заведения за болнична и извънболнична медицинска помощ, аптеки, лаборатории, частнопрактикуващи лекари, лекари по дентална медицина и всякакви други физически и юридически лица, които обработват данните в професионално качество и не за лични цели. Задължени да спазват Регламента са всички организации на частното право, включително търговски дружества, кооперации, неправителствени организации, политически партии и други формирования, както и публични органи, органи на местно самоуправление, свободни професии и самоосигуряващи се лица, когато обработват лични данни за професионални цели. Съгласно чл. 2 (2) Регламентът не се прилага само спрямо физически лица в хода на чисто лични или домашни занимания, както и при някои други изрично изключени хипотези от държавни органи при осъществяване на Общата европейска политика в областта на външните отношения и сигурността, както и за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност.

„Обработване на данни“ е също много широко понятие, което включва всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбинирание, ограничаване, изтриване или унищожаване.

Едно от най-съществените изменения спрямо сега действащия режим е и по-широката дефиниция на лични данни, която занапред ще обхваща всяка информация, свър-

зана не само с идентифицирано физическо лице, но и с такова, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор (като име, ЕГН, местонахождение, IP адрес) или по един или повече признаци, специфични за неговата физическа, физиологична, генетична, психическа, умствена, икономическа, културна или социална идентичност (чл. 4, ал. 1 от [3]). Това е особено важно за общопрактикуващите лекари, които често събират голям обхват от лични данни, включително идентифициращи данни, данни за контакт, пол, възраст, семейно положение, месторабота, данни за личния живот, които могат да са от значение за дадено заболяване като навици, начин на живот и т.н., както и множество здравни данни.

Регламентът предвижда също така специални правила при обработването на специална категория лични данни, т.нар. „чувствителни данни“, в това число генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние на лицата (чл. 9, ал. 1 от [3]). Дадени са определения на „генетични данни“ – лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице, „биометрични данни“ – лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни и „данни за здравословното състояние“, като последните се определят като „лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние“ (чл. 4, т. 15 от [3]). Подобно е определението и в чл. 27, ал. 1 от Закона за здравето, съгласно който „здравна информация са личните данни, свързани със здравословното състояние, физическото и психическото развитие на лицата, както и всяка друга информация, съдържаща се в медицинските рецепти, предписания, протоколи, удостоверения и в друга медицинска документация“. Макар да съществуват известни разлики в двете определения по Регламента и Закона за здравето, между тях като цяло няма противоречие и може да се приеме, че те са с еднакъв обхват на действие. Дефиницията на здравни данни по Закона за здравето всъщност набляга на медицинските документи, като носители на здравна информация, които по същество също попадат в приложното поле на Регламента и към тях трябва да се прилагат всички негови изисквания. Важно е да се отбележи също така, че носителите на медицинска информация, както и използваните начини за запис на същата се характеризират с някои особености. Резултатите от образни и апаратни изследвания, не само тяхното разчитане, а и физическите носители (графи, запис от ЕКГ, ЕМГ и т.н.) се включват в понятието медицинска документация и са носители на здравни данни.

4. Принципи при обработването на личните данни

При обработването на личните данни, включително здравните данни, действат няколко основополагащи принципа, които винаги трябва да се спазват от всички без изключение. Макар тези принципи да съществували в голямата си част и досега, в Регламента те намират много по-конкретно изражение в задълженията и изискванията, които администраторите на здравни данни трябва да изпълняват, като някои от основните промени ще бъдат разгледани по-долу в анализа.

4.1. Принцип на законосъобразност

Основен принцип при защитата на личните данни е, че администраторът може да събира и обработва лични данни на физически лица, само когато има законово основание за това. В тази връзка е изключително важно да се избере правилното основание за всяка конкретна операция по обработването на данни, като съгласно чл. 6, ал. 1 от Регламента са възможни следните хипотези:

- а) *съгласие на лицето*, чиито данни се обработват;
- б) *необходимост от данните за сключване или изпълнение на договор с лицето*;
- в) *законово задължение* по българското или европейско право, което се прилага спрямо администратора;
- г) *защитата на жизненоважни интереси* на лицето, чиито данни се обработват, или на друго физическо лице;
- д) *необходимост от данните за изпълнението на задача от обществен интерес* или *при упражняването на официални правомощия*, които са предоставени на администратора;
- е) *наличието на легитимни интереси* на администратора или на трето лице, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на лицата, които изискват защита на личните данни, по-специално, когато субектът на данните е дете.

Достатъчно е администраторът да може да се позове на едно от посочените основания, за да докаже, че обработва данните законосъобразно. Най-подходящо например за публичните органи и други организации, на които са им възложени официални правомощия или изпълняват задачи от обществен интерес, свързани с превенцията и контрола на заболяванията или др. общественоползните дейности е да се позоват на основанията, посочено в буква д), което е задача от обществен интерес или при упражняване на официални правомощия.

От друга страна, за всички лечебни заведения и практикуващи лекари изглежда подходящо основание, посочено в буква в), което е изпълнение на законово задължение (напр. за спазване на изискванията на задължителното обществено осигуряване и Националния рамков договор, законово изискване за водене на медицинска документация, събиране на определена медико-статистическа информация или други специални разпоредби в областта на здравеопазването) или буква г), което е защита на жизненоважни интереси, доколкото предоставянето на здравни грижи са от основно значение за здравето и живота на пациентите.

