

УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

**Управноправни режим остваривања права на
приступ личним подацима**

(мастер рад)

Ментор
проф. др Милош Прица

Студент
Христина Митић
Број индекса: М011/23-ИТ

Ниш, 2024. године

САДРЖАЈ

	УВОДНЕ НАПОМЕНЕ.....	1
I	ПОДАЦИ О ЛИЧНОСТИ	4
1.	Појам података о личности.....	4
1.1.	<i>Нормативно одређење података о личности.....</i>	4
1.2.	<i>Практични аспекти података о личности.....</i>	6
2.	Подела података о личности.....	7
II	ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ - НОРМАТИВНИ ОКВИР	9
1.	Европска унија.....	9
1.1.	<i>General Data Protection Regulation - GDPR.....</i>	9
1.2.	<i>Остали прописи.....</i>	10
2.	Република Србија.....	11
2.1.	<i>Устав Републике Србије.....</i>	11
2.2.	<i>Закони.....</i>	12
2.3.	<i>Подзаконски акти и остали акти.....</i>	15
III	КОРПУС ПРАВА ЛИЦА ЧИЈИ СЕ ПОДАЦИ ОБРАЂУЈУ	16
IV	ОДРЕЂЕЊЕ ПРАВА НА ПРИСТУП ЛИЧНИМ ПОДАЦИМА	18
1.	Појам права на приступ личним подацима.....	18
2.	Елементи права на приступ личним подацима.....	20
V	ПРИСТУП ЛИЧНИМ ПОДАЦИМА У ИЗАБРАНИМ ПРАВНИМ ПОРЕЦИМА.....	21

1.	Словенија.....	21
2	Хрватска.....	22
3	Пракса Европског суда за људска права.....	23
4.	Пракса Суда правде Европске уније.....	25
VI	ОСТВАРИВАЊЕ ПРАВА НА ПРИСТУП ЛИЧНИМ ПОДАЦИМА	27
1.	Овлашћени подносиоци и форма захтева.....	27
2.	Поступање по захтеву за приступ подацима.....	29
3.	Рокови и последице пропуштања.....	33
4.	Поступак пред Повереником за заштиту података о личности	34
VII	ОГРАНИЧЕЊА ПРАВА НА ПРИСТУП ПОДАЦИМА О ЛИЧНОСТИ	36
1.	Обрада личних података у посебне сврхе.....	36
2.	Законска ограничења права на приступ подацима о личности.....	36
	ЗАКЉУЧНА РАЗМАТРАЊА.....	39
	ПОПИС КОРИШЋЕНЕ ЛИТРАТУРЕ.....	42
	ПОПИС ОСТАЛЕ ИСТРАЖИВАЧКЕ ГРАЂЕ.....	43
	ЕЛЕКТРОНСКИ ИЗВОРИ	44
	РЕЗИМЕ	46
	SUMMARY.....	47
	БИОГРАФИЈА.....	48

УВОДНЕ НАПОМЕНЕ

У савременом друштву, обрада личних података постала је неизоставан део свакодневног живота. Дигитализација и све већа зависност од информационих технологија доносе бројне бенефите, али и изазове, посебно када је реч о заштити приватности грађана. Право на приступ личним подацима, као једно од кључних права у овој области, омогућава појединцима да контролишу информације које се о њима прикупљају, обрађују и користе. Ова контрола је од суштинског значаја за заштиту приватности и остварење других људских права, укључујући право на достојанство, слободу изражавања, као и право на слободно кретање.

Овај мастер рад усредсређује се на правни оквир заштите података о личности, са посебним нагласком на право на приступ подацима о личности. Право на приступ подацима о личности представља једно од најважнијих права појединаца у контексту заштите података о личности. Ово право омогућава појединцима да сазнају које се информације о њима обрађују, за које сврхе, од стране кога и на који начин. Право на приступ подацима је од суштинског значаја за осигурање транспарентности у обради података и омогућава појединцима да задрже контролу над својим личним информацијама. Поред тога, оно служи као основа за остваривање других права у области заштите података о личности, као што су право на исправку, брисање или ограничење обраде.

Предмет овог истраживања је анализа правног оквира и праксе остваривања права на приступ подацима о личности, са посебним освртом на управноправни режим остваривања права на приступ личним подацима. Мастер рад ће пружити детаљну анализу правних норми које уређују ово право, идентификују изазови са којима се суочавају руковооци података у примени тих норми, те да се оцени ефикасност постојећих механизма заштите права субјеката података. Рад ће приказати нормативни оквир који уређује заштиту података о личности у Европској унији, као и нормативни оквир који ову област уређује у Србији; такође ће извршити упоредну анализу прописа. Поред анализе правног оквира, истраживање ће обухватити и преглед конкретних случајева из праксе како би се указало на кључне проблеме и могућа решења у области остваривања права на приступ подацима. Мастер рад ће настојати да прикаже различите случајеве из праксе где ће бити обухваћени и случајеви из већег броја земаља, како чланица ЕУ тако и Србије те ће на основу тога настојати да прикаже сличности и разлике у погледу регулисања ове области у конкретној земљи.

Овај рад има за циљ да допринесе бољем разумевању како руковооци података поступају по захтевима за приступ подацима о личности, које препреке постоје у пракси, и како се право на приступ може ефикасније заштитити. Поред тога, рад ће понудити препоруке за унапређење законодавног оквира и праксе, како би се осигурало да ово основно право појединаца буде у потпуности поштовано.

Први кораци у погледу регулисања заштите података о личности у нашој земљи начињени су деведесетих година прошлог века, почев од Устава Савезне Републике Југославије, донетог 1992. године, којим се први пут гарантује заштита података о личности¹, преко Закона о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података² па до првог Закона о заштити података о личности³.

Република Србија, као држава која тежи придруживању Европској унији, препознала је важност усклађивања свог законодавства са европским стандардима у области заштите података о личности. Усвајање важећег Закона о заштити података о личности (у даљем тексту: ЗЗПЛ)⁴, 2018. године, представља значајан искорак у том правцу, али и одговор на све већи притисак да се обезбеди одговарајући ниво заштите личних података грађана у дигиталној ери. Овај закон је у великој мери заснован на GDPR-у (*General Data Protection Regulation*, у даљем тексту: GDPR)⁵, који се примењује на нивоу Европске уније и уводи низ права за појединце, међу којима право на приступ личним подацима заузима централно место. Право на приступ омогућава појединцима да сазнају које се информације о њима прикупљају, како се обрађују и за које сврхе, што им пружа могућност да, ако је потребно, предузму мере за заштиту својих права.

Међутим, иако је нормативни оквир унапређен, поставља се питање колико су ове норме ефикасне у пракси и у којој мери грађани Србије заиста остварују своје право на приступ личним подацима. Наиме, заштита приватности у дигиталном добу суочава се са бројним изазовима, укључујући сложеност технолошких система, недовољну свест грађана о њиховим правима, као и недостатак ефикасних механизма за спровођење закона. У том контексту, неопходно је испитати како се право на приступ

¹ Устав Савезне Републике Југославије, "Службени лист СРЈ", бр.1/92, чл. 33. ст. 1.

² Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података, „Сл. лист СРЈ — међународни уговори”, бр. 1/92.

³ Закон о заштити података о личности, "Службени лист СРЈ", бр. 24/98.

⁴ Закон о заштити података о личности, "Сл. гласник РС", бр. 87/2018.

⁵ *General Data Protection Regulation, (EU) 2016/679*, извор: <https://gdpr-info.eu/>, приступљено: 01.08.2024. године

личним подацима примењује у пракси, какви су ставови и искуства грађана, као и како се овај институт може даље унапредити у складу са савременим потребама и стандардима.

Мотив за истраживање ове теме проистиче из чињенице да је заштита личних података постала кључно питање у савременом друштву, посебно у светлу убрзане дигитализације и глобализације. У време када се велики део наших активности обавља онлајн, права грађана у вези са обрадом њихових података постају од изузетне важности. У Србији, усвајање новог законодавног оквира указује на тежњу ка побољшању заштите података, али и даље остаје питање колико су грађани свесни својих права и колико се она ефикасно остварују. Проучавање овог аспекта важно је за боље разумевање тренутног стања и за давање препорука које би могле да унапреде ову област.

У истраживању ће примарно бити коришћена правна анализа, кроз проучавање законских текстова, прописа, и подзаконских аката који регулишу право на приступ личним подацима у Републици Србији. Компаративна анализа примењена је приликом упоредне анализе српског правног оквира са европским стандардима. Затим, анализа случајева има за циљ испитивање релевантних судских пресуда, одлука Повереника за информације од јавног значаја и заштиту података о личности, као и других надлежних органа.

У погледу структуре рада, рад је организован у неколико тематских целина које прате логички ток истраживања. У првом поглављу биће одређени појам и врсте података о личности, као и конкретни примери података о личности. У другом поглављу, дефинисаће се нормативни оквир којим је уређена област заштите података о личности. Треће поглавље бавиће се правима субјеката података и обавезама руковалаца у вези са остваривањем права на приступ подацима, док ће четврто поглавље приказати појам и елементе овог права. Затим, пето поглавље приказује начин остваривања права на приступ подацима о личности у изабраним правним порецима. Шесто поглавље за предмет има остваривање права на приступ подацима о личности са посебним акцентом на управноправни режим Републике Србије. У седмом поглављу биће приказана ограничења која су присутна у домену права на приступ подацима о личности. Коначно, закључак ће сумирати кључне налазе рада и понудити препоруке за унапређење заштите права на приступ подацима о личности, са посебним нагласком на побољшање транспарентности и ефикасности у обради захтева за приступ подацима.

І ПОДАЦИ О ЛИЧНОСТИ

1. Појам података о личности

1.1. Нормативно одређење података о личности

Наш Закон о заштити података о личности даје дефиницију појма “*податак о личности*”, који је полазна тачка за разумевање садржине овог рада. Наиме, у смислу одредаба овог Закона, податак о личности јесте “сваки 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.”⁶ Ова дефиниција је готово у потпуности идентична дефиницији коју даје GDPR.

Наиме, GDPR истиче да су подаци о личности “сви подаци који се односе на физичко лице чији је идентитет одређен или се може одредити; физичко лице чији се идентитет може одредити је лице која се може идентификовати посредно или непосредно, посебно помоћу идентификатора као што су име, идентификациони број, подаци о локацији, мрежни идентификатор или помоћу једног или више фактора својствених за физички, физиолошки, генетски, ментални, економски, културни или друштвени идентитет тог физичког лица.”⁷ Дакле, дефиниције се разликују само у нијансама које су занемарљиве. На идентичан начин су дефинисани и сви остали појмови те ЗЗПЛ практично представља копију GDPR-а.

У теорији се истиче да “податак о личности представља сваку информацију која се односи на физичко лице, које се у неком тренутку може идентификовати.”⁸ Суштина дефиниције података о личности јесте могућност идентификације физичког лица на основу одређених идентификатора који су специфични за то лице. Врло је важно истаћи да се прописи о заштити података о личности примењују искључиво на физичка лица, тј. штите се искључиво подаци физичких лица док подаци правних лица не уживају

⁶ Закон о заштити података о личности, чл. 4. ст. 1. тач. 1.

⁷ *General Data Protection Regulation, (EU) 2016/679, art. 4.*

⁸ Данило Кривокапић, Ђорђе Кривокапић, Иван Тодоровић, Стефан Комазец, Андреј Петровски, Катарина Ерцеговић, “*Водич за органе власти – Заштита података о личности*”, Share фондација, Београд, 2016, стр. 13.

заштиту - они су јавно доступни. Правна лица, с друге стране, имају обавезу да штите податке физичких лица.

Одређеност идентита физичког лица подразумева да је име лица познато те да се може разликовати од других лица. На пример, уколико два лица имају идентично име и презиме, лице ће бити идентификовано путем додатних одредница, попут датума рођења. Одредивост лица, пак, значи да се то лице може врло лако идентификовати путем додатних података, попут датума и места рођења.⁹

У погледу значаја података о личности, треба указати на мисао познатог теоретичара Пола Шварца, који податке о личности назива “важном валутом у новом миленијуму”.¹⁰ Ипак, подаци о личности и новац су нераскидиво повезани. На пример, помоћу података о личности, лица која се баве недозвољеним активностима веома лако приступају банковним рачунима грађана и узимају некада огромне количине новца са њих, па можемо рећи и да су подаци о личности и значајнија валута од било ког новца.

Такође, треба направити разлику између појмова “податак” и “информација”. Наиме, савремено доба јесте на неки начин информационо доба.¹¹ Информација, заправо, представља шири појам у односу на података и сачињена је од више међусобно повезаних и обрађених података који се односе на конкретан предмет, описујући његове кључне карактеристике.¹²

У теорији се истиче и да податак представља неку врсту „основне сировине“, док се информација добија након обраде податка.¹³ Дакле, информацију бисмо могли назвати “избрушеним дијамантом”, док је податак “небрушени дијамант”.

У правној теорији истакнути теоретичар Нибле истиче да „информацију није лако дефинисати, с обзиром да се овом изразу придају различита значења. Она се користи за означавање одређених операција у процесу управљања, за обавештења која су садржана у књигама, документима, чланцима, новинама, различитим евиденцијама и досијеима који се могу обрађивати електронским путем“. ¹⁴ С друге стране, „податак се

⁹ <https://www.poverenik.rs/images/stories/dokumentacija-nova/prirucnik/zastitapodatakaprirucnikrukovaoci.pdf>, приступљено: 26.08.2024. године

¹⁰ Paul Schwartz, *Property, Privacy and Personal Data*, Harvard Law Review, vol. 117, Harvard 2003, p. 2056.

