Стална конференција
градова и општина

Савез градова и општина Србије

АНАЛИЗА УТИЦАЈА ПРОЦЕСА ЕВРОПСКИХ ИНТЕГРАЦИЈА НА ЛОКАЛНУ САМОУПРАВУ У СРБИЈИ У ОБЛАСТИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ И ПРИСТУПА ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА

Шведска
Sverige

АНАЛИЗА УТИЦАЈА ПРОЦЕСА ЕВРОПСКИХ ИНТЕГРАЦИЈА НА ЛОКАЛНУ САМОУПРАВУ У СРБИЈИ У ОБЛАСТИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ И ПРИСТУПА ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА (ДЕО ПРЕГОВАРАЧКОГ ПОГЛАВЉА 23 – ПРАВОСУЂЕ И ОСНОВНА ПРАВА)

СТАЛНА КОНФЕРЕНЦИЈА ГРАДОВА И ОПШТИНА
– САВЕЗ ГРАДОВА И ОПШТИНА СРБИЈЕ

Ана Тоскић
Маја Стојановић Керић
Дејвид Јанг

АНАЛИЗА УТИЦАЈА ПРОЦЕСА ЕВРОПСКИХ ИНТЕГРАЦИЈА НА ЛОКАЛНУ САМОУПРАВУ У СРБИЈИ У ОБЛАСТИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ И ПРИСТУПА ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА (ДЕО ПРЕГОВАРАЧКОГ ПОГЛАВЉА 23 – ПРАВОСУЂЕ И ОСНОВНА ПРАВА)

Београд, 2020.

АНАЛИЗА УТИЦАЈА ПРОЦЕСА ЕВРОПСКИХ ИНТЕГРАЦИЈА НА ЛОКАЛНУ САМОУПРАВУ У СРБИЈИ У ОБЛАСТИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ И ПРИСТУПА ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА (ДЕО ПРЕГОВАРАЧКОГ ПОГЛАВЉА 23 – ПРАВОСУЂЕ И ОСНОВНА ПРАВА)

Аутори
Ана Тоскић
Маја Стојановић Керић
Дејвид Јанг

Издавач
Стална конференција градова и општина
– Савез градова и општина Србије
Македонска 22, 11000 Београд

За издавача
Ђорђе Станичић, генерални секретар СКГО

Лектура
Ивана Андрић

Дизајн и припрема за штампу
Атеље, Београд
www.atelje.rs

Штампа
Досије студио, Београд
www.dosije.rs

Тираж
300 примерака

ISBN 978-86-80480-07-7

Шведска
Sverige

Израду ове публикације помогла је Влада Шведске у оквиру програма „Подршка локалним самоуправама у Србији на путу ка ЕУ – Друга фаза".
Садржај публикације је искључиво одговорност аутора.

Садржај

АПСТРАКТ

Анализа утицаја процеса европских интеграција на локалну самоуправу у Србији у области заштите података о личности и приступа информацијама од јавног значаја (део преговарачког поглавља 23 – правосуђе и основна права) настала је у оквиру програма „Подршка локалним самоуправама у Србији на путу ка ЕУ – Друга фаза", који финансира Влада Шведске, а спроводи Стална конференција градова и општина – Савез градова и општина Србије (СКГО), као једна у низу анализа посвећених процени утицаја европских интеграција Републике Србије на надлежности и капацитете локалне самоуправе у различитим преговарачким поглављима. Наиме, ова Анализа је проистекла из препорука Основне анализе утицаја усклађивања прописа из преговарачког поглавља 23 (правосуђе и основна права) на локалну самоуправу у Републици Србији, припремљене у оквиру наведеног програма и њен је природни и логични наставак. С обзиром на то да Основна анализа укратко истражује европски правни оквир и национално законодавство Републике Србије у погледу заштите података о личности и приступа информацијама од јавног значаја као релевантне за локалну самоуправу, а имајући у виду развој прописа о заштити података на европском и нивоу Републике Србије, као и обавезе утврђене у процесу преговора о приступању за поглавље 23, СКГО је сматрала да би утицај нових прописа у овој области на локалну самоуправу требало додатно истражити.

Током претходне деценије у Европској унији спроведена је свеобухватна реформа у области заштите података о личности. До најзначајнијег помака у овој реформи дошло је 2016. године, када је усвојена Општа уредба о заштити података, која се од маја 2018. непосредно примењује у државама чланицама ЕУ. Уредба доноси низ новина у област заштите података о личности, почев од нових обавеза за субјекте који обрађују податке (руковаоце и обрађиваче), проширења права лица чији се подаци обрађују, строжих захтева у погледу безбедности података, те високих казни за кршење прописаних правила. За оцену утицаја примене Уредбе на ниво заштите података о личности у ЕУ је још увек рано, али се већ сада може закључити да је овај документ ставио заштиту података у фокус шире јавности.

Имајући у виду обавезе Републике Србије преузете у процесу европских интеграција у виду усклађивања правног оквира са *acquis communautaire*, као и чињеницу да домаћи Закон о заштити података о личности из 2008. године није могао

да испрати промене условљене технолошким развојем, Србија је новембра 2018. године добила нови Закон о заштити података о личности, који се у великој мери по усвојеним решењима ослања на Општу уредбу о заштити података. Закон, који се примењује од 22. августа 2019, не предвиђа посебна правила обраде и заштите података од стране јединица локалне самоуправе, али несумњиво може имати значајан утицај на њихово свакодневно функционисање, како у организационом смислу, тако и у финансијском смислу. Локалне самоуправе обрађују у великој мери податке о грађанима, корисницима својих услуга, запосленима итд. и од изузетног је значаја да адекватно примене нове одредбе и успоставе праксе и стандарде заштите података о личности. Такође, као обвезници Закона о слободном приступу информацијама од јавног значаја, локалне самоуправе се неретко налазе у ситуацији да процењују које је од два права – право на заштиту података о личности или слободан приступ информацијама – значајније, што често није лак задатак.

Циљеви и методологија Анализе – Имајући све горенаведено у виду, ова Анализа има циљ да представи новине у области заштите података о личности у Европској унији и посебно укаже на њихов утицај на развој новог правног оквира у нашој земљи. У Анализи је, стога, дат детаљан приказ правног оквира ЕУ у овој области и представљене су основне промене које доноси наш Закон о заштити података о личности, уз указивање на сличности и разлике између два система. Такође, анализиран је однос права на приступ информацијама од јавног значаја и заштиту података о личности, са фокусом на неким од најчешћих дилема са којима се у том домену локалне самоуправе сусрећу. Даље, представљени су резултати Анализе капацитета ЈЛС за усклађивање са новим правним оквиром за заштиту података о личности, како би се проценила спремност и информисаност ЈЛС за примену новог Закона.[1] Представљањем искустава Шведске у примени Опште уредбе о заштити података од стране ЈЛС у тој земљи указује се на низ изазова са којима се могу сусрести локалне самоуправе у Србији, али и законодавац када буде разматрао измене секторских закона релевантних за локални ниво. Коначно, Анализа даје препоруке, и то јединицама локалне самоуправе, Сталној конференцији градова и општина, као и јавним органима на националном нивоу за кораке које би могли предузети како би се рад ЈЛС ускладио са новим правилима заштите података о личности, а грађанима пружила адекватна заштита њихових права.

1 Више о циљевима и методологија Анализе капацитета ЈЛС за усклађивање са новим правним оквиром за заштиту података о личности видети на страни 81.

ABSTRACT

Analysis of the Impact of European Integration Processes on Local Self-Government in Serbia in the Area of Personal Data Protection and Access to Information of Public Importance (part of negotiation Chapter 23 – Judiciary and Fundamental Rights) has been created under the programme "Strengthening Local Self-Government in Serbia, Phase 2", funded by the Government of Sweden, and implemented by the Standing Conference of Towns and Municipalities – Association of Towns and Municipalities of Serbia (SCTM), as one of many analyses addressing the impact assessment of European integrations of the Republic of Serbia on competencies and local government capacities in different negotiation chapters. In fact, this Analysis has stemmed out of recommendations defined in the Basic analysis of impact of harmonisation of regulations from Negotiating Chapter 23 (Judiciary and Fundamental Rights) on local self-government in the Republic of Serbia, prepared within the framework of the said programme and is a natural and logical continuation thereof. Given that Basic analysis briefly examines the European legal framework and national legislation of the Republic of Serbia regarding the protection of personal data and access to information of public importance as relevant for local self-government, having in mind the development of data protection regulations at European and Serbian levels, as well as commitments established in the accession negotiation process for Chapter 23, the SCTM deemed that impact of new regulations in this area on local self-government should be further explored.

Over the past decade, the European Union has implemented a comprehensive reform of personal data protection. The most significant breakthrough therein was recorded in 2016, when the General Data Protection Regulation was adopted, that became directly applicable in the EU Member States in May 2018. The Regulation has brought a number of innovations in the field of personal data protection, starting with new obligations for data processors (data managers and analysts), extended rights of the data subject, stricter requirements regarding data security, and serious penalties for violations of the prescribed rules. It is still early to assess the impact of the application of the Regulation at the level of personal data protection in the EU, but it can already be concluded that subject document has put data protection into the focus of general public.

Bearing in mind obligations taken by the Republic of Serbia in the European integration process in terms of aligning the legal framework with the *Acquis Communautaire*, as well as the fact that domestic Law on Personal Data Protection from 2008 could not

have kept up with the changes brought by technological development, Serbia passed a new Law on Personal Data Protection in November 2018, which strongly relies on adopted decisions derived from the General Data Protection Regulation. The Law, effective from 22nd August 2019, does not envisage specific rules for data processing and protection by local government units, but there is no doubt it can considerably influence their day-to-day functioning, both organisationally and financially. Local self-governments extensively process data of citizens, users of their services, employees, and other entities, and it is of the utmost importance that they adequately implement new provisions and establish practices and standards for the protection of personal data. In addition, as subjects of the Law on Free Access to Information of Public Importance, local self-governments often find themselves in a position to assess which of the two rights – the right to protection of personal data and free access to information – is more significant, which is not always an easy task.

Objectives and Methodology of the Analysis – Bearing all of the above in mind, this Analysis aims to present innovations in the field of personal data protection in the European Union, particularly to point out their impact on the development of new legal framework in our country. The Analysis, therefore, provides a detailed account of the EU legal framework in this area, and outlines the main changes made by our Law on Personal Data Protection, indicating similarities and differences between the two systems. Moreover, the relationship between the right of access to information of public importance and the protection of personal data has been analysed, focusing on some of the most common dilemmas encountered in this area of local government. Furthermore, the results of the Analysis of LSG' capacities to comply with new legal framework on personal data protection have been presented in order to assess the readiness and awareness of LSGs for the implementation of the new Law[2]. Presentation of Swedish experience in implementing the General Data Protection Regulation in their LSGs highlighted a number of challenges that local governments, but also the legislator, in Serbia can face when considering amendments of sectoral laws relevant for the local level. Finally, the Analysis contains recommendations for local self-government units, Standing Conference of Towns and Municipalities, and public authorities at the national level, regarding the steps they can take to bring the work of LSGs in line with the new rules on personal data protection, and to provide citizens with adequate protection of their rights.

2 For more information about objectives and the methodology of the Analysis of LSG' capacities to comply with new legal framework on personal data protection, please see page 81.

ЛИСТА СКРАЋЕНИЦА

CAB	*County Administrative Board* (*Länsstyrelse*) – Административни одбор округа
Директива о заштити података	Директива 95/46/ЕЗ о заштити појединаца у погледу обраде података о личности и о слободном кретању тих података
DPA	*Swedish Data Protection Authority* (*Datainspektionen*) – Агенција за заштиту података Шведске
DPO	*Data protection officer* (*datakskyddsombud*) – службеник за заштиту података
ЕКЉП	Европска конвенција за заштиту људских права и основних слобода
ЈЛС	јединица локалне самоуправе
Конвенција 108	Конвенција Савета Европе о заштити лица у односу на аутоматску обраду личних података
ОЦД	Организација цивилног друштва
Општа уредба, Уредба, *GDPR*	(*General Data Protection Regulation*) – Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о заштити појединаца у вези са обрадом података о личности и о слободном кретању тих података, као и о стављању ван снаге Директиве 95/46/ЕЗ
Полицијска директива	Директива (ЕУ) 2016/680 о заштити физичких лица у погледу обраде података о личности коју врше надлежни органи у сврху превенције, истраге, откривања или гоњења кривичних дела или извршења кривичних санкција и о слободном кретању таквих података, као и о стављању ван снаге Оквирне одлуке Савета 2008/977/ПУП

Повеља	Повеља ЕУ о основним правима
Повереник	Повереник за информације од јавног значаја и заштиту података о личности
SALAR	*Swedish Association of Local Authorities and Regions* (*Sveriges kommuner och regioner*) – Шведска асоцијација локалних власти и региона
SAP	*Swedish Agency for Participation* (*Myndigheten för delaktighet*) – Шведска агенција за учешће
СКГО	Стална конференција градова и општина
ЗЗПЛ	Закон о заштити података о личности
ЗСПИЈЗ	Закон о слободном приступу информацијама од јавног значаја

1. О ПРАВУ НА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ

Право на заштиту података о личности један је од елемената права на приватност, ширег и историјски старијег концепта.[3] Поред приватности података, шири појам приватности данас подразумева и приватност тела, приватност преписке, односно комуникацијску приватност, те приватност територије.[4] Право на приватност се данас сврстава у једно од основних људских права, која су гарантована најзначајнијим међународним документима о заштити људских права, укључујући и *Универзалну декларацију Уједињених нација о људским правима*[5], *Међународни пакт о грађанским и политичким правима*[6], *Конвенцију Уједињених нација о правима детета*[7] итд. За нашу земљу и разумевање концепта приватности, међу међународним инструментима свакако је најважнија *Европска конвенција за заштиту људских права и основних слобода*, која у члану 8. гарантује право на поштовање приватног и породичног живота, како следи:

Свако има право на поштовање свог приватног и породичног живота, дома и преписке.