Администратори на здравни данни, които сключват договори с пациентите за определени медицински услуги, които се заплащат, пък могат да се позоват на буква б), което е сключване и изпълнение на договор. На това основание следва да се обработват също така личните данни на всички служители на лечебните заведения и на други организации – работодатели, доколкото липсват други законови задължения. Легитимните интереси на администратора (буква е) пък ще са основание напр., когато се прилагат системи за видеонаблюдение в лечебните заведения или контрол на посетителите от охраната, доколкото е налице легитимен интерес да се пази редът и поддържа сигурността на територията на лечебното заведение.

В тази връзка буди недоумение фактът защо много от аптеките и лечебните заведения са посъветвани да изберат съгласието на пациентите, което всъщност е едно от най-нестабилните законови основания. Това е така, защото една от основните промени, които въвежда Регламентът спрямо сега действащия режим, са значително по-строгите изисквания за съгласието, което трябва да е дадено чрез ясно утвърдителен акт, с който да се изразява свободно дадено конкретно, информирано и недвусмислено заявление за съгласие

от страна на лицето (чл. 4, т. 11 от [3]). Смята се, че съгласието не е дадено свободно, ако не се предоставя възможност да бъде дадено отделно съгласие за различните операции по обработване на лични данни, макар и да е подходящо в конкретния случай, или ако изпълнението на даден договор, включително предоставянето на услуга, се поставя в зависимост от даването на съгласие, въпреки че това съгласие не е необходимо за изпълнението (съображение 43 от [3]). Трябва да е предвидена също така възможност лицето да оттегли съгласието си по всяко време, като това трябва да става толкова лесно, колкото и даването му и лицето, в случая пациентът, да е предварително информирано за това (съображение 32 и чл. 7 от [3]). Можем да си представим какъв хаос ще настане в системата на здравеопазване, ако пациентите в болниците и аптеките оттеглят даденото си съгласие и възразят срещу обработване на данните им.

Вероятно объркването за използването на съгласието като основание за обработката идва от факта, че освен общите законови основания за обработването на лични данни, съществуват и специални основания за обработването на „чувствителни данни“, в това число и здравни, биометрични и генетични данни. Съгласно чл. 9, ал. 2 от Регламента, такива данни могат да се обработват само при определени основания, като най-релевантните за здравеопазването в случая са следните:

- субектът на данни е дал своето *изрично съгласие* за обработването на тези лични данни за една или повече конкретни цели;
- обработването е необходимо *по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила* – напр. при съставянето на болнични листове за целите на упражняването на осигурителните права на пациента;
- обработването е необходимо, *за да бъдат защитени жизненоважните интереси на субекта на данни или на друго физическо лице*, когато субектът на данни е физически или юридически неспособен да даде своето съгласие – тук могат да се отнесат всички случаи на бърза и неотложна медицинска помощ и други медицински услуги от жизненоважно значение за пациента;
- обработването е необходимо по причини от *важен обществен интерес на основание правото на Съюза или правото на държава членка*, което е пропорционално на преследваната цел, защита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;
- обработването е необходимо за целите на *превантивната или трудовата медицина, за оценка на трудоспособността на служител, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи* въз основа на правото на Съюза или правото на държава членка или съгласно договор с медицинско лице или друго лице, обвързано от задължението за професионална тайна. Това всъщност е най-вероятното основание за обработването на здравните данни, тъй като то обхваща цялата система на здравеопазването и здравното осигуряване, трудовата медицина, медицинските свидетелства за започване на работа, дейността на лечебните заведения, общопрактикуващите и частнопрактикуващите лекари, лекарите по дентална медицина, аптеките, всички дейности на Министерството на здравеопазването, Районните здравни инспекции, Здравната каса и други публични органи, които обработват здравни данни като част от системата за здравеопазване и социални грижи;
- обработването е необходимо от *съображения от*

обществен интерес в областта на общественото здраве, като защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти или медицинските изделия, въз основа на правото на Съюза или правото на държава членка, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна;

- обработването е необходимо за целите на *архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели* – тук например попадат хипотезите за събиране на медико-статистическа информация и научноизследователската дейност на медицинските институти, университетите и лечебни заведения.

Видно е, че в системата на здравеопазването не съществува пречка здравните данни на лицата да се събират и обработват и след въвеждането на Регламента и съгласието на пациента като законово основание за това съвсем не е удачно, доколкото съществуват много по-подходящи и сигурни такива основания, на които администраторите на здравни данни могат да се позоват. Съгласието на пациента следва да е последна опция, само когато не може да се приложи никое друго от посочените по-горе основания за обработването на здравните данни, което, както бе казано по-горе, е малко вероятно да се наложи.

Следва също така да се направи и разграничение между съгласието на пациента за обработване на здравните му данни съгласно Регламента и информираното съгласие на пациента, което винаги се изисква преди всяка медицинска дейност съгласно чл. 87, ал. 1 от Закона за здравето. Тези две съгласия са различни и не бива да се смесват, тъй като те преследват различни цели. Информираното съгласие е с цел да се позволят медицински дейности върху тялото на пациента, като това съгласие е винаги необходимо освен в изрично предвидените изключения съгласно чл. 89, ал. 2 от Закона за здравето. От друга страна, съгласието съгласно чл. 9, ал. 1 буква а) от Регламента цели да се разреши обработването на здравните данни на пациента за една или повече конкретни цели, като това обработване, както бе казано по-горе, може да стане и без да е необходимо съгласието му, ако са налице други законови основания за това.

Накратко, информираното съгласие по Закона за здравето трябва да продължи да се взема, както досега, но не бива да се смята, че щом такова съгласие се изисква е необходимо винаги да се взема и съгласие за обработване на здравните данни на пациентите. От друга страна, в случай, че някои лечебни заведения разчитат на информираното съгласие на пациента като законово основание за обработката на здравните му данни, това трябва да се промени и те да се позоват на друго основание от посочените по-горе, за да изпълнят изискванията на Регламента.

