

УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

Принципи заштите података о личности

(мастер рад)

Ментор

Проф. др Милош Прица

Студент

Александра Милошевић

Број индекса: М009/22-IT

Ниш, 2024.

Садржај

УВОД	1
Глава прва ПОЈАМ ПОДАТАКА О ЛИЧНОСТИ.....	4
Глава друга ВРСТЕ ПОДАТАКА О ЛИЧНОСТИ	7
1. Подаци који се односе на лични, јавни и професионални живот човека	8
2. Подаци о личности који не уживају правну заштиту	9
3. Посебне категорије података о личности	11
4. Базе података о личности и bigdata	13
Глава трећа ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ.....	17
1. Правни режими заштите података о личности.....	18
2. Повесни развој заштите података о личности.....	20
Глава четврта ПРИНЦИПИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ.....	23
1. Начело законитости, поштења и транспарентности	26
2. Начело ограничења у односу на сврху обраде	29
3. Начело минимизације података о личности	31
4. Начело тачности	33
5. Начело ограниченог чувања података о личности.....	34
6. Начело интегритета и поверљивости	36
7. Начело одговорности	38
Глава пета ПРАВНА РЕГУЛАТИВА У ОКВИРУ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ	42
1. Општа Уредба ЕУ	44
2. Прописи у области заштите података о личности у земљама бивше Југославије. 47	
3. Прописи у области заштите података о личности у Србији	49
ЗАКЉУЧНА РАЗМАТРАЊА.....	53
ЛИТЕРАТУРА.....	55
ПОПИС ИСТРАЖИВАЧКЕ ГРАЂЕ.....	Greška! Obeleživač nije definisan.

САЖЕТАК И КЉУЧНЕ РЕЧИ	59
SUMMARY AND KEY WORDS.....	60
Principles of personal data protection	60
БИОГРАФИЈА АУТОРКЕ	62

УВОД

У свету у коме данас живимо се сваког дана сакупља и обрађује огромна количина података. Свакодневно прикупљање милиона података о грађанима и обрада на основу вештачке интелигенције је постала реалност. Томе је умногоме допринело доба у којем данас живимо – доба информационих технологија. Настанак рачунара и рачунарских мрежа је у ствари претеча овог доба. Прекомерно коришћење рачунара и интернета знатно утичу на прикупљање информација о свакој особи на свету. Електронска куповина производа, заказивање термина ради узимања пасоша, дељење фотографија на инстаграму или некој другој друштвеној мрежи су само неке од малих милион ситуација у којима се користе подаци о личности. Управо због тога су подаци нужан елемент комуникације и један од најважнијих чиниоца савремене привреде. У подацима који се прикупљају нон стоп, спадају од података који се тичу личног живота човека, преко оних који се тичу јавног живота, па до оних који се односе на професионалну област појединца. Дакле, може се закључити да се у питању много врсти података који се могу прикупљати и обрађивати. Такође је важно навести да податке прикупљају како приватна и правна лица, тако и државне институције.

На основу свега горе наведеног, важно је знати да у процесу прикупљања, обрађивања и складиштења података о личности, врло лако може доћи и до њиховог повређивања. Порастом количине података о личности, њиховим складиштењем у великим базама података, али и њихова обрада уз употребу вештачке интелигенције уједно је и расла опасност од злоупотребе ових података, како од стране појединаца, тако и од стране компанија и државних институција. Јасно је да све веће количине података представљају ризик по личну приватност појединца тамо где постоје сукоби интереса. Стављање података у средиште развоја индустрије и управљања друштвима захтева подизање на висок ниво, како система информационе безбедности, па тако и система заштите фундаменталних права грађана. Од изузетне је важности, поред техничких и информационих аспеката безбедности прикупљених података, и стварање комплексног и делотворног правног система заштите података о личности. Опасности се јављају како по саме податке, тако и по права и слободе грађана на које се ти подаци односе. Посебно је

потребно обратити пажњу на право на приватност, право на породичан живот, право на слободу и право на неповредивост преписке, која спадају у најугроженију групу права.

Заштита података о личности представља витални аспект индивидуалних права јер се односи на сваку особу. Заштита података је законски прописана уставима и посебним законима многих земаља. Податке о личности могуће је заштити помоћу система физичке, информационе и правне заштите. Сваки од ових система је међусобно нераскидиво повезан. Заштита података о личности се обезбеђује сваком физичком лицу без обзира на држављанство и пребивалиште, расу, године живота, пол, језик, вероисповест, политичко и друго уверење, националну припадност, социјално порекло и статус, имовинско стање, рођење, образовање, друштвени положај или друга лична својства.

Приватан живот представља приватну сферу, право човека да живи на начин на који жели, те да притом буде заштићен од јавности, с тим што до извесне мере обухвата и право на успостављање и неговање односа са другим људима ради развијања и задовољавања сопствене личности. Право на приватност има апсолутни значај и делује *erga omnes* – према свима – вертикални однос има према државним органима, а хоризонталан однос према трећим лицима. Само по себи има важност деловати према свима, али није ограничено. Приватност се може поделити на просторну приватност, информацијску приватност и комуникацијску приватност. Право на приватност, као основно људско право, има посебан значај у корпусу људских права. То се може уочити по томе што сви инструменти за заштиту људских права, како међународни тако и државни и регионални, својим одредбама регулишу заштиту података о личности.

Унапређење система заштите података о личности се може остварити само кроз истовремени развој правних норми у области заштите података, ефективну примену закона и унапређење знања адвоката и странака. Како би дошло до повећања друштвене одговорности за заштиту података о личности и основних људских права и слобода, потребно је подићи свест људима о значају података које деле свесно или несвесно, као и о њиховим правима уколико су она заштићена. Право на заштиту података о личности је установљено Законом о заштити података о личности. Када је овај закон донешен, успоставио се нови ситем за заштиту података о личности и постављени су темељи за даље усклађивање домаћег права са правом ЕУ у овој важној области. Али да би дошло до

имплементације закона у пуној мери, потребно је да држава настоји да утиче на подизање ниво правилног надзора над применом прописа, као и подизање свести људи.

У овом раду ће се најпре говорити о теоријском одређењу појма података о личности и њиховим врстама. Након тога, придаће се значај заштити података о личности, због тога што је то веома важна тема савременог света у коме живимо. У оквиру свега овога, потребно је посебну пажњу посветити принципима заштите података о личности, како би се они адекватно искористили, а уједно су принципи циљ и главни предмет овог мастер рада. На крају ће се говорити на тему правне регулативе у оквиру области заштите података, која је такође веома битна. Користиће се нормативни, статистички и упоредно–правни метод на основу којих ће се сагледати најважнији аспекти заштите података о личности.

Глава прва

ПОЈАМ ПОДАТАКА О ЛИЧНОСТИ

Убрзани развој информационах технологија, довео је до прикупљање огромних количина подата. Када кажемо огромна количина података, можемо рећи да су у питању милијарде података, који се првенствено прикупљају, затим складиште у великим базама података, а на крају и обрађују. С обзиром на овај компликовани процес, неретко долази до повреде и злоупотребе података о личности. Због тога је важно говорити о заштити података, као ефикасном начину у спречавању ових повреда. Али пре тога је потребно одредити појам о личности.

Када говоримо о одређивању појма података, можемо рећи да то није нимало лак задатак, с обзиром да се појам података и информације доста мешају. Подаци могу бити ЈМБГ, име и презиме, датум рођења, адреса становања, број рачуна, али и сваки други податак који нешто говори о људима. Под подацима се подразумевају симболи у облику слова или бројева или у облику аналогне или дигиталне слике или звука. Дакле подаци могу бити чињенице о нечему или некоме, могу бити део информације или статистички бројеви.

Велики број наших личних података се налази на интернету, као што су IP адреса, лозинке, наших налога за електронску пошту, друштвене мреже, историје активности са таквих налога, историје претраге интернета, итд. Иако многи дигитално генерисани подаци на први поглед не делују као подаци о личности, уз помоћ њих се неко лице може идентификовати, у неким случајевима чак и само на основу таквих података, или у комбинацији са још неким подацима.

Врло је важно направити разлику између података и информације. Правничка терминологија познаје и појам податка и појам информације, самим тим право сматра да постоји значајна разлика која изискује различито поступање и различите правне последице. Подаци представљају регистроване чињенице о неком објекту посматрања. Они сами по себи немају никакво значење. На значају податак добије тек кад се споји са још података. Више података који су међусобно повезани и имају неко значење у ствари представља информацију. Информација данас представља један од најпопуларнијих појмова. Појам информација се употребљава свакодневно у најразличитијим темама

разговора, и управо због тога многи људи говоре о информационом добу као уводу за доба знања, а за наше друштво да је информационо друштво. Поред тога, појављује се терминологија попут информационе технологије, информациона револуција, информациони системи, информатика, итд. Термин информација се употребљава свакодневно, тако да је можемо сусрети како у свакодневним разговорима, тако и у специјализованим научним подручјима. Другим речима, срећемо је у праву, у медијским извештајима, науци о рачунарству, итд. Информација може имати пуно различитих значења, али је обично тесно повезана са комуникацијом, знањем, перцепцијом и значењем. Најприближнија дефиниција информације је она представља крајњи резултат анализе података о некој појави или неком предмету.

Што се тиче дефиниције податка, најбоље одређење можемо наћи у Закону о заштити података о личности, који је настао по угледу на ГДПР. Према овом закону, податак о личности представља податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета.¹ Као што и сам назив говори, подаци о личности се односе искључиво на физичка лица, према томе то нису подаци који се односе на ентитете попут правних лица, животиња или друго.

Личност човека је означена као сложена појава и управо због тога је предмет интересовања многих научних дисциплина, а ту наравно спада и правна наука и пракса. Правни системи цене комплексност човекове личности и због тога настоје да је заштите од свих недопуштених утицаја појединца и друштва. Човекова личност се може посматрати из перспективе јавног и приватног права. Што се тиче јавног права, личност се сагледава у односу са државом и њеним органима. Зато постоје норме јавног права које штите вредности које су важне како за појединца, тако и за целокупну друштвену заједницу. Насупрот томе, личност човека се посматра из угла приватног права, што означава да појединац може самостално да тражи заштиту пред државним органима како би заштитио права и основне слободе које му припадају. Колико је човекова личност

¹Чл. 4, ст. 1, тач. 1, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

заправо важна, говори чињеница да је она своје место нашла у највишим правним актима, уставима. Тако је и случај са нашим Уставом који наглашава да је њиме зајемчено да сваки човек има право на слободан развој личности, ако тиме не угрожава права других. Са човековом личношћу су уско повезани подаци о личности, који се свакодневно употребљавају и размењују. С обзиром на уску везу, повреда човекове личности уједно представља и повреду података.

Када говоримо о теоријском одређењу, морамо нагласити да има више различитих дефиниција. Конвенција за заштиту лица у односу на аутоматску обраду података о личности из 1981. године сматра да подаци о личности представљају све информације које се односе на идентификовано лице или лице подложно идентификацији.² Затим Директива ЕУ је предвиђала да су подаци о личности свака информација која се односи на одређено или одредиво лице, при чему се одредиво лице може идентификовати непосредно или посредно, посебно помоћу идентификационог броја, или једног или више специфичних фактора који се односе на његов телесни, физиолошки, психички, економски, културни и социјални идентитет. По угледу на ову дефиницију је настало и дефинисање података о личности од стране Опште уредбе о заштити података о личности ЕУ, који је најважнији европски документ у вези са подацима о личности. УУредби, подаци о личности дефинисани су као 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 лица³. Ова дефиниција је идентична одређењу података о личности из Закона о заштити података о личности Србије. Податке које обухвата ова дефиниција су име, презиме, адреса становања, лична карта, пасош, боја косе, подаци из здравственог картона, профили на друштвених мрежама, фотографије, бројеви телефона и многи други.

²Конвенција о заштити лица у односу на аутоматску обраду података, Савет Европе, бр. 108, Стразбур, 1981.год.

³Чл. 4, ст. 1, тач. 1, Општа Уредба ЕУ.

Глава друга

ВРСТЕ ПОДАТАКА О ЛИЧНОСТИ

Према Закону о заштити података о личности, под појмом податак се подразумева податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, попут имена и идентификационог броја, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког физиолошког, генетског, менталног, економског, културног и друштвеног идентитета,⁴ док је информација дефинисана Законом о слободном приступу информацијама од јавног значаја као информација којом располаже орган јавне власти, која је настала у раду или у вези са радом органа јавне власти, а садржана у одређеном документу и односи се на све оно о чему јавност има оправдан интерес да зна.⁵ На основу изложеног изводи се закључак да је податак „једноставна необрађена чињеница која има неко значење“, док информација представља „резултат анализе и организације података на начин да даје ново знање примаоцу информације“, што даље значи да су подаци „изоловане чињенице“ које постају информације у моменту њихових коришћења и само ако су правовремено дате.⁶ Дакле, податак о личности је свака информација на основу које се може посредно или непосредно одредити идентитет неког лица. Подаци о личности представљају специфичну особину одређеног лица. Они не служе само идентификацији лица, већ представљају аспект одређене личности у правном животу који служи за остваривање разних права и интереса. Дакле подаци о личности су неопходни у великом броју правних односа, како би дошло до стварања правних последица. Користе се као средство распознавања лица, идентификациони фактор, информациони ресурс, итд. На пример, неопходни су за издавање докумената, пренос својине, електронску трговину, затим за преписивање одређене терапије, спровођење казне и још милион других ситуација. С обзиром на то да се користе у свакодневним околностима, постоји и велики број података о личности. Ту спадају име и презиме, адреса становања, број телефона, e-mail адреса, број банковног

⁴Чл. 4, ст. 1, тач. 1 Закон о заштити података о личности („Сл. гласник РС“, бр.87/2018).

⁵Чл. 2, ст. 1, Закон о слободном приступу информацијама од јавног значаја, (Сл. гласник РС, 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021).

⁶Јовановић З., Андоновић С., *Врсте информација и података у јавном праву Републике Србије*, зборник радова „Заштита података о личности у Србији“, Београд 2020, стр. 40.

рачуна, подаци о запослењу лица, вероисповест, пол, национална припадност, политичка опредељеност и још много њих.

Будући да постоји велики број подата о личности, можемо претпоставити да се они могу разврстати на различите начине. Разлика се може правити између података у личној, историјској, финансијској, јавној и друштвеној сфери живота појединца.⁷ Међутим ова подела се може упростити, тако да податке о личности групишемо у три најосновније области живота, а то су приватна, јавна и професионална област. Сваки човек понаособ има своју личну сферу коју чува само за себе и не дели са другим људима, затим јавну сферу која није тајна и коју обично познају остали појединци или сви они коју су за то заинтересовани и последњу, професионалну сферу у коју се убрајају подаци у вези са пословним активностима одређеног лица. Све ове три области су неретко међусобно повезане, тако да лични подаци који се употребљавају у једној области друштвеног живота, имају велики значај и у остале две области.