¹¹ László Z. Karvalics, *Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression)*, Information Society From Theory to Political Practice Coursebook, Budapest 2008, 29-47, извор: https://www.academia.edu/96324490/Information_Society_what_is_it_exactly_The_meaning, приступљено: 26.08.2024. године

¹² Стефан Андоновић, Драган Прља, Андреј Дилигенски, *Заштита података о личности у Србији*, зборник радова, Београд 2020, стр. 40.

¹³ Стеван Лилић, “Правни аспекти заштите података у аутоматизованим службеним евиденцијама”, *Наша законитост*, бр. 5, Загреб, 1989, стр. 616.

¹⁴ G. V. F. Niblett, *Digital Information and the Privacy Problem*, Organization for Economic Cooperation and Development, Paris 1971, p. 9.

односи на чињенице или појмове који могу бити формализовани и као такви бити подобни за комуникациону манипулацију.“¹⁵

Такође, треба напоменути да постоје и збирке податаке о личности. Наиме, према законској дефиницији под појмом “збирка података” подразумева се “сваки структурисани скуп података о личности који је доступан у складу са посебним критеријумима, без обзира да ли је збирка централизована, децентрализована или разврстана по функционалним или географским основама.”¹⁶

У правној теорији среће се појам “big data” који се према мишљењу неких аутора „односи на пројектовање и реализацију поуздане, дистрибуиране и скалабилне инфраструктуре за управљање, анализу, дељење, складиштење и пренос великих количина података. Потреба за оваквом инфраструктуром настаје због скупова података који су толико велики да их није могуће обрадити помоћу стандардних приступа и алата“.¹⁷

1.2. Практични аспекти података о личности

У погледу практичног аспекта појма података о личности треба истаћи да се питање да ли одређена информација представља податак о личности мора посматрати у оквиру околности сваког конкретног случаја.

На пример, “IP” адреса представља податак о личности када је преко ње могуће доћи до идентитета одређеног физичког лица, непосредно или посредно.¹⁸ ово становиште заузео је и Европски суд за људска права у предмету *Benedik v. Slovenia*.¹⁹

Затим, подаци о возилу нису подаци о личности али могу постати подаци о личности у случају када их је могуће повезати са власником, односно када је на основу њих могуће идентификовати лице које је управљало возилом.²⁰ Према томе, број шасије возила, сам по себи, није податак о личности, јер се односи на возило, које представља ствар, а не на лице. Међутим, наведени податак постаје податак о личности када га је

¹⁵ *Ibid.*

¹⁶ Закон о заштити података о личности, чл. 4. ст. 1. тач. 7.

¹⁷ Божидар Раденковић, Маријана Деспотовић Зракић, Зорица Богдановић, Душан Бараћ, Александра Лабус, *Електронско пословање*, Факултет организационих наука, Београд 2015, стр. 278.

¹⁸ Предмет Повереника бр. 073-14-2369/2019-02, од 15.1.2020. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 6, Београд, 2021, стр. 48.

¹⁹ *Case of Benedik v. Slovenia*, The European Court of Human Rights, 24 April 2018, извор: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-182455%22%5D%7D>, приступљено: 23.08.2024. године

²⁰ Предмет бр. 072-16-2201/2020-06, од 21.12.2020. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 6, Београд, 2021, стр. 59.

могуће повезати са власником, тј. када је, на основу њега, могуће утврдити ко је власник возила.²¹ Такође, персонализована адреса електронске поште, која садржи презиме лица, односно почетно слово имена лица и назив привредног друштва у коме је лице било запослено омогућава идентификацију лица па самим тим следи да адреса електронске поште одређеног лица са оваквим елементима представља његов податак о личности.²²

Подаци о занимању идентификованог лица, односно лица које се може идентификовати, такође представљају податке о личности.²³

2. Подела података о личности

У теорији су познате различите поделе података о личности, у зависности од критеријума. Уколико се као критеријум поделе узме сфера живота одређеног лица, издвајају се три велике целине: приватна, јавна и професионална.²⁴ Наиме, податке који припадају приватној сфери лица обично не деле са другима; затим, подаци из јавне сфере доступни су великом броју лица; на крају, подаци из професионалне сфере повезани су са пословним активностима појединца и за њих су обично заинтересована лица која занима пословање појединца.

I. Према сфери, податке о личности најчешће делимо на:

1) *Податке о личности који се односе на лични живот лица* - нпр. године живота, ставови и мишљења, лична уверења и слично;

2) *Податке о личности који се односе на јавни живот лица* - нпр. подаци о породици и пријатељима;

3) *Податке о личности који се односе на професионални живот лица* - нпр. подаци о образовању, занимању, радном месту;

4) *“Обичне” и “посебне” податке о личности* - посебни подаци о личности уживају посебну заштиту;²⁵

²¹ Предмет Повереника бр. 073-14-2973/2021 од 24. 11. 2021. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 7, Београд, 2022, стр. 179.

²² Предмет Повереника бр. 072-16-110/2021-6, од 19.02.2021. године, извор: <https://pn2.propisi.net/Home/ShowDocument/?di=rp210752&dt=rp&dl=79065>, приступљено: 31.07.2024. године

²³ *L'affaire Khelili c. Suisse, La Cour européenne des droits de l'homme*, 18 octobre 2011, извор: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-107032%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-107032%22]}), приступљено: 31.07.2024. годин

²⁴ Стефан Андоновић, Драган Прља, *Основи права заштите података о личности*, Београд, 2020, стр. 18.

²⁵ Paul Lambert, *Understanding the New European Data Protection Rules*, CRC Press, 2018, p. 112-115.

5) *Податке о малолетним и пунолетним лицима* - подаци о малолетним лицима штите се другачијим механизмима и у другачијем обиму у односу на податке о пунолетним лицима.²⁶

II. Уколико као критеријум поделе узмемо сврху обраде, разликују се:

- 1) *Идентификациони подаци* - нпр. број личне карте/пасоша;
- 2) *Контакт подаци* - нпр. e-mail адреса, број телефона, поштанска адреса;
- 3) *Финансијски подаци* - нпр. број банковног рачуна, број кредитне картице;
- 4) *Подаци о понашању и преференцијама* - нпр. подаци о претрагама на интернету, подаци о коришћењу апликација и web страница;
- 5) *Подаци о локацији* - нпр. - ГПС подаци са мобилног телефона.

III. Према извору, податке о личности делимо на следеће врсте:

- 1) *Податке које пружа сам појединац* - то су подаци које појединац свесно даје приликом различитих интеракција, као што су пријаве за услуге, регистрације и слично. Овде спада, на пример, попуњавање online формулара;
- 2) *Податке који се аутоматски прикупљају* - нпр. колачићи на web страници;
- 3) *Подаци добијени од трећих лица* - нпр. кредитни извештаји из банака, подаци добијени од маркетинг агенција, подаци о здравственом стању од здравствених установа, итд.

Осим теоријског аспекта, подела података о личности има и практичне консеквенце када је реч о условима и обиму заштите појединих категорија личних података, али и праву на приступ личним подацима, о чему ће бити више речи у наставку рада, нарочито у делу рада који је посвећен начину остваривања права на приступ подацима о личности. Такође, треба напоменути да је подела података о личности на оне који се односе на малолетна, односно пунолетна лица значајна приликом одређивања лица које је овлашћени подносилац захтева за приступ подацима. Такође, треба напоменути да не уживају сви подаци правну заштиту, те према одредбама ЗЗПЛ-а предмет заштите нису подаци које лице обрађује за своје потребе, односно потребе свог домаћинства.²⁷

²⁶ Стефан Андоновић, Драган Прља, *Op.cit*, стр. 18.

²⁷ *Закон о заштити података о личности*, чл. 3. ст. 2

II ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ - НОРМАТИВНИ ОКВИР

1. Европска унија

1.1. *General Data Protection Regulation - GDPR*

Право на приступ подацима о личности у Европској унији регулисано је Општом уредбом о заштити података (General Data Protection Regulation, скр. GDPR), која је ступила на снагу 25. маја 2018. године.

GDPR представља темељни правни оквир који регулише заштиту података о личности на нивоу целе Европске уније, а његов главни циљ је да појединцима омогући већу контролу над њиховим личним подацима, уз успостављање уједначених правила за све државе чланице ЕУ.

GDPR је усвојен како би се унапредила и модернизовала правила заштите података која су раније била регулисана Директивом 95/46/ЕЦ.²⁸ За разлику од Директиве, која је државама чланицама остављала одређени степен флексибилности у њеном спровођењу, GDPR се примењује директно и обавезујућа је за све државе чланице, чиме се постиже већи степен хармонизације правила о заштити података у целој ЕУ.

Иако GDPR представља јединствен правни оквир за целу ЕУ, државе чланице имају одређени степен слободе у његовој имплементацији, посебно када је реч о примени специфичних аспеката који нису детаљно регулисани GDPR-ом. На пример, GDPR омогућава државама чланицама да додатно регулишу обраду података у контексту запошљавања, као и у вези са обрадом података у сврхе националне сигурности. Међутим, упркос овој флексибилности, све државе чланице су у обавези да се придржавају основних принципа и права која су установљена GDPR-ом. То укључује право на приступ подацима, које се мора примењивати на исти начин у свим државама чланицама.

Правни оквир ЕУ, кроз GDPR, представља свеобухватан и строго регулисан систем заштите података о личности. Право на приступ подацима је једно од основних права које омогућава појединцима да задрже контролу над својим личним информацијама и да осигурају да се њихови подаци обрађују на законит, правичан и транспарентан начин. Хармонизација правила кроз GDPR, уз кључну улогу Европског

²⁸ *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, извор: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>, приступљено 25.08.2024. године

суда правде, пружа јединствен и ефикасан систем заштите података о личности у Европској унији.

1.2. Остали прописи

Осим GDPR-а, правни оквир Европске уније о заштити података о личности укључује и друге прописе и директиве које додатно регулишу специфичне аспекте заштите података и право на приступ подацима о личности.

- **Директива 2002/58/ЕЦ (*ePrivacy Директива*)**²⁹ - Директива о приватности и електронским комуникацијама (позната као *ePrivacy Директива*) усвојена је 2002. године и представља специјализовани закон који се односи на обраду података у контексту електронских комуникација. Ова директива је комплементарна GDPR-у и примењује се на приватност и заштиту података у вези са електронским комуникацијама, укључујући е-mail, телефонске услуге, СМС поруке и колачиће на веб страницама.

Директива регулише начин на који се подаци прикупљају и чувају путем колачића и сличних технологија, захтевајући информисану сагласност корисника и успоставља правила о поверљивости електронских комуникација, укључујући забрану прислушкивања и праћења комуникација без пристанка корисника. Затим, регулише слање нежељених маркетиншких порука, захтевајући претходну сагласност примаоца за слање таквих порука.

Тренутно је у процесу доношење нове *ePrivacy* Уредбе која ће заменити *ePrivacy* Директиву и ускладити се са GDPR-ом, пружајући модернизован и доследан оквир заштите приватности у дигиталном окружењу.

- **Директива 2011/24/ЕУ (Директива о прекограничној здравственој заштити)**³⁰ - уређује право грађана ЕУ на приступ здравственим услугама у другим државама чланицама и регулише обраду и размену здравствених података. Иако се првенствено бави здравственом заштитом, ова директива има значајан утицај на заштиту података о личности јер обухвата обавезу заштите медицинских података који се размењују прекогранично.

²⁹ *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, извор: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058>, приступљено: 24.08.2024. године

³⁰ *Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare*, извор: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024>, приступљено: 24.08.2024. године

Директива осигурава да се здравствени подаци размењују на сигуран начин и да се поштује поверљивост медицинских информација. Грађани ЕУ имају право на приступ својим медицинским подацима, укључујући и податке размењене између здравствених установа у различитим државама чланицама.

- **Директива 2016/680 (Директива о заштити података у области полицијског и правосудног рада)** ³¹ - односи на обраду података о личности од стране полицијских и правосудних органа у сврхе превенције, истраге, откривања или гоњења криминалних дела и извршења кривичних санкција. Ова директива је позната и као “Law Enforcement Directive”.³²

Директива осигурава да се подаци о личности у контексту полицијског и правосудног рада обрађују на начин који поштује основна права, посебно право на приватност. Појединцима се гарантује право на приступ подацима које полиција или правосудни органи држе о њима, као и право на исправку нетачних података. Такође, Директива поставља строге услове за трансфер података о личности у треће земље, осигуравајући да се права појединаца не угрожавају преносом података ван ЕУ.

Уредба (ЕУ) 2018/1725³³ - успоставља правила о заштити података о личности које обрађују институције, тела, канцеларије и агенције Европске уније. Ова уредба је кључна за унутрашње функционисање ЕУ институција и прати основне принципе GDPR-а. Обезбеђује права на приступ, исправку, брисање и ограничење обраде података које се обрађују унутар институција ЕУ.

Уредба обухвата специфичне процедуре и правила која се односе на обраду података унутар институција ЕУ, укључујући Европску комисију, Европски парламент и друге кључне ентитете.

³¹ *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, извор: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>, приступљено: 24.08.2024. године

³² *Ibid.*

³³ *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)*, извор: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>, приступљено: 24.08.2024. године

2. Република Србија

2.1. Устав Републике Србије

Устав Републике Србије у делу посвећеном људским правима и основним слободама гарантује право на заштиту личних података.³⁴ Такође, Уставом је прописано да је се прикупљање, држање, обрада и коришћење података о личности уредити законом.³⁵ Дакле, само се законом може уредити прикупљање, држање, обрада и коришћење података о личности.³⁶

Такође, Устав јемчи да свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом, као и право на судску заштиту због њихове злоупотребе.³⁷ Према томе, Уставни суд је утврдио да није у складу са Уставом законом дато овлашћење царинском службенику да није дужан да обавести лице на које се односе подаци које прикупља за обављање послова из своје надлежности, ако би то онемогућило или отежало извршење одређеног задатка.³⁸

У погледу сврхе прикупљања података о личности Устав прописује да је забрањена и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом.³⁹

2.2. Закони

- **Закон о заштити података о личности** - када је реч о законском регулисању ове области, најважнији акт јесте важећи Закон о заштити података о личности донет 2018. године, а ступио на снагу 1. јануара 2019. године, чији је предмет регулисање права на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, као и право на заштиту физичких лица у вези са обрадом података о личности коју врше надлежни органи из кривичноправне области.⁴⁰

³⁴ Устав Републике Србије, "Сл. гласник РС", бр. 98/2006 и 115/2021, чл. 42. ст. 1.