Јавне власти неће се мешати у вршење овог права сем ако то није у складу са законом и неопходно у демократском друштву у интересу националне безбедности, јавне

---

3 Још 1890. године, два америчка адвоката, Самјуел Д. Ворен (Samuel D. Warren) и Луис Брандајс (Louis Brandeis), написали су чланак под насловом „Право на приватност", у коме су дали прву дефиницију овог појма као „права да будемо остављени на миру".

4 Видети: У. Мишљеновић, Б. Недић, А. Тоскић, *Заштита приватности у Србији – Анализа примене Закона о заштити података о личности*, Партнери за демократске промене Србија, 2013, стр. 7–8, доступно на: *http://www.partners-serbia.org/wp-content/uploads/2013/06/Zastita-privatnosti-u-Srbiji-za-sajt.pdf*.

5 Члан 12. Универзалне декларације: „Нико не сме бити изложен произвољном мешању у приватни живот, породицу, стан или преписку, нити нападима на част и углед. Свако има право на заштиту закона против оваквог мешања или напада."

6 Члан 17. Пакта прописује да „нико не може бити предмет самовољних или незаконитих мешања у његов приватни живот, његову породицу, у његов стан или његову преписку, нити незаконитих повреда нанесених његовој части или његовом угледу", док члан 23. штити породицу и право на склапање брака и оснивање породице, а члан 24. уређује права и заштиту деце и малолетника.

7 Члан 16. Конвенције наводи да „ниједно дете неће бити изложено произвољном или незаконитом мешању у његову приватност, породицу, дом или преписку, нити незаконитим нападима на његову част и углед".

безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, или ради заштите права и слобода других.

Живот члану 8. дала је богата пракса Европског суда за људска права, пре свега у погледу обима појма *приватни живот*[8], али и у питањима попут оправданости ограничења права и квалитета закона који та ограничења прописује.[9]

У односу на правно регулисање права на приватност, уређивање права на заштиту података о личности новијег је датума, а инспирисано је развојем информационих технологија и широм употребом личних података грађана, како од стране субјеката са јавним овлашћењима, тако и од стране привредних субјеката. Тако је први закон о заштити података о личности донет у немачкој Савезној држави Хесен, 1970. године, а пратили су га усвајање закона у Шведској (1973), САД (1974), Немачкој (1977) и Француској (1978).

Све учесталија међународна размена података и прекогранично кретање података, као и широка примена метода аутоматизоване обраде података, указали су на потребу за успостављањем јединствених стандарда заштите података о личности на глобалном нивоу. Међутим, како је разумевање граница приватности (а самим тим и ниво заштите података о личности) у значајној мери условљен и друштвеним контекстом и културолошким специфичностима, овај задатак није био нимало лак. Тако је, 1981. године, у оквиру Савета Европе усвојена *Конвенција Савета Европе о заштити лица у односу на аутоматску обраду личних података* („Конвенција")[10], која је дефинисала основна начела заштите података о личности и која је примењива на обраду података од стране и јавног и приватног сектора. Конвенција није директно примењива, већ успоставља обавезу за државе које су је ратификовале да усвоје и примене законе и адекватне мере у складу са одредбама Конвенције. *Додатни протокол Конвенције у вези са надзорним органима и прекограничним протоком података* усвојен је

8 Видети, на пример, предмете *Леандер против Шведске* (Представка бр. 9248/81), Пресуда од 26. марта 1987, доступно на: *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57519#{"itemid":["001-57519"]*; *Немиц против Немачке* (представка бр. *13710/88*), Пресуда од 16. децембра 1992, доступно на: *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57887#{"itemid":["001-57887"]* или *Халфорд против Уједињеног Краљевства* (Представка бр. 20605/92), Пресуда од 25. јуна 1997, доступно на: *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"dmdocnumber":["695916"],"itemid":["001-58039"]*.

9 Видети, на пример, предмете: *Фон Ханover против Немачке* (Представка бр. 59320/00), Пресуда од 24. јуна 2004, доступно на: *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"appno":["59320/00"],"itemid":["001-61853"]*; *Бушекур против Француске* (Представка бр. 5335/06), Пресуда од 17. децембра 2009, доступно на: *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-96361#{"itemid":["001-96361"]}*; *Гардел против Француске* (Представка бр. 16428/05), Пресуда од 17. децембра 2009, доступно на: *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"appno":["16428/05"],"itemid":["001-96457"]}*; *М. Б. Против Француске* (Представка бр. 22115/06), Пресуда од 17. децембра 2009, доступно на: *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"dmdocnumber":["860002"],"itemid":["001-96363"]}* – странице на француском језику.

10 Доступно на: *https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37*.

2001. године. Република Србија ратификовала је 2005. године Конвенцију 108, а 2008. године и Додатни протокол. Исте године Србија је добила Закон о заштити података о личности („Службени гласник РС", бр. 97/2008, 104/2009 – др. закон, 68/2012 – УС, и 107/2012).[11]

Поред чињенице да успоставља основна начела обраде података о личности, Конвенција 108 даје и једну од најчешће цитираних (и преузиманих) дефиниција појма *податак о личности*. Према члану 2. тачка (а) Конвенције, лични подаци означавају *сваку информацију у вези са идентификованим физичким лицем или лицем које се може идентификовати*. У наставку текста видећемо да је први задатак лица које податке обрађује да утврди да ли се заправо ради о подацима о личности како би се установило да ли се, и какав, режим заштите података примењује. Некада је одговор на то (претходно) питање очигледан, а некада мора бити предмет детаљније анализе и разматрања контекста конкретне ситуације.

Узимајући у обзир нове околности обраде и изазове за заштиту података о личности, у мају 2018. године Савет Европе усвојио је *Протокол којим се мења Конвенција о заштити лица у односу на аутоматску обраду личних података*.[12] Протокол, који је Србија потписала у новембру 2019. године, доноси новине у погледу начела пропорционалности, законитости и транспарентности обраде података, као и начела минимизације података. Протокол, такође, проширује категорију осетљивих података на генетске и биометријске податке, као и податке о чланству у синдикатима и о етничком пореклу. Додатно, Протоколом се прописују обавезе пријављивања повреде података, предвиђа се виши степен одговорности руковалаца подацима и прописују нова правна лица чији се подаци обрађују у контексту доношења одлука коришћењем алгоритама. Коначно, Протокол предвиђа примену начела обраде података на све радње обраде, укључујући и националну безбедност, прописује јаснији режим прекограничног протока података, а као циљ има и јачање овлашћења и независности органа за заштиту података о личности и унапређење правног основа за међународну сарадњу.[13]

11 Први закон који је уређивао ову област у нашој земљи усвојен је 1998. године на нивоу Савезне Републике Југославије – Закон о заштити података о личности („Службени гласник СРЈ", бр. 24/1998 и 26/1998 – исправка), познат по чињеници да није примењен ни у једном случају пред судом или неким управним органом.

12 *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223*, доступно на: *https://rm.coe.int/16808ac918*.

13 Видети: *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223* и *https://www.poverenik.rs/sr/актуелности/3204-србија-потписала-протокол-којим-се-мења-конвенција-о-заштити-лица-у-односу-на-аутоматску-обраду-личних-података-конвенција-108-савета-европе.html*.

2. ПРАВНИ ОКВИР ЗА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ У ЕВРОПСКОЈ УНИЈИ

2.1. Први кораци ка стварању јединственог правног оквира за заштиту података у ЕУ

Право на заштиту података о личности гарантовано је највишим правним актима Европске уније.

- Тако члан 16. *Уговора о функционисању Европске уније*[14] предвиђа да свако има право на заштиту својих података о личности, те предвиђа обавезу Европског парламента и Савета да утврде правила у погледу обраде података о личности од стране органа, тела, служби и агенција ЕУ. За доношење оваквих одлука, предвиђен је тзв. *редован законодавни поступак*, у ком Европски парламент и Савет деле законодавна овлашћења.
- Даље, члан 39. *Уговора о Европској унији*[15] предвиђа обавезу Савета да усвоји правила о заштити појединаца у погледу обраде података о личности од стране држава чланица, као и о слободном кретању тих података. Наведена правила треба да обухвате случајеве обраде података о личности од стране држава чланица у оквиру активности које спадају у тзв. други стуб ЕУ, односно заједничку спољну и безбедносну политику.
- *Повеља ЕУ о основним правима ЕУ*[16] (у даљем тексту „Повеља") у члану 7. гарантује право на поштовање приватног и породичног живота, дома и комуникације (дакле, право на приватност, у ширем смислу), док је члан 8. посвећен заштити података о личности и предвиђа да: „свако има право

14 Consolidated version of the Treaty on the Functioning of the European Union, *Official Journal of the European Union C 326/47*, од 26. октобра 2012, доступно на: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN*.

15 Consolidated version of the Treaty on European Union, *Official Journal of the European Union C 326*, од 26. октобра 2012, доступно на: *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT&from=EN*.

16 Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities No. C 364/01* од 18. децембра 2000, доступно на: *http://www.europarl.europa.eu/charter/pdf/text_en.pdf*.

на заштиту података о личности који се на њега или њу односе". Међутим, поред утврђивања општег права на заштиту података о личности, Повеља разрађује и неколико посебних аспеката овог права:

- *квалитет обраде података* – подаци о личности морају се обрађивати поштено, за одређену сврху и на основу пристанка лица на које се подаци односе или на неком другом легитимном основу утврђеном законом. Треба напоменути да Повеља не наводи који су то легитимни интереси, већ препушта државама чланицама да их дефинишу у свом националном законодавству;
- *права лица на која се подаци односе* – сваком појединцу гарантује се право на приступ прикупљеним подацима који се на њега/њу односе, као и право да захтева исправљање тих података. Повеља, међутим, не предвиђа право на брисање података;
- *независни надзорни орган* – Повеља предвиђа да контролу над применом правила из члана 8. треба да врши независни орган. На основу ове одредбе, усвојена је Уредба Европског парламента и Савета бр. 45/2001 о заштити појединаца у погледу обраде података о личности од стране органа и тела Заједнице и о слободном кретању тих података[17], којом је успостављен Европски супервизор за заштиту података, као независан орган задужен за праћење примене правила о заштити података о личности од стране органа Уније. Додатно, све државе чланице имају националне независне органе задужене за надзор над применом прописа о заштити података о личности.

Треба напоменути да је Повеља, иако усвојена 2000. године, правно дејство добила тек ступањем на снагу Лисабонског уговора, 1. децембра 2009. године и има исту правну снагу као и оснивачки уговори ЕУ.

Први правни акт на нивоу Европске уније који се бави искључиво заштитом података о личности била је *Директива 95/46/ЕЗ о заштити појединаца у погледу обраде података о личности и о слободном кретању тих података*. Усвајање Директиве о заштити података представљало је прекретницу у развоју правног оквира за заштиту података у Европској унији, посебно ако се има у виду да су кроз овај документ прожете неке од најстаријих вредности процеса европских интеграција: заштита основних људских права и слобода, и омогућавање функционисања јединственог унутрашњег тржишта.[18] Од њеног усвајања, Директива о заштити података утицала је на законодавство у области заштите личних

17 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *Official Journal of the European Communities No. I 8/1* од 12. јануара 2001, доступно на: *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=en*.

18 Видети: *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and Committee of the Regions (COM (2010) 609)*, од 4. новембра 2010, доступно на: *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF*, стр. 2.

података, како у државама чланицама ЕУ, стварањем обавезујућег и хармонизованог оквира за заштиту података о личности у Унији, тако и у земљама кандидатима и потенцијалним кандидатима за чланство у ЕУ. На основу Директиве о заштити података, већина држава чланица ЕУ усвојила је „технолошки неутралне" дефиниције појма *података о личности* које би могле обухватити различита значења и садржаје кроз време. Тако, члан 2. тачка а) Директиве о заштити података дефинише податке о личности *као сваку информацију у вези са идентификованим физичким лицем или лицем које се може идентификовано.* Према Директиви о заштити података, *лице које се може идентификовати* је оно лице које може бити идентификовано, непосредно или посредно, пре свега позивањем на идентификациони број или на један или више чинилаца који су карактеристични за његов физички, физиолошки, ментални, економски, културни или друштвени идентитет.

Директива о заштити података примењивала се и на аутоматску обраду података и на обраду која се не врши аутоматским путем. Директивом о заштити података је такође утврђена обавеза држава чланица ЕУ да надзор над применом закона усвојених у складу са Директивом повере независном надзорном органу. На основу члана 29. Директиве о заштити података, формирана је *Радна група за заштиту појединаца у погледу обраде података о личности* (позната и као „Радна група 29"), као независно саветодавно тело ЕУ. Радна група 29 разматрала је примену националних мера усвојених на основу Директиве о заштити података, обавештавала Европску комисију о нивоу заштите података о личности у државама чланицама и трећим земљама, и, уопште, својим ставовима и тумачењима давала је велики допринос развоју регулативе и пракси у области заштите података о личности на нивоу ЕУ.

- Одредбе Директиве о заштити података даље су уређене *Уредбом (ЕЗ) бр. 45/2001 о заштити појединаца у вези са обрадом података о личности од стране органа и тела Заједнице и о слободном кретању таквих података.* Међутим, за разлику од Директиве о заштити података која се односила на државе чланице у смислу усвајања њихових националних закона о заштити података о личности, Уредба се бавила обрадом података о личности у свим органима и телима ЕУ која се спроводи приликом примене права Заједнице. Чланом 41. Уредбе успостављен је Европски супервизор за заштиту података, са циљем да се осигура да органи и тела Заједнице поштују право на приватност физичких лица, те да појединци имају коме да се обрате у случајевима наводног кршења права на заштиту података о личности.
- *Директива 2002/58/ЕЗ о обради података о личности и заштити приватности у сектору електронских комуникација*[19] прописивала је за државе чланице обавезе које се односе на усклађивање њихових правних оквира

19 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), *Official Journal of the European Communities L 201 од 31. јула 2002, доступно на: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:32002L0058&from=EN.*

у области обраде података у сектору електронских комуникација, као и у погледу слободног кретања таквих података, опреме и услуга електронских комуникација у оквиру Заједнице. Директива се бавила и питањима безбедности електронских комуникација, поверљивошћу комуникација (у погледу забране неовлашћеног пресретања или надзора над комуникацијама), комуникација у сврху директног маркетинга итд.