4.2. Принцип на ограничение на целите

Друг основополагащ принцип е, че личните данни трябва да се събират винаги за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, несъвместим с тези цели. В този смисъл е важно администраторът на здравни данни да определи точно целите, за които събира и ще използва здравните данни на лицата, като напр. предоставянето на здравни грижи/медицински услуги, превенция и диагностика на заболявания и последващо лечение на лицата, оценка на трудоспособността и т.н. Често, макар здравните данни да се събират за една цел, те се използват и за други цели като например за медико-статистически цели в изпълнение на задължението на лечебните заведения да предоставят определена информация на Нацио-

налния статистически институт съгласно [7] или за научни, или исторически изследвания след премахване на идентифициращите данни на пациентите и анонимизирането им. Всички цели, за които ще се ползват данните, трябва да се определят конкретно и предварително от администратора и той да информира предварително пациента за тях (виж т.5.1 от анализа по-долу). Някой път, лечебните заведения може да решат да използват данните на пациентите и за маркетинг цели (напр. да им изпращат по имейл рекламни материали за медицински продукти или медицински услуги), като в този случай те трябва да получат изричното съгласие на пациентите за това, доколкото това представлява нова цел, несъвместима с тази, за която данните са събрани.

4.3. Принцип на ограничение на срока на съхранение

Данните трябва да се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни. Личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели след предоставянето на достатъчно гаранции за защита на правата на лицата (напр. анонимизирането на данните).

В случай, че има законоустановен срок за съхранение на здравните данни, той следва да се спазва, като след това данните да се унищожат по сигурен начин (напр. чрез нарязване на шредер или окончателното им изтриване от информационните системи). За някои медицински документи са определени точно сроковете, за които те следва да се пазят – напр. до 1 г. – за бланки за искания за лабораторни изследвания; до 3 г. – книга за повикванията за БМП или за аптекните дейности; до 25 г. – болнични листове и история на заболяванията; до 50 г. – книга за приетите болни в стационар; до 100 г. – книга за ражданията в родилно отделение.

Въпреки че чл. 27, ал. 3 от Закона за здравето предвижда да се издаде специална наредба за формите и съдържанието, както и условията и реда за обработване, използване и съхраняване на медицинската документация, такава и до ден днешен липсва. В здравната литература това се определя като съществен пропуск и основна причина за недоброто водене на медицинската документация [8, 9]. Съществуват някои специални разпоредби основно в областта на общественото осигуряване и в Националния рамков договор относно първичната и отчетната медицинска документация (направления, болнични листове и т.н.) или в подзаконовите нормативни актове в отделни области на здравеопазването (превенция на СПИН, заразни болести и др.), но като цяло уредбата е разпокъсана и съществува правна неяснота в много аспекти, особено за документацията, водена в извънболничната медицинска помощ. Това вероятно ще затрудни прилагането на Регламента, доколкото много от администраторите на здравни данни няма да са наясно за какъв точно срок ще е необходимо да съхраняват чувствителните здравни данни, което може да доведе до неоснователно дълго пазене на тази информация, което пък да застраши правата и интересите на пациентите, особено в случай на нерегламентиран достъп или други нарушения на сигурността.

4.4. Принцип на точност и актуалност

Принципът на точност и актуалност е изключително важен за здравните данни, тъй като от това зависи правилното диагностициране и лечение на пациентите. Например, допускането на грешки в идентифициращите данни на пациента (години, самоличност) може да доведе до грешни заключения за неговото здравословно състояние и да породи висок риск

за неговите права и интереси, включително като застраши живота му. Нерядко в големите болнични заведения стават и грешки при воденето на медицинската документация, има много случаи на негълна регистрация или изобщо липса на регистрация на пациента [8]. При лабораторните изследвания недобрата организация или хигиена пък може да доведе до грешни лабораторни резултати. Възможно е също така неточността да се дължи и на корупционни практики, особено при удостоверяващи медицински документи за здравното състояние на лицата – напр. медицински свидетелства за професионална годност, решения на ТЕЛК за инвалидност, които са основа за предоставянето на определени социални помощи и придобивки и др. Съвсем съзнателно допуснати грешки са възможни и поради съществуващата недобра практика на отчитане на клиничните пътеки към здравната каса, където понякога се достига до изкривяване и дори фалшифициране на първичната медицинска документация с цел получаване на повече финанси [10].

Освен от жизненоважно значение за пациента, пълното и точно отразяване на здравните данни в медицинските документи е наложително, защото повечето от тях представляват официални удостоверителни документи, които се ползват с материална доказателствена сила по отношение на отразените в тях факти (напр. амбулаторен лист, болничен лист, медицински удостоверения и др.) [11]. При възникване на съдебен спор това означава, че фактите, които са вписани в тези медицински документи, ще се смятат за установени от съда до доказване на противното. В случай, че се установи съзнателно вписване на неточни данни, това съставлява и престъпление, т.нар. интелектуална подправка на документ, за което съставителят носи наказателна отговорност, а също и гражданска за причинените вреди на пациента.

За да се решат посочените по-горе проблеми, е изключително важно да се въведат високи стандарти на медицинско обслужване, строги вътрешно-организационни правила в лечебните заведения и контрол по спазването им, включително в областта на документооборота и корупционните практики. Необходими са също така и някои законодателни решения за промяна на отчитане на финансирането по здравната каса, за да се разкъса порочната практика на изкривяване на здравната статистика и информация с цел получаване на повече средства от болниците за сметка на интересите на пациента. Въвеждане на електронната здравна карта също се очаква да допринесе за намаляване на злоупотребите при отчитане на клиничните пътеки и грешките в здравните данни на пациентите, доколкото последните ще получат пълен контрол и директен достъп до здравните си досиета.