³⁵ Устав Републике Србије, чл. 42. ст. 2

³⁶ Одлука Уставног суда Србије, У. бр. 41/10 од 30. 5. 2012. године, извор: <https://www.ustavni.sud.rs/sudska-praksa/baza-sudske-prakse/pregled-dokumenta?PredmetId=7752>, приступљено: 01.08.2024. године

³⁷ Устав Републике Србије, чл. 42. ст. 4.

³⁸ Одлука Уставног суда Србије, У-бр. 41/04 од 26. 11. 2009. године, извор: <https://pn2.propisi.net/Home/ShowDocument/?di=sp31038&dt=sp&dl=31038>, приступљено: 01.08.2024. године

³⁹ Устав Републике Србије, чл. 42. ст. 3.

⁴⁰ Закон о заштити података о личности, чл. 1.

Закон о заштити података о личности обраду личних података заснива на следећим начелима:

- **Начело законитости, правичности и транспарентности** - подаци о личности се морају обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе.⁴¹
- **Начело ограничења сврхе** - подаци о личности се морају 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.⁴²
- **Начело минимизације података** - подаци о личности морају бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде.⁴³
- **Начело тачности** - подаци о личности морају бити тачни и, ако је то неопходно, ажурирани.⁴⁴ Дакле, подаци морају бити усклађени са чињеничним стањем, док се само начело односи и на орган који врши обраду података.⁴⁵
- **Начело ограничења чувања** - подаци о личности се морају чувати у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде.⁴⁶
- **Начело интегритета и поверљивости** - 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 одговарајућих техничких, организационих и кадровских мера.⁴⁷
- **Начело одговорности за поступање** - овим начелом прописана је одговорност руковоаца за примену начела којима се регулише обрада података, и то начела законитости, правичности и транспарентности; ограничења сврхе; минимизације података; тачности; ограничења сврхе, као и интегритета и поверљивости; при чему руковалац мора бити у стању да лицу чији се подаци обрађују предочи примену ових начела.⁴⁸

⁴¹ Закон о заштити података о личности, чл. 5. ст. 1. тач. 1.

⁴² Закон о заштити података о личности, чл. 5. ст. 1. тач. 2.

⁴³ Закон о заштити података о личности, чл. 5. ст. 1. тач. 3.

⁴⁴ Закон о заштити података о личности, чл. 5. ст. 1. тач. 4.

⁴⁵ Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer, eBook, online 2017, 91

⁴⁶ Закон о заштити података о личности, чл. 5. ст. 1. тач. 5.

⁴⁷ Закон о заштити података о личности, чл. 5. ст. 1. тач. 6.

⁴⁸ Закон о заштити података о личности, чл. 5. ст. 2.

Такође, овим Законом уређена су и права лица на која се подаци односе, о чему ће бити више речи у наставку.

- **Закон о слободном приступу информацијама од јавног значаја**⁴⁹ - регулише право грађана да добију информације од јавног значаја које су у поседу државних органа. Право на приступ информацијама често подразумева и обраду података о личности, посебно када су у питању подаци о службеницима или лицима која су на неки начин укључена у јавне послове. Такође, доношењем овог Закона 2004. године је први пут у наш систем уведено независно надзорно тело - Повереник за информације од јавног значаја и заштиту података о личности, који контролише област информација од јавног значаја, према ингеренцијама из Закона о слободном приступу информацијама од јавног значаја, и заштиту података о личности, према ингеренцијама које му пружа Закон о заштити података о личности.
- **Закон о електронским комуникацијама**⁵⁰ - уређује сектор електронских комуникација, укључујући обраду података о личности у контексту телекомуникација и прописује специфичне обавезе оператера у вези са заштитом приватности и података о личности корисника.
- **Закон о информационој безбедности**⁵¹ - поставља правни оквир за заштиту информационих система од претњи и ризика, што укључује и заштиту података о личности који се налазе у тим системима. Закон предвиђа мере за заштиту од неовлашћеног приступа, губитка, уништења или оштећења података о личности, као и обавезе органа и организација у вези са имплементацијом безбедносних стандарда.
- **Закон о здравственој документацији и евиденцијама у области здравства**⁵² - уређује вођење здравствене документације, укључујући и податке о здрављу пацијената, који се сматрају осетљивим подацима о личности. Прописује обавезе здравствених установа у вези са чувањем, обрадом и заштитом ових података, као и права пацијената да приступе својој здравственој документацији.

⁴⁹ Закон о слободном приступу информацијама од јавног значаја, "Сл. гласник РС" бр.120/04, 54/07, 104/09, 36/210 и 105/21.

⁵⁰ Закон о електронским комуникацијама, "Сл. гласник РС", бр. 44/2010, 60/2013 - одлука УС, 62/2014, 95/2018 - др. закон и 35/2023 - др. закон

⁵¹ Закон о информационој безбедности, "Сл. гласник РС", бр. 6/2016, 94/2017 и 77/2019.

⁵² Закон о здравственој документацији и евиденцијама у области здравства, "Сл. гласник РС", бр. 87/2018.

- **Закон о раду**⁵³ - у контексту радних односа, овај закон садржи одредбе које се односе на обраду података о личности запослених. То укључује податке који се прикупљају током запошљавања, вођења евиденције о запосленима, обрачуна зарада, као и у вези са коришћењем права запослених. Закон прописује обавезе послодаваца у вези са заштитом ових података.
- **Закон о матичним књигама**⁵⁴ - уређује вођење матичних књига, које садрже основне податке о личности, као што су подаци о рођењу, венчању, и смрти. Прописује мере за заштиту тих података и права грађана на приступ подацима из матичних књига.

Свакако, ово је само део закона који регулишу ову сложену материју.

2.3. Подзаконски акти и остали акти

Подзаконски акти који прате Закон о заштити података о личности и друге релевантне законе у Републици Србији служе за детаљније уређивање специфичних аспеката заштите података о личности, као што су техничке и организационе мере, вођење евиденција, и поступци за остваривање права лица на која се подаци односе. С обзиром на обимност подзаконских аката у овој области, у наставку рада биће изложени само неки од примера подзаконских аката којима се уређују поједини сегменти заштите података о личности.

- **Правилник о обрасцу и начину вођења евиденције лица за заштиту података о личности**⁵⁵ - уређује прописани образац и начин вођења евиденција о личним подацима.
- **Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности**⁵⁶ - утврђује образац за обавештење Повереника о насталим повредама података о личности.

⁵³ *Закон о раду*, "Сл. гласник РС", бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - одлука УС, 113/2017 и 95/2018 - аутентично тумачење

⁵⁴ *Закон о матичним књигама*, "Сл. гласник РС", бр. 20/2009, 145/2014 и 47/2018.

⁵⁵ *Правилник о обрасцу и начину вођења евиденције лица за заштиту података о личности*, "Сл. гласник РС", бр. 40/2019.

⁵⁶ *Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности*, "Службени гласник РС", број 40/2019.

- **Правилник о заштити података о личности**⁵⁷ који је донела Комора јавних извршитеља - уређује заштиту личних података којима рукују јавни извршитељи.
- **Стратегија заштите података о личности за период од 2023. до 2030. године**⁵⁸ - представља план развоја ове области у периоду од 2023-2030. године.

⁵⁷ *Правилник о заштити података о личности*, "Сл. гласник РС", бр. 98/2021.

⁵⁸ *Стратегија заштите података о личности за период од 2023. до 2030. године*, "Сл. гласник РС", бр. 72/2023.

III КОРПУС ПРАВА ЛИЦА ЧИЈИ СЕ ПОДАЦИ ОБРАЂУЈУ

Закон о заштити података о личности гарантује лицима чији се подаци обрађују одређена права, као посебна права у вези са заштитом података о личности. Реч је о идентичном корпусу права која гарантује и GDPR, а то су:

- **Право на транспарентност** - право субјекта чији се подаци обрађују да на јасан и транспарентан начин буде обавештен о свим аспектима прикупљања података који се односе на њега.⁵⁹
- **Право на информисање и приступ подацима**⁶⁰ - о коме ће бити више речи у наставку.
- **Право на исправку и допуну** - лице на које се подаци односе има право да тражи да се изврши исправка нетачних података или допуна непотпуних података.⁶¹ На пример, у случају правописних или граматичких грешака исправка нетачних података мора се извршити без непотребног одлагања. С друге стране, у одређеним случајевима је на лицу чији се подаци обрађују да одговарајућим доказим поткрепи своје тврдње.⁶²

Такође, ово право је уско повезано са правом на приступ подацима о личности; односно, након што лице оствари право на приступ подацима о личности и на тај начин се упозна са личним подацима који су предмет обраде, има могућност да оствари и право на исправку нетачних података о личности, односно допуну непотпуних података о личности.

- **Право на брисање података, тј. право на заборав**⁶³ - одредбама члана 30. ЗЗПЛ-а прописано је право на брисање података о личности, које подразумева обавезу руковоаца да, под одређеним условима, на захтев лица чије податке обрађује, обрише те податке, као и да, уколико је податке јавно објавио, предузме све разумне мере, у складу са доступним технологијама и могућностима сношења трошкова њихове употребе, у циљу обавештавања других руковалаца који те податке обрађују да је лице на које се подаци односе

⁵⁹ Закон о заштити података о личности, чл. 21-22.

⁶⁰ Закон о заштити података о личности, чл. 23-28.

⁶¹ Закон о заштити података о личности, чл. 29.

⁶² Приручник о европском праву заштите података, издање 2018, стр. 219-221, извор: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_sr.pdf, приступљено: 02.09.2024. године

⁶³ Закон о заштити података о личности, чл. 30. ст. 1-2.

поднело захтев за брисање свих копија података и упућивања, односно електронских веза према тим подацима.⁶⁴

- **Право на ограничење обраде**⁶⁵ - у одређеним ситуацијама, на пример: уколико лице на које се подаци односе оспорава тачност података о личности; односно, уколико је обрада незаконита, а лице на које се подаци односе се противи брисању података о личности и уместо брисања захтева ограничење употребе података; затим, уколико руковаоцу више нису потребни подаци о личности за остваривање сврхе обраде, али их је лице на које се подаци односе затражило у циљу подношења, остваривања или одбране правног захтева; као и уколико је лице на које се подаци односе поднело приговор на обраду, а у току је процењивање да ли правни основ за обраду од стране руковаоца претеже над интересима тог лица.⁶⁶

Попут права на исправку и допуну и права на брисање података о личности, и право на ограничење обраде је уско повезано са правом на приступ подацима о личности.

- **Право на преносивост података** - омогућава лицу на које се подаци односе да добије од руковаоца податке, које му је претходно дало, у структурисаном, уобичајено коришћеном и електронски читљивом облику, као и да их пренесе другом руковаоцу.⁶⁷
- **Право на приговор** - лице на које се подаци односе има право да у сваком тренутку поднесе руковаоцу приговор на обраду његових података о личности, у складу са законом. Уколико је поднет приговор, руковалац је дужан да прекине са обрадом података о лицу које је поднело приговор, изузев у одређеним, законом прописаним, случајевима. Такође, код обраде података за потребе директног оглашавања, укључујући и профилисање које је повезано са директним оглашавањем, лице на које се подаци односе може увек поднети приговор и у том случају се подаци о личности не могу даље обрађивати у такве сврхе.⁶⁸

⁶⁴ Предмет Повереника бр. 073-14-1720/2019-02, од 1.10.2019. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 6, Београд, 2021, стр. 59.

⁶⁵ Закон о заштити података о личности, чл. 31. ст. 1. тач. 1-4.

⁶⁶ *Ibid.*

⁶⁷ Закон о заштити података о личности, чл. 36.

⁶⁸ Закон о заштити података о личности, чл. 37. ст. 1-3.

IV ОДРЕЂЕЊЕ ПРАВА НА ПРИСТУП ЛИЧНИМ ПОДАЦИМА

1. Појам права на приступ личним подацима

Право на транспарентност састоји се из два елемента: први елемент јесте право на обавештеност, док је други елемент право на приступ подацима. Уколико посматрамо са становишта улоге грађана, закључујемо да код права на обавештеност грађани имају пасивну улогу, док код права на приступ подацима грађани имају активну улогу.⁶⁹

У погледу правне природе права на приступ подацима о личности истичу се неке сличности са правом на слободан приступ информацијама од јавног значаја. Право на слободан приступ информацијама од јавног значаја засновано је на принципу јавности, који је контрадикторан концептима тајности и затворености.⁷⁰ Ово право омогућава приступ информацијама које су значајне за ширу друштвену заједницу и које поседују органи јавне власти.⁷¹ С друге стране, право на приступ подацима о личности омогућава грађанима да од руковооца или обрађивача, тј. правног или физичког лица, државног органа, агенције или другог тела које обрађује податке о личности, затраже информације у вези са својим подацима.⁷²

Уопштено, “приступ” се односи на скуп радњи које руковалац предузима да прикаже особи податке који се обрађују. Право на приступ има за циљ да омогући приступ самим личним подацима, а не опису обраде.