Током прве деценије 21. века, Европска унија и њени органи усвојили су још низ докумената са циљем хармонизације и унапређења правног оквира и праксе у области заштите података о личности. Између осталог, усвојени су: *Директива 2002/22/ЕЗ о универзалном сервису и правима корисника која се односе на електронске комуникационе мреже и услуге*[20], *као и Директива 2009/136/ЕЗ*[21] *која је допуњује, а која уређује права крајњих корисника и обавезе компанија које пружају јавно доступне електронске комуникационе мреже и услуге; Уредба (ЕК) бр. 2006/2004 о сарадњи између националних органа одговорних за спровођење закона о заштити потрошача*[22], чији је крајњи циљ усклађеност националних закона о заштити потрошача, несметано функционисање унутрашњег тржишта и јачање заштите економских интереса потрошача; *Оквирна одлука Савета 2008/977/ПУП од 27. новембра 2008. о заштити података о личности обрађених у оквиру полицијске и правосудне сарадње у кривичним стварима*[23], чији је циљ био да се обезбеди висок ниво заштите основних права и слобода физичких лица, а посебно права на приватност у погледу обраде података о личности у оквиру правосудне и полицијске сарадње у кривичним стварима.

20 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services, *Official Journal of the European Communities No. L 108 од 24. априла 2002*, доступно на: *http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0022*.

21 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, *Official Journal of the European Communities No I. 337/11 од 18. децембра 2009,* доступно на: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.*

22 Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), *Official Journal of the European Communities No. L 364/1 од 9. децембра 2004*, доступно на: *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R2006&from=en*.

23 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *Official Journal of the European Communities No. I. 350/60 од 31. децембра 2008,* доступно на: *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0977&from=EN*.

2.2. Нова ера заштите података о личности у ЕУ

Развој технологије и глобализација у 21. веку донели су нове изазове у заштити података грађана које правни оквир 20. века није предвидео. Све већи број услуга које се пружају путем интернета, *cloud* технологија, мобилне апликације и сл., као да су избрисале границе, али и одузеле контролу појединцу над кретањем његових података. Из тих разлога је у Европској унији још 2010. године покренута иницијатива за измену правног оквира, формализована усвајањем *Саопштења Европске комисије Европском Парламенту, Савету, Економском и социјалном комитету и Комитету региона*, која је инсистирала на свеобухватном приступу заштити података у ЕУ са следећим циљевима:

- Оснаживање права појединаца;
- Јачање димензије унутрашњег тржишта у оквиру ЕУ;
- Ревидирање правила о заштити података у области полицијске и правосудне сарадње у кривичним стварима;
- Узимање у обзир глобалне димензије заштите података (у смислу њиховог прекограничног кретања односно размене);
- Јачање институционалног оквира за ефикаснију примену правила о заштите података.[24]

У складу са овим циљевима, у годинама које су уследиле органи ЕУ интензивно су радили на усвајању новог правног оквира који би одговорио новим изазовима. Најзначајнији акт у овом смислу јесте *Општа уредба о заштити података ЕУ*[25] (енгл. *General Data Protection Regulation – GDPR*), која ће бити детаљније представљена у наставку текста, а која је послужила и као узор за усвајање новог Закона о заштити података о личности Републике Србије. Уз решења из Уредбе, наш Закон преузима и низ одредби тзв. *Полицијске директиве*[26], о којој ће такође бити речи у наставку.

---

24 Видети: Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and Committee of the Regions (COM (2010) 609), од 4. новембра 2010, доступно на: *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF*

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), доступно на: *https://eur-lex.europa.eu/eli/reg/2016/679/oj*. Незваничан превод Уредбе на српски језик доступан је на страници Повереника: *https://www.poverenik.rs/sr/међународни-документи6/2502-уредба-2016-679-незваничан-превод.html*.

26 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, доступно на: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680*.

2.2.1. Општа уредба Европске уније о заштити података

Након готово четири године дугог консултативног процеса, са преко 4000 поднетих амандмана током израде коначног текста[27], у априлу 2016. године усвојена је Општа уредба о заштити података у ЕУ. Примена Уредбе у државама чланицама ЕУ почела је две године након усвајања документа, односно 25. маја 2018. године.

Општа уредба ставља ван снаге Директиву о заштити података и, за разлику од Директиве која је хармонизовала право држава чланица у области заштите података о личности, Уредба врши *унификацију права* и *непосредно се примењује* у држава чланицама ЕУ. Међутим, од 99 чланова Уредбе подељених у 11 поглавља, преко педесет њих су тзв. „отворене" одредбе, којима се омогућава државама чланицама да усвоје националне прописе којима ће додатно уредити поједина питања.[28] С обзиром на то да Општа уредба уводи низ нових решења и појмова, од којих су многи техничког карактера, додатна образложења дата су у 173 тачке Преамбуле Уредбе.

Уредба регулише општи режим заштите података о личности, док је посебан осврт дат у погледу обраде података у следећим околностима: у контексту слободе изражавања, приступа информацијама од јавног значаја, обраде националног идентификационог броја појединаца, у контексту запошљавања, обраде података у сврхе архивирања у јавном интересу, научног или историјског истраживања или у статистичке сврхе, заштите података о личности у контексту обавезе чувања тајности података, те обраде података од стране цркава и верских удружења. Дакле, Општа уредба *не садржи посебна правила која би се могла применити на обраду података коју врше јединице локалне самоуправе*, већ се и овим случајевима *примењује општи режим* у погледу начела обраде података, права лица на која се подаци односе, обавеза руковалаца подацима и обрађивача података, безбедности података, преноса података у треће земље, казнених одредби итд.

2.2.1.1. Примена Опште уредбе о заштити података

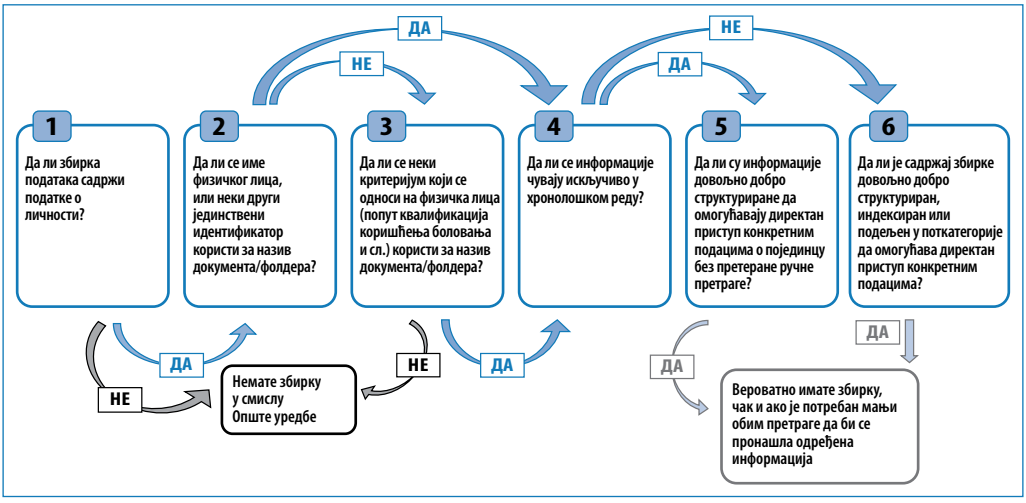
Уредба прописује правила која се односе на *заштиту физичких лица*, без обзира на њихово држављанство или пребивалиште, приликом обраде података о личности. Дакле, режим заштите који Уредба прописује не односи се на правна лица.[29] Уредба се примењује како на *аутоматску обраду података, тако и на неаутоматску* (ручну) обраду, и то у односу на оне збирке података или скупове

27 Видети: *Grupa autora, Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – Tumačenje novog pravnog okvira, Misija OEBS-a u Srbiji i SHARE Fondacija,* доступно на: *https://www.sharefoundation.info/Documents/Vodic_ZZPL.pdf*, стр. 13.

28 Видети: *Baker McKenzie, GDPR National Legislation Survey, 5.0*, January 2019, доступно на: *https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2019/01/gdprnationallegislationsurvey_jan2019.pdf*.

29 Тачка 14. Преамбуле Опште уредбе.

збирки који су структуирани према посебним критеријумима.[30] Слика у наставку даје опште смернице на основу којих руковалац може да утврди да ли у конкретном случају води збирку података о личности, односно да ли ће се на тај случај примењивати Општа уредба.



Слика 1. Смернице за процену да ли је збирка података у конкретном случају збирка података о личности[31]

Уредба се не примењује на обраду података коју врше физичка лица за потребе личних или кућних активности. Тако приватни телефонски именик не би био предмет заштите Уредбе, као ни подаци који су предмет активности друштвеног умрежавања на интернету.[32] Међутим, компаније које пружају услуге које омогућавају овакво умрежавање или коресподенцију (на пример, Фејсбук) јесу обвезници Уредбе, уколико испуњавају услове територијалне примене Опште уредбе. Такође, Уредба се не примењује на заштиту података у вези са делатностима које не спадају у подручје примене права ЕУ, попут делатности у вези са националном безбедношћу[33], као ни на обраду података коју врше надлежни органи у сврхе спречавања, истраге, откривања и гоњења кривичних дела или извршења кривичних санкција, укључујући и заштиту од претњи за јавну безбедност. У односу на заштиту физичких лица у овим случајевима обраде података, примењује се Полицијска директива.[34] Међутим, на обраду података које врше надлежни органи у својству органа управе (на пример, приликом обраде података за вршење

30 Тачка 15. Преамбуле Опште уредбе.
31 Преузето и прилагођено са странице *https://medium.com/golden-data/what-is-a-filing-system-under-eu-data-protection-law-6e7222743f71*.
32 Тачка 18. Преамбула опште уредбе.
33 Тачка 16. Преамбуле Опште уредбе.
34 Тачка 19. Преамбуле Опште уредбе.

различитих управних послова или приликом обраде података запослених), примењује се општи режим из Уредбе.

Територијална примена Опште уредбе, једно је од питања које изазива највише недоумица у примени, с обзиром на то да су одредбе Уредбе обавезујуће и за одређени круг субјеката који немају седиште у државама чланицама Европске уније. Наиме, Уредба се примењује:

- на обраду података о личности у оквиру активности оснивања седишта руковаоца или обрађивача у ЕУ, независно од тога да ли се обрада врши у ЕУ или не.
- на обраду података о личности лица у ЕУ коју врши руковалац или обрађивач који нема седиште у ЕУ, ако су активности обраде повезане са:
  - нуђењем робе или услуга таквим лицима у ЕУ на које се подаци односе, независно од тога да ли лице на које се подаци односе треба да изврши плаћање; или
  - праћењем њиховог понашања, уколико се оно одвија унутар ЕУ.
- на обраду података о личности коју врши руковалац који нема седиште у Унији, већ у месту где се право државе чланице примењује на основу међународног јавног права.[35]

За руковаоце подацима и обрађиваче података о личности[36] од кључног је значаја да утврде да ли су обухваћени режимом из Опште уредбе или пак националног законодавства државе у којој имају седиште, због чињенице да Уредба прописује строже санкције у односу на било који национални закон који уређује заштиту података о личности, и то у висини од 20.000.000 евра, или, у случају корпорација, до 4% укупног годишњег промета на светском нивоу за претходну финансијску годину, у зависности од тога који је износ већи.[37] Због тога је Европски одбор за заштиту података, тело које је заменило Радну групу 29, издало *Смернице о територијалној примени Опште уредбе о заштити података ЕУ* (члан 3)[38], у којима даје упутства за утврђивање да ли је одређени руковалац подацима или обрађивач обвезник Уредбе.

Дакле, руковаоци и обрађивачи података о личности основани у Европској унији обвезници су Опште уредбе, без обзира на то да ли се обрада података о личности одвија у ЕУ. Седиште у ЕУ односи се на „*ефективно и стварно обављање пословне активности у ЕУ кроз стабилне пословне аранжмане*."[39] Обрађивачи

35 Члан 3. Опште уредбе.

36 За дефиницију појмова *руковалац* и *обрађивач* видети стр. 16.

37 Члан 83. став 5. Опште уредбе.

38 European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation*, од 16. новембра 2018, доступно на: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf*.

39 I. Milošević, *GDPR – Uputstvo za upotrebu*, Janković – Popović – Mitić, 2018, *https://www.jpm.rs/wp-content/uploads/2018/04/gdpr.pdf*, стр. 8.

који су успостављени у Европској унији биће обвезници Опште уредбе чак и када обрађују податке у име руковаоца који сам није обвезник, односно нема седиште или не послује на територији Уније.

Даље, руковаоци подацима и обрађивачи који „таргетирају" лица на која се подаци односе у Европској унији биће обвезници Опште уредбе, чак и уколико нису основани у Унији. Смернице Европског одбора за заштиту података упућују на двостепени тест на основу којег се може утврдити да се циљање лица на која се подаци односе догађа у ЕУ, који обухвата следећа питања:

- Да ли се подаци односе на лица у Унији?
  Под лицима у Европској унији подразумевају се сва лица на територији ЕУ чији се подаци прикупљају, без обзира на њихово држављанство или пребивалиште.

ПРИМЕР

Уколико је држављанин Србије на пропутовању у Француској и користи апликацију на мобилном телефону која му даје информације о знаменитостима које тамо може видети прикупљајући његове личне податке (на пример, године, пол, тренутну локацију), тај држављанин Србије сматраће се лицем на које се подаци односе према Општој уредби, односно моћи ће да заштити своја права према правном режиму из Уредбе.[40] Са друге стране, уколико би сличну апликацију у Србији користио држављанин Француске како би упознао знаменитости наше земље (а уколико апликација није посебно рекламирана за француске држављане као циљну групу), компанија из Србије која управља апликацијом не би аутоматски била обвезник Опште уредбе.