4.5. Принцип на минимизация на данните

Този принцип изисква здравните данни да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват. В тази връзка е важно да се каже, че лекарската професия не е точна наука и лекуващият лекар трябва да запази правото си на преценка какви данни смята, че са необходими, за да постави диагнозата и да предпише необходимото лечение. Това е особено важно и свързано с друг споменат по-горе принцип, а именно необходимостта от точност на здравните данни и поставената диагноза. Трябва обаче също да се подчертае, че порочни практики, при които съзнателно се назначават допълнителни изследвания или медицински манипулации с цел да се използват клинични пътеки или да се получи допълнително заплащане от пациента, без външно да е необходимо тяхното извършване, са в ясно противоречие с добрата лекарска практика, принципа на минимизиране на данните, а също и задължението за добросъвестното им обработване от администратора.

4.6. Принцип на цялостност и поверителност

Този принцип изисква личните данни да се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. Предвид това, че здравните данни са чувствителни данни, които могат да поставят сериозни рискове за правата и свободите на пациентите, принципът на поверителност и сигурност на данните е от основополагащо значение за всички лечебни заведения и практикуващи лекари и други администратори на здравни данни. Тук е удачно да споменем, че в Закона за здравето и сега съществува задължение за защита на данните и хипотези, при които здравната информация може да бъде разкрита на трети лица. (Съгласно чл. 28, ал. 1 от Закона за здравето здравни данни могат да бъдат разкрити, когато: лечението на лицето продължава в друго лечебно заведение; съществува заплаха за здравето или живота на други лица; необходими са при идентификация на човешки труп или за установяване на причините за смъртта; за нуждите на държавния здравен контрол за предотвратяване на епидемии и разпространение на заразни заболявания; за нуждите на медицинската експертиза и общественото осигуряване; за нуждите на медицинската статистика или за медицински научни изследвания, след като данните, идентифициращи пациента, са заличени; необходима за нуждите на Министерството на здравеопазването, Националния център по здравна информация, НЗОК, Регионалните здравни инспекции и Националния статистически институт, необходима за нуждите на лицензиран застраховател.) Регламентът с неговите конкретни изисквания относно сигурността на данните се очаква да повиши значително защитата на здравните данни с прилагането на практика на необходимите технически и организационни мерки за тази цел, описани в т. 6 от анализа по-долу.

4.7. Принцип на отчетност

Една от най-съществените промени, въведени с Регламента, е завишената отговорност и новия принцип на отчетност за всички администратори, обработващи лични данни, които трябва да са в състояние да докажат на практика, че спазват разгледаните в анализа принципи и изисквания при обработването на лични данни (чл. 6, ал. 2 от [3]). В това отношение, Регламентът радикално променя съществуващия досега режим, като прехвърля тежестта на доказване върху самите администратори за сметка на много от досегашните административни процедури по регистрация и докладване към Комисията за защита на личните данни (КЗЛД), които отпадат занапред.

От 25 май 2018 г., когато Регламентът започна да се прилага, всички администратори, включително лечебни заведения, общопрактикуващи лекари, публични органи и т.н. трябва да са въвели съответните организационни и технически мерки, за да гарантират, че спазват Регламента. Такива мерки включват, *inter alia*: документиране на всички действия по обработването на данните; гарантиране на сигурността и защитата на данните; приемане на вътрешни процедури и правила за обработване и защита на личните данни; водене на вътрешни регистри за обработването на лични данни; назначаването при необходимост на длъжностно лице по защита на личните данни и извършване на оценка на въздействието върху защитата на данните; актуализиране на договорите с всички доставчици на услуги, обработващи данните от името на лечебното заведение (напр. доставчици на информационни услуги, охрана, счетоводство и т.н.), като тези договори следва да включват определени клаузи, описани в чл. 28 от Регламента, изготвяне на уведомления за повери-

телност за пациентите, навременно и законосъобразно обработване на исканията на пациентите при упражняване на правата им и др., част от които ще бъдат разгледани в следващите точки от анализа.

5. Повече и по-лесни за упражняване права на субектите на данни

Регламентът значително разширява и улеснява упражняването на правата на субектите на данни във връзка с техните лични данни, като всички администратори на здравни данни следва да осигурят възможност на пациентите да упражняват тези свои права, като разгледат исканията им възможно най-скоро и не по-късно от 1 месец (чл. 12, ал. 2 и ал. 3 от [3]). По-долу ще бъдат разгледани някои от основните права, доколкото съществуват особености при тяхното упражняване от пациентите.

5.1. Право на информираност

Специално внимание следва да се обърне на правото на информираност на субектите на данни, което е пряко свързано с принципа на прозрачност. Регламентът въвежда задължение за всички администратори на данни да информират лицата, чиито данни обработват както, когато получават тези данни пряко от тях (чл. 13 от [3]) (с тяхно знание или чрез наблюдение през камери, следене на wifi и др.), така и, когато това става посредствено (чл. 14 от [3]) (напр. чрез други организации или физически лица, от публично достъпни ресурси). Информацията, която пациентите следва да получат, включва данни за администратора и длъжностното лице по защита на данните (в случай, че има такова), какви техни лични данни се обработват, на какво законово основание и за какви цели, с кого се споделят, за какъв срок се пазят и при какви мерки за сигурност, дали се прехвърлят данни извън Европейския съюз и какви са свързаните с това рискове, задължително ли е предоставянето на данните и какви са последствията от непредоставянето им, налице ли е профилиране и автоматизирано вземане на решения, какви са правата на пациентите във връзка със защита на личните им данни, включително правото им на жалба до надзорния орган КЗЛД.