У многим случајевима, овај аспект права на приступ материјализује се у облику “копије” оригиналних личних података. Међутим, право на приступ и право на добијање копије личних података су два одвојена права. Треба напоменути да обезбеђивање “копије” података није једини начин на који контролор може да обезбеди приступ. У неким случајевима копија може бити најприкладнији приступ, али копија не мора увек бити транспарентна. У одређеним околностима, може бити адекватније понудити алтернативне методе приступа подацима уместо пружања копије. Ове привремене методе приступа могу укључивати вербалну комуникацију, преглед фајлова или приступ на лицу места који омогућава преглед личних података у корисничком интерфејсу. Ове методе могу бити одговарајуће када су интереси особе

⁶⁹ Стефан Андоновић, Драган Прља, *Op.cit.*, стр. 97.

⁷⁰ Владимир Водинелић, *Право на слободан приступ информацијама од јавног значаја као уставно право*, Слободан приступ информацијама – уставно јемство и законске гаранције, Београд 2004, стр. 9.

⁷¹ Стефан Андоновић, Драган Прља, *Op.cit.*, стр. 97.

⁷² *Ibid.*

чији се подаци обрађују у питању или ако она то посебно захтева. Приступ на лицу места може такође бити почетни корак када се обрађује велики обим недигиталних података, омогућавајући особи да разуме који се лични подаци обрађују и донесе информисану одлуку о томе које податке жели да добије кроз копију.⁷³

Такође, треба поменути случај који је разматрала Данска агенција за заштиту података (ДПА). Наиме, након што је престао да ради у општини, бивши запослени је затражио приступ свим комуникацијама које су се односиле на његове радне дужности, како би прикупио доказе за могући спор са општином око свог отпуштања. Општина је пружила неке информације у складу са правилима о приступу документима и покушала да наведе бившег запосленог да појасни и ограничи свој захтев, објашњавајући да је жељени материјал био обиман након неколико година рада. Међутим, захтев није био разјашњен од стране субјекта података. Упркос томе, општина је касније одбила да обезбеди додатне информације, позивајући се на чињеницу да је тражени материјал обухватао огромну количину белешки, писама и мејлова који су се односили на његове радне задатке. Општина је да је захтев бившег запосленог за приступ свим мејловима, белешкама и писмима које је послао или потписао пре него што је напустио посао био претеран према члану 12(5)(б) GDPR-а. Овај захтев је обухватао велики број личних података који су углавном били везани за његове радне обавезе, а не за његове личне карактеристике. Дански ДПА је потврдио да, према члану 15. GDPR-а, субјекат података има право на приступ својим личним подацима које обрађује руковалац података, али да ово право није апсолутно, те да руковалац података може одбити да удовољи захтеву ако је он очигледно неоснован или претеран. ДПА је такође нагласио да, иако информације у таквим комуникацијама представљају личне податке, те информације се пре свега односе на радне дужности субјекта података, а не на његове личне атрибуте. Због тога, ДПА је одлучио да није имао разлога да поништи одлуку општине, јер су се тражене информације односиле на неколико година и биле су везане искључиво за његове радне задатке.⁷⁴

⁷³ [https://gdprhub.eu/index.php?title=Article_15_GDPR#\(1\)_The_Right_of_Access](https://gdprhub.eu/index.php?title=Article_15_GDPR#(1)_The_Right_of_Access), приступљено: 06.09.2024. године

⁷⁴ Tidligere arbejdsgiver kunne afvise at efterkomme anmodning om indsigt, извор: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/tidligere-arbejdsgiver-kunne-afvise-at-efterkomme-anmodning-om-indsigt>, приступљено: 06.09.2024. године

2. Елементи права на приступ личним подацима

У складу са Законом, грађани су овлашћени да затраже информацију о томе да ли руковалац поседује одређене податке о лицу које остварује право на приступ и да ли се ти подаци обрађују, те, у случају потврђених одговора на ова питања, лице има право да приступи својим подацима и добије информације о питањима која се односе на обраду.⁷⁵

Законодавац таксативно набраја елементе које садрже ове информације, и то:

- 1) *сврха обраде* - право да зна за које сврхе се подаци обрађују;
- 2) *врсте података о личности који се обрађују* - информације о врстама личних података који се обрађују;
- 3) *податке о примаоцима којима су подаци о личности откривени или ће им бити откривени, а посебно примаоцима у другим државама или међународним организацијама* - право да зна ко су примаоци или категорије прималаца којима су подаци откривени или ће бити откривени, укључујући примаоце у трећим земљама или међународним организацијама;
- 4) *предвиђени рок чувања података о личности, односно критеријумим за одређивање рока* - право да зна колико дуго ће се подаци чувати или критеријуме за одређивање тог периода;
- 5) *постојање права на исправку или заборав података о личности, права на ограничење обраде и права на приговор на обраду*;
- 6) *право на притужбу Поверенику* - право да зна коме може поднети притужбу (надзорном органу за заштиту података);
- 7) *доступне информације о извору података о личности, ако подаци о личности нису прикупљени од лица на које се односе*;
- 8) *могућност аутоматизованог доношења одлуке* - информације о постојању аутоматизованог одлучивања, укључујући профилисање, те значај и предвиђене последице такве обраде.⁷⁶

Када су појединци свесни начина на који се њихови подаци обрађују, могу донети информисане одлуке о томе да ли ће пристати на даљу обраду или ће искористити своја права да затраже ограничење или брисање података.

⁷⁵ Стефан Андоновић, Драган Прља, *Op.cit.*, стр. 97.

⁷⁶ Закон о заштити података о личности, чл. 26. ст. 1. тач. 1-6.

V ПРИСТУП ЛИЧНИМ ПОДАЦИМА У ИЗАБРАНИМ ПРАВНИМ ПОРЕЦИМА

1. Словенија

Словенија важи за најразвијенију земљу бивше Југославије и чланица је Европске уније већ двадесет година, односно од 2004. године. У том смислу, усвојила је европске принципе и вредности и у област заштите података о личности и имплементирала GDPR, поред којег примењује и свој национални закон којим уређује заштиту података о личности⁷⁷. Велики допринос заштити података о личности, а самим тим и праву на приступ подацима о личности, дало је словеначко надзорно тело, тј. агенција.⁷⁸

У пракси се појавио и један веома занимљив и унеколико специфичан случај. Случај пружа важан увид у правне и етичке аспекте приступа личним подацима након смрти. Наиме, кћер чији је отац преминуо је затражила приступ медицинској документацији свог преминулог оца. Пружалац здравствених услуга одбио је овај захтев, наводећи документ који је наводно потписао покојни отац, а који забрањује откривање његових медицинских података ћерци. Тврдећи да је овај документ у складу са жељама преминулог. Међутим, кћер је оспоравала валидност тог документа, тврдећи да није изричито забранио приступ медицинској документацији након очеве смрти и да њен отац, због деменције, можда није био способан да разуме последице потписивања документа. Пружилац здравствених услуга није реаговао на овај захтев. Кћер се затим обратила тамошњем надзорном телу притужбом због ускраћивања приступа медицинској документацији њеног преминулог оца. У поступку надзора, агенција је утврдила да документ који је потписао преминули отац није јасно и недвосмислено забранио приступ ћерци и истакла право на информисање о здравственој документацији после смрти пацијента, у складу са чланом 42. словеначког Закона о правима пацијената који предвиђа да право на приступ документацији након смрти пацијента обухвата, између осталог, децу пацијента, под условом да је приступ неопходан за постизање легитимне сврхе, као што је утицај на здравље.⁷⁹

⁷⁷ Zakon o varstvu osebnih podatkov, Uradni list RS, št. 163/22, извор: <https://pisrs.si/pregledPredpisa?id=ZAKO7959>, приступљено: 05.09.2024. године

⁷⁸ <https://www.apvp.si/si>, приступљено: 05.09.2024. године

⁷⁹ IP (Slovenia) - 07106-8-2023, извор: [https://gdprhub.eu/index.php?title=IP_\(Slovenia\)_-_07106-8-2023&mtc=today](https://gdprhub.eu/index.php?title=IP_(Slovenia)_-_07106-8-2023&mtc=today), приступљено: 03.09.2024. године

Дакле, документ мора бити јасан и недвосмислен у вези са забраном приступа. Ако документ није јасно дефинисао да забрањује приступ након смрти, може бити правно оспорен. На основу анализе, документ није био довољно јасан, што је довело до оспоравања његове валидности.

2. Хрватска

Можемо рећи да је у области заштите података о личности међу земљама бивше Југославије Хрватска на другом месту, одмах иза Словеније.

Као последња држава која се придружила Европској унији и Хрватска је била у обавези да своје законодавство усклади са европским стандардима, укључујући и GDPR, па је у том циљу донела спроведбени закон.⁸⁰ Надзор над заштитом личних података поверен је Агенцији за заштиту особних података, познатој под скраћеницом АЗОП.⁸¹

У једном од многобројних случајева који су се нашли пред АЗОП-ом, подносилац притужбе упутио је компанији захтев за приступ личним подацима који су били у њиховом поседу. Међутим, компанија је одговорила генеричким информацијама о обради личних података, уопштено, а не конкретно на питања подносиоца. Након што подносилац није добио задовољавајући одговор, поново је упутио прецизнији захтев, али није добио никакав одговор. Компанија је образложила да су права на приступ и брисање података прописана у њиховој Изјави о заштити података и да се могу остварити искључиво на одређеном месту, што није било у складу са прописима. У овом случају, компанија је пружила генеричке информације које нису обухватиле конкретне податке који су се односили на подносиоца захтева. АЗОП је обавезао компанију да подносиоцу захтева у року од 8 дана достави потпун одговор на све аспекте његовог захтева и истакао да неиспуњавање обавеза и генерички одговори које је компанија доставила подносиоцу захтева представљају повреду права на приступ личним подацима.⁸²

Овај случај илуструје важност поштовања права на приступ личним подацима у складу са законским захтевима. Генерички одговори који не обухватају специфичне информације о подносиоцу захтева представљају повреду права на приступ. Компаније

⁸⁰ Zakon o provedbi Opće uredbe o zaštiti podataka, NN 42/18, извор: <https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka>, приступљено: 04.09.2024. године

⁸¹ <https://azop.hr/>, приступљено: 04.09.2024. године

⁸² Rješenje AZOP-a, Zagreb, 10. prosinca 2021. године, извор: <https://azop.hr/wp-content/uploads/2022/09/Rjesenje-pristup-osobnim-podacima.pdf>, приступљено: 04.09.2024. године

морају осигурати да одговори на захтеве за приступ буду јасни, прецизни и у складу са законом.

3. Пракса Европског суда за људска права

У случају Гаскин против Уједињеног Краљевства⁸³ који се нашао пред ЕСЉП-ом, подносилац представке, господин Гаскин, покренуо је поступак против локалних власти тражећи надокнаду штете због немара током свог периода у старатељству од 1960. до 1974. године, када је био смештен код различитих усвојитеља. Он је тврдио да је током тог периода лоше поступано с њим и да му је потребна документација о условима и особама које су биле одговорне за његово старатељство како би разумео своју прошлост и превазишао проблеме. Локалне власти су имале законску обавезу да воде поверљиве архиве везане за њега и његово старатељство. Подносилац представке је тражио приступ тим документима на основу права на информације које је желео да користи за правне поступке и како би се преиспитао стандард бриге о деци.

Суд је узео у обзир да је захтев подносиоца представке за приступ досијеу део његовог права на приватни и породични живот према члану 8. Европске конвенције о људским правима. Суд је утврдио да је досије у вези са личном историјом подносиоца представке и да би му приступ тим информацијама помогао у разумевању његовог детињства, што је од значаја за његов приватни живот. Иако је поверљивост документације важна за функционалност система старања о деци и заштиту права давалаца информација, Суд је закључио да систем Уједињеног Краљевства, који захтева пристанак даваоца информација за приступ досијеима, не пружа довољну заштиту приватности појединца када давалац није доступан или одбија дати пристанак. Суд је нашао да систем није пружио одговарајућу процедуру за доношење одлука о приступу документима у случајевима када давалац није доступан, што је представљало кршење члана 8. Конвенције. Суд је закључио да је дошло до повреде члана 8. Европске конвенције. Међутим, Суд је једногласно одлучио да члан 10. Конвенције не укључује обавезу државе да саопшти информације појединцу, што значи да право на слободу изражавања у овом случају није прекршено.

Овај случај наглашава важност постојања одговарајућих процедура за заштиту права на приватност и приступ информацијама, посебно у контексту старатељства и архивирања поверљивих података.

⁸³ Case of Gaskin v. The United Kingdom , (Application no. 10454/83), ECHR, Strasbourg, 07 July 1989, извор: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-57491%22%7D>, приступљено: 06.09.2024. године

У случају К.Х. и остали против Словачке⁸⁴ подносиоце представке јесу осам жена ромског порекла, које су биле хоспитализоване на гинеколошком и акушерском одељењу у две болнице у источној Словачкој и сумњале су да су током порођаја царским резом нелегално стерилизоване без њиховог знања и пристанка. Иако су покушавале да поново остану трудне, ниједна од њих није успела. У 2004. години, подносиоце представке су се обратиле невладиној организацији и затражиле приступ и фотокопије своје медицинске документације. Док су им одобрени увид у документацију, њихови захтеви за фотокопирање су одбијени на основу домаћих прописа који су сматрали да је медицинска документација имовина болнице и да је потребно ограничити приступ како би се спречила злоупотреба података. Након увођења нових прописа 2005. године, свим женама, осим једној чија је документација изгубљена, одобрен је приступ медицинској документацији и дозвољено им је да је фотокопирају.

Суд је утврдио да државе имају позитивну обавезу да омогућавају појединцима приступ документацији која садржи личне податке. Иако је национални закон оправдавао ограничења приступа документацији због заштите података од злоупотребе, Суд је сматрао да је таква забрана фотокопирања неприхватљива. С обзиром на то да су подносиоце већ имале приступ својој документацији, није било оправдано спречити их да праве фотокопије, посебно јер би злоупотреба информација могла бити спречена другим мерама. Држава није успела да докаже да је постојала довољна потреба за одбијањем фотокопирања документације. Суд је једногласно закључио да је дошло до повреде члана 8. Конвенције.