- Да ли се ради о нуђењу роба и услуга лицима у Унији или праћењу лица на које се подаци односе у ЕУ?
  Нуђење роба и услуга подразумева постојање *намере* да се робе и услуге понуде лицима на територији ЕУ, без обзира на то да ли је та намера праћена и одређеном трговинском или економском активношћу.

ПРИМЕР

Смернице указују на низ фактора који се могу узети у обзир при оцени да ли се у конкретном случају ради о нуђењу роба и услуга лицима у ЕУ: *а) Европска унија или бар једна њена чланица су наведене или означене називом у вези са робама или услугама које се нуде (на пример, „Повољна путовања у Србију за путнике из Немачке"); б) руковалац подацима или обрађивач података плаћају интернет претраживачу за специфичне резултате претраге како би се омогућио приступ њиховим веб страницама од стране потрошача у ЕУ, или спроводе маркетинг кампање усмерене на циљну групу у држави чланици ЕУ; в) међународни карактер активности у датом случају, попут туристичких активности; г) навођење посебне адресе или броја телефона путем којих се може остварити контакт из државе чланице ЕУ;*

40 *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation*, стр. 13–14.

ПРИМЕР

д) коришћење препознатљивог домена различитог од оног који се користи у земљи у којој су руковалац или обрађивач успостављени, попут „.еи"; ђ) упутство за путовање из једне или више држава чланица ЕУ у место где се пружа конкретна услуга; е) навођење међународних корисника/клијената који су резиденти различитих држава чланица ЕУ; ж) коришћење језика или валуте различитих од оних који се уобичајено користе у земљи пружаоца роба/услуга, посебно уколико се ради о језику или валути неке од држава чланица ЕУ; з) руковалац нуди достављање робе у државе чланице ЕУ.[41]

Коначно, Општа уредба примењује се приликом *праћења понашања лица у ЕУ*, када се такво понашање дешава на територији Уније. Под праћењем се подразумевају активности које као посебан циљ имају прикупљање и накнадну поновну употребу података о понашању појединца у ЕУ. Као примере ових активности Смернице наводе онлајн праћење употребом тзв. колачића или других техника праћења (попут отисака прстију), коришћење видео-надзора, услуге израде персонализованих дијета или здравствених анализа путем интернета, истраживања тржишта или друге анализе понашања засноване на индивидуалном профилу лица, праћење или редовно извештавање о здравственом стању појединца итд.[42]

2.2.1.2. Основни појмови

У члану 4, Општа уредба даје дефиниције низа појмова чије је разумевање кључно за даљу адекватну примену решења из Уредбе. Па тако, према Уредби:

Податак о личности је свака информација која се односи на физичко лице које је идентификовано или се може идентификовати, непосредно или посредно, посебно помоћу идентификатора, као што су име и идентификациони број, подаци о локацији, онлајн идентификатора или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета. Дакле, подаци о личности су име и презиме, јединствени матични број грађана (ЈБМГ), порески број, број здравственог осигурања, број телефона, број личне карте, пасоша, слика, видео-запис особе, тонски запис особе, отисци прстију, ДНК, подаци о локацији и кретању итд.

Обрада података је свака радња или скуп радњи које се врше аутоматизовано или неаутоматизовано са подацима о личности или њиховим скуповима, као што су прикупљање, бележење, разврставање, груписање, односно структурирање, похрањивање, прилагођавање или мењање, откривање, увид, употреба, обелодањивање преносом, односно достављањем, умножавање, ширење или чињење

41 *Ibid*, стр. 15–16.
42 *Ibid*, стр. 18.

доступним на други начин, упоређивање, ограничавање, брисање или уништавање. Дакле сваки вид коришћења, чувања података или манипулисања подацима сматра се обрадом, чак и у случајевима када се подаци не користе „активно", већ су просто похрањени на одређеној локацији.

Профилисање је сваки облик аутоматизоване обраде података о личности који се састоји од коришћења података о личности за процену одређених личних аспеката у вези са физичким лицем, посебно за анализу или предвиђање аспеката у вези с радним учинком, материјалним стањем, здрављем, личним склоностима, интересима, поузданошћу, понашањем, локацијом или кретањем тог физичког лица. Три су, дакле кључна елемента које одређена радња обраде мора да испуни да би се сматрала профилисањем: *1)* да се ради о аутоматизованом облику обраде података; *2)* да се изводи над подацима о личности; *3)* да има за сврху да процени одређене аспекте физичког лица како би се предвидело његово понашање и донела одређена одлука у вези са тим.

Руковалац подацима о личности је физичко или правно лице, орган власти, агенција или друго тело које само или заједно са другим телима одређује сврху и средства обраде података. Сврха обраде може бити одређена и законом, што је најчешћи случај када обраду података врше носиоци јавних овлашћења. Тако су јединице локалне самоуправе у највећем броју случајева руковаоци подацима. Могуће је и да два или више руковалаца заједнички одређују сврху и средства обраде, у ком случају ће се радити о *заједничким руковаоцима*.[43]

Обрађивач је физичко или правно лице, орган власти, агенција или друго тело које обрађује податке о личности у име руковаоца.

ПРИМЕР

Уколико јединица локалне самоуправе ангажује треће лице (фирму) за пружање услуга видео-надзора, за потребе и сврхе које одреди ЈЛС, то треће лице имаће својство обрађивача података и поступаће само на основу и у оквиру налога ЈЛС.

Корисник података је физичко или правно лице, односно орган власти коме су подаци о личности откривени, без обзира на то да ли се ради о трећем лицу или не, осим ако се ради о органима власти који у складу са законом примају податке о личности у оквиру истраживања одређеног случаја и обрађују ове податке у складу са правилима о заштити података о личности која се односе на сврху обраде.

Треће лице је физичко или правно лице, односно орган власти који није лице на које се подаци односе, руковалац или обрађивач, као ни лице које је овлашћено да обрађује податке о личности под непосредним надзором руковаоца или обрађивача.

Генетски подаци су подаци о личности који се односе на наслеђене или стечене генетске особине физичког лица које дају јединствене информације о

43 Члан 26. Опште уредбе.

физиологији или здрављу тог физичког лица, и који су добијени пре свега анализом биолошког узорка тог физичког лица.

Биометријски подаци су подаци о личности добијени посебном техничком обрадом у вези са физичким особинама, физиолошким особинама или карактеристикама понашања физичког лица који омогућавају или потврђују јединствену идентификацију тог физичког лица, као што су фотографије или дактилоскопски подаци.

Такође, Уредба препознаје и тзв. *посебну категорију података о личности*, односно:

- податке који откривају расно или етничко порекло, политичко опредељење, верска или филозофска уверења или чланство у синдикату,
- генетске податке, биометријске податке у сврху јединствене идентификације лица,
- податке о здравственом стању, податке о сексуалном животу или сексуалној оријентацији физичког лица.

Обрада података који спадају у посебну категорију података о личности је забрањена, осим уколико је испуњен неки од услова из члана 9. став 2. Уредбе – на пример, када је лице дало изричит пристанак за обраду тих података, а позитивни прописи не забрањују обраду посебне категорије података на основу пристанка, или уколико је обрада потребна ради заштите животних интереса лица на које се подаци односе или другог лица, када лице на које се подаци односе није физички или правно способно да дâ пристанак итд.[44]

2.2.1.3. Начела обраде података о личности

Поглавље II Опште уредбе посвећено је начелима обраде података о личности и представља надоградњу начела које је прописивала Директива о заштити података о личности. Треба напоменути да начела обраде података немају само декларативан карактер, већ успостављају стандарде законитости обраде података о личности и основ су за дефинисање права лица поводом заштите података о личности, те обавеза руковалаца подацима и обрађивача података.

Законитост, правичност и транспарентност

Уредба предвиђа да се подаци о личности морају обрађивати законито, правично и транспарентно. *Законитост* обраде подразумева да руковалац има широко разумевање Уредбе и њених правила, а пре свега својих обавеза поводом заштите података о личности, те да обраду врши у складу са Уредбом и другим прописима који уређују заштиту података о личности. *Правичност* обраде података подразумева да руковаоци увек узимају у обзир контекст, интересе лица чије податке обрађују и њихова очекивања у погледу приватности у датим околностима, а посебно да не смеју искоришћавати своју несразмерно јачу позицију у

44 Видети: Члан 9. став 2. Опште уредбе.

односу на лице чије податке обрађују (на пример, у односу органа власти и грађана, послодавца и запосленог и сл.).[45] *Транспарентност* подразумева да лице на које се подаци односе мора бити обавештено о свим аспектима обраде пре отпочињања обраде података, те да се током обраде у сваком моменту може обратити руковаоцу тражећи информације о томе да ли обрађује његове/њене податке, у које сврхе, по ком правном основу, да ли их уступа неком трећем лицу итд.

Правни основ за обраду зависи од специфичне сврхе и контекста обраде података. Уредба предвиђа шест могућих правних основа за обраду података, чије постојање обраду чини законитом, и то:

а) Лице на које се подаци односе је дало свој *пристанак* за обраду његових података о личности у једну или више конкретних сврха.

Приликом процене законитости пристанка лица као правног основа за обраду података битно је узети у обзир неколико елемената:

Пристанак је дат слободно – лицу се не може бити стављено у изглед да ће трпети последице нити да ће бити у неповољнијем положају уколико не жели да дâ пристанак за обраду података о личности.

Пристанак мора бити специфичан, односно дат за конкретну сврху обраде.

Пристанак мора бити безуслован, што значи да није условљен прихватањем других услуга или услова.

Пристанак мора бити заснован на обавештености, што подразумева да руковалац лицу од којег тражи сагласност унапред достави све информације везане за обраду података, правима која лице ужива у односу на руковаоца и начинима за заштиту својих права.

Пристанак мора бити недвосмислен – сагласност мора бити таква да се из ње јасно може закључити да лице даје свој пристанак за конкретну обраду личних података.

Пристанак мора бити документован – без обзира на начин на који је пристанак прибављен, руковалац мора бити у могућности да докаже да је лице дало сагласност.

Пристанак мора да буде такав да се може повући у сваком тренутку. Овде је важно нагласити да поступак повлачења сагласности не сме бити сложенији од поступка којим је лице дало сагласност. Такође, повлачење пристанка не утиче на законитост обраде података која је вршена пре повлачења пристанка.

Уредба не прописује општу старосну границу за пристанак малолетног лица. Међутим, та граница прописана је у случајевима непосредног нуђења услуга информационог друштва детету, те Уредба прописује да је у овим случајевима сагласност законита уколико дете има *16 година*, док би у супротном пристанак у име детета морао дати или одобрити вршилац родитељског права. Уредбом се оставља могућност да државе чланице, у складу

45 Видети: *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – Tumačenje novog pravnog okvira,* стр. 33.

са својим позитивним прописима, предвиде и нижу старосну границу за малолетнике, али не испод 13 година.

б) Обрада је потребна ради *извршења уговора* у којем је лице на које се подаци односе уговорна страна или ради предузимања мера на захтев лица на које се подаци односе *пре закључења уговора*.

У овом случају, обрада података мора бити неопходна. Уколико се иста сврха може постићи обрадом мањег обима података, или мање инвазивном обрадом (на пример, уместо узимања копија личних докумената, узети само њихове бројеве или извршити увид у те документе), овај правни основ се не би могао применити.

в) Обрада је потребна за *извршавање законске обавезе* која се примењује на руковаоца.

Најчешћи основ обраде података у јавном сектору је извршавање законске обавезе руковаоца. Уредба прописује да се ради о обавези која је прописана правом Уније или конкретне државе чланице.

г) Обрада је потребна ради *заштите животних интереса* лица на које се подаци односе или другог физичког лица.

Овај правни основ треба тумачити рестриктивно. Заштита животних интереса лица као правни основ може се користити када је обрада података неопходна за заштиту живота лица. Овај правни основ не може се користити за обраду посебне категорије података уколико је лице способно да дâ пристанак.[46]

д) Обрада је потребна за *извршење задатка који се обавља у јавном интересу или у оквиру извршавања службених овлашћења* додељених руковаоцу.

Према Уредби, задаци који се обављају у јавном интересу или у оквиру вршења јавних овлашћења морају бити прописани правом Уније или држава чланица. Руковалац мора бити у могућности да докаже да је обрада неопходна и сразмерна сврси која се жели постићи. Уколико постоји други разуман и мање инванзиван начин за постизање исте сврхе, овај правни основ се не би могао користити.

ђ) Обрада је потребна због *легитимних интереса* чијем остварењу тежи руковалац или треће лице, осим када над тим интересима преовлађују интереси основних права и слобода лица на које се подаци односе, а који захтевају заштиту података о личности, посебно ако је лице на које се подаци односе дете.

Легитимни интерес као могући правни основ за обраду података представља новину коју уводи Уредба, а из ње је преузима и наш Закон о заштити података о личности. Ради се о настојању да се релаксира обрада података, пре свега у привредном контексту, кроз увођење могућег правног основа који се не везује за специфичан закон или пристанак лица. Легитимни интерес се стога примењује углавном када руковалац не може да прибави

46 Видети: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/*.

сагласност лица, уз испуњење одређених услова. За процену да ли је легитимни интерес адекватан основ за обраду података, руковалац може применити тзв. троделни тест:

- *тест сврсисходности: да ли податке обрађује за остварење неког легитимног интереса (да ли је обрада у интересу руковаоца; да ли је законита; да ли је етична)?*
- *тест неопходности: да ли је обрада података у датом случају неопходна руковаоцу (да ли је обрада сразмерна циљу који се жели постићи; да ли постоје мање инвазивне мере)?*
- *тест баланса: да ли су права лица чији се подаци обрађују претежнија од легитимног интереса руковаоца (да ли се ради о обради високог ризика; који ће бити највероватнији ефекат обраде на лице)?*[47]

Као примере легитимних ситуација у којима се легитимни интерес може користити као правни основ за обраду података, Уредба наводи обраду података клијената или запослених, обраду у сврхе маркетинга, спречавања преваре, преноса података унутар међународних групација компанија или обезбеђивања безбедности мреже и информација.[48]

Легитимни интерес не би требало да се примењује на обраду коју врше органи власти приликом вршења својих овлашћења.