1. Подаци који се односе на лични, јавни и професионални живот човека

Постоје подаци који се односе на лични, јавни и професионални живот човека, где спадају:

- психо-физички елементи лица (године живота, физичке и психичке карактеристике као што су висина, тежина, боја очију, облик тела, развијеност, итд.)
- лични ставови и наклоност према стварима, лицима и појавама (омиљено јело, омиљени филм, омиљена књига, итд.)
- историја о личном животу (подаци о дешавањима у животу одређеног лица и са њиме повезаним лицима)
- уверења и мишљења (религијска уверења, филозофска уверења, лична мишљења у вези са одређеном темом, итд.).

Што се тиче личних података који се односе на лични живот човека, осим горе наведених, могу се навести и други идентификациони подаци личне природе, као што су

⁷Enterprivacy Consulting Group, „Categories of PersonalInformation“, online 2017, <https://enterprivacy.com/2017/03/01/categories-of-personal-information>.

подаци о етничком и социјалном пореклу (раса, језик, национална и етничка припадност, и др.), подаци о сексуалности (родна припадност, сексуална наклоност, и др.), медицински подаци и подаци о здрављу (физичка и психичка зрелост и здравље, физички и психички недостаци, крвна група, здравствени картон, и др.).

Такође, ту су подаци о личности који се односе на јавни живот човека су они подаци који се односе на аспекте живота појединца који су познати широј јавности, где спадају:

- подаци о породичном животу (породица појединца, чланови те породице, односи у породици, итд.)
- подаци о социјалном окружењу (пријатељи, конекције, припадност у формалним и неформалним организацијама, итд.)
- подаци о криминалној прошлости појединца (да ли је био у затвору, да ли се води неки поступак против њега, итд.)

Следећа група личних података се односи на професионалну област појединца фокусирају се на друштвене активности лица у вези са радом и обављањем професионалних делатности. У ову групу спадају следећи подаци:

- подаци о образовању (школа или факултет који је лице завршило, ако је завршило, оцене, курсеви, итд.)
- пословни подаци (да ли лице ради, и ако да на ком радном месту, затим подаци о одсуству са посла, оцена његовог рада, итд.)
- финансијски подаци (подаци о имовини коју поседује лице, број банковног рачуна, кредитни статус, итд.)
- радна историја (подаци о фирмама у којој је радило лице, подаци о запосленима у фирми тог лица, подаци о новчаним примањима и транскацијама, итд.)

За све горе наведене врсте података се може рећи да су некад доступни само лицу на кога се односе, док су у неким ситуацијама доступни и широј друштвеној заједници.

2. Подаци о личности који не уживају правну заштиту

Када говоримо о подацима о личности који не уживају правну заштиту, можемо их посматрати из две перспективе: у правном систему Србије и у праву Европске Уније.

Иако механизам заштите података о личности тежи да обухвати што више личних података како би се заштитио што већи део приватности и личности човека, ипак постоје и подаци који остају изван опсега заштите. У правном систему Србије, у ову групу података спадају они подаци који се обрађују од стране физичких лица за личне потребе или потребе њиховог домаћинства.⁸ Када се обрађују подаци о личности у личне и породичне сврхе, физичко лице на које се односе ти подаци и које врши обраду, мора само водити рачуна о безбедности те обраде. Ови подаци су у ствари и једини подаци којима је онемогућена заштита на основу Закона о заштити података о личности. Закон о заштити података о личности из 2008.године је подразумевао знатно више података о личности који не уживају правну заштиту. Ту су спадали:

- подаци који су доступни свакоме и објављени у јавним гласилима и публикацијама или приступачни у музејима, архивима итд. Ту спадају подаци у писаним документима, фотографије, аудио записи, итд.;
- подаци који се обрађују у породичне и друге личне потребе, као што су албум са породичним сликама, телефонски именик, итд.;
- подаци о члановима политичких странака, удружења, синдиката и других облика удруживања и ту припадају подаци о члановима групе, начин обављања делатности у групи, итд.;
- подаци које је лице које је способно да се само стара о својим интересима објавило о себи. Овде се ради о фотографијама, аудио записима и писаним објавама које је лице објавило на друштвеним мрежама.⁹

За разлику од Закона из 2008.године, Закон о заштити података о личности из 2018.године предвиђа само једну групу података која не ужива правну заштиту и на тај начин се повећава ниво заштите података, јер је већина њих унутар зоне заштите.

У правном систему заштите података ЕУ такође постоје одређени лични подаци који остају изван оквира заштите података. Ту спадају следеће групе података:

⁸Андоновић, С., Прља, Д., *Основи права заштите података о личности*, Институт за упоредно право, Београд, 2020.година, стр.21.

⁹Чл. 5,ст. 1, Закон о заштити података о личности, („Сл. гласник РС“ 97/08, 104/09-др.закон, 68/12-одлука УС и 107/12).

- подаци који се обрађују у оквиру делатности која није обухваћена подручјем примене права Уније, дакле ради се о обради личних података која се одвија у државама које нису чланице ЕУ, као и у међународним организацијама које нису повезане са ЕУ;
- подаци које државе чланице ЕУ обрађују приликом објављивања активности које су обухваћене подручјем примене поглавља 5. Дела Уговора о ЕУ. У овом делу се регулишу питања као што су заједничка трговинска политике држава чланица, сарадња са трећим државама, међународни споразуми, итд.;
- подаци које обрађује физичко лице за искључиво личне или породичне активности. У овим ситуацијама држава не реагује, јер не постоји потреба за деловањем у строго личну сферу лица;
- подаци које обрађују надлежни органи у сврху спречавања истраге, откривања или гоњења учиниоца кривичних дела или извршења кривичног дела, јер се са оваквим подацима поступа на основу посебних прописа;
- подаци који се односе на лица која нису жива.¹⁰

3. Посебне категорије података о личности

Као и претходна група података, и ова се може посматрати из угла правног система Србије и права ЕУ.

Посебне категорије личних података постоје и у праву Републике Србије. Податке које се односе на расно или етничко порекло, верско уверење, филозофско уверење, политичко мишљење, чланство у синдикату, генетске и биометријске податке, као и податке о здравственом стању, сексуалном животу или сексуалној оријентацији, Закон третира као посебне врсте података о личности. У питању су дакле подаци који су нарочито осетљиви и чија обрада захтева виши степен пажње у односу на остале податке. Повреда или злоупотреба ових података може довести до настанка негативних последица по физичко лице на које се односе. Закон о заштити података о личности из 2018. године предвиђа следеће посебне податке који се не смеју обрађивати, осим у одређеним условима:

- расно и етничко порекло,

¹⁰Чл. 2, ст. 2, Општа Уредба ЕУ.

- политичкомишљење,
- верско и филозофскоуверење,
- чланство у синдикату,
- генетскеподатке,
- биометријскеподатке,
- податке о здравственомстању,
- податке о сексуалном животу и сексуалној оријентацији лица.¹¹

За разлику од закона који је тренутно на снази, Закон о заштити података је подразумевао дужу листу посебних података, па је поред горе набројаних података, у ову групу су спадали и: пол, језик, припадност одређеној политичкој странци, подаци о примању социјалне помоћи, подаци о жртвама насиља и подаци о осуди за учињено кривично дело.

Основна идеја законодавца је да као основно правило успостави забрану обраде посебних врста података о личности, али да у исто време предвиди изузетке у којима је обрада оваквих података допуштена. Приликом обраде ових података потребно је пре свега применити начело минимизације података, односно да се обрада сведе на минимум који је довољан да се оствари сврха обраде. Као што је већ наведено ови подаци се ипак обрађују у одређеним условима, јер да није тако, правни систем не би могао нормално да функционише и друштвени токови би били успорени. Обрада посебних категорија података се може вршити када на то пристану лица о чијим подацима је реч. Поједине посебне врсте података могу обрађивати различите организације попут удружења, фондација и задужбина, али само у сврху функционисања организације. Судски органи исто могу вршити обраду ових података када поступају у пословима из своје надлежности. Управни органи могу вршити обраду посебних категорија података када постоји потреба за остваривањем „значајног јавног интереса“.¹² Веома је важно навести да се обрада посебних категорија података може предузети ради остваривања превентивних дужности у медицини или медицини рада, а у циљу оцењивања радне способности тренутно запослених и будућих запослених. Могућност обраде ових података у сврхе архивирања у јавном интересу, научног или историјског истраживања и у статистичке сврхе је

¹¹Чл. 17, ст. 1, Закона о заштити података о личности („Сл. гласник РС“, бр.87/2018).

¹²Андоновић, С., Прља, Д., *Основи права заштите података о личности*, оп. cit. стр.26.

постављена превише широко и дозвољава релативно лак приступ овој категорији података.¹³ Изузетак од поштовања правила обраде посебних врста података о личности који се примењују на обраду коју надлежни органи врше у посебне сврхе, указује да постоје прилике када је сврха обраде претежнија од заштите посебних података о личности, у овом случају ради откривања, спречавања и кажњавања за кривична дела, односно претњи по јавну и националну безбедност.

Посебна категорија података о личности у праву Европске Уније се дефинишу као подаци који су по својој природи посебно осетљиви у погледу основних права и слободе и заслужују посебну заштиту, зато што би њиховом обрадом дошло до ризика за основна права и слободе. Општа Уредба ЕУ као најважнији документ у области заштите података о личности познаје ову категорију података. Уредба у ове податке убраја етничко и расно порекло, политичко опредељење, верска и филозофска убеђења, припадност синдикату, обраду генетских и биометријских података, здравствено стање, сексуални живот и сексуалну оријентацију личности.¹⁴ Као и у нашем закону, и у ЕУ је забрањена обрада ових података, осим у одређеним ситуацијама. Дакле прво је група ситуација која дозвољава обраду ових података уколико постоји изричит пристанак појединца чији се подаци обрађују, кад је потребно обрадити их ради заштите животних интереса и када је такве податке објавили лице на кога се подаци и односе. Друга група ситуација обухвата обраду у ситуацијама као што су запошљавање, остваривање права из социјалне заштите и осигурања, као и обраду коју извршавају фондације или удружења, када је то усмерено на податке њихових чланова. Приликом обраде обих податке посебна пажња се мора посветити заштити људских права у вези са оваквом обрадом обрадама, при чему морају имати у виду право ЕУ и право државе чланице.

4. Базе података о личности и bigdata

Милиони података се прикупљају свакодневно и користе се у различите сврхе. Њих прикупљају како приватна и правна лица, тако и државни органи. Прикупљање великог броја личних података стварају се организовани скупови личних података, односно базе података. База података је скуп, односно колекција података који су организовани тако да

¹³Чл. 17, ст. 2, тач. 10, Закона о заштити података о личности („Сл. гласник РС“, бр.87/2018).

¹⁴Чл. 9, ст. 1, Општа Уредба ЕУ.

је кориснику обезбеђен првенствено брз приступ подацима, а затим и њихово брзо претраживање. Као што је наведено, база података представља организован скуп података, дакле није довољно само прикупити податке, већ и систематизовати их и чувати по одређеном образцу. Подаци могу бити различитог типа: текстуални, нумерички, слике, аудио и видео записи итд. Подаци су представљени на униформни начин, што олакшава приступ и коришћење од стране екстерних програма. Тако једну базу података може користити низ различитих програма, писаних у разноврсним програмским језицима. Базе података и технологија база података имају велики утицај на растућу употребу рачунара. Поштено је рећи да базе података играју кључну улогу у скоро свим областима у којима се користе рачунари, укључујући пословање, електронску трговину, инжењерство, медицину, генетику, права, образовање и библиотекарство.¹⁵ Важно је нагласити да без база података, информациони системи се не могу ни замислити.

С обзиром на то да Закон о заштити података о личности не уређује ближе начин на који је потребно управљати базама података, потребно је нагласити да њихово управљање треба да буде уређено законом или неким другим подзаконским актом. Управљање базама података представља један од предмета уређења Закона о информационом систему Републике Србије.¹⁶ Овај закон уређује начин поступања управних органа приликом вођења евиденција и управљања подацима у вези са информационом системом Републике Србије. Такође и Закон о електронској управи одређује базе података као уређен и организован скуп међусобно повезаних структурираних података који може имати једну или више евиденција.¹⁷ Закон о информационом систему такође познаје и категорију заједничке базе података које представљају електронску магистралу којој се може приступити под одређеним условима ради преузимања појединог податка. Важно је напоменути да управни органи морају да воде и алтернативне базе података које омогућавају константан рад, уколико се јаве проблеми на примарној бази податка.

Што се тиче функције база података, оне смањују појаву дупликата, повећава поузданост података, обезбеђују интегритет података при вршењу више трансакција и стварају независност података од софтвера. База података се може генерисати и

¹⁵Ramez Elsmari, Shamkant Navathe, Fundamentals of Database Systems, Addison-Wesely Publishing Company, Boston – Columbus – ets. 2010, p.4.

¹⁶Закон о информационом систему Републике Србије, („Сл.Гласник РС“, бр. 12/1996).

¹⁷Чл. 4, ст. 1, тач. 1 Закона о електронској управи, („Сл. Гласник РС“, бр. 27/2018).

одржавати ручно или може бити компјутеризована.¹⁸Због тога што се у великој мери примењују у различитим областима, као што су здравство, култура, образовање, итд., базе података представљају средство који помаже развоју државе и друштва. Разноврсне базе података могу помоћи у решавању спорних и неспорних ситуација друштва и грађана, што може бити од значаја за убрзање управног поступка. Такође оне служе органима да брже и ефикасније обављају своје делатности било да је у питању јавни или приватни интерес. Подаци о личности и базе података о личности посебно добијају на значају и практичној примени садејству са информационо-комуникационим технологијама.¹⁹То је нарочито важно када се говори о иновативној области великих база података у којој се све више улаже и све се више развија, а то је *bigdata*.

Са појавом рачунара, у информатичком добу, поготово коришћењем интернета, прилив података је постао вишеструко већи. Корисници интернета остављају са собом драгоцене податке сваком акцијом коју обаве на интернету. Међутим, та количина података била би неупотребљива без истовременог развоја већих складишних капацитета, процесорске снаге и софтвера за обраду тих података, која се одиграла истовремено са појавом и развојем највећих претраживача и друштвених мрежа. *Bigdata* не представља јединствену технологију, већ мешавину старих и нових технологија, који омогућавају обраду огромне количине података која није могућа обичним анализама. Instagram, Facebook, online куповина, претраживање на Google-у, итд. се у свакој секунди пуне новим информацијама. Проблем не настају у прикупљању информација, већ у њиховом смештању и анализирању. Данас напokon, имамо све предуслове за анализу података и самим тим ти подаци добијају већу вредност. Ти предуслови су: могућност складиштења, брзи процесори, cloud технологије, итд. Дакле подаци имају вредност тек када се помоћу њих дође до корисних закључака. Ово нема вредност само у комерцијалнох индустрији већ и здравству, метеорологију, астрономију, очувању животне средине, итд.