Важно е да се отбележи, че това задължение за информиране на пациентите съществува независимо от правното основание, въз основа на което се обработват личните данни, т.е. и в случаи, в които не се иска съгласието на пациентите за обработване на данните. Новите изисквания налагат предоставянето на кратка, прозрачна, разбираема информация в лесно достъпна форма, представена на ясен и прост език. Информацията трябва да е под формата на уведомления за поверителност/политика за защита на данните, което трябва да се предостави на пациента преди регистрирането му. Уведомлението също така трябва да е закачено на видно място в кабинета/регистратурата и на сайта на заведението в случай, че съществува такъв.

Докато администраторът на здравни данни е длъжен винаги да предостави тази информация преди обработването на данните, когато получава последните пряко от пациента, това не винаги е така в случаите, в които информацията се получава посредствено – напр. пациент разкрива данни за предишни заболявания на членове от семейството си. В този случай лечебното заведение или общопрактикуващият лекар биха били освободени от задължението да предоставят на тези трети лица посочената по-горе информация, ако личните данни трябва да останат поверителни при спазване на задължение за опазване на професионална тайна, в случая лекарска тайна (чл. 14, ал. 5, буква г от [3]). Позицията се на задължението си за поверителност, лекарят не бива да уведомява тези лица, че разполага с данни за тях, тъй като това

би нарушило задължението му да опази лекарската тайна. В останалите случаи обаче, задължението за информираност продължава да действа, освен ако лицето вече не е запознато с посочената информация във връзка с обработването на данните му или предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия (по-специално за обработване на данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели).

5.2. Право на достъп

Правото на достъп до личните данни не е ново и съществува както по досегашния режим за защита на личните данни, така и по силата на чл. 28б от Закона за здравето. Често пъти досега обаче администраторите са събирали такси, за да предоставят такъв достъп или копие от документите. Сега Регламентът изисква изрично първото копие от всички данни, с които разполага лечебното заведение или практикуващият лекар, да бъдат предоставени на пациента безплатно, като за последващи копия може да се събират разумни такси съобразно направените административни разходи (чл. 15 от [3]). Пациенти ще могат също така занапред да посочат как желаят да им бъде предоставена информацията – на хартия или на дигитален носител. Заедно с копието от данните за лицето, администраторът следва да предостави и информацията, посочена в т. 5.1. по-горе, във връзка с обработването на данните. В случай на смърт правото на достъп преминава към наследниците на починалото лице – това е предвидено изрично в чл. 28б, ал. 3 от Закона за здравето, като КЗЛД и досега е предписвала многократно на лечебни заведения да предоставят такъв достъп на наследниците (напр. [12]).

5.3. Право на коригиране

Правото на коригиране също не е новост, като то дава възможност лицето да поиска да бъдат коригирани неточни данни за него или да бъдат допълнени с други данни, ако личните данни са непълни, включително чрез добавяне на декларация. В тази връзка трябва да се спомене, че ако пациентът оспорва дадена диагноза, това не значи, че лекуващият лекар е длъжен да изтрие или коригира последната, тъй като диагнозата се смята за точна спрямо фактите към момента на поставянето ѝ, доколкото лекарят действително е смятал така. Запазването на тази информация е важно, тъй като то отразява мнението на даден специалист и може да има значение за по-нататъшното лечение на пациента и преценката за състоянието му от други лекари. Все пак, в случай, че пациентът оспорва дадена диагноза трябва да му се даде възможност да напише декларация към медицинската документация, в която заявява несъгласието си. По силата на чл. 8б, ал. 1 т. 4. от Закона за здравето, пациентът има също така специално право на повече от едно медицинско становище относно диагнозата, лечението и прогнозата на заболяването, което следва да допринесе за точността на здравните му данни.

5.4. Правото на изтриване/„да бъдеш забравен“

Друго право, което заслужава специално внимание, е най-новото признато право на субектите на данни да искат изтриването на личните си данни или т.нар. „право да бъдеш забравен“, прогласено от Съда на ЕС [13] и предвидено в чл. 17 от Регламента. То обаче съвсем не е абсолютно и съществуват определени изключения, на които администраторите на здравни данни могат да се позовават. Така, например, лечебните заведения и лекуващите лекари могат да откажат изтриването на лични данни, когато обработването

на данни е необходимо за:

- спазването на законово задължение (напр. задължение за водене на медицинска документация и съхранение на данните съгласно сроковете по НРД);
- за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора (т.е. правото е неприложимо спрямо всички публични органи);
- по причини от обществен интерес в областта на общественото здраве;
- за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;
- за установяването, упражняването или защитата на правни претенции, доколкото лекарите често могат да бъдат обект на съдебни искове от недоволни пациенти, включително поради предполагаема лекарска грешка.

5.5. Право на прехвърлимост на данните

Особеност съществува и при новопризнатото право на прехвърлимост на личните данни, което задължава администратора на данни да предостави на пациента или трето лице (напр. друго здравно заведение) свързаните с него лични данни в „структуриран, широко използван и пригоден за машинно четене формат“, когато обработването е автоматизирано и основано на съгласие или договорно задължение (чл. 20 от [3]). Доколкото това основание се прилага само при съгласие и договор за медицински услуги, администраторите на здравни данни няма да са длъжни да се съобразяват с такива искания, ако обработват данните на някое от другите законови основания (напр. изпълнение на законово задължение, защита на жизненоважни интереси, задача от обществен интерес и при упражняване на официални правомощия). Все пак, редно е да кажем, че в системата на общественото здравно осигуряване вече е наложена като добра практика преносимостта на здравните картони на пациентите при смяна на общопрактикуващите лекари, което става автоматично в системата.