Ограничење сврхе обраде

Прикупљање личних података може се вршити само уз постојање претходно одређене, изричите и законите сврхе. Подаци се могу обрађивати само онолико дуго колико је потребно да би се остварила унапред одређена сврха. Већа флексибилност остављена је у погледу даље обраде података у сврхе архивирања у јавном интересу, научног или историјског истраживања или у статистичке сврхе, која се не сматра неусклађеном са првобитном сврхом.[49]

Минимизација података

Начело минимизације података предвиђа да обим података који се прикупљају ради обраде буде примерен и ограничен само на оне податке који су неопходни за сврху која се жели постићи прикупљањем података. Минимизација података, са једне стране, корисна је у ситуацијама угрожавања безбедности података, јер би у том случају неауторизована лица имала приступ само ограниченом обиму података, а са друге стране, олакшава захтев руковаоцу да чува ажурне и тачне податке.[50]

47 Видети: *https://www.termsfeed.com/blog/gdpr-legitimate-interests-3-part-test/*.
48 Тачке 47–49. Преамбуле Опште уредбе.
49 Члан 5. став 1. тачка б) Опште уредбе.
50 Видети: *https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles.*

Тачност

Начело тачности тражи да подаци о личности који се обрађују буду тачни и, ако је могуће, ажурни, при чему се предузимају све разумне мере којима се може обезбедити да се нетачни или неажурни подаци избришу или измене.

Ограничење чувања података

Лични подаци, у облику који омогућава идентификацију лица на које се подаци односе чувају се само у оном року који је неопходан за остварење предвиђене сврхе обраде. Једини изузетак односи се на обраду у сврхе архивирања у јавном интересу, научног или историјског истраживања или у статистичке сврхе, када се подаци могу чувати дуже, уз обавезу предузимања одговарајућих техничких и организационих мера.

Начело интегритета и поверљивости

Начело интегритета и поверљивости односи се на безбедност личних података који се обрађују. Радње обраде податка морају бити уређене тако да су лични подаци у сваком тренутку заштићени, да је приступ личним подацима ограничен, те да су подаци у техничком и организационом смислу заштићени од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења.

Наведена начела представљају низ стандарда који се морају поштовати у односу на личне податке. Поштовање начела обраде података, кроз правилно унапред одређену сврху због које се прикупљају подаци, ограничење обима личних података који се прикупљају, јасно унапред одређен рок чувања података, постојање техничких услова за заштиту личних података, као и кадровска ограничења у погледу тога ко све има приступ подацима, предуслови су за заштиту личних података. Уз то, Уредба посебно предвиђа и *начело одговорности руководаоца подацима*, који је одговаран за поштовање и усклађеност са наведеним начелима обраде и који мора да буде у могућности да докаже ту усклађеност.[51]

2.2.1.4. Права лица на која се подаци односе

У односу на Директиву о заштити података, Уредба проширује сет права лица на која се подаци односе, стављајући у фокус транспарентност обраде података, као и потребу да контролу над подацима имају управо грађани. Тако су Уредбом прописана следећа права лица:

Право на обавештеност, које подразумева да руковалац приликом прикупљања података лицу пружа информације о различитим аспектима обраде. Те информације односе се на идентитет и контакт руководаоца, сврху обраде података, правни основ за обраду, легитимни интерес руководаоца уколико је то правни основ за обраду података, кориснике података, уколико постоје, или су то информације

51 Члан 5. став 1. тачка б) Опште уредбе.

о преносу података у трећу земљу или међународну организацију. Такође, како би обрада података била правична и транспарентна, руковалац приликом прикупљања података лицу на које се подаци односе даје информације и о року чувања података или критеријуму на основу којег се тај рок одређује, правима лица поводом обраде података о личности, укључујући и право да се повуче сагласност уколико је пристанак правни основ за обраду података, те информације о томе да ли је пружање података о личности законска или уговорна обавеза, да ли лице има обавезу да пружи податке, које су последице уколико их не пружи, те да ли у датом случају постоји аутоматизовано доношење одлука, укључујући и профилисање.

Уредба предвиђа и одређене случајеве у којима руковалац нема обавезу да лицу пружа наведене информације, и то уколико лице на које се подаци о личности односе већ има те информације; пружање таквих информација је немогуће или би захтевало несразмеран утрошак времена и средстава – а нарочито у случају обраде у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања, као и у статистичке сврхе – или битно отежало остваривање сврхе обраде. У тим случајевима руковалац је дужан да предузме одговарајуће мере заштите права и слобода, као и легитимних интереса лица на које се подаци односе, што укључује и јавно објављивање информација. Прикупљање или откривање података о личности изричито је прописано правом Уније или правом државе чланице које се примењује на руковаоца, а којим се обезбеђују одговарајуће мере заштите легитимних интереса лица на које се подаци односе. Поверљивост података о личности мора се чувати у складу са обавезом чувања професионалне тајне која је прописана позитивним прописима.

Право на приступ, које подразумева да лице на које се подаци односе има право да добије потврду од руковаоца о томе да ли обрађује његове/њене податке о личности, те, ако се подаци обрађују, има право да приступи тим подацима, као и да добије следеће информације: која је сврха обраде података, које категорије података се обрађују, категорије корисника којима се подаци откривају, рокови чувања, као и информације о праву на приступ подацима, праву на подношење притужбе надзорном органу, извору података, уколико се они не прикупљају од самог лица, о постојању аутоматизованог доношења одлука, као и међународном преносу података. Право на приступ остварује достављањем захтева руковаоцу, који обезбеђује копије података који се обрађују.

Право на исправку и на брисање података („право на заборав"), којим се лицу чији се подаци обрађују омогућава да тражи, слањем захтева руковаоцу података, исправљање нетачних личних података, допуном непотпуних података или брисањем личних података у случају да *i)* подаци више нису потребни за првобитну сврху због које су прикупљени (а не постоји нова законита сврха), *iii)* основ за обраду података јесте сагласност лица на које се подаци односе, а лице тај пристанак повуче (а да, при томе, нема другог законског основа), *iii)* лице на које се подаци односе је уложило приговор на обраду података и не постоје преовлађујући законски разлози за наставак обраде, *iv)* подаци су незаконито

обрађени, *v)* брисање података је потребно за усклађеност са правом ЕУ или националним законодавством, или *vi)* подаци су прикупљени у вези са услугама информационог друштва које се нуде деци. По узору на право на заборав, утврђено 2014. године пресудом Европског суда правде у случају *Google Spain и Google Inc. против Шпанске агенције за заштиту података и Марија Костеха Гонзалеса*[52], Уредба уводи и нови елемент права на брисање. Наиме, поред обавезе да избрише податке лица (под горе наведеним условима), у случају да је руковалац објавио податке о личности, дужан је да их обрише, али и да обавести друге руковаоце подацима да је лице затражило брисање да би они обрисали све линкове до тих података, копије или реконструкције тих података.

Право на ограничење обраде, које подразумева да лице чији се подаци обрађују има право да добије ограничење обраде у случајевима када: *i)* лице сматра да су лични подаци нетачни, у периоду који руковаоцу омогућава да провери тачност личних података; *ii)* обрада јесте незаконита, али лице не жели да се подаци обришу, већ само да се ограничи њихова употреба; *iii)* руковаоцу подаци више нису потребни, али их лице тражи за успостављање, спровођење или одбрану правног захтева или *iv)* лице јесте поднело приговор на обраду података, а још није утврђено да ли је легитимни интерес руковаоца претежнији у односу на интересе лица чији се подаци обрађују. Дакле, ово право не подразумева трајно брисање података, већ њихову „пасивизацију", у смислу да их руковалац не сме активно користити. Обрада оваквих података је могућа само уз пристанак лица на које се подаци односе, изузев њиховог чувања, или пак за потребе успостављања, остваривања или одбране правног захтева односно заштите права другог физичког или правног лица, или због важног јавног интереса Уније или државе чланице.

Право на преносивост података омогућава лицу да прими податке о личности који се на њега односе, а које је пружило руковаоцу у структурираном, уобичајеном и машински читљивом формату, те да их пренесе другом руковаоцу или да захтева непосредан пренос тих података са једног на другог руковаоца, уколико је то технички изводљиво. Два су услова за остварење овог права: *i)* да је обрада података заснована на пристанку лица и *ii)* да се ради о аутоматској обради података.

Право на приговор даје лицу чији се подаци обрађују могућност да, подношењем приговора у било ком тренутку, заустави даљу обраду или спречи руковаоца да обрађује његове податке. Уколико се обрада података врши за сврхе директног маркетинга (укључујући и профилисање које је повезано са директним маркетингом)[53], ово право је апсолутно, односно руковалац је дужан

52 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Предмет C 131/12, Пресуда од 13. маја 2014. доступно на: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN.

53 Директни маркетинг обухвата активности оглашавања које подразумевају непосредну комуникацију са купцима/клијентима, без укључивања посредника за оглашавање. Најчешће се директни маркетинг спроводи слањем брошура, каталога, билтена, и сличних промотивних имејл садржаја, SMS порука, телефонским позивима или таргетираним онлајн рекламама.

да прекине обраду података о лицу у ове сврхе. Међутим, уколико се обрада података врши *i)* за извршење задатка који се обавља у јавном интересу, *ii)* у оквиру извршења службених овлашћења руковаоца или *iii)* за потребе легитимних интереса руковаоца или трећих лица, право на приговор *није апсолутно*. У овим случајевима, лице на које се подаци односе улаже приговор позивајући се на специфичне разлоге засноване на његовом/њеном конкретном положају. Приговор се може односити на све податке које руковалац обрађује о том лицу или само на одређени круг података, а може се односити и на само одређену сврху обраде. Како се не ради о апсолутном праву (осим у поменутом случају директног маркетинга), руковалац може одбити да поступи по приговору *i)* уколико докаже да постоје уверљиви легитимни интереси за обраду података који претежу над интересима, правима или слободама лица на које се подаци односе или *ii)* уколико се обрада врши зарад успостављања, остваривања или одбране правних захтева.

Лице чији се подаци обрађују има *право да се* на њега *не примењује одлука заснована искључиво на аутоматској обради података* (дакле, без људске интервенције), укључујући и профилисање, а која производи правне последице на њега или на сличан начин значајно утиче на њега. Ово право лица није гарантовано уколико је поменута одлука *i)* неопходна за закључење или извршење уговора између руковаоца или лица на које се подаци односе, *ii)* дозвољена правом Уније или држава чланица или *iii)* заснована на експлицитној сагласности лица. Међутим, и у овим случајевима у којима је дозвољено доношење одлука засновано на искључиво аутоматској обради података, Уредба захтева да руковалац омогући лицу да захтева људску интервенцију при доношењу одлуке, да изрази сопствени став, као и да оспорава дату одлуку. Односно, када је одлука заснована искључиво на аутоматизованој обради дозвољена правом Уније или државе чланице, Уредба тражи и одређени квалитет тих прописа, односно да се предвиде и одговарајуће заштитне мере за права и слободе, односно легитимне интересе лица.

2.2.1.5. Обавезе руковаоца подацима и обрађивача података о личности

Уредба детаљније разрађује постојеће обавезе и прописује низ нових обавеза руковаоца подацима и обрађивача података о личности. Неке од најважнијих наводимо у наставку.

Подразумевана и уграђена приватност

Уредба предвиђа обавезу руковаоца да примени одређене техничке и организационе мере за потребе делотворног спровођења начела заштите података.[54] Овај концепт заправо подразумева да је руковалац дужан да инкорпорира

54 Члан 25. став 1. Опште уредбе.

заштиту података у своје радње обраде и пословне процесе, од њиховог дизајна до реализације. Руковалац је дужан да сталном применом одговарајућих техничких, организационих и кадровских мера обезбеди да се увек обрађују само они подаци о личности који су неопходни за остваривање сваке појединачне сврхе обраде. Та се обавеза примењује у односу на број прикупљених података, обим њихове обраде, рок њиховог похрањивања и њихову доступност.

Именовање представника руковаоца или обрађивача у Европској унији

Уколико обраду података лица у ЕУ врше руковалац или обрађивач који немају седиште у Унији, ови субјекти имају обавезу да именују свог представника у једној од држава чланица у којој се налазе лица чији се подаци обрађују. Од ове обавезе изузети су руковаоци и обрађивачи који спадају у групу јавних органа/тела, односно они који врше само повремену обраду података која не подразумева у већој мери обраду посебних категорија података или обраду података који се односе на кривичну и прекршајну осуђиваност, те за коју није вероватно да ће проузроковати ризик за права и слободе лица, узимајући у обзир природу, околности, обим и сврхе обраде података.[55]

Обавеза вођења евиденције о радњама обраде података о личности

Руковаоци и обрађивачи, као и њихови представници (уколико постоје) дужни су да воде писану евиденцију о радњама обраде података о личности. Уредба детаљно прописује које све информације евиденције треба да садрже, између осталог: *имена и контакт податке руковалаца, заједничких руковалаца, представника руковалаца и службеника за заштиту података*[56] *о личности, ако они постоје, односно ако су одређени; сврха обраде; врста лица на које се подаци односе и врста података о личности; врста прималаца којима су подаци о личности откривени или ће бити откривени, укључујући и примаоце у другим државама или међународним организацијама итд.*[57]

Од обавезе вођења евиденције изузети су предузећа и организације у којима је запослено мање од 250 лица. Међутим, и субјект у коме је запослено мање од 250 лица ће имати обавезу да води евиденцију уколико постоји вероватноћа да ће обрада проузроковати ризик за права и слободе лица, ако обрада није повремена, односно ако обухвата посебне категорије података или обраду података који се односе на кривичну и прекршајну осуђиваност. Такође, треба узети у обзир језик Уредбе, по коме се од обавезе вођења евиденција изузимају *предузећа и организације, али не и органи власти који имају мање од 250 запослених*.