Bigdata је појам који означава велике и комплексне сетове података, код којих традиционалне апликације за обраду података нису применљиве. Те скупове података карактеришу разноврсност формата, велике брзине обраде и приступа, и велики обим

¹⁸Ramez Elsmari, Shamkant Navathe, Fundamentals of Database Systems, Addison-Wesely Publishing Company, Boston – Columbus – ets. 2010, p.5.

¹⁹Андоновић, С., Прља, Д., *Основи права заштите података о личности*, op. cit. стр.31.

информација.²⁰ Дакле *bigdata* су у ствари велике базе података, које су повезане коришћењем информационо-комуникационим мрежама. Користи се као средство ефикаснијег доношења пословних и државних одлука, унапређења стручних поступака и за предвиђање понашања субјекта на које се подаци из базе односе. Главна карактеристика *bigdata* је то што садржи различитост садржаја и подаци могу бити у различитим облицима, као што су текст, звук и слике. Систематска повезаност између ових података омогућава велику брзину у њиховој размени и приступу.

²⁰ Раденковић, Б. Деспотовић – Зракић, М. Богдановић, З. Бараћ, Д. Лабус, А. *Електронско пословање*, Факултет организационих наука, Београд, 2015, стр.278.

Глава трећа

ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ

У околностима у којима живимо данас (модерно доба), омогућено је да се значајно повећа количина прикупљених података о свакој особи на планети земљу. Ту можемо сврстати најразличитије врсте података, па чак и оне додатне податке за које никада не бисмо помислили да су прикупљени. Често се догађа да нисмо ни свесни да се подаци о нама негде воде или да они уопште постоје. Коју је књигу особа прочитала, где се преселила, која јој је омиљена песма, где иде на море су само пар од многих података који се могу прикупити о тој одређеној особи. Дакле постоји много ситуација у којима се користе подаци о личности и због тога се за њих каже да су једни од најбитнијих чиниоца савремене привреде и нужан сегмент комуникације у 21.веку.

Податке о личности користе грађани, привредни субјекти, органи јавне власти и међународне организације, дакле сви субјекти који учествују у правном и пословном промету.²¹ Међутим важно је навести да се коришћењем података отварају многе могућности за прогрес модерног друштва, али исто тако и отварају врата многим опасностима. Податке о личности све више злоупотребљавају многе институције и појединци. Потребно је нагласити да нема безопасних података. Сваки, па чак и неки најбезначајнији податак, може представљати потенцијалну претњу за физичка лица, јер се могу користити у најразличитије сврхе, које на први поглед не можемо ни замислити. Свакодневно расту начини њиховог прикупљања, складиштења, обраде и коришћења, као и круг субјеката о којима се подаци прикупљају. Томе нарочито погодује развој информационих технологија. У савременом добу, већина људи оставља информациони траг своје комуникације са најразличитијим државним органима, јавним институцијама и недржавним организацијама. Излагање опасности је нпр. куповина путем интернета где се плаћа кредитном картицом, али под тим спада чак и само претраживање на интернету. Иако ово изгледа безазлено, многи претраживачи складиште податке о појединцима, како

²¹Андоновић, С., Прља, Д., *Основи права заштите података о личности*, оп. cit. стр. 33.

би napravili њихов профил и сазнали њихове куповне склоности. Дакле приватност је оно што је највише угрожено. Углавном су жртве злоупотребе података о личности:

- појединци као корисници интернета телекомуникационог сектора, дигиталних услуга, онлајн услуга, web страница,
- појединци – потрошачи
- малолетници и
- „обичнипојединци“ о којима се стварају базе података о личности.

Заштита података о личности је један од најбитнијих и најизазовнијих проблема са којима се суочава савремено доба. Злоупотреба личних података је њихово коришћење у недозвољене сврхе, односно сваки догађај везан за податке због којих је субјекат претрпео или могао да претрпи губитак. Управо због овога је у последњих година појачана правна регулатива у области заштите података о личности.

1. Правни режими заштите података о личности

Заштита података о личности је тема која у свету у коме живимо, привлачи доста пажње. Она је постала нужан део наше свакодневнице, како би могли колико толико да живимо безбедно у дигитално оријентисаном свету. Као што је већ горе пар пута наведено, подацима о личности прети повреда и злоупотреба приликом њиховом обрађивања и складиштења. У последње две деценије дошло је до значајног развоја интернета, прекомерног коришћења друштвених мрежа и других видова комуникације. Пре појаве информационо-комуникационих технологија, лични подаци нису имали превелики значај. Међутим, данас се то све променило. Лични подаци се осим за легитимне сврхе, користе и у сврху проучавања понашања корисника, за посматрање и разумевање понашања људи, па чак и њихово прислушкивање, праћење и много друге активности. Због тога је потребно говорити о заштити података о личности, а самим тим и о заштити људских права и основних слобода.

Заштита податка о личности је скуп међусобно повезаних активности, метода, техника и норми којима се обезбеђује приватност, сигурност, поверљивост,

расположивост и интегритет података од свих опасности које им прете.²²За заштиту података о личности се може рећи да је законски механизам који обезбеђује приватност појединаца. Приватност је основно људско право, које представља право сваког човека да контролише своје личне информације и да одлучује о њима. Право човека на заштиту личних података је праћено обавезама других да поштују то право. Ово право није апсолутно, јер може бити нарушено у специјалним условима, нпр. уколико је то прописано законом или уколико то захтевају интереси јавног поретка.

Заштита података о личности представља комплексно право јер је сачињено од више мањих права:

- право на обавештеност
- право на одговарајуће коришћење података
- право приступа и увида
- право на исправку података
- право на правна средства заштите.

Заштита личних података је уоквирена Законом о заштити података о личности из 2018.године. Овим законом уређује се право на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, кодекс поступања, пренос података о личности у друге државе и међународне организације, надзор над спровођењем овог закона, правна средства, одговорност и казне у случају повреде права физичких лица у вези са повредом података о личности као и посебни случајеви обраде. Овим законом се уређује и право на заштиту физичких лица у вези са обрадом података о личности коју врше надлежни органи у сврху спречавања, истраге и откривања кривичних дела, гоњења учиниоца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности, као и слободан проток таквих податка.²³

Правна норма је правило о понашању које прописује држава и за њихово непоштовање прописује санкције. Правне норме се могу схватити као најпростији елементи права који

²²Дракулић, М. *Основи компјутерског права*, Друштво операционих истраживача Југославије – ДОПИС, Београд, 1996, стр. 56.

²³Чл. 1, ст. 2, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

се не могу разложити на простије правне елементе. Њих не треба изједначавати са одређеним члановима закона или неког правног акта, јер се изузетно може десити да се правна норма поклопи са неким таквим чланом. Један члан садржи или део једне или више норми, а ретко потпуну правну норму. Што се тиче правног система заштите података о личности, њихов основни елемент јесу управо правне норме. Ту се оне односе на регулисање, усмеравање, координацију и обликовање људског понашања. Циљ правних норми јесте успостављање кохерентног и ефикасног система у коме се смањује могућност злоупотребе података и ризик од непрописане и незаконите употребе података.²⁴ Успостављањем оваквог система се штите грађани, њихова права, интереси и слободе. Такође правне норме омогућавају сигурност грађана у односу према држави и њеним органима. Осим правних норми, могу се навести и моралне, техничке, организационе и друге врсте норми. Правне норме се разликују од осталих по томе што само оне имају правно дејство које се остварује кроз правно релевантне последице у виду обавеза и права. Остале врсте норми могу имати само посредни ефекат, док правне норме делују директно кроз војску, полицију, извршитеље, итд.

2. Повесни развој заштите података о личности

Кроз историју, систем заштите од података се развијао постепено. Прво је кренуло са успостављањем права на приватност и развојем права на поштовање приватног живота. Потом су се широм Европе доносила правна документа од великог значаја и дошло је до усвајања појединачних законодавних аката којима се ове категорије штите и дефинишу. На овај начин је дошло до стварања мреже правне заштите података о личности, која се даље развија успостављањем и развијањем правних институција и механизма за њено остварење.

Право на приватност једно је од универзалних људских права утврђених у Универзалној декларацији о људским правима усвојеној у Паризу 1948. године.²⁵ У Декларацији се наводи да нико не сме бити подвргнут произвољном мешању у његов

²⁴Андоновић, С., Прља, Д., Основи права заштите података о личности, *op. cit.* стр.34.

²⁵Универзална декларација Уједињених нација о људским правима, Организација Уједињених Нација 217 (ИИИ), од 10. децембра 1948. године, Париз.

приватни живот, породицу, стан или преписку, нити нападима на његову част и углед, као и да свако има право на заштиту закона од таквог мешања или напада.²⁶ Потписници Декларације дужни су да у свом свакодневном животу обезбеде овако постављена права. Ово право није апсолутног карактера, али, као што је предвиђено у самом члану, пружа заштиту од произвољног мешања других. То значи да физичка и правна лица, а посебно државни органи, могу да се мешају у права појединаца, али само ако је то мешање засновано на прописима и, што је још важније, приватним или јавним интересима.

Након Универзалне декларације, усвојен је један од најзначајнијих докумената данашњице – Европска конвенција за заштиту људских права основних слобода. Ова конвенција је усвојена од стране Савета Европе и ступила је на снагу 1953. године.²⁷ На овај начин је дошло до стварања Европског суда за људска права који је допринео успостављању богате праксе на коју се данас ослањамо и када је реч о праву на приватност, и када је реч о заштити података о личности уопште. Друга права су се развила из права на приватност, укључујући право на поштовање приватног живота и право на заштиту личних података. Ова права спадају у категорију универзалних људских права и најосновнија су грађанска и политичка права. Заснована су на принципу слободе и регулишу однос између државе и појединца. Они гарантују људско достојанство и штите најприватније области живота сваке особе. У ствари, они су заштићени чл. 8 Европске конвенције које каже да свако има право на поштовање свог приватног и породичног живота, дома и преписке. Важна компонента ова четири права, која уједно представљају независна права, јесте право на заштиту података о личности, јер уколико лични подаци појединца нису заштићени у оквиру сваког од тих права, ни ова права неће бити заштићена.²⁸ Наведеним чланом је предвиђено да јавна власт не може да се меша у вршење овог права. Изузетак је само у случају ако је мешање јавне власти предвиђено законом и ако то представља неопходну меру у деморатском друштву у циљу заштите интереса националне безбедности, јавне сигурности, економске добробити, спречавања нереда или спречавања злочина, заштите здравља и морала или заштите права и слободе других. Када је реч о праву на заштиту података о личности, оно није наведено као

²⁶Члан 12, *ibid.*

²⁷ Конвенција Савета Европе о заштити људских права и основних слобода, Рим, 1950.

²⁸Гасми Г., Прља Д., *Право на поштовање приватног живота и право на заштиту података о личности*, зборник радова „Заштита података о личности“, Београд, 2020, стр. 7.

основно људско право, нити се наводи као посебно гарантовано право у претходно поменутих међународним правним актима. Међутим, када је реч о праву на поштовање приватног живота, подаци о личности се морају штитити.

Право на заштиту података о личности је касније било одвојено од права на поштовање приватног живота и развило се као посебно људско право. Право на заштиту личних података и право на поштовање приватног живота су уско повезана права која штите међусобно повезане вредности, слободу, људско достојанство и личну аутономију, омогућавајући појединцима да развију своје области личности. Ова два права су неопходни предуслови за остваривање других основних људских права, као што су слобода изражавања, слобода удруживања, слобода вероисповести итд. Ова два права, иако слична, разликују се по свом тексту и обиму. Право на поштовање приватног живота укључује општу забрану мешања, као и одређене стандарде јавног интереса који могу оправдати мешање у одређеним околностима. Заштита личних података се посматра као модерно и активно право, успостављање система провере и равнотеже ради заштите појединаца када се њихови лични подаци обрађују. Обрада у том случају мора бити у складу са основним компонентама заштите личних података, односно независним надзором и поштовањем права субјекта података.

Међународна документа у којима је предвиђена заштита података на приватност, али и сва друга права која из њега произилазе су усвојена пре саме појаве интернета и развоја информационог друштва. Иако је развој информационог друштва и интернета донео значајне олакшице свакодневном животу, ипак је са друге стране донео нове ризике за право на поштовање приватног живота и заштиту података о личности. Све то је довело до потребе за усвајањем посебног законодавства које треба да обезбеди да се подаци о личности штите на поуздан начин.

Глава четврта

ПРИНЦИПИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ

Да бисмо лакше објаснили значај принципа заштите података о личности, потребно је првенствено говорити о правним принципима. Колевка правних принципа јесте римско право и они су доста допринели конституисању савремених европских правних система, као и уобличавању доктрине о владавини права уопште. Међутим у нашој правној књижевности се правним принципима одузима самостални карактер и због тога је ниво њихове заступљености у правној књижевности и судској јуриспруденцији низак. Управо због тога је потребно посветити пажњу излагању аргумената који могу доказати самосталност правног карактера правних принципа, али и направити разлику између правних нормих и правних принципа.

Док се правне норме могу дефинисати као правила понашања која уређују одређене односе међу људима, која су обезбеђена државном принудом, правни принципи су зрачећи телеолошки правни ставови који изражавају основне правне идеје. Они усмеравају правну свест и надахњују основ правног уређивања у поретку правне државе и на тај начин, они усмеравају правни основ правних норми и активности субјеката правног поретка. Правни принципи у ствари представљају градивне законе и области правног поретка. У том смислу, правни принципи би требало да изразе „правну перспективу објективног духа“ и да усмере правну свест у правном поретку. Такође, правни принципи су један од критеријума на којем почивају велики правни системи као резултат сагледавања упоредног права. Они следе кружну линију функционисања правног поретка, опредељену комплентарношћу институционалног поретка јавне власти, институционалног поретка државне власти и институционалног поретка просторне заједнице. Правни принципи имају општи правни карактер, при чему систематско-телеолошка конкретизација писаног права исходује да се правни принципи развијају као снопови општих и конкретизованих телеолошких правних ставова. Потребно је навести да на правним принципима почивају:

1. уставноправни систем – утемељен на Уставу у формално смислу и уставности чија се садржина обликује и развија ауторитетом систематско-телеолошке интерпретације уставног судства;

2. системи регулативних правних ставова у различитим областима правног поретка (грађанскоправни, управноправни, кривичноправни, итд.)