Подносиоце представке су тврдиле да им је одбијање да фотокопирају медицинску документацију отежало приступ суду и ефикасно тражење правде за могуће повреде. Иако приступ суду није био потпуно онемогућен, строга примена закона о документацији умањила је њихову способност да се бране и траже обештећење. Суд је сматрао да је национална ограничења за приступ документима негативно утицала на њихово право на ефикасан приступ суду. Због тога је пресудом утврђено да је дошло до повреде члана 6. Конвенције и Суд је наложио да се свакој од жена, подносиоце представке, исплати 3.500 евра на име надокнаде нематеријалне штете.

⁸⁴ Case of K.H. and others v. Slovakia (Application no. 32881/04), ECHR, Strasbourg, 28 April 2009, извор: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-92418%22%5D%7D>, приступљено: 07.09.2024. године

Овај случај илуструје важност омогућавања приступа личним подацима и документацији у контексту заштите приватности и права на ефикасан приступ суду.

4. Пракса Суда правде Европске уније

У пресуди C-487/21⁸⁵, у вези са случајем који је вођен у Аустрији, Европски суд је утврдио да право на приступ копији личних података значи да испитивани појединац треба да добије верну и разумљиву репродукцију свих својих личних података.

Ово право укључује право на добијање копија извода из докумената или чак целих докумената, односно извода из база података које садрже те податке, ако је то неопходно како би се омогућило ефикасно остваривање права на заштиту својих личних података, узимајући у обзир права и слободе других лица.

Европски суд даје дословно и систематско тумачење прве реченице члана 15. став 3. GDPR-а, који предвиђа право испитаника да добије копију својих личних података које водитељ обраде обрађује. Иако овај члан не садржи дефиницију појма “копија”, мора се водити рачуна о уобичајеном значењу тог појма, које се односи на верну репродукцију или препис изворника.

Даље, суд сматра да овај члан GDPR-а даје испитанику право на добијање верне репродукције својих личних података, подразумеваних у ширем смислу, који су предмет обраде од стране водитеља обраде. Суд утврђује да се појам “копија” не односи се на документ као такав, већ на личне податке које документ садржи, и који морају бити потпуни. Стога, копија личних података мора садржавати све личне податке који се обрађују. При томе, треба водити рачуна о дефиницији личних података. Према GDPR-у, лични подаци су свака информација о појединцу на основу које се тај појединац може “изравно или неизравно” идентификовати, укључујући и информације које омогућавају идентификацију када се комбинују с другим евиденцијама или изворима информација. Стога је важно препознати све информације унутар документације које се могу сматрати личним подацима појединца и обезбедити их у форми копије када испитивани појединац захтева приступ својим личним подацима према члану 15. GDPR-а.

⁸⁵ Case C-487/21, F.F. v Österreichische Datenschutzbehörde, Österreichische Datenschutzbehörde and CRIF, Judgment of the Court (First Chamber) of 4 May 2023, извор: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=274764&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2379483>, приступљено: 12.09.2024. године

Међутим, овај случај је имао велики утицај на аустријску судску праксу. Наиме, физичко лице у Аустрији, је закупило одређени простор и у својству закупца затражило је право на приступ својим личним подацима у складу са чланом 15. GDPR-а. У том слислу, лице је очекивало да ће у достављеној документацији добити и копије личних података, укључујући копију уговора о закупу простора и копију комуникације између закупца и закуподавца. Међутим, копије уговора о закупу и комуникације са закуподавцем нису биле достављене, па се физичко лице обратило надзорном телу за заштиту података. Надзорно тело је истакло да се право на приступ личним подацима односи само на личне податке, што значи да није обавезно пружити копије целокупне документације. Европски суд у је у поменутој пресуди Ц-487/21 претходно утврдио да право на копију личних података значи да испитаник мора добити верну и разумљиву репродукцију свих својих личних података. Незадовољно решењем надзорног тела, физичко лице је поднело тужбу аустријском савезном суду. Аустријски суд је, како се очекивало, следио претходну пресуду Европског суда и пресудио да нема основа за давање копија целе тражене документације.

Посебно занимљив део пресуде аустријског суда односи се на захтев за копију комуникације између закуподавца и закупца, где се суд позвао на члан 15. став 4. GDPR-а, који наглашава да право на приступ личним подацима не сме негативно утицати на права и слободе других. Суд је утврдио да је физичко лице, као купац, већ било у потпуности упознато са садржајем комуникације с најмодалцем. Истовремено, суд је задржао став да закуподавац, кога на суду заступа адвокат, има право на поверљивост документације, укључујући и копију комуникације са тужиоцем, коју је дао свом адвокату у оквиру адвокатске тајне. Право на очување адвокатске тајне превладава над правом физичког лица на приступ својим личним подацима у вези с претходном комуникацијом.⁸⁶

⁸⁶ W252 2246156-1, Bundesverwaltungsgericht, 22.01.2024, извор: https://www.ris.bka.gv.at/JudikaturEntscheidung.wxe?Abfrage=Bvvg&Dokumentnummer=BVWGT_20240122_W252_2246156_1_00, приступљено: 14.09.2024. године

VI ОСТВАРИВАЊЕ ПРАВА НА ПРИСТУП ЛИЧНИМ ПОДАЦИМА

1. Овлашћени подносиоци и форма захтева

Остваривање права и слобода других лица не може се угрозити остваривањем права на достављање копије лицу на које се ти подаци односе.⁸⁷ Такође, у поступку остваривања права на приступ подацима о личности физичко лице може да оствари право на приступ само оним подацима о личности који се односе на њега.⁸⁸ Дакле, физичко лице најчешће само, лично, подноси захтев за остваривање права на приступ личним подацима.

У претходном делу рада приказана је подела података о личности, те је истакнуто да се подаци могу поделити на оне који се односе на пунолетна лица и податке који се односе на малолетна лица. Када је реч о значају ове поделе у смислу остваривања права на приступ подацима о личности, треба истаћи да остваривање права на приступ, у вези са обрадом података који се односе на малолетно дете, припада законском заступнику детета, односно родитељима када заједнички врше родитељско право или једном родитељу коме је судском одлуком поверено дете на самостално старање.⁸⁹

Ипак, треба напоменути да надзорно тело Уједињеног Краљевства Велике Британије и Северне Ирске препоручује да се у случају тражења приступа подацима детета, треба најпре проверити да ли је дете довољно зрело да разуме своја права. Ако је захтев од поднет од стране самог детета и ако је неспорно да дете може да разуме своја права, препоручује се давање одговора директно детету. Међутим, могуће је дозволити родитељу или старатељу да остварује права детета у њихово име ако дете то одобри или ако је очигледно да је то у најбољем интересу детета. Ако је дете довољно зрело, оно може овластити неког другог, осим родитеља или старатеља, да затражи приступ подацима о личности у дететово име.⁹⁰

⁸⁷ Предмет Повереника бр. 072-16-2992/2019-06 од 28. 1. 2020. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 6, Београд, 2021, стр. 97.

⁸⁸ Предмет Повереника бр. 072-16-705/2020-06 од 13. 4. 2020. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 6, Београд, 2021, стр. 50.

⁸⁹ Предмет Повереника бр. 072-16-5724/2019-06 од 7. 8. 2020. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 6, Београд, 2021, стр. 103.

⁹⁰ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-of-access/>, приступљено: 09.09.2024. године

Такође, и у другим случајевима у којима субјекат података није у могућности да сам поднесе захтев на пример, због здравственог стања, законски заступник може поднети захтев у његово име. Наиме, одредбама Закона о општем управном поступку, прописано је да странку која није процесно способна заступа законски заступник.⁹¹ Затим, странке се неретко одлучују да за подношење захтева за остваривање права на приступ подацима о личности ангажују пуномоћника из реда адвоката. Међутим, осим адвоката, у управном поступку се у улози пуномоћника странке може појавити свако пословно способно лице, изузев лица које се бави надриписарством.⁹² Ипак, странке у пракси често нису свесне ове могућности, с обзиром на то да је управни поступак специфичан и пружа веће могућности у односу на парнични поступак у којем пуномоћник физичког лица може бити адвокат, крвни сродник у правој линији, брат, сестра или брачни друг, као и представник службе правне помоћи јединице локалне самоуправе који је дипломирани правник са положеним правосудним испитом.⁹³

Такође, треба напоменути да приликом подношења захтева од стране пуномоћника треба пажљиво поступати. На пример, АА, кога заступа адвокат НН, поднео је 23.11.2022. године притужбу Поверенику због повреде права на приступ подацима о личности од стране Банке, након што је 4.7.2022. године поднео захтев за доставу документације. АА је тврдио да је Банка требала да му достави податке о уговору који он не поседује, у складу са чланом 36. Закона о адвокатури и да је поступила супротно одредбама члана 21. и 26. ЗЗПЛ-а. Повереник је разматрао притужбу и утврдио да се притужба не односи на повреду права на приступ подацима о личности, већ на одбијање Банке да достави документацију на основу Закона о адвокатури. Повереник је закључио да није надлежан за поступање у овом случају, јер се предметни захтев односио на закон који регулише адвокатуру, а не на ЗЗПЛ.⁹⁴

У погледу форме захтева за приступ подацима, нема сметњи да се захтев упути и усменим путем, али је руковалац дужан да сачини записник у овом случају.⁹⁵

⁹¹ Закон о општем управном поступку, "Сл. гласник РС", бр. 18/2016, 95/2018 - аутентично тумачење и 2/2023 - одлука УС, чл. 47. ст. 1.

⁹² Закон о општем управном поступку, чл. 49. ст. 3.

⁹³ Закон о парничном поступку, "Сл. гласник РС", бр. 72/2011, 49/2013 - одлука УС, 74/2013 - одлука УС, 55/2014, 87/2018, 18/2020 и 10/2023 - др. Закон, чл. 85. ст. 2.

⁹⁴ Предмет Повереника бр. 072-16-1809/2022-06, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 8, Београд, 2023, стр. 46.

⁹⁵ Стефан Андоновић, Драган Прља, *Op.cit.*, стр. 98.

Остваривање права на приступ подацима о личности не може се условити подношењем захтева на обрасцу који је прописао руковалац подацима.⁹⁶

Такође, постоје схватања да се захтев може упутити и путем друштвених мрежа, као што су Facebook, Instagram или LinkedIn.⁹⁷ Међутим, захтев упућен компанији Meta ради омогућавања поновног приступа фејсбук налогу не може се сматрати захтевом за приступ подацима о личности.⁹⁸ Такође, ни приговор клијента није захтев за остваривање права на приступ подацима.⁹⁹

Дакле, захтев за приступ подацима о личности мора бити јасан, прецизан и поднет у писаном облику, електронским путем или на други начин који омогућава несумњиву идентификацију подносиоца захтева. Законски оквир не прописује строгу форму захтева, али је уобичајено да захтеви садрже следеће елементе:

- а) идентификацију подносиоца захтева - име, презиме, адреса, контакт подаци (е-маил, телефон), као и други подаци који омогућавају идентификацију субјекта података;
- б) спецификацију захтева - јасно наведено шта се тачно тражи (нпр. да ли се захтева само потврда да ли се подаци обрађују, или се тражи копија свих података који се обрађују);
- в) додатне информације - информације које би могле олакшати идентификацију података, попут временског периода у којем су подаци обрађивани, конкретне активности или сврхе обраде.

2. Поступање по захтеву за приступ подацима

Када лице чији се подаци обрађују (субјект података) поднесе захтев за приступ својим подацима, руковалац подацима (правно или физичко лице које врши обраду података) има обавезу да поступи у складу са захтевом и да одговори у законом прописаном року. Први корак у поступању по захтеву за приступ подацима о личности је пријем захтева од стране руковаоца подацима. Сви захтеви морају бити евидентирани

⁹⁶ Предмет Повереника бр. 072-16-1184/2023-06, *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 9, Београд, 2024, стр. 95.

⁹⁷ Стефан Андоновић, Драган Прља, *Op.cit.*, стр. 98.

⁹⁸ Предмет Повереника бр. 072-16-2536/2022-06, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 8, Београд, 2023, стр. 58.

⁹⁹ Предмет бр. 072-16-1213/2022-06, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 8, Београд, 2023, стр. 44.

у регистру захтева, који треба да садржи податке о подносиоцу захтева, датуму пријема захтева, опис захтева и све друге релевантне информације које могу бити потребне за обраду захтева. Такође, руковалац има право да затражи додатне информације ради верификације идентитета подносиоца захтева како би се осигурало да се подаци не откривају неовлашћеним лицима.

Када је реч о правној природи одговора руковоаца подацима на захтев субјекта чији се подаци обрађују да приступи својим личним подацима, постоји схватање да је реч о управној радњи.¹⁰⁰ У смислу одредаба Закона о општем управном поступку, управна радња јесте материјални акт органа који утиче на права, обавезе или правне интересе странака, као што су вођење евиденција, издавање уверења, пружање информација, примање изјава и друге радње којима се извршавају правни акти.¹⁰¹

Законодавац прописује да је руковалац података у обавези да, на захтев лица на које се подаци односе, њему достави копију података које обрађује, при чему има право на накнаду нужних трошкова за израду додатних копија које захтева лице на које се подаци односе.¹⁰² Руковалац мора доставити копију свих личних података које поседује о подносиоцу захтева, укључујући све информације о сврси обраде, категоријама података, примаоцима података, периоду чувања података и другим релевантним информацијама. Поред копије података, руковалац мора пружити све релевантне информације које захтева закон, као што су обавештења о праву на исправку, брисање података или ограничење обраде.