55 Члан 27. Опште уредбе.

56 У преводима правних аката ЕУ користи се термин „службеник за заштиту података“ као превод за „*data protection officer*“. У складу са том праксом, овај термин се користи у деловима текста где се говори о европској уредби. Домаћи законски термин је „овлашћено лице за заштиту података“.

57 Члан 30. Опште уредбе.

Именовање службеника за заштиту података о личности

Уредба предвиђа још једну нову обавезу, а то је одређивање службеника за заштиту података о личности као једна од кадровских мера које треба да примене руковаоци и обрађивачи с циљем заштите података о личности приликом радњи обраде. Члан 37. Уредбе прописује у којим ситуацијама је руковалац односно обрађивач дужан да именује службеника за заштиту података о личности:

- *ако се обрада врши од стране органа власти или јавног тела, осим ако се ради о обради коју врши суд у сврху обављања његових судских овлашћења;*
- *ако се основне активности руковаоца или обрађивача састоје у радњама обраде које по својој природи, обиму, односно сврхама захтевају редовно и систематско праћење лица на које се подаци односе;*
- *ако се основне делатности руковаоца или обрађивача састоје из масовне обраде посебних категорија података и података о личности који се односе на кривичну и прекршајну осуђиваност.*

Уколико су руковалац или обрађивач органи јавне власти или јавна тела, Уредбом је предвиђена могућност да се за више таквих субјеката именује заједничког службеника за заштиту података.

Службеник за заштиту података може бити лице запослено код руковаоца/обрађивача или пак лице ангажовано као спољни сарадник на основу уговора. Без обзира на радноправни положај овог лица, оно мора бити *независно у свом раду*, и не сме примати инструкције приликом обављања својих задатака. Руковалац и обрађивач података дужни су да службеник за заштиту података укључе у сва питања која се тичу заштите података о личности. Ово лице такође је и контакт особа за лица чији се подаци обрађују у погледу свих питања у вези са обрадом њихових података о личности. Стога је једна од обавеза руковаоца и обрађивача да објаве контакт податке службеника за заштиту података и доставе их и надзорном органу.

У погледу *квалификација* и услова које треба да испуњава службеника за заштиту података, Уредба прописује опште смернице, односно да се ово лице именује се на основу стручних квалификација, а посебно стручног знања о праву и праксама у подручју заштите података те способности извршавања задатака намењених лицу задуженом за заштиту података. Преамбула Уредбе прецизира да би нужан ниво стручног знања требало утврдити у односу на радње обраде података које се спроводе, односно на заштиту потребну за податке које обрађују руковалац или обрађивач.[58] Смернице за службеника за заштиту података, које је израдила Радна група 29, додатно наводе да ово лице треба да буде стручњак у области националног и европског права, као и да дубински разуме Уредбу. Такође, од значаја је да лице познаје организациону структуру, пословне моделе, односно процедуре руковаоца, односно обрађивача.[59]

58 Тачка 97. Преамбуле Уредбе.

59 Article 29, Data Protection Working Party, *Guidelines on Data Protection Officers ("DPOs")*, децембар 2016, доступно на: *http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A*, стр. 11.

Службеник за заштиту података има задатак да:

а) информише и саветује руковаоца или обрађивача, као и њихове запослене о обавезама у погледу заштите података о личности;
б) прати усклађеност са правним оквиром за заштиту података, као и политикама руковаоца или обрађивача у вези са заштитом података о личности, укључујући и поделу одговорности, подизање нивоа свести и оспособљавање особља које учествује у радњама обраде, као и с тим повезаним ревизијама;
в) пружа савете, када је то затражено, у погледу процене утицаја у вези са заштитом података и прати примену те процене;
г) сарађује с надзорним органом;
д) делује као контактна тачка за надзорни орган о питањима која се тичу обраде података о личности.[60]

Треба напоменути да *посао службеника за заштиту података није доношење одлука у вези са радњама обраде података*, као ни спровођење интерних истрага у случајевима компромитације безбедности података.

Безбедност података о личности

Руковалац и обрађивач дужни су предузму одговарајуће техничке и организационе мере како би се обезбедио одговарајући ниво безбедности података. Приликом одабира одговарајућих мера, руковалац и обрађивач узимају у обзир природу, обим, околности и сврху обраде, као и вероватноћу наступања ризика и ниво ризика за права и слободе физичких лица.[61] Неке од *мера* за остваривање безбедности података обухватају:

- псеудонимизацију[62] и криптозаштиту[63] података о личности;
- обезбеђивање трајне поверљивости, интегритета, расположивости и отпорности система и услуга обраде;
- обезбеђивање успостављања поновне расположивости и приступа подацима о личности у случају физичких или техничких инцидената у најкраћем року;
- редовно тестирање, оцењивање и процењивање делотворности техничких, организационих и кадровских мера безбедности обраде.

60 Члан 39. Опште уредбе.

61 Члан 32, став 1. Опште уредбе.

62 Псеудонимизација је скуп радњи чији је циљ заштита приватности лица на које се подаци односе. Псеудонимизација је поступак замене података о личности и других података тако да се не може идентификовати лице на које се подаци односе.

63 Криптографија је наука која се бави методама заштите података. Члан 2. ст.1. тачка 20. Закона о информационој безбедности дефинише криптозаштиту као примену метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима (Закон о информационој безбедности, „Службени гласник РС", бр. 6/2016, 94/2017 и 77/2019).

Овим се не исцрпљује списак мера које је потребно предузети с циљем заштите података о личности, јер се мере заштите морају процењивати од случаја до случаја.

Обрада података условљена је и са аспекта постојања техничких односно организационих услова и процедура које морају бити установљене пре почетка обраде података, а с циљем заштите података о личности. Ово подразумева и спровођење кадровских мера код руковаоца с циљем едукације и оспособљавања запослених за руковање подацима о личности, као и ограничавања круга запослених који имају приступ подацима о личности. Како је документовање једна од кровних обавеза руковалаца и обрађивача, они морају бити у могућности и да докажу да су предузели неопходне мере заштите података, а један од начина да се демонстрира усклађеност јесу и одобрени кодекси понашања и сертификација.

Члан 40. Уредбе предвиђа *могућности израде кодекса понашања* како би удружења и други субјекти који представљају групе руковалаца или обрађивача ефикасније примењивали Уредбу. Институт кодекса узима у обзир специфичности обраде података у одговарајућим секторима и конкретне потребе малих и средњих компанија. Кодекси би требало да ближе регулишу начела поштене и транспарентне обраде, подробније објасне легитимни интерес руковаоца као правни основ за обраду у конкретном случају, додатно регулишу прикупљање и псеудонимизацију података о личности, начин на који се остварују права лица на које се подаци односе, пренос података у друге државе и међународне организације, начин решавања спорова између руковаоца и лица на које се подаци односе мирним путем итд.

Ради доказивања усклађености радњи обраде са Уредбом, члан 42. предвиђа могућност успостављања *механизма сертификације заштите података*, са одговарајућим жиговима и ознакама за заштиту података, који се на захтев могу издати руковаоцима и обрађивачима. Издавање сертификата могу вршити сертификациона тела или надзорни орган у држави чланици.

Руковалац и обрађивач који захтевају издавање сертификата дужни су да сертификационом телу, односно надзорном органу, ако је захтев упућен њему, омогуће приступ радњама обраде и пруже све информације о обради које су неопходне за спровођење поступка издавања сертификата. Постојање издатог сертификата не може утицати на законске обавезе руковаоца и обрађивача. Сертификат се издаје руковаоцу и обрађивачу на период који не може бити дужи од три године, а може се обновити ако они и даље испуњавају исте прописане услове и критеријуме за издавање сертификата. Сертификат ће бити одузет у случају кад сертификационо тело, односно надзорно тело, ако је захтев упућен њему, утврди да руковалац, односно обрађивач више не испуњава прописане критеријуме за издавање сертификата.

Процена утицаја обраде на заштиту података о личности

У складу са начелима интегрисане и претпостављене приватности, Уредба предвиђа нову обавезу руковаоца, а то је да, пре започињања нове обраде података, извршри процену утицаја те радње обраде на заштиту података о личности. Према члану 35. Уредбе, ова обавеза постоји уколико је *вероватно да ће*

нека врста обраде, посебно употребом нових технологија и с обзиром на природу, обим, околности и сврху обраде, проузроковати висок ризик за права и слободе физичких лица. Уколико се планира предузимање више сличних радњи обраде које могу проузроковати сличне високе ризике за заштиту података о личности, предвиђена је могућност спровођења заједничке процене.

Поред ових општих смерница за ситуације у којима је потребно извршити процену, Уредба прописује и када се процена мора извршити, као и које све елементе она минимално мора да подразумева. Руковалац је *обавезан* да изврши процену утицаја када се радња обраде података односи на:

- систематске и свеобухватне процене личних аспеката физичког лица која се заснива на аутоматизованој обради података о личности, укључујући и профилисање, на основу које се доносе одлуке од значаја за правни положај појединца или на сличан начин значајно утичу на њега;
- масовне обраде посебних врста података о личности из члана 9 (1) Уредбе, или података о личности у вези са кривичним пресудама и кажњивим делима из члана 10 Уредбе, у великом обиму;
- обимног систематског надзора над јавно доступним површинама.[64]

Радна група 29 као критеријуме за процену потребе за спровођењем процене утицаја наводи следеће:

- обрада је таква да подразумева велики број лица на које се обрада односи, обим и/ или опсег различитих података који се обрађују;
- обрада података подразумева усклађивање или комбиновање скупова података који потичу из два или више процеса обраде података који се обављају у различите сврхе и/ или од стране различитих руковалаца, и то на начин који би премашио разумна очекивања лица на која се подаци односе;
- обрада података рањивих лица код којих постоји значајан дисбаланс моћи између њих и руковалаца подацима, односно лица чији су подаци предмет обраде неће моћи лако да прихвате обраду или се супротставе обради (нпр. деца, запослени, лица са посебним потребама, старија лица);
- обрада података подразумева коришћење иновативних технологија или организационих решења, као што је комбиновање отисака прстију са препознавањем лица за напредну контролу физичког приступа.[65]

Процена утицаја поступака обраде на заштиту података о личности подразумева сет мера које се спроводе пре започињања радњи обраде података о личности с циљем процењивања какве последице по личне податке може да проузрокује конкретна радња обраде података. Ова процена треба да олакша пословање и управљање

64 Члан 35. став 3. Опште уредбе.

65 Grupa autora, *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – Tumačenje novog pravnog okvira,* Share fondacija, 2019, стр. 60–61, доступно на: *https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf.*

ризицима тако што омогућава идентификацију стварних или потенцијалних ефеката које конкретна радња или радње обраде могу имати на право на приватност и заштиту података о личности. Она олакшава избегавање идентификованих ризика или њихово свођење на прихватљиву меру. Овај процес треба да осигура заштиту података о личности у будућим обрадама података односно пословима руковаоца, као и поштовање релевантног правног оквира. За све утврђене ризике, правни тим и/или службеник за заштиту података треба да предложи стратегије за смањење ризика, а у случајевима, када процена покаже да би обрада довела до високог ризика ако се не предузму мере за смањење ризика, обавезно је посаветовати се с надзорним органом. Важно је да у процес процене утицаја на обраду података о личности поред службеника за заштиту података о личности буду укључени и инжењери, програмери, одељење за ИКТ и сл., чија знања могу да допринесу изналажењу алтернативних приступа смањивању ризика на основу технологије, у погледу процене њихове изводљивости те предности и недостатака алтернативних решења. Процена утицаја на заштиту података о личности треба да се спроведе приликом, на пример, постављања видео надзора у једном граду или некој компанији. Оваква врста обраде погађа широк круг лица која нису дала своју сагласност за обраду података, нити најчешће имају знања да се над њима врши надзор, у које сврхе, ко тим подацима има приступ и сл. Зато унапред урађена процена утицаја треба да има циљ да се утврди да ли је заиста такав надзор неопходан, како се он може ограничити, а да се и даље сврха због које се поставља може испунити, које све мере заштите је неопходно предузети ради заштите података о личности итд.

Обавеза обавештавања надзорног органа и лица на које се подаци односе о повреди података о личности

Руковалац је дужан да у свакој ситуацији повреде података о личности која може да произведе ризик по права и слободу физичких лица *обавести надзорни орган*. Дакле, није неопходно да се деси нека конкретна штета по лице на које се подаци односе већ је потребно само да дође до повреде личних података и да постоји ризик по права и слободе лица. Уредба оставља рок од 72 сата од момента повреде података о личности да руковалац поднесе обавештење надзорном органу. Ово обавештење треба да садржи следеће елементе:

- опис природе повреде података о личности, укључујући врсте података и приближан број лица на која се подаци те врсте односе, као и приближан број података о личности чија је безбедност повређена;
- име и контакт податке службеника за заштиту података о личности или информације о другом начину на који се могу добити подаци о повреди;
- опис могућих последица повреде;
- опис мера које је руковалац предузео или чије је предузимање предложено у вези са повредом, укључујући и мере које су предузете с циљем да се умање штетне последице.[66]

66 Члан 33. став 3. Опште уредбе.

Обавеза обрађивача је да, у случају повреде личних података приликом обраде, без непотребног одлагања обавести руковаоца о тој повреди.

Ако руковалац не поступи у року од 72 сата од сазнања за повреду, дужан је да образложи разлоге због којих није поступио у том року.

Поред обавештавања надзорног органа, руковалац је дужан и да *обавести лице* на које се подаци односе о повреди његових личних података.[67] С тим што Уредба овде прави разлику и предвиђа да је овакво обавештење неопходно када је вероватно да ће повреда безбедности података проузроковати висок ризик по права и слободе физичких лица. Међутим руковалац неће бити дужан да обавести лице на које се подаци односе уколико је:

- предузео одговарајуће техничке, организационе и кадровске мере заштите у односу на податке о личности чија је безбедност повређена, а посебно ако је енкрипцијом или другим мерама онемогућио разумљивост података свим лицима која нису овлашћена за приступ овим подацима;
- накнадно предузео мере којима је обезбедио да више није вероватно да ће доћи до високог ризика за права и слободе лица на које се подаци односе;
- обавештавање лица на које се подаци односе несразмеран утрошак времена и средстава. У том случају, руковалац је дужан да путем јавног обавештавања или на други делотворан начин обезбеди пружање обавештења лицу на које се подаци односе.