3. “унутрашњи правни систем” заснован на правним облицима.

У погледу уређивања правних предмета, правни принципи не делују у правном смислу једнако у свим областима правног поретка. Најзаступљеније дејство правних принципа постоји код грађанског права, због слободне воље код правотворачког извора и широке заступљености правних стандарда као регулативних правних ставова, и због тога судови испитују њихово дејство на правне принципе грађанског права. Правни принципи директно делују у областима правног поретка где владају императивне законске норме. То су управноправна и кривичноправна област. Метафору обесмишљавања правних принципа уопште, можемо исказати као људска права без слободе, страначка представничка демократије без демократског друштва и владавина закона без владавине права. Одавде потиче потреба за већом употребом правних принципа у поретку савремене правне државе, у формално-правном и историјско-политичком смислу.

Свака грана права заснива се на принципима, који представљају изворе из којих произилазе одређена правила понашања. Принципи се обично одређују као начела, који су у ствари најмањи заједнички именитељ смисла свих норми неког закона или гране праве, па самим тим могу да се употребе за изналажење смисла било које норме.²⁹

С обзиром на то да је заштита података о личности посебна грана права, она такође садржи принципе на којима је заснован целокупни систем. Обрада личних података је глобализован процес који захтева увођење и развој универзалних принципа физичких лица у погледу њихових личних података обрада. Тема која се тиче принципа заштите података о личности су од великог интереса како за теорију, тако и за праксу. Принципи заштите података о личности последњих година добијају све већи значај и признање, јер готово да не постоји сфера у савременом друштвеном, економском, јавном и политичком животу која не захтева обављање послова који се односе на обраду и коришћење личних

²⁹Вуковић, М. *Интерпретација правних прописа*, Школска књига, Загреб 1953, стр.128.

података, као и могућност приступа тим подацима. Принципи заштите података о личности која се успостављена новом европском регулативом, а самим тим се налазе и у Закон о заштити података о личности Србије, имају вишеструки значај. Првенствено се начелима за заштиту података о личности усмерава тумачење конкретних одредби, који могу бити неразумљиве. Они важе за све руковоаце и односе се на све радње обраде података, због чега њихово добро познавање није само по себи циљ. Њихова основна сврха је одржавање релевантне контроле над приватним подацима који се односе на идентификацију одређеног физичког лица. Имају посебан значај јер представљају основу за правилно тумачење и примену Уредбе, као и упутства за руковоаце приликом обраде личних података. Због тога је кључ за поштовање Закона управо придржавање ових принципа. Важно је навести да руковоаци и обрађивачи могу прекршајно одговарати због непоштовања неког од ових принципа. Кршење начела личних података са собом повлачи и најтеже казне. Према домаћем закону, казна за појединачни прекршај којим се крши неко од начела износи 2 милиона динара, док у стицају казна може бити и дупло већа. Према Општој Уредби ЕУ, за кршење ових начела може се изрећи казна у висини од 20 милиона евра или 4% укупног годишњег прихода, шта год је веће.³⁰

Начела заштите података о личности се означавају и као „принципи квалитетних података“ Код ових начела, фокус је стављен на акутелне и модернизоване основе заштите података као гаранција за бољу контролу и безбедност података физичког лица у савременом дигиталном свету.³¹ Што се тиче ових принципа, може се рећи да је у питању итекако млада област и непрекидно се мења под утицајем развоја информационо-комуникационих технологија. Управо због тога је веома важно поставити принципе коју су непролазни и не зависе од развоја технологије, будући да они постављају основе на којима се заснива заштита права грађана. Начела помажу тумачима (независно да ли се ради о физичком лицу, правном лицу или неком органу власти)у тумачењу неразумљивих и непотпуних норми, попуњавању правних празнина и решавају сложене практичне ситуације.

³⁰Кривокапић Д., *Водич кроз закон о заштити података о личности и ГДПР – тумачење новог правног оквира*, Београд: Мисија ОЕБС-а у Србији и Share Фондација, 2019, стр.33.

³¹Stoyanova Z. Principles of personal data protection, University of Economics, Audit 2 (2022), Vol.28,p.95.

Принципи, тачније, начела заштите података о личности, су већином истоветна у различитим државама и правним системима. Начела су у највећој мери иста у праву Републике Србије и ЕУ. Основна начела заштите података о личности су:

1. Начело законитости, поштења и транспарентности;
2. Начело ограничења у односу на сврху обраде;
3. Начело минимизације података о личности;
4. Начело потпуности и тачности;
5. Начело ограниченог чувања података о личности;
6. Начело интегритета и поверљивости;
7. Начело одговорности руковооца за поступање у вези са подацима о личности.

1. Начело законитости, поштења и транспарентности

Прво начело које предвиђа Општа Уредба ЕУ, али и наш Закон о заштити података о личности јесте начело законитости, поштења и транспарентности. То у глобалу значи да на првом месту увек мора постојати законски основ за обраду података о личности, да никада не треба користити такве податке на начин који може имати неоправдане последице по заинтересована лица и да је потребно доставити информације о правном основу обраде података. Улога овог начела је од кључне важности за функционисање читавог правног система, јер потиче од принципа владавине права и правне државе. Подаци о личности морају се обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе („законитост, поштење и транспарентност“)³². Ово конкретно значе следеће:

- подаци се могу обрађивати само уз постојање правног основа за обраду и уз поштовање свих прописа за обраду;
- руковооци и обрађивачи се морају понашати поштено у конкретним околностима, зависно од тога чије податке прикупљају;
- од тренутка када почне прикупљање, лице чији се подаци прикупљају и обрађују има право да зна како се са њима поступа.

³²Чл. 5, ст. 1, тач. 1, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

Сама формулација овог начела показује да се оно састоји из три засебних али међусобно повезаних делова.

Начело законитости је основни елемент сваког правног система. Основна улога начела законитости је осигуравање законите примене норми у вези са заштитом података о личности. Законитост усмерава сваку обраду података о личности тако да буде заснована на одговарајућој законској или другој општој правној норми. Податке је потребно обрађивати на основу следећих законских услова:

1. када постоји сагласност физичког лица;
2. извршавање уговорних споразума у којима је субјект података страна;
3. за поштовање законске обавезе којој руковаоц подлеже;
4. обрада је неопходна за заштиту виталних интереса субјекта података;
5. за обављање задатака који се обавља у јавном интересу или у вршењу службених овлашћења трећег лица коме се подаци откривају;
6. за сврхе легитимних интереса, осим када над таквим интересима имају предности интереси или основна права и слободе субјекта чији се подаци обрађују.

Обрада података о личности је законита када постоји сагласност физичког лица чији се подаци обрађују. Сагласност тј. пристанак физичког лица се одређује као свако добровољно, одређено, информисано и недвосмислено изражавање воље којим то лице, изјавом или јасном потврдом радњом, даје пристанак за обраду података о личности које се на њега односе³³. Што се тиче давања пристанка, наш Закон о заштити података не садржи одређену одредбу о формама у којима се пристанак може дати, мада због каснијег коришћења доказа, пожељно је да буде у писаном или електронском облику. У неким случајевима, могуће је дати пристанак и конклюдентним радњама, које представљају посредно изјављивање воље.

Како би се осигурала безбедност и убрзао пословни промет, сматра се законитом она обрада података која је неопходна за извршење уговора или предузимање радњи које воде закључавању уговора. Важно је навести да је законита она одредба података о личности која је неопходна у циљу поштовања правних обавеза руковаоца. У неким ситуацијама, дужност руковаоца је да достави податке о личности органу јавне власти или другом лицу.

³³Чл. 4, ст. 1, тач. 12, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

Ово је потребно поштовати ради нормалног и ефикасног одвијања друштвених, правних и привредних токова.

Лични подаци могу носити информацију о некој околности или чињеници која може спасити живот одређеног лица. Обрада личних података има законит карактер када је потребна за заштиту важног интереса лица на које се подаци односе или другог физичког лица. Нужан услов је угроженост животу важног интереса физичких лица.

Органи јавне власти, под којима спадају сви иамоци јавних овлашћења који одлучују о стањима грађана, обављају доста послова који се односе на лична стања грађана. С тим у вези, они имају потребу да приступе одређеним личним подацима како би се решила одређена животна ситуација, као што су утврђивање права, обавезе и интереси грађана. Законита је обрада података о личности која је неопходна у циљу остваривања легитимних интереса руковооца или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се подаци односе, а посебно ако је лице на које се подаци односе малолетно лице³⁴.

Начело законитости се може сагледати из неколико угла. У најширем смислу, оно означава сагласност свих аката са законом као највишим актом. У нешто ужем смислу, односи се на то да сви правни акти и материјалне радње које предузимају државни органи и грађани, морају бити у складу са законом, дакле морају се донети и вршити на основу закона. У најужем смислу, законитост означава то да сви правни акти са мањом правном снагом морају бити у складу са правним актима са већом правном снагом.

Начело поштења се односи на посебно понашање руковооца према субјекту на кога се подаци односе, које мора бити адекватно и не претерано у односу на сврху обраде и оно не сме бити у супротности са прихваћеним начелима морала. Важност овог начела се односи на то да оно захтева од руковооца да податке обрађује поштено и отворено, као и да даје довољно информација о обављању активности обраде и њиховој сврси. Дакле ово начело тежи да усмери све оне које обрађују правне норме да воде рачуна о свакој обради. Са обради података о личности је потребно поступати са пуном пажњом и поштовањем, јер се ту у ствари користи туђе лично добро.

Транспарентност је трећи елемент овог принципа и представља веома важну карику система правне заштите података о личности. Транспарентност се односи на то да

³⁴Чл. 12, ст. 1, тач. 6, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

субјекти чији се подаци обрађују морају бити информисани на јасан, недвосмислен и лак начин за разумевање о томе на који тачно начин се њихови подаци обрађују. Руковаоц има обавезу да обавести лице чији се подаци обрађују о операцијама које се изводе зарад обраде његових података, о основама и сврси ове обраде података, правима које има у погледу заштите његових личних података и начина њиховог коришћења. Дакле захваљујући овом начелу, грађани имају могућност да буду упознати са свим активностима које се односе на њихове личне податке, тачније да добију одговоре на питања ко када, на који начин и како употребљава њихове податке о личности.³⁵Императив је на томе да се информација коју је руковаоц дао субјекту чији се подаци обрађују буду објављени и лако доступни, тј. да није потребно уложити много труда да буду нађени. Ово је посебно релевантно за интернет медије, где су прилично често саопштења која се односе на заштиту података о личности нејасна, тешко доступна, нису транспарентна и не увек у потпуности у складу са важећим правилима.

Дакле, другим речима, принцип законитости, поштења и транспарентности захтева од руковаоца да не злоупотребљавају своју несразмерно јачу позицију наспрам власника података, у односу на које постоји асиметрија информација, већ да према њима имају поштен и искрен став.³⁶

2. Начело ограничења у односу на сврху обраде

Модерни правни системи, међу којима се налази и правни систем Републике Србије, теже да спрече самовољно и непотребно коришћење туђих података. Због тога ја за све те правне системе важно увођење принципа ограничења у односу на сврху обраде. Овај принцип захтева да се лични подаци прикупљају само у одређене, експлицитне и легитимне сврхе, дакле да се не обрађују на начин који је супротан тим сврхама. Овај принцип претпоставља да сврха за коју се подаци прикупљају треба да буде јасно дефинисана пре процеса којим почиње прикупљање података. Ово ће ограничити и спречити било какву неконтролисану обраду података. Подаци о личности се морају

³⁵ Андоновић С., Прља Д., *Основи права заштите података о личности*, *op.cit.* стр. 57.

³⁶ Кривокапић Д., *Водич кроз закон о заштити података о личности и GDPR – тумачење новог правног оквира*, *op. cit.* стр.33.

прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама.³⁷ Принцип ограничености сврхе обраде се у суштини састоји од два основна захтева – да се пре започињања обраде прецизно дефинише и изричито објасни због чега се подаци прикупљају, као и да се подаци прикупљени за иницијалну сврху не могу даље обрађивати за било коју другу, некомпатибилну сврху.³⁸ Дакле, ово начело у ствари значи да се подаци могу прикупљати само на основу законом предвиђених разлога.

Руководалац и обрађивач могу предузети радње обраде само у односу на одређене, изричите и оправдане сврхе.³⁹ Одређеност сврхе означава вршење делатности у вези са којом су потребни одређени подаци. Изричитост сврхе означава упознатост лица чији се подаци обрађују са сврхом обраде, на размљив и јасан начин. Оправданост сврхе означава стварну потребу за прикупљање и обраду података. Практично, руководалац мора унапред јасно и експлицитно дефинисати сврху за коју треба да обради такве податке. Лични подаци се могу прикупљати и обрађивати само у ту унапред јасно дефинисану сврху. Свака нова намена, другачија од оне која је првобитно наведена, значи нову обраду података. На пример, уколико су подаци прикупљени за сачињење неког одређеног уговора, ти подаци се не могу искористити за неки промотивни материјал.

Потребно је навести да постоје ипак изузетне ситуације у којима је могуће обрађивати податке, без обзира на сврху због које су прикупљени. Ту се ради о ситуацијама где се обрађивање врши у циљу статистичких, историјских или научних истраживања. Накнадна обрада се предузима са циљем задовољења неког облика јавног интереса, дакле ради се о делатностима важним за читаву друштвену заједницу. Међутим, овде руководалац мора да процени да ли је првобитна сврха обраде у складу са новом обрадом. Због тога руководалац мора да процени следеће:

(1) Однос и везу између сврхе због које су подаци првобитно прикупљени и намераване (нове) сврхе обраде;

³⁷Чл. 5, ст. 1, тач. 2, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

³⁸Кривокапић Д., Водич кроз закон о заштити података о личности и GDPR – тумачење новог правног оквира, *op. cit.* стр.34.

³⁹Андоновић, С., Прља, Д., *Основи права заштите података о личности*, *op. cit.* стр.66.

- (2)Околности у којима су подаци прикупљени, под чиме се подразумева и однос руковоаца и лица на које се подаци односе (примера ради – да ли су они у односу субординације, радном односу или другој врсти односа поверења);
- (3)Врсту података који се обрађују;
- (4)Потенцијалне ризике и негативне последице које се могу јавити у случају обраде у нове сврхе;
- (5)Одговарајуће техничке мере заштите података (примера ради: криптозаштита и псеудонимизација)⁴⁰

Грађани чији се подаци обрађују би требало да буду обавештени када долази до оваквих ситуација, тачније о мењању сврхе обраде. То би требало да обезбеде руковаоц и обрађивач. Управо, на овај начин се такође остварује горе наведени принцип транспарентности.