У случају из 2021. године, лице је поднело притужбу Поверенику јер му руковалац није доставио копију уговора о кредиту са пратећом документацијом, иако је тај уговор део збирке података које руковалац обрађује. Повереник је утврдио да је притужба основана, јер је руковалац прекршио обавезу прописану чланом 26. став 3. ЗЗПЛ-а, који даје право лицу да добије копију својих података. У својој одбрани, руковалац је навео да је став Народне банке Србије да се обавеза достављања копије уговора односи само на постојеће уговорне односе, а не на оне који су престали, те да је притужилца већ добила примерак документације приликом закључења уговора. Међутим, Повереник је оценио да је овакво тумачење закона неосновано, јер Закон о заштити података о личности даје лицу право на приступ подацима без обзира на друге правне основе или активност пословног односа. Руковалац није у обавези да проверава

¹⁰⁰ Стефан Андоновић, *Op.cit.*, стр. 182.

¹⁰¹ Закон о општем управном поступку, чл. 27.

¹⁰² Закон о заштити података о личности, чл. 26. ст. 3.

сврху захтева лица, нити лице мора да објасни зашто тражи своје податке. На основу свега наведеног, Повереник је наложио руковоаоцу да достави тражену документацију у року од осам дана, уз заштиту података трећих лица.¹⁰³ Ова одлука наглашава важност права на приступ подацима и јасно дефинише обавезе руковоаоца у смислу заштите података о личности у Србији.

У погледу праксе, треба напоменути да захтев за издавање копије посебних података о личности садржаних у извештају лекара није захтев за издавање потврде за коју се плаћа накнада.¹⁰⁴

Закон допушта и достављање података у електронској форми. Уколико је лице захтев за приступ подацима о личности поднело електронским путем, информација се мора пружити електронским путем ако је то могуће, осим ако је то лице захтевало да се информација пружи на други начин.¹⁰⁵ Општи тренд дигитализације и увођење е-управе у наш правни живот на најбољи начин приказује и тежњу државних органа да поступак заштите података о личности учине ефикаснијим и економичнијим.

У погледу одређења појма “руководилац података о личности”, треба истаћи законску дефиницију према којој се руководилац података о личности дефинише као “физичко или правно лице, односно орган власти који самостално или заједно са другима одређује сврху и начин обраде”¹⁰⁶. Такође, неретко се срећемо и са појмом “обрађивач података о личности” који је одређен као “физичко или правно лице, односно орган власти који обрађује податке о личности у име руковоаоца”.¹⁰⁷ Дакле, обрађивач је “продужена рука” руковоаоца података.

Затим, треба напоменути да је руководилац подацима у обавези да примени одговарајуће техничке и организационе мере како би обезбедио сигурност података током обраде захтева за приступ. Ово може укључивати мере као што су шифровање и заштита података, контрола приступа, тј. ограничење приступа подацима само овлашћеним лицима која имају потребу да приступе подацима ради обраде захтева или евидентирање активности, што подразумева чување евиденција о томе ко је приступао

¹⁰³ Предмет Повереника бр. 072-16-1129/2021-6, од 3. 8. 2021. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 7, Београд, 2021, стр. 101.

¹⁰⁴ Предмет Повереника бр. 072-16-815/2023-06, од 23.3.2023. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 9, Београд, 2024, стр. 81.

¹⁰⁵ Предмет Повереника бр. 072-16-1857/2020-06, од 5.10.2020. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 6, Београд, 2021, стр. 123.

¹⁰⁶ *Закон о заштити података о личности*, чл. 4. ст. 1. тач. 8.

¹⁰⁷ *Закон о заштити података о личности*, чл. 4. ст. 1. тач. 9.

подацима и у коју сврху, као и о свим другим активностима везаним за обраду података.

Када је реч о преносу података о личности у другу државу или међународну организацију, лицу на које се односе припада право да буде информисано о одговарајућим мерама заштите које се односе на пренос.¹⁰⁸ Ово право је веома значајно имајући у виду да излажење из националних правних оквира са собом носи бројне специфичности, па је потребно пажљиво уредити ову област. Према томе, Пореска управа, као руковалац подацима о личности чија је обрада неопходна у циљу извршавања законских обавеза тог органа, има обавезу пружања информација у вези са обрадом података о личности приликом размене података, који се односе на пореске обвезнике, са другим државама на основу међународних уговора о узајамној административној помоћи у пореским питањима, при чему се пружање података врши на начин утврђен Законом о заштити података о личности, осим ако је посебним законом, у складу са Законом о заштити података о личности, уређено одступање од те обавезе.¹⁰⁹

Дакле, одговор на захтев за право приступа обухвата две фазе. Прво, руковалац мора да провери да ли се лични подаци особе која тражи информације уопште обрађују. У сваком случају, мора се пријавити позитиван или негативан резултат. Ако би одговор требао бити позитиван, друга фаза укључује читав низ информација. Право приступа обухвата информације о сврхама обраде, категоријама личних података који се обрађују, примаоцима или категоријама прималаца, планираном трајању складиштења или критеријумима за њихово дефинисање, информације о правима носиоца података као што су исправљање, брисање или ограничење обраде, право на приговор, упутства о праву на подношење жалбе надлежним органима, информације о пореклу података, све док они нису прикупљени од самог носиоца података, и свако постојање аутоматизоване одлуке - процес узимања, укључујући профилисање, са смисленим информацијама о логици која је укључена, као и импликацијама и намераваним ефектима таквих процедура. На крају, али не и најмање важно, ако се лични подаци преносе у трећу земљу без адекватног нивоа заштите, субјекти података морају бити обавештени о свим одговарајућим мерама заштите које су предузете.¹¹⁰

¹⁰⁸ Закон о заштити података о личности, чл. 26. ст. 2.

¹⁰⁹ Предмет Повереника бр. 073-14-3287/2023-02, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 9, Београд, 2024, стр. 166.

¹¹⁰ <https://gdpr-info.eu/issues/right-of-access/>, приступљено: 09.09.2024. године

3. Рокови и последице пропуштања

Руковалац је дужан да поступи по захтеву у року од 30 дана од дана пријема захтева, при чему може да продужи рок за додатних 60 дана, због сложености или бројности захтева и да о томе обавести подносиоца захтева.¹¹¹

У једном од случајева који се нашао пред Повереником, притужилац је 23.12.2022. године поднео захтев руковоацу са молбом да обрише одређене податке о њему уписане у књигу крштених и да исправи те податке. Тражио је, између осталог, да се упишу исправни подаци као што су адреса породилишта, презиме, занимање оца, адреса становања оца и занимање мајке, као и да се укаже да није крштен. Повереник за заштиту података о личности утврдио је да Руковалац није поступио по захтеву у року од 30 дана, није пружио информације о разлозима за непоступање, нити је обавестио подносиоца захтева о могућности подношења притужбе. Због тога је Повереник закључио да је притужба делимично основана и да је дошло до повреде права притужиоца. Руковалац је тврдио да Повереник није надлежан јер је Српска православна црква независна од државе. Међутим, Повереник је указао да се, према закону, ако цркве или верске заједнице примењују своја правила о заштити података, она морају бити усклађена са законом и да Повереник има надлежност у овом случају јер Руковалац није образовао посебно независно надзорно тело. Без даљег разматрања основаности захтева, Повереник је одлучио да Руковалац мора поступити по захтеву.¹¹²

Међутим, овакве ситуације не дешавају се само код нас. У Италији је бивши запослени тражио приступ својим личним подацима из процена учинка, али је захтев послао на општу е-маил адресу компаније и директору људских ресурса, а не на званичну адресу службеника за заштиту података. Како није добио одговор у року од месец дана, послао је подсетник и касније захтев поновио директно службенику који је одговорио тек након три недеље, али директор људских ресурса није поступио по захтеву. Подносилац захтева се обратио надзорном телу за заштиту података, које је покренуло надзор. Компанија је покушала да се оправда тврдећи да захтеви нису били послати на праву адресу и да су подаци већ били познати запосленом. Међутим, надзорно тело је утврдило да компанија није обавестила запосленике о тачној

¹¹¹ Стефан Андоновић, Драган Прља, *Op.cit.*, стр. 99.

¹¹² Предмет Повереника бр. 072-16-113/2023-06, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 9, Београд, 2024, стр. 106.

процедуре за слање захтева, што је довело до непоштовања GDPR-а. Директор људских ресурса није реаговао на захтев, вероватно сматрајући да је то одговорност службеника. Надзорно тело је казнило компанију са 30.000 евра због кршења GDPR-а, наглашавајући важност правилне процедуре за обраду захтева за приступ подацима и обавештавања свих запослених о томе.¹¹³

Такође, руковалац је дужан да подносиоца захтева обавести о праву на подношење притужбе Поверенику, односно тужбе суду.¹¹⁴ Аутор је мишљења да би требало скратити рокове за поступање по захтеву за приступ с обзиром на то да се, по правилу, у већини случајева рок продужава иако то није оправдано.

4. Поступак пред Повереником за заштиту података о личности

Повереник за информације од јавног значаја и заштиту података о личности представља независно надзорно тело у правном систему Републике Србије. Његов значај огледа се у снази личног ауторитета као и ауторитета саме институције, али и у поседовању одређених специјалних овлашћења којима располаже.¹¹⁵

Повереник за информације од јавног значаја и заштиту података о личности има широк круг послова и овлашћења у области заштите података о личности.¹¹⁶ У погледу овлашћења Повереника у поступку остваривања права на приступ подацима о личности важно је напоменути да постоји обавеза руковоаца да обавести подносиоца захтева обавести о праву да поднесе притужбу Поверенику¹¹⁷ у случају да руковалац не поступи по захтеву за приступ подацима у року од 30 дана од дана пријема захтева, односно у року од најдуже 90 дана уколико је због сложености или бројности захтева рок претходно продужен.¹¹⁸

Наиме, одредбама члана 82. ЗЗПЛ-а предвиђено је право на притужбу, те је прописано да лице на које се подаци односе има право да поднесе притужбу Поверенику уколико сматра да је обрада података о његовој личности извршена супротно законским одредбама. Повереник је у обавези да подносиоца притужбе

¹¹³ Provvedimento del 24 aprile 2024 (10018813), извор: <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10018813>, приступљено: 05.09.2024. године

¹¹⁴ Закон о заштити података о личности, чл. 21. ст. 4.

¹¹⁵ Georges Dupuis, Marie-Jose Guedon, *Institutions administratives – Droit administratif*, Armand Colin, Paris, 1988, 59.

¹¹⁶ Видети: Закон о заштити података о личности, чл. 78-79.

¹¹⁷ Закон о заштити података о личности, чл. 21. ст. 4.

¹¹⁸ Стефан Андоновић, Драган Прља, *Op.cit.*, стр. 99.

обавести о току поступка који води, резултатима поступка, као и о праву лица да покрене судски поступак у циљу заштите права.¹¹⁹

Овлашћено лице може поднети притужбу Поверенику, како на прописаном обрасцу који се налази на интернет презентацији Повереника¹²⁰, тако и у слободној форми. У складу са тежњама ка реформи јавне управе и процесом дигитализације, омогућено је, поред стандардних начина подошења правних аката, и подношење притужбе електронским путем. Подношење притужбе Поверенику не утиче на право овог лица да покрене друге поступке управне или судске заштите.

Сам поступак спроводи се у складу са одредбама ЗЗПЛ-а којима је регулисано спровођење инспекцијског надзора.¹²¹ Према томе, Повереник је овлашћен да:

- 1) наложи руковоацу и обрађивачу, а према потреби и њиховим представницима, да му пружи све информације које затражи у вршењу својих овлашћења;
- 2) проверава и оцењује примену одредби закона и на други начин врши надзор над заштитом података о личности коришћењем инспекцијских овлашћења;
- 3) проверава испуњеност услова за сертификацију;
- 4) обавештава руковоаца, односно обрађивача о могућим повредама овог закона;
- 5) затражи и добије од руковоаца и обрађивача приступ свим подацима о личности, као и информацијама неопходним за вршење његових овлашћења;
- 6) затражи и добије приступ свим просторијама руковоаца и обрађивача, укључујући и приступ свим средствима и опреми.¹²²

Повереник је дужан да поступи по притужби у року од 60 дана. Повереник одлучује решењем којим може одбацити притужбу, одбити притужбу, обуставити поступак, односно издати налог. Против решења се може покренути управни спор.

Уколико не поступи по притужби у прописаном року, односно не обавести подносиоца притужбе у наведеном року од 60 дана о току и резултатима поступка, као и о праву лица да покрене судски поступак, подносилац притужбе може да покрене управни спор из разлога ћутања управе, сходно одредбама Закона о управним споровима¹²³.

¹¹⁹ Закон о заштити података о личности, чл. 82. ст. 1-2.

¹²⁰ Више о томе: <https://www.poverenik.rs/sr/%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%B0%D0%BA%D0%B0/%D1%84%D0%BE%D1%80%D0%BC%D1%83%D0%BB%D0%B0%D1%80%D0%B8.html>, приступљено: 29.10.2024. године

¹²¹ Закон о заштити података о личности, чл. 82. ст.1.

¹²² Закон о заштити података о личности, чл. 79. ст.1. тач. 1-6.

¹²³ Закон о управним споровима, чл. 19.