2.2.1.6. Међународни пренос података

Поглавље V Опште уредбе уређује питања међународног преноса података *трећим земљама или међународним организацијам*а. Под трећим земљама подразумевају се све земље које не спадају у тзв. Европски економски простор (уз земље чланице ЕУ, ту спадају и земље чланице ЕФТА: Исланд, Норвешка, Лихтенштајн). Поред услова да се подаци преносе у неку од трећих земаља или међународних организација, режим међународног преноса података из Опште уредбе примењиваће се уколико се подаци преносе *другој организацији, субјекту или појединцу*. То подразумева пренос и у другу компанију унутар исте групације, али не и слање података појединцу који се налази ван зоне важења Опште уредбе, али је запослен у истом субјекту. [68]

Пренос података подразумева сваки прекогранични трансфер података – било електронским или физичким путем. Чување података у трећој земљи такође се сматра међународним преносом података.

67 Члан 34. Опште уредбе.

68 Видети: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/*.

Како пренос података представља радњу обраде података о личности, мора постојати адекватан правни основ за његово предузимање. Уколико су испуњени горе наведени услови, постоји неколико могућих *правних основа* за међународни пренос података, односно неколико механизама који омогућавају да тај пренос буде законити:

- пренос података врши се у земљу у погледу које је Европска комисија донела тзв. *Одлуку о адекватности*.[69] Ова одлука подразумева да је Комисија утврдила да правни оквир у датој држави или организацији односно на територији пружа адекватан ниво заштите права и слобода појединаца у погледу њихових података о личности;[70]
- постоји *правно обавезујући и извршни инструмент између органа јавне власти или јавних тела*; ови инструменти такође морају садржати адекватне гаранције права појединаца чији подаци се преносе;
- усвојена су *обавезујућа корпоративна правила*[71], односно интерни кодекс поступања који важи унутар мултинационалне групације, а који се примењује на пренос података из земаља у којима важи Уредба у треће земље; обавезујућа пословна правила, пре ступања на снагу, подносе се на одобрење надзорном органу у једној од држава у којој се примењује Уредба;
- субјект који врши пренос података и прималац података потписали су уговор који садржи тзв. *стандардне уговорне клаузуле* које доноси Европска комисија; ове клаузуле предвиђају обавезе уговорних страна у погледу заштите података, као и права лица чији подаци се преносе;
- субјект који врши пренос података и прималац података потписали су уговор који садржи тзв. *стандардне уговорне клаузуле* које доноси надзорни орган државе чланице, а одобрава Европска комисија;
- прималац података у трећој земљи приступио је одобреном кодексу поступања, који укључује адекватне гаранције заштите права појединаца чији подаци се преносе, а које су директно извршиве;
- прималац података у трећој земљи има одговарајући сертификат, одобрен од стране надзорног тела, који садржи и обавезујуће и извршне обавезе руковалаца и обрађивача у трећој земљи за примену одговарајућих заштитних мера, укључујући и мере у погледу права лица чији подаци се преносе.[72]

Уредба додатно релаксира правила међународног преноса података, предвиђајући низ *изузетака* у којима је могуће извршити међународни пренос и без испуњења једног од горенаведених услова. Ти изузеци укључују следеће

69 Члан 45. Опште уредбе.

70 Списак земаља у односу на које је донета Одлука о адекватности редовно се ажурира и доступан је на страници: *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*.

71 Овај институт уређен је чланом 47. Опште уредбе.

72 Члан 46. Опште уредбе.

ситуације: *i)* лице на које се подаци односе изричито је пристало на пренос; *ii)* пренос је потребан ради извршења уговора између руковаоца и лица на које се подаци односе, односно примене предуговорних мера на захтев лица; *iii)* пренос је потребан ради закључења или извршења уговора закљученог у интересу лица на које се подаци односе; *iv)* пренос је потребан због важних разлога јавног интереса; *v)* пренос је потребан за постављање, остваривање или одбрану правних захтева; *vi)* пренос је потребан ради заштите животно важних интереса лица на која се подаци односе или других лица ако лице на које се подаци односе није физички или правно способно да дâ пристанак; *vii)* пренос се врши из јавног регистра.[73]

2.2.1.7. Надзорни орīани држава чланица

Уредба прописује обавезу држава чланица да именују, у складу са правилима сопственог правног система, надзорне органе који су надлежни да прате примену Уредбе. Надзорни органи независни су у свом раду, а државе чланице дужне су да им обезбеде адекватне ресурсе како би ефикасно могли да врше своје надлежности. Такође, државе чланице морају обезбедити засебан буџет намењен надзорним органима, као и финансијску контролу њиховог рада која не утиче на независност ових органа.[74]

Утврђивање процеса именовања надзорног органа препуштено је државама чланицама, док Уредба предвиђа да чланове надзорних органа именују парламенти држава чланица, њихове владе, шеф државе или независно тело које је правом државе чланице овлашћено да врши именовање.

Неки од задатака надзорних органа обухватају:

- праћење и обезбеђивање примене Уредбе;
- подизање нивоа свести руковалаца и обрађивача о њиховим обавезама;
- саветовање националне институције о законодавним и управним мерама у вези са заштитом права лица;
- решавање притужби лица на која се подаци односе;
- сарадња са другим надзорним органима;
- давање савета у вези са поступцима обраде;
- доношење стандардних уговорних клаузула, одобравање уговорних клаузула и обавезујућих корпоративних правила;
- подстицање израде кодекса поступања, давање мишљења на нацрте и њихово одобравање;
- израда критеријума за акредитацију тела за праћење кодекса поступања и њихова акредитација итд.

73 Члан 49. Опште уредбе.

74 Члан 52. Опште уредбе.

У случајевима прекограничне обраде података, тј. уколико руковалац или обрађивач имају испоставе у две или више држава чланица ЕУ, или уколико радње обраде које предузимају утичу или могу утицати на лица у две или више држава чланица, Уредба предвиђа да ће водећи надзорни орган (енгл. *lead supervisory authority*) бити орган у држави у којој се налази главно седиште руковаоца/обрађивача. Ово правило значајно је због координације надзорних органа приликом поступања по захтевима лица за остварење права, али и надзора и санкционисања због непоштовања одредаба Уредбе. Међутим, ова правила не примењују се уколико радњу обраде врши орган јавне власти или други субјекти када обраду података врше у јавном интересу, па ће у том случају једини надлежни надзорни орган бити орган државе чланице у којој је успостављен руковалац/обрађивач.

2.2.1.8. Правна средства, одговорност и санкције

Уредба предвиђа два могућа *механизма заштите права лица* чији се подаци обрађују, и то *поступак пред надзорним органом*, уколико лице сматра да се обрадом података крши Уредба, и *судски поступак*, уколико лице сматра да су му права гарантована Уредбом прекршена услед обраде података противно правилима Уредбе. Ова два механизма се међусобно не искључују, што би лицу на које се подаци односе, као и државама чланицама, приликом прецизнијег дефинисања поступка заштите права, требало да дâ више флексибилности.

Уколико лице на које се подаци односе сматра да се обрадом података која се на њега односе крше одредбе Уредбе, има право да поднесе притужбу надзорном органу. Државе чланице дужне су да обезбеде лицима чији се подаци обрађују делотворно правно средство против правно обавезујуће одлуке надзорног органа, као и за случајеве када овај орган не реши притужбу или не обавести лице на које се подаци односе о напретку или исходу притужбе у року од три месеца.

Са друге стране, лице чији се подаци обрађују може се обратити и суду, уколико сматра да су му права прекршена услед обраде података противно правилима Уредбе.

Уредба предвиђа и могућност накнаде материјалне и нематеријалне штете лицима чији се подаци обрађују. *Одговорност за насталу штету* је на руковаоцу, док обрађивач одговара само уколико није поштовао обавезе прописане Уредбом, односно инструкције које је добио од руковаоца. И руковалац и обрађивач могу се ослободити одговорности уколико докажу да ни на који начин нису одговорни за догађај који је проузроковао штету. Уколико су, са друге стране, у обраду укључена два или више руковалаца, односно руковалац и обрађивач који су одговорни за насталу штету, њихова одговорност је солидарна.

Једно од обележја по којима је Уредба постала најпрепознатљивија су и високе *новчане казне* које прописује. Наиме, ради се о новчаним казнама у износу до 10.000.000 евра или, у случају групе друштава, до 2% укупног годишњег промета у свету за претходну финансијску годину, у зависности од тога који је износ већи, а

за повреду одредаба о подразумеваној и уграђеној приватности, заједничким руковаоцима, обрађивачима, уређивању односа руковалац–обрађивач итд. Са друге стране, за повреду начела обраде података, укључујући и услове за сагласност лица, кршење одредаба које уређују права лица на која се подаци односе, пренос података у треће земље или међународне организације итд., може бити изречена казна до 20.000.000 евра, односно до 4% укупног годишњег промета у свету.[75]

С обзиром на широк распон новчаних казни које могу бити изречене, Уредба прописује и опште смернице за изрицање казни. Пре свега, наводи се да казне морају бити делотворне, сразмерне и да морају имати одвраћајуће дејство, као и да се у сваком појединачном случају морају узети у обзир конкретне околности, попут природе, тежине и трајања повреде, постојања намере или нехатног карактера повреде, активности руковаоца или обрађивача усмерене на смањење штете по лица чији се подаци обрађују, степен њихове сарадње са надлежним органом итд.[76]

Надлежни органи држава чланица ЕУ у првих годину и по дана примене Опште уредбе изрицали су руковаоцима и обрађивачима новчане казне у износима од неколико стотина евра до неколико стотина милиона евра. Према доступним подацима, највише казни изречено је у Шпанији (15), док је укупна вредност изречених казни највиша у Великој Британији (преко 300 милиона евра).[77] Казне су изрицане и приватним и јавним субјектима – један од, за сада, најпознатијих случајева је изрицање казне од 50.000.000 евра компанији *Google* од стране француске Националне комисије за заштиту података због непоштовања начела транспарентности, неадекватног информисања лица чији се подаци обрађују, те недостатка валидне сагласности за активности персонализованог рекламирања. Кажњавања нису биле поштеђене ни локалне самоуправе.

ПРИМЕР

Неименовани градоначелник једног белгијског града кажњен је са 2000 евра јер је личне податке прикупљене за потребе обављања управних делатности локалне самоуправе злоупотребио у сврхе политичке кампање.
Мађарски надлежни орган казнио је износом од 3100 евра локалну самоуправу која је обелоданила личне податке узбуњивача који се самоуправи обратио притужбом против свог послодавца. Као отежавајућу околност надлежни орган узео је чињеницу да је узбуњивач, након што је дошло до повреде права на заштиту података о личности, добио отказ.

75 Члан 83. Опште уредбе.

76 Смернице за одмеравање висине новчаних казни додатно је прецизирала и образложила и Радна група29. Видети: *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, од 3. октобра 2017, доступно на: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237*.

77 Информације су преузете са веб странице *www.enforcementtracker.com*, која прикупља јавно доступне информације о изреченим казнама у државама чланицама, па су могућа појединa одступања од фактичког стања, с обзиром на чињеницу да сви надзорни органи не објављују ажурно детаље о својој пракси.

ПРИМЕР

Норвешка општина Берген дужна је да плати казну у висини од 170.000 евра због тога што није заштитила податке ученика и запослених у школама којима општина управља. Казна је изречена након пријаве ученика који је у бази која је била јавно доступна и незаштићена на информационом систему општине пронашао податке о 35.000 налога (корисничка имена и шифре) ученика и запослених.

2.2.2. Полицијска директива Европске уније

У оквиру истог пакета реформи у области заштите података о личности у Европској унији, заједно са Општом уредбом, 27. априла 2016. усвојена је Директива (ЕУ) 2016/680 о заштити физичких лица у погледу обраде података о личности коју врше надлежни органи у сврху превенције, истраге, откривања или гоњења кривичних дела или извршења кривичних санкција и о слободном кретању таквих података, и о стављању ван снаге Оквирне одлуке Савета 2008/977/ПУП.[78]

За разлику од директно примењиве Опште уредбе, *Полицијска директива као циљ има хармонизацију права држава чланица ЕУ*, те подразумева да ће њене одредбе свака држава чланица пренети у свој правни поредак адекватним националним правним актима. Овакво решење произлази из чињенице да предмет Полицијске директиве улази у оквире у некадашњег трећег стуба Европске уније[79], односно област полицијске и правосудне сарадње у кривичним стварима, у којој државе чланице и даље имају већи степен самосталности.

Полицијска директива се не примењује на органе локалне самоуправе, укључујући и оне у државама чланицама ЕУ. Међутим, због чињенице да Закон о заштити података о личности Републике Србије преузима и одредбе Полицијске директиве, потребно је основно разумевање сврхе и појмова и овог акта (пре свега, за потребе прецизног читања ЗЗПЛ) те се у наставку текста даје кратак осврт на његове специфичности.

78 Directive (EU) 2016/680 of the European Parliaments 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, *Official Journal of the European Union L 119/89*, доступно на: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN*.

79 На основу Уговора из Мастрихта (1992), Европска унија била заснована на три стуба. Први су чиниле Европске заједнице (Европска заједница за угаљ и челик, Европска заједница за атомску енергију и Европска економска заједница), други заједничка спољна и безбедносна политика, а трећи сарадња у области правосуђа и унутрашњих послова. У оквиру сваког од стубова постојао је различит однос супранационалног и међувладиног принципа, односно различит ниво интеграције држава чланица. Интеграција је била најјача у оквиру првог стуба. Лисабонским уговором (2009) укинута је стубовска структура ЕУ, са циљем дубље интеграције Уније. Тако су надлежности које су раније биле структуриране у оквиру сваког од стубова пренете на органе Уније, а истим Уговором ЕУ добија и правни субјективитет.