3. Начело минимизације података о личности

Као што и само име овог начела каже, оно захтева обраду личних података која је ограничена само на оно што је апсолутно неопходно за сврхе ради које се подаци обрађују. Подаци о личности морају бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде.⁴¹ Примереност представља количину података која је довољна како би се остварила сврха обраде, која је претходно утврђена. Важност, тачније релевантност података означава потребну конекцију између података који се обрађују и сврху обраде тих података. Ограниченост у овом начелу значи да се подаци могу употребљавати само за сврху обраде података, а у супротном би била незаконита. Уколико би дошло до злоупотребе или повреде неког од ових елемената, то би значило повреду овог начела.

Руководалац има обавезу да обрађује личне податке само када је таква обрада адекватна и одговарајућа. Он је слободан да обрађује само оне податке који су релевантни

⁴⁰Чл. 6, ст. 2, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

⁴¹ Чл. 5, ст. 1, тач. 3, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

и пресудни за постизање сврхе и без којих њена реализација није могућа. Дакле, руковалац или обрађивач не треба да постављају неприкладне захтеве лицима чији се подаци обрађују, тако да ти захтеви превазилазе сврху због које су прикупљени. На пример, уколико би руковалац клијентима желео да пошаље нека обавештења путем имејла, за то би му требале само имејл адресе, док је обрада других података за ову сврху била потпуно непотребна.

Начело минимизације података је у уској вези са ГДПР институтима уграђене и подразумеване приватности, који су у ЗЗПЛ имплементирани чланом 42 и називају се „мере заштите”. Наиме правила овог члана налажу руковаоцима и обрађивачима да се још у фази развоја и обликовања начина обраде и планирања тока података, системи који обрађују податке подесе тако да се у њима не налазе подаци чија обрада није неопходна.⁴² Свако прикупљање података изнад прописаног минимума је претерано и непропорционално. Примера ради, када би физичко лице поднесе захтев за кредит у банци, банка прикупља податке о том лицу, како би се осигурала да ће то лице редовно плаћати рату. Међутим, прикупљање свих осталих информација које нису релевантне за ову сврху је неоправдано и банка нема право да захтева тако нешто. Дакле обрађивачу, у овом случају банци, нису потребни подаци који делују претерано и несразмерно, посебно у ситуацији где се сврха може испунити и без тога.

Важно је напоменути да се овај принцип, тачније начело може повредити уколико се прикупљају додатни подаци о одређеном физичком лицу, како би се искористили убудуће. Никако није допустиво да се за сваки случај подаци прикупљају и чувају. Шта више, и да је само лице дало изрзичит пристанак за овако нешто, не постоји законски основ за овакву обраду.

На пример, послодавац може имати обавезу да чува податке о крвним групама појединих запослених на високо ризичним пословима које могу угрозити здравље и

⁴²Кривокапић Д., *Водич кроз закон о заштити података о личности и GDPR – тумачење новог правног оквира*, op. cit. 35.

безбедност запослених (висински радови).⁴³ Овакви подаци су неопходни за спречавање настанка штетних последица у ванредним ситуацијама које се могу десити обављањем послова. Међутим, подаци се могу обрађивати у ванредним ситуацијама, када је то неопходно ради заштите живота и здравља запослених на високо ризичним радним местима.⁴⁴

4. Начело тачности

Поштовањем начела тачности омогућава се да свака правилн и законита обрада буде заснована на тачним и комплетним подацима. Подаци о личности морају бити тачни и, ако је то неопходно, ажурирани. Узимајући у обзир сврху обраде, морају се предузети све разумне мере којима се обезбеђује да се нетачни подаци о личности без одлагања избришу или исправе.⁴⁵

Ово начело практично захтева од руковоаца педантност у обради података о личности.⁴⁶ Руковоац у том смислу треба да провери поузданост извора информација. Подаци морају бити тачни и усклађени са евентуалним променама. Дакле, руковоаци и обрађивачи морају искористи све могуће мере зарад исправности података. Они морају прецизно водити базе података о грађанима. Такође, морају без одлагања да исправе податке који су непотпуни или да избришу нетачне податке. Подаци се могу сматрати нетачним и у ситуацијама када су непотпуни или када су извучени из контекста.⁴⁷

Иако је важно говорити о томе да је одговорност руковоаца и обрађивача да поштују овај принцип, ипак је потребно навести да то не зависи увек од њиховог понашања, колико и од савесности лица чији се подаци обрађују и користе. Због тога је

⁴³Андоновић, С., Прља, Д., *Основи права заштите података о личности*, *op. cit.* стр. 69.

⁴⁴Upr. UKInformationCommissioner’sOffice, Principle (c): Dataminimisation, <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/dataminimisation3>.

⁴⁵Чл. 5, ст. 1, тач. 4, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

⁴⁶Кривокапић Д., Водич кроз закон о заштити података о личности и ГДПР – тумачење новог правног оквира, *op. cit.* стр.37.

⁴⁷Rücker, D., Kugler, T. *New European General Data Protection Regulation: APractitioner’sGuide*, C.H. Beck, Hart, Nomos, 2018, 68.

пожељно да руковаоц благовремено обавести лица чији се подаци обрађују о неопходности њихове сарадње за ажурирање њихових података, када год дође до њихове промене. Начело тачности се односи и на саму обраду. Подаци који се складиште у базама података морају бити ажурирани и усклађивани у односу на промене чињеничног стања.⁴⁸ Начело тачности има огроман значај како у јавном сегменту, тако и у приватном, с обзиром на то да многи интереси и права људи зависе од правилне обраде података. Ту спада лечење грађана, добијање кредита од банке и још многе друге ситуације у којима је потребна правилна обрада података.

До сада смо говорили о ситуацији где подаци морају бити тачни, међутим у неким ситуацијама може бити јако битно да руковалац чува потупуну историју одређеног податка, тј. да чува и претходне нетачне податке и информацију када су и зашто измењени. Чување нетачног податка може бити легитимно, када се на тај начин штите интереси лица на кога се подаци односе. На пример, имамо ситуацију где је пацијент добио погрешну дијагнозу, па затим након откривања погрешне дијегнозе добио ону која му одговара и која је тачна. Међутим, погрешна дијагноза је оставила последице, које је потребно пратити. Дакле, да би лечење било успешно, потребно је чувати и тачне и нетачне податке.

Још једном, руковаоци и обрађивачи требају редовно проверавати тачност података које чувају и користе, с обзиром да до њихове промене долази проласком времена, али и под утицајем других околности.

5. Начело ограниченог чувања података о личности

Начело ограниченог чувања података о личности предвиђа да се подаци о личности чувају у облику који дозвољава идентификацију субјеката података, не дуже него што је то неопходно да се испуни сврха због којих се ти подаци обрађују. Подаци о личности морају се чувати у облику који омогућава идентификацију лица само у року који је

⁴⁸Voigt, P. Bussche, A. The EU General Data Protection Regulation (GDPR)- A Practical Guide, Springer, eBook, online 2017, 91.

неопходан за остваривање сврхе обраде.⁴⁹Другим речима, ово начело поставља временске границе чувања података, искључиво на време које је заиста потребно да се оствари циљ обраде.Ово начело у себи садржи две компоненте:

(1)обавезу да се унапред одреди период чувања података, у зависности од сврхе обраде, при чему тај период мора бити неопходан за испуњење сврхе, тј. мора постојати рационално и убедљиво образложење зашто сврха не може бити остварена у краћем року;
(2)брисање или анонимизацију података (тако да више није могућа идентификација) после истека тог периода.

Када се оствари сврха због које су одређени лични подаци у ствари прикупљени, не постоји више потреба за чувањем тих података, тачније губи се основ обраде. Предуго чување података о личности, као операција обраде, може довести до озбиљних проблема, као што су повреда приватности лица на кога се подаци односе, његових личних података и његових других права и слобода и виталних интереса. Управо из тог разлога, овај принцип предвиђа чување података само у одређеном периоду. Увођењем овог начела у систему за заштиту података о личности, смањује се могућност злоупотребе, застарелости и нетачности личних података који се чувају. Брисањем непотребних података, олакшава се рад руковоаца и обрађивача, тако што се смањују трошкови и ангажовани ресурси.

Период чувања података се може регулисати од стране органа јавне власти или од стране руковоаца. Може се рећи да је рок за чување података у непосредној вези са правним основом за обраду података. Уколико се подаци обрађују за испуњавање одређеног уговора, када се тај уговор испуни, обрада ће по том правном основу престати. Али, руковалац по правилу може имати интерес да одређене податке настави да чува по основу легитимног интереса, све док не истекну рокови застарелости. На пример, у Пољској је послодавац дужан да чува радни досије запосленог до 50 година након престанка радног односа, на основу уговора о раду.

Када у посебним законима није одређен рок за чување података, руковалац мора сам одредити такав рок, на основу сврхе за коју су подаци били прикупљени. Битно је да

⁴⁹Чл. 5, ст. 1, тач. 5,Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

руководилац поткрепи евентуални разумни временски период потребан за постизање сврхе због које се подаци чувају. Да би гарантовао поштовање овог принципа, руководиоца треба да провери повремено потребу за константним складиштењем података. Поента оваквих провера је утврђивање да ли постоји законска основа за чување већ прикупљених података од стране руковоаца, да ли потреба за обрадом ових података и даље постоји, као и да ли сврха због које су подаци прикупљени није већ остварена пре истека предвиђеног рока за складиштењем података.

Подаци о личности који се обрађују искључиво у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања, као и статистичке сврхе, могу се чувати и у дужем року, уз поштовање одредаба овог закона о примени одговарајућих техничких, организационих и кадровских мера, а у циљу заштите права и слобода лица на које се подаци односе. Ако се ради о подацима о личности који обрађују надлежни органи у посебне сврхе, мора се одредити рок када ће се ти подаци избрисати, односно рок за периодичну оцену потребе њиховог чувања.⁵⁰

Пример за ово начело је да медицинска управа чува медицинске податке пацијента само онолико колико је потребно за пружање тренутне медицинске помоћи, а затим безбедно уништава непотребне податке.

6. Начело интегритета и поверљивости

Начело интегритета и поверљивости поставља обавезу руковоацима и обрађивачима да обрађују личне податке на начин који гарантује одговарајући ниво безбедности. Овај принцип се односи на сигурност у свим сегментима обраде података о личности и има за циљ спречавање настајање штетних последица које могу угрозити податке о личности. Подаци о личности морају се обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом

⁵⁰Чл. 8, ст. 2, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

одговарајућих техничких, организационих и кадровских мера.⁵¹Осим у Закону наведених последица, ово начело се односи и на све друге ситуације у којима подаци о личности на било који начин могу бити компромитовани.

Приликом обраде података о личности, руковооци и обрађивачи могу доћи до значајних информација о животу појединца чији се подаци обрађују.⁵²Обрада коју они врше треба да буде затвореног типа, како би се подаци и резултат обраде заштитили од неовлашћеног приступа и злоупотребе других лица. Као што је већ наведено, користе се техничке, организационе и кадровске мере за заштиту података. Међутим ни Закон о заштити података о личности РС ни GDPR не прописују стриктно које би мере требало да се користе, већ то зависи од одређене ситуације и низа фактора, као што су: врста података, количина података која се обрађује, која је сврха обраде, на који начин и у којим системима се подаци чувају, итд. Претња може постојати како од спољних напада, тако и из унутрашњости саме организације.

Руковаоц треба да процени све ризике који се односе на обраду података, како би могао да одреди које мере треба да искористи у одређеној ситуацији. На основу процене ризика, руковооц треба да искористи ефикасне механизме заштите у циљу гарантовања безбедности података. Одлуку о томе које ће мере користити требало би да донесе пре почетка обраде. Али, због муњевитог развоја технологије, потребно је проверавати да ли су постојеће мере адекватне, како би се сачувао оптимални ниво сигурности и безбедности обраде.Податке треба да обрађује само овлашћено лице за ову сврху, зграде и просторије у којима се чувају подаци морају бити отпорни на ватру и провали, да буду заштићени од више силе, лозинке за приступ подацима треба да знају само овлашћена лица и редовно их мењати, као и предузети мере које ће гарантовати враћање оштећених или уништених података.⁵³

Нарушавање информационе безбедности може довести до стварне штете за физичко лице. То може бити крађа идентитета, лажно пријављивање, лажне трансакције кредитном

⁵¹Чл.5, ст. 1, тач. 6, Закон о заштити података о личностим („Сл. гласник РС“, бр.87/2018).

⁵²Андоновић, С., Прља, Д., Основи права заштите података о личности, *op. cit.* стр.72;

⁵³Stoyanova Z. Principles of personal data protection, University of Economics, Audit 2 (2022), Vol.28, 102.

картицом, објављивање строго поверљивих података о личности, хипотекарне преваре, итд.

На пример, дерматолошка ординација је у улози руковоаца, која о својим клијентима чува информације о томе које проблеме имају и које производе и где треба да користе, што укључује и осетљиве здравствене податке. Поред тога, што се те информације чувају у електронској форми, сигурније је да их има и на папиру. Одговарајуће мере заштите подразумевају да се папирна форма чува закључана и да приступ том папиру имају само лица која су овлашћена, као и да се тај папир уништава након што се испуни његова сврха.

7. Начело одговорности

Начело одговорности руковоаца за поступање у вези са подацима о личности означава обавезу руковоаца да обезбеди имплементацију свих шест претходно наведених принципа у својој организацији, тачније да мора бити у могућности да докаже своју усклађеност. Руковалац је одговоран за примену одредаба става 1, члана 5 Закона о заштити података о личности и мора бити у могућности да предочи њихову примену.⁵⁴

Да би систем правне заштите података о личности могао да обавља заштитну функцију, првобитно је потребно одредити права и обавезе свих лица која учествују у активностима обраде. У обради учествују лица која се баве обрађивањем подата, а то могу бити физичка лица, правна лица и орган власти, и лица чији се подаци обрађују, а то могу бити само физичка лица. У активностима обраде могу учествовати и примаоци података и трећа лица, али немају велики значај за обраду података. Овлашћено лице за заштиту података и организације које обрађују податке о личности морају бити одговорне за поштовање принципа за заштиту података о личности. То у суштини значи да је руковалац одговоран за правилност и законитост обраде података, али и за евентуалне последице. Управо тако је и настао један од важнијих принципа заштите података, принцип одговорности руковоаца за правилну обраду података о личности.