6. Сигурност на данните

Както бе споменато по-горе, сигурността на данните е друга ключова област, където Регламентът съществено завишава изискванията, като администраторите на данни ще трябва занапред да прилагат подходящи технически и организационни мерки за осигуряване на съобразено с оценения риск ниво на сигурност, включително защита срещу неразрешено разкриване или достъп до данни, както и случайно или неправомерно унищожаване, загуба или промяна на данните. Тези мерки може да включват, *inter alia*, псевдонимизация (съгласно чл. 4, ал. 5, псевдонимизация означава обработването на лични данни по такъв начин, че те не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие, че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано) и криптиране на личните данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване, способност за своевременно възстановяване на наличността и достъпа до личните данни и процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки (чл. 32 от [3]). В момента минималните мерки са разписани в НАРЕДБА № 1 на КЗЛД [14], която предстои да бъде актуализирана в съответствие с Регламента и трансформирана в Методическо ръководство.

Съществена промяна е новото задължение при нарушения на сигурността на данните администраторът на данни да уведоми без ненужно забавяне и при всички положения не по-късно от 72 часа:

- *КЗЛД*, винаги когато съществува вероятност нарушението на сигурността на личните данни да породи *риск* за правата и свободите на физическите лица (чл. 33, ал. 1 от [3]), и
- *засегнатите пациенти*, винаги когато съществува вероятност нарушението на сигурността на личните данни да породи *висок риск* за правата и свободите на физическите лица (чл. 34 от [3]).

При оценката на риска е важно да се отбележи, че висок риск за субектите на данни ще има винаги, когато нарушението може да доведе до физически, имуществени или неимуществени вреди за лицата, чиито данни са били засегнати, като например нарушаване на поверителността на личните данни при разкриване на професионална тайна, дискриминация, кражба на самоличност или измама, имуществени загуби или засягане на репутацията (Съображение 75 и 85 от [3]). Когато нарушението на сигурността се отнася до „чувствителни данни“ като здравни, генетични и биометрични данни, такива вреди трябва да се считат за вероятни да настъпят.

В тази връзка повишаването на сигурността се оказва от изключително значение за администраторите на здравни данни, тъй като всяко допуснато нарушение на сигурността на данните на пациентите е много вероятно да породи висок риск за техните права и да наложи съответно пациентите и КЗЛД да бъдат уведомени за нарушението, в случай че лекарската тайна е била разкрита или нарушението засяга чувствителна здравна информация. Допускането на такива нарушения може не само сериозно да навреди на репутацията на лечебното заведение, но и да породи проверка от КЗЛД дали нарушението не е резултат от неспазване на изискванията за сигурност на Регламента, което може да доведе и до административни санкции в размер до 4% от годишния оборот на лекуващия лекар или лечебното заведение.

Изискванията, които администраторите на здравни данни трябва да изпълняват в тази област са множество, като някои добри практики ще бъдат описани по-долу. Лечебните заведения и лекуващите лекари напр. са длъжни да повишат сигурността на информационните системи и да ползват само доставчици на информационни услуги, които спазват Регламента (напр. техн. поддръжка, хостинг услуги, сигурност на сървърите, облачни услуги). Във Франция, която е една от европейските страни с най-висока защита на здравните данни, е въведен напр. специален разрешителен режим за доставчиците на информационни услуги за сектора на здравеопазване. Препоръчително е също така да се въведат логове (данни за това кой, кога и какви промени е правил) за всички дейности по обработването на личните и здравни данни на пациентите, които ясно да показват кой е отговорен за отделните операции. Това ще бъде особено важно също при въвеждането на електронната здравна карта, за да може ефективно да се проследят промените и злоупотребите със здравната информация на пациентите. Друга добра практика за големите лечебни заведения е да се въведе цялостна политика за информационна сигурност, както и политика по документооборота с ясни отговорности за персонала, включително по архивирането и унищожаване на здравните данни. Достъпът на служителите до информационните системи, както и до помещенията, в които се съхраняват здравни данни, трябва да е ограничен и предоставен единствено на служители, които имат необходимост да боравят с конкретната информация. Обучение на персонала и контрол по спазване на задълженията по сигурността и вътрешните процедури

за защита на личните данни са от първостепенно значение за точното приложение на всички изисквания. Технически мерки като заключване на шкафови и помещения, контролиран достъп с магнитни карти, поставянето на видеонаблюдение и др. също могат да допринесат значително за повишаване на сигурността.

Особено препоръчително е също така да се криптират базите-данни, служебните пощи и мобилните устройства, на които се съхраняват лични здравни данни и поверителна информация, тъй като това би направило нечетима информацията за неотроризирания получател на данните. Предвид заплахите пред киберсигурността е наложително здравни данни да се споделят само и единствено чрез сигурни комуникационни канали, които изискват верификация на получателя или чрез криптиране на данните. В този случай, дори да има допуснато нарушение на сигурността, уведомяване на КЗЛД и пациентите няма да е необходимо, доколкото няма да съществува риск за правата и свободите на засегнатите лица, тъй като неотроризирания получател няма да могат да разчетат информацията (чл. 34, ал. 3 от [3]).