VII ОГРАНИЧЕЊА ПРАВА НА ПРИСТУП ПОДАЦИМА О ЛИЧНОСТИ

1. Обрада личних података у посебне сврхе

Законодавац је одредбом члана 27. Закона о заштити података о личности¹²⁴ регулисао остварење овог права уколико подаци обрађују од стране надлежних органа у посебне сврхе. Посебне сврхе јесу спречавање, истрага и откривање кривичних дела, гоњење учинилаца кривичних дела или извршење кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности.¹²⁵ Међутим, ова одредба је у потпуности идентична одредби члана 26. став 1. тач. 1-7. Закона о заштити података о личности, о којој је било речи у претходном делу рада. Треба напоменути да лице на које се односе подаци има право да од руковоаца који врши обраду захтева приступ подацима у складу са законом, при чему код обрада у “опште” сврхе то лице може од руковоаца да затражи и достављање копије података, што није могуће код обраде у тзв. посебне сврхе.¹²⁶

2. Законска ограничења права на приступ подацима о личности

У погледу ограничења права на приступ подацима о личности које надлежни органи обрађују у посебне сврхе треба напоменути да се ово право може ограничити у потпуности или одређеном делу. Међутим, ограничење је могуће само у мери и трајању које је неопходно за то, у сразмерној мери у демократском друштву. Приликом ограничења права на приступ неопходно је поштовати основна права и легитимне интересе лица чији се подаци обрађују. Законом су такставивно набројани разлози за овакво поступљење, и то:

1) избегавање ометања службеног или прикупљања информација, истрага или поступци који се спроводе у складу са посебним законима;

2) спречавање, истрага и откривање кривичних дела, гоњење учинилаца кривичних дела или извршење кривичних санкција;

3) заштита јавне безбедности;

4) очување националне безбедност и одбрана;

¹²⁴ Видети: Закон о заштити података о личности, чл. 27.

¹²⁵ Закон о заштити података о личности, чл. 6. ст. 3.

¹²⁶ Предмет Повереника бр. 073-14-2058/2022-02, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 8, Београд, 2023, стр. 77.

5) очување права и слободе других лица.¹²⁷

“У једном демократском друштву оправдано је ускратити приступ информацијама о „негативним“ безбедносним проверама које су у вези са издржавањем казне затвора, јер би се објављивање таквих информација могло нарочито омести или отежати спровођење казне. Чињеница да је жалилац на ког се односе информације о „негативној“ безбедносној провери дао сагласност да се информације објаве није од утицаја, јер у траженим документима постоје подаци о личности и осталих лица која су учествовала у безбедносним проверама.”¹²⁸

У случају који се нашао пред румунском агенцијом за заштиту података о личности, субјект чији се подаци обрађују је поднео захтев за приступ лични подацима супермаркету Кауфланд, тражећи да добије копију видео снимака када је посетио Кауфланд супермаркет. Међутим, Кауфланд је одбио да понуди све постојеће снимке који укључују носиоца података, тврдећи да би откривање таквог материјала утицало на права и слободе других појединаца који су такође снимљени на том видео снимку. Румунска агенција за заштиту података одлучила је да руковалац треба да предузме све неопходне техничке и организационе мере када одговара на захтев за приступ како би се уверио да не утичу на личне податке и права других. Агенција је сугерисала да би се у оваквим случајевима, како би се подносиоцу захтева дали лични подаци у његовом захтеву за приступ, ово могло да се реши замагљивањем (“блуровањем”) слике других појединаца који се појављују на снимку. Због тога је Агенција сматрала да Кауфланд није испунио своју обавезу да одобри податке у захтеву за приступ подносиоцу захтева кршећи члан 15(3) GDPR-а и изрекао је Кауфланд супермаркету казну од 14.846,40 леј, што је приближно 3000 евра.¹²⁹ Дакле, овај пример нам показује да није нужно ограничити право на приступ подацима о личности у свим ситуацијама када се појављују и друга лица, осим подносиоца захтева. Заправо, уз одговарајуће мере заштите, субјекту чији се подаци обрађују може се дозволити приступ подацима, уз истовремену заштиту података других лица.

Законодавац оставља могућност да се посебним законом одреде врсте обраде које, у целини или делимично, могу бити обухваћене ограничењима.

¹²⁷ Закон о заштити података о личности, чл. 28. ст. 1. тач. 1-5.

¹²⁸ Предмет Повереника бр. 071-01-1730/2021-03 од 1. априла 2022. године, у: *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 11, Београд, 2022, стр. 62.

¹²⁹ Sancțiune pentru încălcarea RGPD, извор: https://www.dataprotection.ro/?page=Comunicat_Presa_20_01_2022&lang=ro, приступљено: 07.09.2024. године

У погледу поступања руковоаца по захтеву за приступ подацима од стране овлашћеног лица треба напоменути обавезу руковоаца да писменим путем обавести лице на које се подаци односе да је приступ његовим подацима о личности одбијен или ограничен, као и о разлозима за одбијање или ограничење, без непотребног одлагања, а најкасније у року од 15 дана.¹³⁰ Међутим, ова обавеза не постоји у случају када се тиме може довести у питање остваривање сврхе због које је приступ одбијен или ограничен.¹³¹ Такође, у овом случају, али и када утврди да се подаци о личности подносиоца захтева не обрађују, руковалац је дужан да без одлагања, а најкасније у року од 15 дана, писменим путем обавести подносиоца захтева да је провером утврђено да не постоје подаци о личности у вези којих се могу остварити права предвиђена законом, као и да се може притужбом обратити Поверенику, односно тужбом суду.¹³²

Као и у случају рокова у општем режиму обраде, аутор је мишљења да је рок за обавештавање подносиоца захтева о исходу поступања предугачак те да не иде у прилог остваривању самог права на приступ подацима о личности. Према томе, било би целисходно одредити рок за поступање по захтеву од најдуже осам дана.

Дакле, ова правила и ограничења служе као баланс између права појединаца на приступ својим подацима и потребе да се одређене информације задрже конфиденцијалне ради заштите јавних интереса и правде. Прецизност и транспарентност у примену ових права и ограничења су кључне за очување интегритета система заштите података и поверења јавности у правни систем.

¹³⁰ Закон о заштити података о личности, чл. 28. ст. 3.

¹³¹ Закон о заштити података о личности, чл. 28. ст. 4.

¹³² Закон о заштити података о личности, чл. 28. ст. 5.

ЗАКЉУЧНА РАЗМАТРАЊА

Право на приступ личним подацима, које је тема овог рада, представља једно од основних права у савременим правним системима, а његова заштита је од суштинског значаја за очување приватности и личних слобода појединаца. Једноставније речено, право на приступ личним подацима представља једно од темељних права зајамчених европским и националним законодавствима у области заштите података, које омогућава појединцима да сазнају да ли се њихови лични подаци обрађују, на који начин, у које сврхе и ко је приматељ тих података. На тај начин, право на приступ је кључно за остваривање транспарентности и поверења у односу између субјеката података (појединаца чији се подаци обрађују) и руковалаца подацима (ентитета који обрађују податке).

Право на приступ је такође важно јер помаже у осигуравању усклађености са законодавним оквирима. Организације које обрађују податке су обавезне да пруже јасне и прецизне информације субјектима података, чиме се осигурава да се обрада врши у складу са законом и уз одговарајућу заштиту права појединаца.

У Републици Србији, ово право је нормативно уређено кроз Закон о заштити података о личности, који је усклађен са међународним стандардима и европским правним оквиром, пре свега са Општом уредбом о заштити података (GDPR).

Кроз анализу нормативног оквира и праксе, обављену за потребе писања овог рада, уочено је да грађани Србије имају право да затраже и добију информације о својим личним подацима који се обрађују, али и да постоје специфична ограничења овог права када су у питању подаци који се обрађују у посебне сврхе, као што су национална безбедност или спречавање кривичних дела. Упркос овим ограничењима, правни механизми омогућавају појединцима да заштите своја права кроз правне лекове, попут притужби Поверенику за информације од јавног значаја и заштиту података о личности или покретањем судских поступака. У том циљу, у овом раду изложени су и неки од примера из праксе, по притужбама по којима је поступао Повереник. Међутим, судска пракса у овој области још увек није богата колико и пракса Повереника.

У пракси се јављају одређени изазови у остваривању права на приступ, који се односе на недовољну информисаност грађана, сложеност поступака, као и на техничке и организационе препреке код руковалаца подацима. Стога је неопходно додатно унапредити механизме за заштиту овог права, кроз јачање капацитета институција, едукацију грађана и обезбеђивање транспарентнијег и ефикаснијег поступања

руководилаца. Наиме, иако је Закон о заштити података о личности усклађен са европским стандардима, потребно је континуирано пратити и прилагођавати га новим изазовима који се јављају са развојем технологије и глобалним трендовима у заштити података. Такође, потребно је доношење додатних подзаконских аката који би прецизирали поједине аспекте примене закона, као и увођење додатних правних механизма за заштиту права грађана. Затим, неопходно је спроводити обимне едукативне кампање које би грађанима омогућиле боље разумевање њихових права у вези са личним подацима, како би могли адекватно користити механизме заштите који им стоје на располагању. Едукација би требало да буде усмерена ка различитим циљним групама, укључујући децу и младе, запослене у јавном сектору, као и приватне организације које обрађују податке.

Следећи корак јесте јачање капацитета институција. Институције попут Повереника за информације од јавног значаја и заштиту података о личности треба додатно оснажити, како у кадровском тако и у техничком смислу. То укључује обуку запослених, повећање броја стручњака за заштиту података, као и модернизацију ИТ система који се користе у процесу надзора и обраде захтева грађана. Затим, руковооци подацима треба да обезбеде већи степен транспарентности у вези са начином обраде личних података, укључујући редовно обавештавање грађана о њиховим правима, као и о мерама које предузимају ради заштите тих података. Такође, потребно је увести строже санкције за непоштовање прописа, како би се подигао ниво одговорности и обезбедила ефикаснија заштита права грађана. Примере добре праксе у погледу казнене политике треба тражити у земљама чланицама Европске уније које прописују казне од неколико милиона евра у случају непоштовања права која се односе на заштиту података о личности.

С обзиром на све већу дигитализацију података, неопходан је развој и имплементација нових технолошких решења која би омогућила лакши и бржи приступ личним подацима. То може укључивати развој електронских платформи за подношење и праћење захтева, аутоматизоване системе за информисање грађана, као и дигиталне алате за заштиту података. Такође, имајући у виду чињеницу да обрада личних података често укључује међународни трансфер, Србија треба да настави да развија и унапређује сарадњу са међународним организацијама и регулаторним телима, како би осигурала висок ниво заштите података својих грађана у међународним оквирима. Осим тога, потребно је да се Србија активно укључи у размену најбољих пракси са

другим државама, нарочито у вези са новим изазовима као што су вештачка интелигенција и биг дата аналитика.

У том погледу, важно је истаћи значај заштите права на приступ подацима о личности, као једног од права из корпуса заштите личних података, у праву Европске уније и земаља чланица ЕУ.

Наиме, у циљу унапређења заштите личних права и јачања транспарентности, ЕУ непрестано развија нормативни оквир којим је ова област регулисана. Иако није једини, GDPR је свакако најзначајнији акт у овој области. Такође, у многим земљама постоје и национални прописи, усклађени са њим, који регулишу ову област.

Такође, примери из праксе надзорних тела многих земаља у великој мери доприносе заштити права на приступ подацима о личности и тумачењу прописа. У том циљу, у претходном делу рада приказани су неки од примера одлука надзорних тела из упоредног права.

Затим, судска пракса Европског суда за људска права јесте веома значајан извор права иако правним актима којима се руководи овај орган није експлицитно зајемчено право на приступ личним подацима већ је то учињено кроз заштиту права на приватност. Важно је напоменути да судови Републике Србије пажљиво прате праксу Европског суда за људска права и усклађују своје одлуке са европским стандардима.

Даље, Суд правде Европске уније, који настоји да успостави јединствену примену права на територији држава чланица Европске уније, донео је велики број одлука у којима је разматрана заштита права на приступ личним подацима. Важност праксе Суда правде Европске уније огледа се у томе што национална надзорна тела настоје да ускладе своје одлуке са одлукама Суда како би избегле поништавање у случају тужби лица која сматрају да су им повређена права. Свакако, Република Србија, водећи се жељом за чланством у Европској унији, настоји да усклади своју праксу и са одлукама Суда.

Свеукупно, право на приступ личним подацима игра кључну улогу у заштити приватности појединаца и изградњи поверења у правни систем и институције које руководе подацима. Даљи развој и примена овог права у Србији захтевају континуирани напор како државних органа, тако и грађанског друштва, како би се обезбедила адекватна заштита личних података и ефикасно остваривање права на приступ, у складу са најбољим европским и светским праксама.

ПОПИС КОРИШЋЕНЕ ЛИТЕРАТУРЕ

1. Андоновић Стефан, Прља Драган, Дилигенски Андреј, *Заштита података о личности у Србији*, Зборник радова, Београд 2020.
2. Андоновић Стефан, Прља Драган, *Основи права заштите података о личности*, Београд, 2020.
3. Водинелић Владимир, *Право на слободан приступ информацијама од јавног значаја као уставно право*, Слободан приступ информацијама – уставно јемство и законске гаранције, Београд 2004.
4. Karvalics László Z, *Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression)*, Information Society From Theory to Political Practice Coursebook, Budapest 2008.
5. Кривокапић Данило, Кривокапић Ђорђе, Тодоровић Иван, Комазец Стефан, Петровски Андреј, Ерцеговић Катарина, *”Водич за органе власти – Заштита података о личности”*, Share фондација, Београд, 2016.
6. Лилић Стеван, *”Правни аспекти заштите података у аутоматизованим службеним евиденцијама”*, Наша законитост, бр. 5, Загреб, 1989.
7. Милков, Драган, *Управно право II – управна делатност*. Нови Сад: Правни факултет, 2017.
8. Мајсторовић, Марија, Општа уредба Европског парламента и Савета Европске уније о заштити података (GDPR) – преглед и новине. *Библид. XIX(73-74)*, 2020, 99-117.
9. Раденковић Божидар, Деспотовић Зракић Маријана, Богдановић Зорица, Бараћ Душан, Лабус Александра, *Електронско пословање*, Факултет организационих наука, Београд 2015.
10. Симоновић, Ивана, Лазић, Мирослав, Грађанско правна заштита права личности. *Зборник радова Правног факултета у Нишу*, 68/2014, 269-290.
11. Dupuis Georges, Guedon Marie-Jose, *Institutions administratives – Droit administratif*, Armand Colin, Paris, 1988.
12. Lambert Paul, *Understanding the New European Data Protection Rules*, CRC Press, 2018.
13. Niblett G. V. F, *Digital Information and the Privacy Problem*, Organization for Economic Cooperation and Development, Paris, 1971.
14. Schwartz Paul, *Property, Privacy and Personal Data*, Harvard Law Review, vol. 117, Harvard 2003.
15. Voigt Paul, Bussche Axel von dem, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer, eBook, online, 2017.
16. *Закон о електронским комуникацијама*, “Сл. гласник РС”, бр. 44/2010, 60/2013 - одлука УС, 62/2014, 95/2018 - др. закон и 35/2023 - др. Закон.
17. *Закон о информационој безбедности*, “Сл. гласник РС”, бр. 6/2016, 94/2017 и 77/2019.
18. *Закон о заштити података о личности*, “Службени лист СРЈ”, бр. 24/98.
19. *Закон о заштити података о личности*, “Сл. гласник РС”, бр. 87/2018.
20. *Закон о здравственој документацији и евиденцијама у области здравства*, “Сл. гласник РС”, бр. 87/2018.
21. *Закон о матичним књигама*, “Сл. гласник РС”, бр. 20/2009, 145/2014 и 47/2018.
22. *Закон о општем управном поступку*, “Сл. гласник РС”, бр. 18/2016, 95/2018 - аутентично тумачење и 2/2023 - одлука УС.
23. *Закон о парничном поступку*, “Сл. гласник РС”, бр. 72/2011, 49/2013 - одлука УС, 74/2013 - одлука УС, 55/2014, 87/2018, 18/2020 и 10/2023 - др. Закон.