⁵⁴Чл.5, ст. 2, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

Одговорност руковаоца се заснива на односу одговорности са лицем чији се подаци обрађују, али и на односу према целокупној друштвеној заједници и јавном поретку. Тако долази до заштите универзалних друштвених вредности и целокупног правног система. Под појмом одговорности се у општем смислу подразумева поступање према правилима које прописује нека друштвена норма. У правном смислу појам одговорности значи поступање према предвиђеним правним нормама и сношење последица због њиховог непоштовања. Према томе, начело одговорности у вези са заштитом података установљава општу обавезу лица које обрађује податке да поштује предвиђене норме и правилност обраде.⁵⁵

Важно је направити разлику између старог и новог Закона заштити о података у погледу одговорности руковаоца. Према старом Закону, руковаоц је био обавезан да збирке података пријави Поверенику који је надлежан орган за то, а тај механизам би требао да обезбеди руковаоцима потврду да је њихова обрада законита. Према новом Закону, збирке се не пријављују, руковаоци морају сами да обезбеде примену свих потребних правила у својим системима обраде личних података, њихова провера се врши само уколико је руковалац у обавези мора своју усклађеност са прописима да доказује у неком поступку.

Према овом начелу, руковалац мора да своје пословање извршава у складу са општим прописима који се односе на заштиту података и на област његових делатности. Наиме, он би требало да докаже постојање те усклађености, а усклађеност се односи на примену правних, техничких и организационих мера. Овај принцип се односи на дужност руковаоца да води рачуна како о подацима које чува и обрађује, тако и о развоју технологије и мера заштите. Дакле, начело одговорности побољшава позицију грађана и њихових података, управо из разлога јер они напоскон знају коме могу да се обрате уколико дође до повреде или злоупотребе њихових података, а руковаоци не могу више тек тако да избегну одговорност уколико дође до тога. Предвиђене казне се могу јавити у новчаном, дисциплинском, кривичном или прекршајном облику одговорности.

⁵⁵Андоновић, С., Прља, Д., Основи права заштите података о личности, *op. cit.* стр. 74.

Практичан аспект овог начела се огледа у томе да би руковоаци требало да документују све своје одлуке у вези са применом ЗЗПЛ начела.⁵⁶ Та документа могу да укључе политику приватности или политику заштите података о личности, која су у пракси доказала да су корисна. Ти документи могу бити јавно доступни, али и могу бити изграђени као интерни акти, како би се регулисали интерни поступци и процедуре.

Како би се теорија овог начела применила у пракси, Радна група члана 29 говори о минималним мерама за руковоаце, које помажу остварењу овог принципа:

-одређивање унутрашњег (интерног) поступка, од самог почетка обраде података о личности;

-креирање стратегије заштите података која се заснива на начелима заштите података;

-мапирање поступака који служе одређивању свих активности у вези са подацима о личности;

-одређивање лица овлашћеног за заштиту података или других лица која су одговорна за личне податке;

-омогућавање одговарајуће обуке, тренинга и усавршавања запослених (под којима се подразумевају и ИТ менаџери људских ресурса и сви други који рукују подацима о личности) у вези са заштитом личних података;

-успостављање унутрашњих правила у вези са ефикасним управљањем и пријављивањем повреде података о личности;

-успостављање поступка у којима се остварују људска права у вези са подацима о личности;

-спровођење процене утицаја у посебним случајевима обраде;

-имплементација и контрола примене свих мера.

Примена ових мера не значи аутоматски и усклађивање са правним прописима у овој области, већ треба да служе као одлична полазна основа и смерница руковоацима у креирању свог интерног система заштите података о личности.⁵⁷

Принцип одговорности се остварује кроз обавезе руковоаца, које могу бити опште и посебне. У општим обавезама руковоаца спадају:

⁵⁶ Кривокапић Д., Водич кроз закон о заштити података о личности и ГДПР – тумачење новог правног оквира, *op. cit.* стр. 38.

⁵⁷ Андоновић, С., Прља, Д., Основи права заштите података о личности, *op. cit.* стр. 75.

- примена свих горе наведених начела обраде података;
- поступање по захтевима;
- обавештење о обради;
- остваривање права лица.

Посебне обавезе обухватају:

- уговорни однос са обрађивачем;
- евиденције о радњама обраде;
- бележење радњи обраде надлежних органа;
- обавештење о повреди заштите података;
- процена утицаја на заштиту података;
- лице за заштиту података;
- кодекс поступања;
- посебне обавезе у погледу преноса података о личности у друге државе и међународне организације.

У сврху остваривања начела одговорности служе и механизми сертификације. Сертификацију треба посматрати као доказ, да је руковалац испунио начела заштите података и спровео адекватне мере, које је редовно проверавао.⁵⁸

⁵⁸ Дилигенски А., Прља Д., Церовић Д., „Право заштите података ГДПР“, Институт за упоредно право Београд, 2018.г.

Глава пета

ПРАВНА РЕГУЛАТИВА У ОКВИРУ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ

Право на заштиту података о личности заштићено је у већини земаља на основу националних и међународних прописа. Због тога је важно осврнути се на те прописе, па ће се првенствено говорити о међународним документима, а затим и о документима који су важни за заштиту података о личности у Србији.

У Стразбуру, 28. јануара 1981. је усвојен један од најзначајнијих међународних докумената под окриљем Савета Европе, а то је Конвенција о заштити лица у односу на аутоматску обраду личних података⁵⁹. Сврха ове Конвенције је да заштити сваког појединца, без обзира на његово/њено држављанство или пребивалиште, у погледу обраде његових/њених података о личности, доприносећи тиме поштовању његових/њених људских права и основних слобода, а нарочито права на приватност.⁶⁰ Дакле, с обзиром на то да аутоматска обрада захтева коришћење компјутера и интернета, сврха Конвенције 108 је да заштити податке у тим новонасталим условима.

Аутоматска обрада личних података коју предвиђа Конвенција 108 се базира на осам принципа заштите података о личности, а то су:

- (1) подаци о личности се морају обрађивати на поштен и законит начин;
- (2) располагање података о личности мора бити у складу са унапред одређеном или правно дефинисаном сврхом;
- (3) подаци о личности се смеју користити или обелоданити само компатибилно одређеној сврси;
- (4) подаци о личности морају бити адекватни, релевантни и у довољном броју, у односу на сврху коју треба да служе;
- (5) подаци о личности морају бити тачни и ажурни;

⁵⁹Конвенција о заштити лица у односу на аутоматску обраду података, Савет Европе, бр.108, Стразбур, 1981.година.

⁶⁰Конвенција о заштити лица у односу на аутоматску обраду података, Савет Европе, бр.108, Стразбур, 1981.година.

- (6) подаци о личности не смеју се држати дуже него што је потребно;
- (7) субјекат података мора бити упознат о вођењу података о његовој личности и о могућностима приступа;
- (8) мере сигурности предузимају се против неауторизованог приступа, мењања, откривања и уништења података о личности – принцип обухвата и намерно вршење ових радњи и случајно губљење и уништење.

С обзиром на то да ова Конвенција има велики значај у области заштите података, уследила је њена модернизација амандманима из 2016. године и додатног Протокола који је усвојен 2018. године, због нових изазова за заштиту података.

Други важни документ који је потребно навести је Директива 95/46/ЕЦ који је настао 1995. године и донета је од стране Европског парламента и Савета. Њен циљ се огледа у њеном пуном називом, а то је Директива о заштити појединца у погледу обраде личних података и о слободном кретању таквих података. Она се односи на обраду личних података у целини или делимично аутоматским или неаутоматским средствима, а односи се на личне податке који чине део збирке или су намењени да чине део збирке. Предмет Директиве је да државе чланице неће ограничавати нити ће забранити слободни проток података о личности између држава чланица из разлога који су у вези са предвиђеном заштитом. Када је реч о подацима који се упућују лицу на кога се подаци и односе, Директива захтева од чланица да одреде да руковоаци морају да обезбеде лицу информације о њиховим идентитетима, сврси обраде података, податке и друге информације.

С обзиром на то да је у међувремену ова Директива застарела, јер су се догодиле друштвене прилике и модернизација на коју она није могла да се примени, дошло је до настанка нових докумената.

Пре него што наведемо конкретни документ за заштиту података о личности, корисно би било да поменемо Директиву 2002/58/ЕЗ Европског парламента и Савета о обради података о личности и заштити приватности у сектору електронских комуникација. Ова Директива је донета 2002. године и другачије се назива Директива о приватности и

електронским комуникацијама. Директива о е-приватности се односи на приватност и податке о личности у дигиталном свету, тачније – на њихов однос са информационо-комуникационим технологијама.⁶¹ Основна сврха Директиве јесте усаглашавање законодавства држава чланица када се ради о поштовању права на приватност у делатности електронских комуникација. Она тежи да направи безбедан простор за слободан пренос података и електронске комуникационе опреме и услуге на територији целе ЕУ. И за ову, као и за претходно наведену Директиву се може рећи да није директно примењивана на државе чланице.

Због горе поменутих проблема са претходним документима, постојала је потреба за доношењем правног акта који би био обавезујући за све државе чланице и који би објединио целокупну заштиту података о личности на једном месту. Тада је настала Општа Уредба Европске Уније.

1. Општа Уредба ЕУ

Општа Уредба о заштити података о личности ЕУ (General Data Protection Regulation) је усвојена 27. априла 2016. године, а онда је ступила на снагу 25.маја 2018. године. До ступања на снагу је дошло тек две године касније, како би се компаније прилагодили овом иновативном систему, а то није нимало лако. Једна од основних идеја Уредбе јесте да надзор над коришћењем података о личности учини доступним грађанима, који ће сами моћи да контролишу и воде рачуна о својим подацима које користе друга лица.⁶²

Приоритети Уредбе су обезбеђивање поштовања основних права и слобода, а нарочито поштовање приватног и породичног живота, заштите података о личности, комуникације, вероисповести, слобода мишљења, слобода изражавања и информисања, правно на културну, језичку и верску различитост, слобода предузетништва, право на

⁶¹Директива 2002/58 Европског парламента и Савета од 12. 07. 2002. године, која се односи на обраду личних података и заштиту приватности у сектору електронских комуникација.

⁶²Андоновић, С., Прља, Д., *Основи права заштите података о личности*, op. cit. стр. 120.

ефиксан правни лек и поштено суђење. Колики је значај ове Уредбе, показује и прилично дугачак уводни део. Наиме, преамбула Уредбе садржи преко 170 тачака.⁶³ Аутори су у преамбули Уредбе објаснили циљеве и мотиве њеног настанка и на који начин је потребно применити материјалне одредбе.

Када говоримо о ГДПР-у, заправо се мисли на нови правни оквир који се бави уређивањем начина за коришћење података о личности грађана Европске уније. Наиме, свака организација која било како обрађује податке грађана ЕУ, али и оних лица која нису држављани ЕУ, али станују унутар ње, мора да се придржава нових правила о заштити података о личности. Самим тим, може се видети да се овај документ првенствено односи на руководиоце различитих фирми. Примена ГДПР-а омогућава појединцима већу контролу над њиховим личним подацима и намеће многе обавезе компанијама које прикупљају и анализирају личне податке.⁶⁴ Значајно је поменути да се то односи на фирме чије је седиште изван територије ЕУ, као што је то случај и са нашим компанијама. Закључак је да сви који се налазе на територији ЕУ су заштићени Уредбом.⁶⁵ ГДПР штити сваки податак који омогућава приступ физичком лицу. То може бити име, ЈМБГ, мејл адреса, број телефона, итд.

Уредба је постала модел за многе друге законе широм света, укључујући Турску, Маурицијус, Чиле, Јапан, Бразил, Јужну Кореју, Јужну Африку, Аргентину и Кенију. Након што је напустило Европску унију, Уједињено Краљевство је усвојило свој „УК ГДПР“, идентичан Општој Уредби ЕУ. Калифорнијски закон о потрошача, својен 28. јуна 2018., има много сличности са Уредбом. Такође, Закон о заштити података о личности Републике Србије је урађен по угледу на Општу Уредбу ЕУ.

Циљ Опште Уредбе је побољшање прописа о заштити података о личности а све у складу са технолошким напретком, те обезбеђење поштовања свих основних људских права и слобода у овој области.⁶⁶ Истакнуто је да се ГДПР-ом жели допринети формирању слободе, сигурности и правде унутар ЕУ, као и јачању и приближавању држава чланица на унутршњем нивоу. Праву на заштиту података о личности се приступа у односу на начело

⁶³Преамбула Опше уредбе о заштити података о личности – ГДПР;

⁶⁴Spalević Ž., Vićentijević K., GDPR and challenges of personal data protection, The European Journal of Applied Economics, Beograd, 2022, 56.

⁶⁵<https://www.paragraf.rs/dnevne-vesti/200418/200418-vest12.html>;

⁶⁶Ђукић, Д. *Заштита података о личности са освртом на ново законодавство Европске Уније у овој области*, Правни записи, бр. 1, Београд, 2017, стр. 49-60.

пропорционалности, јер оно није прописано апсолутно право. Важно је нагласити да се Уредба односи само на живе особе. Ова Уредбе се не примењује на податке о личности преминулих особа. Државе чланице могу да пропишу правила у вези са обрадом података о личности преминулих особа.⁶⁷ Такође је наглашено да заштита података мора бити примењена, независно од тога да ли се примењује аутоматизована или ручна обрада података. ГДПР-ом се промовише принцип неутралне технологије, из разлога што заштита права приватности и података о личности не сме да зависи од технологије која се користи у том тренутку, тачније мора бити технолошки неутрална.

Принципи које познаје Општа Уредба су сви горе већ наведени принципи, с тим што је принцип одговорности најважнији, јер захтева од руковоаца усклађеност са свим стандардима. Поред тога, Уредба прописује неколико мера, којима се повећава сигурност процеса обраде и самих података. Темересеодносена:

1. псеудонимизација и енкрипција података;
2. могућност трајне поверљивости, целовитости, доступности и отпорности система и услуга обраде;
3. способност поновног и благовременог успостављања доступности података о личности и приступа, у случају физичког или техничког инцидента;
4. обезбеђивање поступка редовног тестирања, оцењивања и процене делотворности техничких и организационих мера за постизање безбедности обраде.⁶⁸

Повреда неке норме ГДПР-а као последицу предвиђа веома високе санкције, које би требало да мотивишу руковоаце, обрађиваче и сва друга лица да поштују њене одредбе. Најосновније право у вези са заштитом личних података јесте право на правно средство. Општа Уредба ЕУ познаје право на притужбу надзорном органу, правно на делотворно правно средство против одлуке надзорног органа и право на правно средство против руковоаца или обрађивача.⁶⁹

Општа Уредба садржи неколико завршних процедуралних одредби, у којима се дају аргументи за позивање на друге прописе, као и објашњење о укидању Директиве 95/46 ЕЗ. Како би се осигурала примена одредби Уредбе, Европска Комисија има обавезу

⁶⁷Чл. 27, Општа Уредба ЕУ.

⁶⁸Члан 32, ст. 1, Општа Уредба ЕУ.