7. Длъжностни лица по защита на данните

Едно от най-съществените и първостепенни нови задължения на администраторите и обработващите данни е да имат длъжностно лице по защита на данните (ДЛЗД) винаги, когато основните им дейности се състоят в операции по обработване, които изискват редовно и систематично мащабно наблюдение на субектите на данни, или се състоят в мащабно обработване на „чувствителни данни“, в това число здравни, генетични и биометрични данни (чл. 37, ал.1 от [3]). Докато самостоятелно практикуващите лекари и други здравни работници са изрично освободени от задължението да имат ДЛЗД (Съображение 91 от [3]), уточнението „мащабно“ е много важно в случая, тъй като не е ясно дали малки амбулатории за извънболнична медицинска помощ или диагностични-консултативни кабинети и центрове (от 2-5 лекаря) са също длъжни да назначат такова длъжностно лице, тъй като липсва установен минимален праг или практика по въпроса. В указания по приложението на Регламента все пак се посочват някои критерии, които да служат за ориентир при преценката дали посочените данни се обработват „мащабно“ (напр. брой физически лица; обем и обхват на личните данни, които се обработват; продължителност на съхранението; географски обхват; специфични характеристики на администратора и субектите на данни) [7].

Режимът за назначаване на длъжностното лице е относително гъвкав, като лечебните заведения могат, например, да назначат такова длъжностно лице само на тази позиция или да определят работник/служител, който да изпълнява задълженията на ДЛЗД по съвместимост, доколкото няма конфликт на интереси с другите му функции. ДЛЗД може да бъде и външно за лечебното заведение лице, което да изпълнява тази функция въз основа на договор за услуги (чл.37, ал.6 от [3]).

Каквато и форма от посочените по-горе да се избере, длъжностното лице трябва да бъде независимо предвид възложените му важни задачи и сериозните правомощия, с които разполага, като участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни, информира и съветва администратора и служителите му относно задълженията при обработката на лични данни; контролира спазването на правните задължения и вътрешноорганизационните политики по защита на личните данни; участва в обучения на персонала и одити; действа като точка за контакт с надзорния орган по защита на личните

данни и др. (чл. 39 от [3]) ДЛЗД трябва да докладва на най-високо управленско ниво, а освен това да разполага и с достатъчно време и ресурси, за да изпълнява функциите си (чл. 38, ал. 2 и 3 от [3]). Лечебните заведения са длъжни да уведомят КЗЛД за назначението и да публикуват данни за ДЛЗД, към което всеки субект на данни трябва да има възможност да се обърне при необходимост.

8. Оценка за въздействието върху защитата на данните

Когато съществува вероятност определен вид обработване да породи *висок риск* за правата и свободите на физическите лица, администраторите на лични данни са длъжни да изготвят оценка за въздействието върху защитата на данни (ОВЗД) преди самото обработване да е започнало. В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове (чл. 35, ал.1 и ал. 10 и Съображения 90 и 93 от [3]). Когато обработването се осъществява изцяло или отчасти от адвокат като „обработващ данни“, съгласно чл. 28, ал. 3, буква е) от Регламента той следва да подпомогне клиента – „администратор на данни“ и да му предостави всякаква необходима информация за изготвянето на оценката.

По-конкретно за сферата на здравеопазване ОВЗД ще е задължителна, винаги, когато се обработват мащабно „чувствителни данни“, в това число здравни данни, генетични и биометрични данни (чл. 35, ал. 26 от [3]). Докато лекарите и други здравни работници на самостоятелна практика са изрично освободени от това задължение (Съображение 91 от [3]), всяка дори и малка амбулатория би могла да попадне в обхвата, доколкото обработва такива данни „мащабно“, като при преценката за това се прилагат същите критерии, както при необходимостта от ДЛЗД (виж т.7 по-горе). Уязвимостта на пациентите, които администраторите на здравни данни по принцип обслужват, също може да предполага извършването на ОВЗД (напр. деца, възрастни хора, инвалиди, психичноболни и др.) (Съображение 75 от [3]). Предвидена е възможност КЗЛД да внесе повече яснота кога такава оценка се налага, като състави списък на видовете операции по обработване, за които ОВЗД се изисква, като може да състави списък и на операциите, за които ОВЗД не се изисква (чл. 35, ал. 4 и 5 от [3]). За съжаление, такава яснота не е въведена с проекта за Изменение и допълнение на Закона за личните данни, за сметка на някои други спорни предложения.

Препоръчва се разработването на методологии за ОВЗД, които са специфични за отделните сектори, като се отчитат спецификите на дейността по обработването и вида данни, както и възможния риск за правата и свободите на физическите лица (насоки на Работна група 29 относно оценка за въздействието върху защитата на данни, стр. 17, достъпни на [15]). При липсата на специфична методология в сферата на здравеопазване следва да се спазват общите изисквания на Регламента (чл. 37, ал. 7 от [3]) и Насоките на Работна група 29, достъпни на [15], като в някои европейски държави надзорните органи са вече разработили специални насоки или софтуери, които да подпомогнат организациите в този процес (напр. софтуер, разработен от Комисията за защита на личните данни във Франция (CNIL), достъпен на [16]).

Макар че възлага ново административно задължение, ОВЗД ще има като цяло положителен ефект, тъй като ще спомогне за установяването на рискове, които иначе лечебните заведения може би не биха отчели, като по този начин спомогне да бъдат избегнати евентуални нарушения на сигурността.

9. Регистри по дейностите по обработване

Регламентът задължава всеки администратор и обработващ лични данни да води регистър на дейностите по обработването, който КЗЛД може да изисква да ѝ бъде предоставен при проверки. От това задължение са освободени единствено предприятия или дружества с по-малко от 250 служители, но само ако не съществува вероятност извършването от тях обработване да породи риск за правата и свободите на субектите на данни, ако обработването не е спорадично или включва чувствителни данни. Тоест, в случая всички администратори на здравни данни дори общопрактикуващите лекари ще бъдат длъжни да водят такъв регистър.