24. *Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података*, “Сл. лист СРЈ — међународни уговори”, бр. 1/92.
25. *Закон о раду*, “Сл. гласник РС”, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - одлука УС, 113/2017 и 95/2018 - аутентично тумачење
26. *Закон о слободном приступу информацијама од јавног значаја*, “Сл. гласник РС” бр.120/04, 54/07, 104/09, 36/210 и 105/21.
27. *Закон о управним споровима*, “Сл. гласник РС”, бр. 111/2009.
28. *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 6, Београд, 2021.
29. *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 7, Београд, 2022.
30. *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 8, Београд, 2023.
31. *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 9, Београд, 2024.
32. *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, Публикација бр. 11, Београд, 2022.
33. *Правилник о заштити података о личности*, “Сл. гласник РС”, бр. 98/2021.
34. *Правилник о обрасцу и начину вођења евиденције лица за заштиту података о личности*, “Сл. гласник РС”, бр. 40/2019.
35. *Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности* “Сл. гласник РС”, број 40/2019.
36. *Приручник о европском праву заштите података*, издање 2018.
37. *Устав Републике Србије*, “Сл. гласник РС”, бр. 98/2006 и 115/2021.
38. *Устав Савезне Републике Југославије*, “Службени лист СРЈ”, бр.1/92.
39. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*
40. *General Data Protection Regulation, (EU) 2016/679.*
41. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).*
42. *Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare.*
43. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.*
44. *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance).*
45. *Sanctiune pentru încălcarea RGPD*
46. *Tidligere arbejds giver kunne afvise at efterkomme anmodning om indsig*t
47. *Закон о provedbi Opće uredbe о заштити података*, NN 42/18.
48. *Закон о varstvu osebних podatkov*, Uradni list RS, št. 163/22.

ПОПИС ОСТАЛЕ ИСТРАЖИВАЧКЕ ГРАЂЕ

1. Одлука Уставног суда Србије, У-бр. 41/04 од 26. 11. 2009. године
2. Одлука Уставног суда Србије, У. бр. 41/10 од 30. 5. 2012. године
3. Предмет Повереника бр. 073-14-1720/2019-02, од 1.10.2019. године, Повереник за информације од јавног значаја и заштиту података о личности
4. Предмет бр. 073-14-2369/2019-02, од 15.1.2020. године, Повереник за информације од јавног значаја и заштиту података о личности
5. Предмет Повереника бр. 072-16-2992/2019-06 од 28. 1. 2020. године, Повереник за информације од јавног значаја и заштиту података о личности
6. Предмет Повереника бр. 072-16-705/2020-06 од 13. 4. 2020. године, Повереник за информације од јавног значаја и заштиту података о личности
7. Предмет Повереника бр. 072-16-5724/2019-06 од 7. 8. 2020. године, Повереник за информације од јавног значаја и заштиту података о личности
8. Предмет Повереника бр. 072-16-1857/2020-06, од 5.10.2020. године, Повереник за информације од јавног значаја и заштиту података о личности
9. Предмет бр. 072-16-2201/2020-06, од 21.12.2020. године, Повереник за информације од јавног значаја и заштиту података о личности
10. Предмет бр. 072-16-110/2021-6, од 19.02.2021. године, Повереник за информације од јавног значаја и заштиту података о личности
11. Предмет Повереника бр. 072-16-1129/2021-6, од 3. 8. 2021. године, Повереник за информације од јавног значаја и заштиту података о личности
12. Предмет бр. 073-14-2973/2021, од 24. 11. 2021. године, Повереник за информације од јавног значаја и заштиту података о личности
13. Предмет Повереника бр. 071-01-1730/2021-03 од 1. априла 2022. године, Повереник за информације од јавног значаја и заштиту података о личности
14. Предмет Повереника бр. 072-16-1184/2023-06, Повереник за информације од јавног значаја и заштиту података о личности
15. Предмет бр. 072-16-1213/2022-06, Повереник за информације од јавног значаја и заштиту података о личности
16. Предмет Повереника бр. 072-16-1809/2022-06, Повереник за информације од јавног значаја и заштиту података о личности
17. Предмет Повереника бр. 073-14-2058/2022-02, Повереник за информације од јавног значаја и заштиту података о личности
18. Предмет Повереника бр. 072-16-2536/2022-06, Повереник за информације од јавног значаја и заштиту података о личности
19. Предмет Повереника бр. 072-16-815/2023-06, од 23.3.2023. године, Повереник за информације од јавног значаја и заштиту података о личности
20. Предмет Повереника бр. 073-14-3287/2023-02, Повереник за информације од јавног значаја и заштиту података о личности
21. Предмет Повереника бр. 072-16-113/2023-06, Повереник за информације од јавног значаја и заштиту података о личности
22. Rješenje AZOP-a, Zagreb, 10. prosinca 2021. godine
23. *Case of Benedik v. Slovenia, The European Court of Human Rights, 24 April 2018.*
24. *Case C-487/21, F.F. v Österreichische Datenschutzbehörde, Österreichische Datenschutzbehörde and CRIF, Judgment of the Court (First Chamber) of 4 May 2023.*
25. *Case of Gaskin v. The United Kingdom , (Application no. 10454/83), ECHR, Strasbourg, 07 July 1989.*
26. *Case of K.H. and others v. Slovakia (Application no. 32881/04), ECHR, Strasbourg, 28 April 2009.*

27. *IP (Slovenia) - 07106-8-2023.*
28. *L'affaire Khelili c. Suisse, La Cour européenne des droits de l'homme, 18 octobre 2011.*
29. *Provedimento del 24 aprile 2024 (10018813).*
30. *W252 2246156-1, Bundesverwaltungsgericht, 22.01.2024.*

ЕЛЕКТРОНСКИ ИЗВОРИ

1. <https://www.academia.edu/>
2. <https://www.apvp.si/>
3. <https://azop.hr/>
4. <https://curia.europa.eu/>
5. <https://www.dataprotection.ro/>
6. <https://www.datatilsynet.dk/>
7. <https://eur-lex.europa.eu/legal-content/EN/TXT/>
8. <https://fra.europa.eu/>
9. <https://gdpr-info.eu/>
10. <https://gdprhub.eu/>
11. <https://hudoc.echr.coe.int/eng>
12. <https://ico.org.uk/>
13. <https://www.gdpd.it/>
14. <https://www.poverenik.rs>
15. <https://pisrs.si/>
16. <https://pn2.propisi.net/>
17. <https://www.ris.bka.gv.at/>
18. <https://www.ustavni.sud.rs/sudska-praksa/>
19. <https://www.zakon.hr/>

РЕЗИМЕ

Мастер рад на тему “*Управноправни режим остваривања права на приступ личним подацима*” бави се анализом права на приступ подацима о личности које омогућава појединцима да стекну увид у то које информације о њима прикупљају и обрађују различити субјекти, чиме се обезбеђује транспарентност обраде података и омогућава појединцима да задрже контролу над својим личним подацима.

У раду је анализиран правни оквир Републике Србије, првенствено Закон о заштити података о личности, који је усклађен са GDPR-ом, који представља кључни правни акт на нивоу ЕУ који гарантује право на приступ подацима и поставља строге услове за руковоаоце подацима како би осигурали заштиту приватности грађана. Поред тога, разматрани су и други релевантни прописи ЕУ, попут ePrivacy Директиве, као и пракса Европског суда за људска права и Суда правде Европске уније, али и националних надзорних тела у вези са применом ових правних норми.

Истраживање обухвата детаљну анализу елемената права на приступ, укључујући право на потврду о обради, приступ подацима, информације о сврси обраде, категоријама података, примаоцима, року чувања и правима субјекта података. Такође, анализирани су и изазови у примени овог права у пракси, као што су технички проблеми у обради захтева, административни терети за руковоаоце подацима, као и ограничења и изузеци предвиђени законом.

Упоредна анализа између српског и европског правног оквира показује да, иако Србија предузима значајне кораке ка усклађивању са европским стандардима, постоје изазови у примени права на приступ у пракси, пре свега због недовољне свести грађана и техничко-организационих препрека са којима се суочавају правна лица. Закључак рада указује на потребу за додатним напорима у унапређењу имплементације закона, јачању капацитета надзорних органа, као и повећању свести грађана о њиховим правима. Такође, пружене су препоруке за даље усклађивање српског законодавства са праксом ЕУ и предложена конкретна решења за унапређење заштите података о личности у Србији.

Кључне речи: податак о личности, приступ личним подацима, GDPR, приватност, Закон о заштити података о личности

SUMMARY

The master's thesis on the topic “*Administrative legal regime for exercising the right to access personal data*” deals with the analysis of the right to access personal data, which allows individuals to gain insight into what information about them is collected and processed by different entities, which ensures transparency of data processing and enables individuals to maintain control over their personal data.

The paper analyzes the legal framework of the Republic of Serbia, primarily the Law on the Protection of Personal Data, which is harmonized with the GDPR, which represents a key legal act at the EU level that guarantees the right to access data and sets strict conditions for data handlers to ensure protection citizens' privacy. In addition, other relevant EU regulations were considered, such as the ePrivacy Directive, as well as the practice of the European Court of Human Rights and the Court of Justice of the European Union, as well as national supervisory bodies regarding the application of these legal norms.

The research includes a detailed analysis of the elements of the right of access, including the right to confirmation of processing, access to data, information on the purpose of processing, categories of data, recipients, retention period and data subject rights. Challenges in the application of this right in practice were also analyzed, such as technical problems in processing requests, administrative burdens for data handlers, as well as limitations and exceptions provided for by law.

A comparative analysis between the Serbian and European legal framework shows that, although Serbia is taking significant steps towards harmonization with European standards, there are challenges in applying the right of access in practice, primarily due to insufficient awareness of citizens and technical and organizational obstacles faced by legal entities. The conclusion of the paper indicates the need for additional efforts in improving the implementation of the law, strengthening the capacity of supervisory authorities, as well as increasing citizens' awareness of their rights. Also, recommendations were provided for further harmonization of Serbian legislation with EU practice and concrete solutions were proposed to improve the protection of personal data in Serbia.

Key words: personal data, access to personal data, GDPR, privacy, Personal Data Protection Act

БИОГРАФИЈА

Христина Митић, ауторка рада, рођена је 27. септембра 1998. године у Нишу. Основну школу “Десанка Максимовић” завршила је 2013. године. Након завшене основне школе уписује Алексиначку гимназију, друштвено језички смер, коју завршава 2017. године.

Након завршетка гимназије, 2017. године, уписује основне академске студије права на Правном факултету Универзитета у Нишу. Дипломирала је 2023. године на Правном факултету за привреду и правосуђе. Затим је, након дипломирања, 2023. године уписала мастер академске студије права на Правном факултету у Нишу, на смеру “Право и информационе технологије”, у жељи да усаврши своја знања у савременим областима права које теже повезивању правне науке и информационих технологија.

Током основних студија, Христина је обавила две стручне праксе у Основном суду у Алексинцу из области радног и породичног права, док је стручну праксу на мастер студијама обавила у адвокатској канцеларији из области заштите података о личности, где је имала прилику да се упозна са практичним аспектима заштите података о личности.

Такође, у жељи да се непрестано усавршава, учествовала је на великом броју семинара, конференција и трибина из области права. Осим тога, важно место у њеном животу заузимају и волонтерски рад и књижевност. Тренутно волонтира у оквиру новинарске редакције “Хоћу у позориште”, на позицији новинара. Учесник је неколико књижевних конкурса, на којима су објављени њени радови.

Христина је за време студија радила годину дана у адвокатској канцеларији, као сарадник на правним пословима, а после дипломирања се запослила у интернационалној компанији, где и данас ради.

Течно говори енглески језик, а служи се и шпанским језиком.

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

Име и презиме аутора мастер рада: Христина Митић

Наслов мастер рада: Управноправни режим остваривања права на приступ личним подацима

Ментор: Проф. др Милош Прица

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

У Нишу, _____

Потпис аутора

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да мастер рад, под насловом *Управноправни режим остваривања права на приступ личним подацима*, пријављен и одбрањен на Правном факултету Универзитета у Нишу:

- представља резултат сопственог истраживачког рада;
- није у целини, нити у деловима с моје стране пријављиван на одбрану на другим факултетима или универзитетима;
- не крши ауторска права или интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу.

Аутор мастер рада: _____

У Нишу, _____

Потпис аутора