⁶⁹Андоновић, С., Прља, Д., *op. cit.* стр.133.

да на сваке четири године подноси извештај Европском парламенту и Савету којим ће дати и своју оцену и евентуално указати на одредбе Уредбе које је потребно преиспитати и унапредити.⁷⁰

2. Прописи у области заштите података о личности у земљама бивше Југославије

Обзиром на то је заштита података о личности тема о којој се говори широм света, државе региона су такође доносиле прописе за заштиту личних података, већином по угледу на Општу Уредбу ЕУ.

Почећемо од Хрватске, која је у обавези да примењује ГДПР, с обзиром да је чланица ЕУ. Хрватска за заштиту података о личности има Закон о примени Опште уредбе о заштити података из 2018.године. Овим законом је установљена Агенција за заштиту личних података (Агенција за заштиту особних података)⁷¹. Агенција је независно државно тело, у свом раду је самостална и независна, и за свој рад одговара Хрватском сабору⁷². Овом агенцијом управља директор, који је именован од стране Хрватског сабора, на предлог Владе. Законом о примени Опште уредбе су продубљене поједине одредбе у вези са обрадом посебних категорија података.

Овај се Закон не односи на обраду личних података коју обављају надлежна тела у сврху спречавања, истраге, откривања, или прогона кажњивих дела или извршавања кажњивих санкција, укључујући заштиту од претњи јавној сигурности и њихова спречавања, као ни на подручје националне сигурности и одбране.⁷³

Словенија је такође члан Европске Уније, па због тога она примењује одредбе Опште Уредбе. Национални пропис који служи за заштиту података о личности у Словенији јесте Закон о заштити личних података, тачније „Zakonovarstvuosebnihpodatkov – ЗВОП-1” који је настао 2007. године. Међутим, овај закон се није ускладио са ГДПР-ом, па се због тога приступило усвајању новог закона, тачније ЗВОП-2, који би требало да се усагласи са Уредбом.

⁷⁰Чл. 97, ст. 1, Општа Уредба ЕУ.

⁷¹Агенција за заштиту личних података Хрватске, <https://azop.hr/>.

⁷²Чл. 4, таč. 2, Закон о примени Опште уредбе о заштити података, NN 42/2018.

⁷³Чл. 1, таč. 2, Закон о примени Опште уредбе о заштити података, NN 42/2018.

Овим Законом уређује се остваривање људског права на заштиту података о личности, обавезе, начела, права, поступци и мере којима се обезбеђује уставна усклађеност, законитост и оправданост задирања у приватност, достојанство, тачност података о личности, самоопредељење података или друга основна права појединаца у обради личних података и правила о слободном протоку личних података за спровођење Уредбе Европског парламента и Савета од 27. априла 2016. о заштити појединаца у обради личних података и о слободном протоку тих података и о укидању Директиве 95/46/ЕЦ и друга питања обраде и заштите података о личности.⁷⁴

У Словенији, функцију независног надзорног тела врши Повереник за информације (Informacijski ooblaščenec) који има седиште у Љубљани.⁷⁵ Према Закону о Поверенику за информације, Повереника бира Народна скупштина на предлог Председника Републике.⁷⁶

Црна Гора није чланица ЕУ, али њено законодавство тежи да се усагласи са европским прописима, јер је она кандидат за чланство. Што се тиче заштите података о личности, на снази је Закон о заштити података о личности из 2008. године. Обзиром на то да тренутни закон нема све институте као што то има европско законодавство, Црна Гора је у поступку усвајања новог закона који ће се усагласити са европским стандардима.

Заштита података о личности обезбеђује се под условом и на начин прописан овим законом, а у складу са принципима и стандардима садржаним у потврђеним међународним уговорима о људским правима и основним слободама и општеприхваћеним правилима међународног права.⁷⁷ Послове независног надзорног тела у Црној Гори обавља Агенција за заштиту личних података и слободан приступ информацијама, која има два органа. То су Савет Агенције и директор Агенције.⁷⁸

У Северној Македонији заштита података о личности је регулисана Законом о заштити личних података, који је усвојен почетком 2020. године. Овим законом се уређује заштита података о личности и право на приватност у вези са обрадом личних података, а посебно принципе који се односе на обраду података о личности, права субјеката личних података, положај руковоаца и обрађивача, пренос личних података у

⁷⁴Čl. 1, tač. 1 Zakon o zaštiti ličnih podataka Slovenije (ZVOP-2), „Uradni list RS“ br.94/07.

⁷⁵Повереник за информације Словеније, <https://www.ip-rs.si/en..>

⁷⁶Закон о Поверенику за информације Словеније, „Урадни лист РС“ ст. 113/05, енглеска верзија текста, <https://www.ip-rs.si/en/legislation/information-commissioner-act>.

⁷⁷Čl. 1, tač. 1, Zakon o zaštiti podataka o ličnosti „Sl. List CG“, br.79/08, 70/09, 44/12, 22/17 <https://www.gov.me/dokumenta/d65b84b4-14df-43e0-aeb2-aadf44149486>.

⁷⁸Агенција за заштиту личних података и слободан приступ информацијама, <http://www.azlp.me/me/oagenciji>.

друге земље, оснивање, статус и надлежности Агенције за заштиту података о личности, посебне послове обраде података о личности, правне лекове и одговорност у обради података о личности, надзор над заштитом података о личности, као и прекршаје и прекршајни поступак у овој области.⁷⁹

Независни надзорни државни орган који се бави применом овог закона јесте Агенција за заштиту личних података и седиште јој је у Скопљу. Агенцијом руководи директор кога бира и разрешава Народна скупштина на предлог Комисије. Директор се бира на основу јавног конкурса, на период од 5 година. Директор Агенције бира заменика директора.⁸⁰

Систем за заштиту података о личности Босне и Херцеговине није тотално усаглашен са ГДПР-ом, али се може рећи да је у почетној фази усаглашења, јер је Босна потенцијални кандидат за чланство. Заштита података о личности је уређена Законом о заштити личних података, који је донешен 2006. године. Циљ овог Закона је да се на територији Босне и Херцеговине свим лицима, без обзира на њихово држављанство или пребивалиште, обезбеди заштита људских права и основних слобода, а нарочито право на приватност и заштиту података у погледу обраде личних података који се на њих односе.⁸¹

Овим Законом основана је Агенција за заштиту личних података.⁸² Агенција представља самосталну, независну организацију која је основана како би заштитила личне податке. Она се налази у Сарајеву, а њом руководи директор који има свог заменика. Именовани су од стране Парламентарне скупштине, на 5 година. Законом о заштити личних података се утврђује њена надлежност, организација и управљање, као и друга питања значајна за њен рад и законито функционисање.

3. Прописи у области заштите података о личности у Србији

Развијање информационих технологија, повећање коришћења података о личности у разним сферама друштвеног живота, а нарочито увођење заштите података у европским

⁷⁹Чл. 1, тач. 1, Закон о заштити личних података Македоније, „Сл. весник РСМ“, бр. 42/2020., https://dzlp.mk/sites/default/files/u4/zakon_za_zastita_na_licnite_podatoci.pdf.

⁸⁰Андоновић, С., Прља, Д., Основи права заштите података о личности, Институт за упоредно право, Београд, 2020. година, стр.148.

⁸¹Чл. 1, Закон о заштити личних података БиХ, „Сл. Glasnik БиХ“, бр. 49/2006, 76/2011 и 89/2011.

⁸²Агенција за заштиту личних података и Босни и Херцеговини, http://www.azlp.ba/Default.aspx?langTag=sr-SP-Cyrl&template_id=147&pageIndex=1.

законодавствима, довело је до тога да и Србија иде у том правцу. Први Закон о заштити података о личности је донет 1998. године. Након тога је Република Србија ову заштиту предвиђала у Уставу РС и донела је нови Закон о заштити података 2008. године. Међутим, због великог утицаја права Европске Уније и ради усаглашавања са европским законодавством, систем заштите података о личности је прошао кроз велике промене. Тако је дошло до настанка новог Закона о заштити података о личности који је ступио на снагу 21. новембра 2018. године, а почео да се примењује 21. августа 2019. године.

Актуелни Закон о заштити података о личности РС је настао као потреба за усаглашавањем са Општом Уредбом, што је доста уочљиво, јер већина чланова Закона су апсолутно исти као и код Уредбе. Закон о заштити података о личности из 2018. године, први пут у историји Србије успоставља темељан систем заштите података који је постављен као штит приватности грађана, преко које се бране и друга људска права и слободе.⁸³ Закон о заштити података о личности састоји се од 10 целина:

1. Основне одредбе;
2. Начела;
3. Права лица на које се подаци односе;
4. Руковалац и обрађивач;
5. Пренос података о личности у друге државе и међународне организације;
6. Повереник;
7. Правна средства, одговорност и казне;
8. Посебни случајеви обраде;
9. Казнене одредбе;
10. Прелазне и завршне одредбе.

Битно је напоменути да је тренутни Закон о заштити података о личности установљен као општи закон ове области. Дакле, овим Законом се уређује право на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, кодекс поступања, пренос података о личности у друге државе и међународне организације, надзор над спровођењем овог закона, правна

⁸³Андоновић, С., Прља, Д., *Основи права заштите података о личности*, *op. cit.* стр.150.

средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом података о личности, као и посебни случајеви обраде. Овим законом уређује се и право на заштиту физичких лица у вези са обрадом података о личности коју врше надлежни органи у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавања и заштиту од претњи јавној и националној безбедности, као и слободни проток таквих података.⁸⁴

Норме Закона о заштити података о личности се примењују код аутоматизоване и неаутоматизоване обраде података. Аутоматизована обрада подразумева коришћење рачунара или других дигиталних уређаја који преко одговарајућег програма (софтвера) обрађују податке – обрада података у MicrosoftWord-у на рачунару. Неаутоматизована обрада у ствари представља ручну обраду – преписивање података у свеску хемијском оловком.⁸⁵ Такође је важно напоменути руковооца и обрађивача који су, поред лица чији се подаци обрађују, главни актери за заштиту података о личности. Руковооц је физичко или правно лице које само или са другима одређује сврху и начин обраде, док је обрађивач физичко или правно лице, тј. орган власти који обрађује податке о личности у име руковооца. У члану 5 Закона о заштити података о личности су предвиђена начела заштите података о личности, што је и главна тема овог рада. Дакле, ЗЗПЛ предвиђа сва већ горе наведена начела, која се морају поштовати како би обрада података о личности била законита и могућа.

Обзиром на то да је ЗЗПЛ већину својих одредби узео од Опште Уредбе ЕУ, главни недостаци Закона су нејасне одредбе и прописани механизми који уопште не постоје у нашем правном систему. Наш Закон, такође не садржи Преамбулу ГДПР-а, која уједно представља и пролазни основ за тумачење прописа.⁸⁶ Закон прописује ниске казне од 50.000 до 2.000.000 динара, што је далеко мање од европског просека. Постоји низ области које ЗЗПЛ није регулисао, а то су примена вештачке интелигенције и других система за аутоматизовану обраду података, затим, није решио питање обраде биометријских и генетских података, као ни посебне облике обраде података као што су видео надзори и обраду у сврху научних, историјских и статистичких сврха.

⁸⁴Чл. 1, ст. 2, Закон о заштити података о личности, („Сл. гласник РС“, бр.87/2018).

⁸⁵Андоновић, С., Прља, Д., Основи права заштите података о личности, оп. cit. стр.152.

⁸⁶<https://www.partners-serbia.org/public/news/zakon-o-zastiti-podataka-licnosti.pdf>

Врло је важно истаћи да је независни надзорни орган у Републици Србији Повереник за информације од јавног значаја и заштиту података о личности. Ради остваривања права на приступ информацијама од јавног значаја, Законом о слободном приступу информацијама од јавног значаја из 2004. године установљава се Повереник за информације од јавног значаја, као самостални државни орган, независан у вршењу своје надлежности.⁸⁷ Тек касније, када је донет Закон о заштити података о личности 2008. године, Повереник добија данашње пуно име. Седиште Повереника је у Београду и он може образовати канцеларије ван свог седишта.⁸⁸

Повереник је посебно независно тело чија је надлежност усмерена на обављање стручних и контролних послова у вези са заштитом права и слобода грађана у области информација од јавног значаја и заштите података о личности, што говори о комплексној правној природи и сложеној функцији које ово тело има у праву Србије.⁸⁹ Повереник има функционалну независност, која се односи на слободно обављање послова из његове надлежности, без мешања других органа и финансијску независност која значи да се за његов рад користе средства из посебних буџета државе. Може се закључити да Повереников основни посао јесте обезбеђивање правилне примене ЗЗПЛ-а и да он представља најважнији орган у области заштите података о личности.

⁸⁷Чл. 1, ст. 2, Закон о слободном приступу информацијама од јавног значаја, („Сл. гласник РС“, 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021).

⁸⁸Чл. 29, ст. 1 и 2, Закон о слободном приступу информацијама од јавног значаја, („Сл. гласник РС“, 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021).

⁸⁹ Давинић, М. *Независна контролна тела у Републици Србији*, Досије, Београд 2018, стр. 23.

ЗАКЉУЧНА РАЗМАТРАЊА

Принципи заштите података о личности чине важан оквир за обезбеђивање приватности појединца и одговорног поступања организација са личним подацима. Ови принципи, усаглашени са европским стандардима, постављају јасна правила која су кључна за очување поверења појединаца у обради њихових података.

Важни аспекти укључују:

1. Захтев за сагласност, што наглашава транспарентност и контролу појединаца над својим подацима;
2. Ограничавање сврхе и минималност података ради спречавања непотребног прикупљања информација;
3. Одржавање тачност података, обезбеђујући ажурност информација које организације држе;
4. Ограничење чувања података, чиме се избегава непотребно задржавање информација;
5. Мере поверљивости и интегритета ради заштите података од неовлашћеног приступа и оштећења;
6. Обезбеђивање одговорности организација кроз постављање овлашћеног лица за заштиту података и спровођење интерних политика и процедура.

Активна улога Повереника за информације од јавног значаја и заштиту података о личности, додатно осигурава имплементацију ових принципа, пратећи поступање организације и пружајући подршку појединцима у остваривању њихових права. У овом контексту, прави оквир у Републици Србији пружа значајан допринос унапређењу стандарда заштите података о личности и пружању етичких и законских норми у дигиталном свету. Важно је даље пратити развој обе области и уједно прилагођавати законске оквире како би се ефикасно носили са изазовима дигиталног доба.