В регистъра следва да се включват данни за администратора и неговото ДЛЗД (в случай, че има такова), целите на обработването, описание на категориите субекти на данни и на категориите лични данни, категориите получатели на данни, включително трансфер извън ЕС, предвидените срокове за изтриване на различните категории данни и общо описание на предвидените технически и организационни мерки за сигурност.

Регистърът може да се води в електронен формат, като някои надзорни органи по защита на личните данни напр. във Великобритания и Франция са предоставили подходящи модели, които могат да се ползват за тази цел [17].

10. Заключение

В заключение може да се каже, че лечебните заведения и общопрактикуващите лекари имат огромна необходимост от практически указания за ефективното и еднакво прилагане на новия Регламент за защита на личните данни. За съжаление, за разлика от други надзорни органи в държави членки като Великобритания, Франция и др., българската Комисия за защита на личните данни не е предоставила конкретни указания и помощни материали, които да подпомогнат организациите при прилагането на Регламента на практика.

Едно предложение, което може да гарантира спазване на Регламента в сферата на здравеопазване, е по примера на Франция да се изготвят съвместни указания от КЗЛД и от браншовите организации напр. на общопрактикуващите лекари или Българския лекарски съюз (например във Франция е изготвен такъв наръчник за общопрактикуващите лекари с ясни указания и задължения за мерките, които трябва да се предприемат по прилагане на Регламента, който е достъпен на [18]). В Регламента е предвидена също така възможност да се изработи специален кодекс за поведение (чл. 40 от [3]),

към който да се придържат администратори или обработващи лични данни. По изработването на такъв кодекс в момента работи Висшия адвокатски съвет, за да гарантира спазване на Регламента от цялото адвокатско съсловие. Това може да е също добър вариант за сферата на здравеопазването, като разработването на единни и прозрачни правила под формата на кодекс ще спомогне значително за правилното изпълнение на Регламента от всички практикуващи лекари и лечебни заведения в страната, като съществено ги улесни и същевременно отчете особеностите и нуждите на лекарската професия, включително задължението за опазване на лекарска тайна и рисковете при обработката на здравни данни.

Библиография

1. КОДЕКС на професионалната етика, обн., ДВ, бр. 79 от 29.09.2000 г.
2. Закон за здравето (обн. ДВ. бр.70 от 10 Август 2004 г. посл. изм. и доп. ДВ. бр.18 от 27 Февруари 2018 г.)
3. Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), OJ L 119, 4.5.2016, p. 1–88
4. https://www.capital.bg/politika_i_ikonomika/bulgaria/2018/05/25/3185116_lekari_i_farmaceuti_ne_triabva_da_iskat_deklaracii_za/
5. <http://old.segabg.com/article.php?id=907250>
6. Проектозаконът е достъпен на https://www.cdpd.bg/?p=news_view&aid=1226
7. Наредба №1 от 27. 02.2013г. на министъра на здравеопазването за предоставянето на медико-статистическа информация и на информация за медицинската дейност на лечебните заведения, обн., ДВ, бр. 24 от 12.03.2013 г.)
8. Цонов П. Досиетата в медицинската практика, сп. „Обща медицина“, №. 2/ 2003, стр. 6-9
9. Радева М. За някои правни аспекти на здравната документация, сп. Медицинско право №1/ 2014, стр. 56-61.
10. Иванов Л. Грешки в здравните реформи, сп., „Социална медицина“, 2013, №2, стр. 4-12
11. Адм. дело 2250/2010 г. на Административен съд – Пловдив
12. Становище на КЗЛД относно искане с вх. № 334/12.03.2008 год.
13. Дело C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2013:424.
14. НАРЕДБА № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.
15. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
16. <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>.
17. <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/> и <https://www.cnil.fr/fr/rpdp-le-conseil-national-de-lordre-des-medecins-et-la-cnil-publient-un-guide-pratique-lattention-des>
18. <https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnil.pdf>.

Автор

Йорданка Иванова – Адвокат от Софийска адвокатска колегия и докторант по Право на ЕС в СУ „Св. Климент Охридски“

Конвенция на ООН за правата на хората с увреждания

Преди 12 години, на 13 декември 2006 г. ООН приема Конвенция за правата на хората с увреждания. Конвенцията на ООН не провъзгласява нови човешки права. Правата, за която тя се отнася, вече са декларираны в Международния пакт за икономически, социални и културни права, Международния пакт за граждански и политически права, Конвенцията за правата на детето, Конвенцията за премахване на всички форми на дискриминация по отношение на жените. Основен мотив за приемане на Конвенцията е продължаващата дискриминация и изолация на хората с увреждания, въпреки наличието на предходно приети международни правни инструменти, регламентиращи защитата на основни човешки права. Едно от основните послания на Конвенцията е, че хората с увреж-

дания заслужават уважение и равнопоставяне, както всички останали граждани, упражняващи лично правата си. Така следва да се направи преход от медицинския модел и разбиране за понятието „увреждане“ към социалния модел, фокусиран върху гарантиране на човешки права и социално включване на хората с увреждания в обществото. Конвенцията на ООН е ратифицирана от Европейския съюз на 23.10.2010 г., като това е първият международен правен акт от подобен вид, с който ЕС се обвързва като регионално обединение на държави. Р България подписва Конвенцията на 27 септември 2007, а на 26 януари 2012 г. Парламентът ѝ ратифицира с пълнен консенсус Конвенцията със Закон, който влиза в сила от 21 април 2012 г.

С М