Додатно је важно истаћи да ефикасна примена принципа заштите података о личности у пракси захтева сарадњу и ангажовање како органа за заштиту података, попут Повереника, тако и самих организација и појединаца. Па се тако могу поменути и нека додатна разматрања као што су:

1. Едукација и свест: Континуирана едукација организација, запослених и појединаца о правилима заштите података и променама у законодавству кључна је за успешну примену принципа. Свест о важности приватности треба бити интегрални део пословних пракси.
2. Технолошки развој: Уз брз технолошки напредак, од изузетног значаја је пратити и развијати одговарајуће технолошке мере заштите података. Ово укључује примену најновијих мера енкрипција, безбедних протокола и других технолошких решења која обезбеђују сигурност података.
3. Међународна сарадња: Како подаци често прелазе границе, међународна сарадња и хармонизација стандарда заштите података играју кључну улогу. Размена искустава и информација са другим земљама и организацијама доприноси ефикасном управљању глобалним питањима приватности.
4. Транспарентност и комуникација: Организације треба да буду транспарентне у вези са својим поступањем подацима, пружајући јасне информације о томе како прикупљају, користе и чувају личне податке. Отворена комуникација са корисницима гради поверење.
5. Континуирано побољшање пракси: Узимање у обзир низ повратних информација од стране корисника, анализа инцидената и стално унапређивање пракси заштите података су кључни за одржавање високих стандарда приватности.
6. Истраживање и иновације: Активно праћење и истраживање најновијих трендова и иновација у области заштите података помаже у прилагођавању законодавства у пракси нових изазова, попут вештачке интелигенције и интернет ствари

На крају се може рећи да усклађивање са принципима заштите података није статичан процес, већ динамичан напор који захтева ангажовање свих релевантних страна и прилагођавање променама у технологији, друштву и самом законодавству.

ЛИТЕРАТУРА

- Antonić N., Submission of a copy of personal data, Bankarstvo, 2021, vol. 50, Issue 4, pages: 152-157;
- Андоновић, С., Правна природа Повереника за информације од јавног значаја и заштиту подата о личности, у: Архив за правне и друштвене науке, год.114, бр.1-2/2019, издавачи: Савез Удружења правника Србије и Републике Српске и Институт за политичке студије, Београд;
- Андоновић С., Заштита података у електронској јавној управи у Републици Србији – правни аспекти, докторска дисертација, Правни факултет Универзитета у Београду, Београд 2019;
- Јовановић З., Андоновић С., Врсте информације и података у јавном праву Републике Србије, зборник радова, „Заштита података о личности у Србији“, Београд, 2020;
- Андоновић С., Прља Д., Основи права заштите података о личности, Институт за упоредно право, Београд, 2020;
- Гасми Г., Прља Д., „Право на поштовање приватног живота и право на заштиту података о личности“, зборник радова „Заштита података о личности“, 2020;
- Вуковић М., Интерпретација правних прописа, Школска књига, Загреб,1953;
- Глушац Л., Разликовање (независних) контролних и регулаторних тела, Зборник радова Правног факултета у Нишу, број 87, 2020, стр.197-216;
- Давинић М., Независна контролна тела у Републици Србији, Досије, Београд 2018.
- Дракулић М., Основи компјутерског права, Друштво операционих истраживача Југославије, ДОПИС, Београд, 1996;
- Data Protection Laws of the World, Serbia, DLA Piper, 2022;
- Ђукић Д., Заштита података о личности са освртом на ново законодавство Европске Уније у овој области, Правни записи, бр.1, Београд, 2017, стр. 49-60;
- Кривокапић Д., Водич кроз закон о заштити података о личности и ГДПР – тумачење новог правног оквира. Београд: Мисија OEBS – у Србији и Share Фондација, 2019;

- Мајсторовић М., Ковачевић Т., Заштита података о личности и пракса независних органа у Србији и Француској, у: Зборних радова: Заштита података о личности, Институт за упоредно право, Београд, 2020;
- Дилигенски А., Прља Д., Церовић Д., „Право заштите података ГДПР“, Институт за упоредно право Београд, 2018;
- Милеуснић Д., Ђурчић Д., Тасић Д., идр., Приватност и заштита података о личности у Србији, Анализа одабраних секторских прописа и њихове примене, Партнери за демократске промене Србије (Партнери Србија), Београд, 2021.године;
- Миленковић Д., Приручник за примену Закона о слободном приступу информација од јавног значаја, Повереник за информације од јавног значаја и заштиту података о личности, Београд, 2010;
- Мишић К., Лубарда М., Заштита података – приручник за руковооце, Повереник за информације од јавног значаја и заштиту података о личности Републике Србије, Београд, 2012;
- Раденковић, Б. Деспотовић – Зракић, М. Богдановић, З. Бараћ, Д. Лабус, А. *Електронско пословање*, Факултет организационих наука, Београд, 2015;
- Rucker D., Kugler T., (eds.), 2018, *New European General Data Protection Regulation: A Practitioner's Guide*, C.H. Beck, Hart, Nomos, p.68;
- Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) – A Practical Guide*, Springer, eBook, online, 2017, p.91.
- Симоновић И., Лазић М., Грађанскоправна заштита права личности, Зборник радова Правног у факултета у Нишу, број 68/2014;
- Simpson A., Sotto L., *Data protection and privacy*, 2022, Lexology, Law Business Research, London, 2021;
- Ramez Elsmari, Shamkant Navathe, *Fundamentals of Database Systems*, Addison-Wesely Publishing Company, Boston – Columbus – ets., 2010;
- Spalević Ž., Vićentijević K., *GDPR and challenges of personal data protection*, *The European Journal of Applied Economics*, Beograd, 2022, pages: 50-65;
- Stoyanova Z., *Principles of personal data protection*, University of Economics, Audit 2 (2022), Vol.28, pages 95-104;

- Штурм Л., Правни аспекти заштите података у савремених информационим системима, у: Анали Правног факултета у Београду, бр. 6, Београд, 1986;

ПРАВНИ ИЗВОРИ

- Закон о заштити података о личности („Сл. гласник РС“, бр. 87/2018);
- Закон о заштити података о личности („Сл. гласник РС“, бр.97/2008);
- Закон о слободном приступу информацијама од јавног значаја („Сл. гласник РС“, 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021);
- Конвенција о заштити лица у односу на аутоматску обраду података, Савет Европе, бр. 108, Стразбур, 1981.година;
- Општа уредба о заштити подата ЕУ – Regulation 2016/679 of the European Parliament and of the Council 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) од 27. априла 2016;
- Закон о информационом систему Републике Србије, („Сл. гласник РС“, бр. 12/1996);
- Закон о електронској управи („Сл. гласник РС“, бр.27/2018);
- Универзална декларација Уједињених нација о људским правима, Организација Уједињених Нација 217(ИИИ), од 10. децембра 1948. године, Париз;
- Конвенција Савета Европе о заштити људских права и основних слобода, Рим, 1950;
- Повереник за информације од јавног значаја и заштиту података о личности;
- Директива 2002/58 Европског парламента и Савета од 12. 07. 2002. године, која се односи на обраду личних података и заштиту приватности у сектору електронских комуникација;
- Преамбула Опше уредбе о заштити података о личности ЕУ –2016/679;
- Закон о примени Опште уредбе о заштити података Хрватске, NN 42/2018, од 25. маја 2018. године;

- Agencija za zaštitu ličnih podataka Hrvatske, <https://azop.hr/>;
- Zakon o zaštiti ličnih podataka Slovenije, „Uradni list RS“ br. 94/07;
- Poverenik za informacije Slovenije, <https://www.ip-rs.si/en>;
- Zakon o zaštiti podataka o ličnosti, „Sl. list CG“, br. 79/08, 70/09, 44/12, 22/17;
- Agencija za zaštitu ličnih podataka i slobodan pristup informacijama, <http://www.azlp.me/me/o-agenciji>;
- Zakon o zaštiti ličnih podataka Makedonije, „Сл. весник РСМ“, br. 42/2020;
- Zakon o zaštiti ličnih podataka BiH, „Sl. glasnik BiH“, be. 49/2006, 76/2011 i 89/2011;
- Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, http://www.azlp.ba/Default.aspx?langTag=sr-SP-Cyrl&template_id=147&pageIndex=1.

ИНТЕРНЕТ ЛИНКОВИ

- <https://enterprivacy.com/2017/03/01/categories-of-personal-information>
- <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/dataminimisation3>
- <https://www.paragraf.rs/dnevne-vesti/200418/200418-vest12.html>
- <https://www.partners-serbia.org/public/news/zakon-o-zastiti-podataka-licnosti.pdf>
- <https://azop.hr/>
- <https://www.ip-rs.si/en>.
- <https://www.ip-rs.si/en/legislation/information-commissioner-act>
- <https://www.gov.me/dokumenta/d65b84b4-14df-43e0-aeb2-aadf44149486>
- https://dzlp.mk/sites/default/files/u4/zakon_za_zastita_na_licnite_podatoci.pdf

САЖЕТАК И КЉУЧНЕ РЕЧИ

Заштита података и приватност су од великог значаја и за појединце и за друштво у целини. У свету у коме данас живимо се свакодневно сакупља и обрађује огромна количина података. Томе у великој количини доприносе информационе технологије и учестало коришћење интернета. Због прекомерне количине података који се прикупљају и обрађују, у овом раду говори се о заштити података о личности, а конкретно о принципима заштите података о личности.

Што се тога тиче, првенствено се говори о правним принципима који представљају градивне законе правног поретка и области правног поретка. Колевка правних принципа је римско право и они су знатно допринели конституисању савремених европских правних система, као и уобличавању доктрине о владавини права генерално. Међутим, у нашој правној књижевности се правним принципима одузима самостални правни карактер и због тога је ниво њихове заступљености у правној књижевности и судској јуриспруденцији низак. Управо због тога се посвећује пажња излагању аргумената који доказују самосталност правног карактера правних принципа, а самим тим и принципа заштите података о личности.

Принципи заштите података о личности имају вишеструки значај. Најпре се њима усмерава тумачење одредби које могу бити нејасне, дакле уколико су руковалац или обрађивач у дилеми како да примене неку одредбу, увек се требају ослонити на тумачење ових начела. Важност ових принципа се пројектује постојањем тешких казни за њихово непоштовање.

У овом раду се пажња посвећује превасходно теоријском одређивању појма података о личности и њиховим врстама, као и са њима уско повезаној заштити података о личности и правној регулативи у оквиру области заштите. Али главни фокус је усмерен ка принципима заштите података о личностим као што су начело законитости, транспарентности и поштења или начело тачности или било које друго начело. Дакле, циљ овог рада јесте утврђивање појма заштите података о личности, а у оквиру тога и појам начела заштите података о личности, како би се и једно и друго адекватно искористили. Имајући у виду да је данас број злоупотреба података о личности велики, у раду се пише о законима који штите право на њихову заштиту, посебно о Општој уредби ЕУ која има

највећи значај за заштиту података, али и одомаћем Закону о заштити података о личности који се не сме занемарити.

С обзиром да веома мали број људи зна о овоме, ауторка сматра да широка маса људи треба да се едукује о постојећим правима која им стоју на располагању када се ради о заштити података о личности, а да се с друге стране активније ради на имплементацији нових права која би их још више заштитила. Такође, ауторка је покушала да у раду прикаже превелики значај заштите података, као и принципа у свету технологије, који је свакако усмерен на податак.

Кључне речи: податак о личности, заштита података, принципи заштите података о личности, ЗЗПЛ, Општа Уредба ЕУ

SUMMARY AND KEY WORDS

Principles of personal data protection

Data protection and privacy are very important both for individuals and for society as a whole. In the world where we live today, a huge amount of data is collected and processed every day. Information technologies and frequent use of the Internet contribute to this in a large amount. Due to the excessive amount of data that is collected and processed, this paper discusses the protection of personal data, specifically the principles of personal data protection.

Primarily we are talking about legal principles that represent the constructive laws of the legal order and the area of the legal order. The cradle of legal principles is Roman law and they contributed to the constitution of modern European legal principles, as well as shaping the doctrine of the rule of law in general. However, legal principles are stripped of their independent legal character, in our legal literature, and because of this, the level of their representation in legal literature and judicial jurisprudence is low. This is reason why attention is paid to the presentation of arguments that prove the independence of the legal character of legal principles, as well as the principle of personal data protection.

Principles of personal data protection have multiple meanings. First of all, they guide the interpretation of provisions that may be unclear, so if the handler or processor are in a dilemma

how to apply some provision, should always rely on interpreting these principles. The importance of these principles is projected by the existence of difficult penalties for their non-existence.

In this paper, primarily attention is paid to the theoretical determination of the term of personal information and their types, as with them closely related data protection and legal regulations within the field of data protection area. But the main focus is on the principles of data protection, as they are principle of lawfulness, fairness and transparency or principle of accuracy or any other principle. So, the goal of this paper is to determine the concept of personal data protection, and within that the concept of principles of personal data protection, in order to use both adequately. Bearing in mind that nowadays the number of abuses of personal data is high, the paper describes the laws that protect the right to their protection especially about General Data Protection Regulation – GDPR that have the greatest importance for data protection, but also about the domestic law of personal data protection, that should not be ignored.

Since very small number of people know about this, the author believes that great mass of people should be educated about the existing right that are available to them when we talk about personal data protection, and on the other side to be more active on the implementation of new rights that would protect them more. The author also tried to show in her paper the excessive importance of data protection, as well as principles in the world of technology, which is certainly focused on data.

Keywords: personal data, data protection, principles of personal data protection, PDP law, GDPR

БИОГРАФИЈА АУТОРКЕ

Александра Милошевић рођена је 13.03.1998.године у Лангенфелду, СР Немачка, а иначе живи у Власотинцу.Основну школу „8.октобар“ завршила је у Власотинцу 2012.године, а након тога је 2016.године завршила језички смер Гимназије „Стеван Јаковљевић“ у Власотинцу, са одличним успехом током свих година школовања.

Правни факултет у Нишу уписала је 2016.године, а дипломирала је на Факултету за пословне студије и право, Универзитет „УНИОН – НИКОЛА ТЕСЛА“ у Београду 2022.године. Након тога, исте године уписала је мастер студије Правног факултета Универзитета у Нишу, на смеру „Право и информационе технологије“.

Кандидаткиња је оспособљена за рад на рачунару. Говори енглески језик и служи се немачким језиком. Тренутно ради у адвокатској канцеларији у Нишу.

**ИЗЈАВА О ИСТОВЕТНОСТИ
ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА**

Име и презиме аутора мастер рада: Александра Милошевић

Наслов мастер рада: „Принципи заштите података о личности“

Ментор: Проф. др Милош Прица

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, _____ 2024.године

Потпис аутора

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом „Принципи заштите података о личности“ пријављен и одбрањен на Правном факултету Универзитета у Нишу:

- резултат сопственог истраживачког рада;
- да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;
- да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: Александра Милошевић

У Нишу, _____ 2024.године

Потпис аутора