Примена Полицијске директиве

Једно од кључних питања у примени Полицијске директиве је њен *однос са Општом уредбом*. Наиме, Општа уредба прописује редован (општи) режим обраде и заштите података о личности, док се Полицијска директива односи на одређени круг органа у вршењу одређеног круга послова. Тако, поред општих услова који важе и за примену Опште уредбе – да се ради о аутоматизованој или неаутоматизованој обради личних података који се налазе у одређеној збирци, или су намењени збирци података, да обрада спада у домен права ЕУ, те да се не односи на органе, тела и агенције ЕУ, за примену Полицијске директиве потребно је да буду кумулативно испуњена два услова:

а) *да обраду врше надлежни орīани*, које Полицијска директива дефинише као сваки орган власти надлежан за превенцију, истрагу, откривање или гоњење кривичних дела или извршење кривичних санкција, укључујући заштиту од претњи по јавну безбедност и њихову превенцију; или свако друго тело или субјект којем је правом државе чланице поверено вршење јавних овлашћења и јавних надлежности у наведене сврхе;[80]

б) *да се обрада се врши у īосебне сврхе*, односно ради превенције, истраге, откривања или гоњења кривичних дела или извршења кривичних санкција, укључујући и заштиту од претњи по јавну безбедност и њихову превенцију.

Појам надлежног органа државе чланице дефинишу различито, што у пракси изазива посебан проблем. Питање које се најчешће поставља јесте да ли у обвезнике Полицијске директиве спада само уски круг органа задужених за истрагу и гоњење, односно кажњавање кривичних дела (полиција, тужилаштво, судови који поступају у кривичним стварима и установе за извршење кривичних санкција) или је тај круг шири и обухвата и, на пример, прекршајне судове, финансијске институције када имају улогу у спречавању или истрази кривичних дела итд. Неке државе чланице, попут Данске, Чешке или Словачке, ове нејасноће отклониле су таксативним набрајањем органа на које се примењује Полицијска директива.[81]

ПРИМЕР

На обраду података о запосленима у полицији или тужилаштву, за сврхе испуњења обавеза ових органа из области радних односа, примењује се општи режим обраде података, односно правила из Опште уредбе.

Такође, казнена евиденција предмета је предмет општег режима обраде података о личности. Међутим, када јој надлежни органи приступају за сврхе превенције, истраге, откривања или гоњења кривичних дела, примењује се режим из Полицијске директиве.

80 Члан 3. став 7. Полицијске директиве.

81 Видети: J. Pejić, *Šta je Policijska direktiva Evropske unije?*, Beogradski centar za bezbednosnu politiku, 2019, стр. 6, доступно на: *http://www.bezbednost.org/upload/document/sta_je_policijska_direktiva_evropske_unije.pdf*.

Без обзира на то који је круг органа обухваћен одредбама Полицијске директиве у државама чланицама, овај посебан режим обраде података није примењив на све активности надлежних органа, већ само на оне активности које се предузимају у сврхе превенције, истраге, откривања или гоњења кривичних дела.

Најзначајније разлике између Полицијске директиве и Опште уредбе

Одредбе Полицијске директиве узимају у обзир специфичности радњи обраде надлежних органа када спроводе активности превенције, истраге, откривања или гоњења кривичних дела. У том смислу, појединим одредбама овим органима дата су шира овлашћења (пре свега у погледу прикупљања података и обавештавања лица на која се подаци односе на радње обраде), док је, са друге стране, појединим решењима предвиђен шири круг обавеза у погледу заштите података од стране надлежних органа. У табели у наставку дат је приказ неких од најзначајнијих разлика између режима обраде и заштите података о личности предвиђених Општом уредбом и Полицијском директивом.

Табела 1. Најзначајније разлике између Опште уредбе и Полицијске директиве

Општа уредба	Полицијска директива
Прописује, између осталих, начело *транспарентне* обраде података (члан 5. став 1. тачка а).	*Не предвиђа начело* ни обавезу *транспарентне* обраде података (члан 4. став 1. тачка а).
Допушта *даљу обраду* података само за потребе јавног интереса, научног или историјског истраживања или за статистичке сврхе (члан 5. став 2).	Допушта *обраду у сврхе другачије* од оних за које су подаци прикупљени, под одређеним условима (члан 4. став 2).
Начело минимизације прописује да подаци морају бити примерени, битни и ограничени на оно што је *неопходно у односу на сврху обраде* (члан 5. став 1. тачка в).	Начело минимизације података је флексибилније дефинисано – морају се прикупљати подаци који су примерени и релевантни, а обим података *није претеран* (члан 4. став 1. тачка в).
Не прави разлику између различитих категорија лица.	Обавеза да руковаоци направе јасну разлику између података различитих категорија лица чији се подаци обрађују – лице за које постоје озбиљне сумње да је извршило кривично дело, осуђено лице, жртва или други учесници у поступку (члан 6).
Предвиђа шест могућих правних основа за обраду података о личности (члан 6).	Једини правни основ за обраду је закон (члан 8).

Општа уредба	Полицијска директива
Обрада посебних категорија података о личности је *забрањена*, осим уколико су испуњени посебни услови (члан 9).	Обрада посебних категорија података је *дозвољена само ако је нужна*, уз испуњење одређених услова (члан 10).
Не предвиђа обавезу вођења записа (логова).	Уводи обавезу вођења записа (логова) за радње обраде података (члан 25).
Прописује шири круг права лица на која се подаци односе (чл. 12–22).	Не предвиђа право на преносивост података и прописује шире могућности за ограничење права лица (нпр. ограничење права приступа, члан 15).
Предвиђа да се, уколико руковалац не поступи по захтеву лица за остварење права, лице може обратити надлежном надзорном телу у поступку по правном леку.	Предвиђа могућност да, у случају ограничења права лица на која се подаци односе од стране руковаоца, лица могу ова права остварити и посредством надлежних надзорних тела (члан 17).
Поставља флексибилнија правила за пренос података трећим земљама или међународним организацијама (чл. 44–50).	За пренос личних података трећим земљама или међународним организацијама, поред других услова, захтева се и сагласност земље која је извор података о личности (члан 35. став 1. тачка в) Такође, ограничава круг прималаца података.
Прописује строге санкције за кршење одредаба Опште уредбе (члан 83).	Не прописује санкције, већ то препушта државама чланицама (члан 57).

Ако се све наведено има у виду, јасно је да Европска унија и њене државе чланице пролазе кроз свеобухватну реформу система заштите података о личности. За оцену ефеката ових реформи за заштиту права грађана и даље је прерано (посебно ако се има у виду да поједине државе чланице и даље нису пренеле све одредбе ова два документа у своја национална законодавства)[82], али је општи закључак да усвајање Опште уредбе (а последично и Полицијске директиве) јесте ставило заштиту података на листу питања која су у фокусу Европске уније.

82 На пример, Словенија још увек није усвојила национални закон којим се прецизирају отворене одредбе Опште уредбе.

Слика 2. Најзначајније промене у правном и институционалном оквиру ЕУ у области заштите података о личности

3. ПРАВНИ ОКВИР ЗА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ

3.1. Опште напомене о правном оквиру за заштиту података о личности у Републици Србији

У време постојања Савезне Републике Југославије, *1998. године донет је Закон о заштити података о личности*[83], који је престанком постојања СРЈ постао део правног поретка Државне заједнице Србија и Црна Гора, да би се престанком постојања и ове заједнице „примењивао" као пропис Републике Србије. Међутим, поменути савезни закон донет је ради реализације обавеза утврђених одредбама *Конвенције Савета Европе бр. 108 о заштити лица у односу на аутоматску обраду података о личности из 1981. године*[84], и може се рећи да је у том тренутку представљао корак напред у контексту унапређења заштите људских права. Иако је био усклађен са наведеном Конвенцијом, с друге стране, није био усклађен са *Директивом 95/46/ЕЗ Европског парламента и Савета о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података* из 1995. године, тако да овај закон већ у тренутку доношења није био потпуно усклађен са постојећим европским стандардима. Његова примена никада није заживела у пуној мери, јер су грађани имали низак ниво свести о сопственим правима и степену њихове угрожености, али и због неспремности надлежних институција да та права штите. Такође, један од навођених разлога за одсуство његове пуне примене јесте то да је, током измена државно-правног поретка, тј. у процесу преноса надлежности савезних органа на органе Републике Србије, пропуштено да се утврди који би орган Републике Србије био надлежан да врши надзор над применом овог закона. То су, између осталог, били разлози за доношење новог закона који би регулисао ову област.

83 „Службени лист СРЈ", број 24/1998.

84 Скупштина Савезне Републике Југославија потврдила је 1992. године Конвенцију Савета Европе о заштити лица у односу на аутоматску обраду личних података (1981), која је тиме постала саставни део унутрашњег правног поретка.

Тако је *2008. донет Закон о заштити података о личности*[85], који је од почетка примене, према извештајима Европске комисије о напретку Републике Србије, оцењиван као закон који је делимично усклађен са релевантним прописима Европске уније. Битно је напоменути да је након доношења овог Закона, у Извештају о напретку Србије за 2008. годину[86] истакнуто да је постигнут „незнатан" напредак у овој области, као и да због непостојања независног и ефикасног надзорног тела није дошло до имплементације постојећих прописа везаних за заштиту података о личности. Мање-више, извештаји Европске комисије о напретку Србије су у периоду 2009–2014. године били врло критични у погледу примене Закона о заштити података о личности и његове усклађености са стандардима ЕУ.[87] Доношење новог Закона о заштити података о личности први пут је поменуто у Извештају Европске комисије за 2015. годину. Посебно је наглашено да су обрада и заштита осетљивих података о личности, обрада биометријских података, видео-надзор, безбедност података на интернету, као и директан маркетинг и даље недовољно регулисани и да због тога остављају значајан простор за злоупотребе.[88] На обавезу законског регулисања заштите података о личности указао је и Акциони план за поглавље 23.[89]

Одсуство у пракси дефинисаних демократских стандарда, с једне стране, и развој модерних технологија, са друге стране, резултирали су доношењем дуго очекиваног *Закона о заштити података о личности*[90]. Нови Закон о заштити података о личности донет је са циљем усклађивања са новим правним тековинама ЕУ, тј. Општом уредбом о заштити података. Након усвајања и почетка примене новог Закона, новембра 2019. године, Србија је потписала и *Протокол о изменама и допунама Конвенције о заштити лица у односу на аутоматску обраду података о личности* од 2018. године, док је 4. марта 2020. године Народна скупштина Републике Србије донела *Закон о потврђивању Протокола о изменама и допунама Конвенције о заштити лица у односу на аутоматску обраду података о личности*.[91]

Новоусвојени Закон о заштити података о личности ступио је на снагу 21. новембра 2018. године, али је његова примена била одложена за 21. август 2019. године, дакле, девет месеци од дана његовог ступања на снагу. Разлози одложене

85 „Службени гласник РС", бр. 97/08, 104/09 – др. закон, 68/12 – одлука УС и 107/12.

86 Видети: Извештај о напретку Србије за 2008. годину који прати Саопштење Комисије Европском парламенту и Савету (стр. 61). Извор: *http://www.europa.rs/upload/documents/key_documents/2008/godisnji_izvestaj_ek_srbija_2008_sr.pdf*.

87 Видети извештаје Европске комисије о напретку Србије за период 2009–2014. године. Извор: *http://www.mei.gov.rs/srp/dokumenta/eu-dokumenta/godisnji-izvestaji-ek*.

88 Међутим, и поред ових сугестија, као и бројних замерки стручне јавности и Повереника, новоусвојени Закон о заштити података о личности, пропустио је да регулише видео-надзор.

89 Видети: Акциони план за преговарање поглавља 23 усвојен на седници Владе Републике Србије 27. априла 2016. године (стр. 360). Извор: *https://www.mpravde.gov.rs/files/Akcioni%20plan%20PG%2023%203.pdf*.

90 „Службени гласник РС", број 87/2018.

91 „Службени гласник РС – Међународни уговори", број 4/20202.

примене огледају се у потреби да се органи власти и други руковаоци подацима припреме за адекватну примену Закона, као и да се припреме и донесу релевантни подзаконски акти. Једини изузетак представља члан 98. Закона, који регулише престанак вођења Централног регистра збирки података, а који је почео да се примењује одмах по ступању на снагу Закона. Постојећи подаци у оквиру Централног регистра збирки података су архивирани и доступни су у машински читљивом формату на Порталу отворених података Повереника за информације од јавног значаја и заштиту података о личности. Предвиђено је да се до краја 2020. године одредбе других закона које се односе на обраду података о личности ускладе са одредбама новог Закона.

С циљем ефикасне примене Закона о заштити података о личности донето је више подзаконских аката. Наиме, пре почетка примене ЗЗПЛ, Влада Републике Србије је донела *Одлуку о Листи држава, делова њихових територија или једног или више сектора одређених делатности у тим државама и међународних организација у којима се сматра да је обезбеђен примерени ниво заштите података о личности*.[92] И Повереник је донео низ подзаконских аката, као што су: *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*[93], *Правилник о обрасцу и начину вођења евиденције лица за заштиту података о личности*[94], *Правилник о обрасцу и начину вођења интерне евиденције о повредама Закона о заштити података о личности и мерама које се у вршењу инспекцијског надзора примењују*[95], *Правилник о обрасцу притужбе*[96]. Од почетка примене Закона о заштити података о личности, Повереник је донео следеће подзаконске акте: *Правилник о обрасцу легитимације овлашћеног лица за вршење инспекцијског надзора по Закону о заштити података о личности*[97], *Одлуку о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности*[98], *Одлуку о утврђивању Стандардних уговорних клаузула*.[99]

92 „Службени гласник РС", број 55/2019.
93 „Службени гласник РС", број 40/2019.
94 „Службени гласник РС", број 40/2019.
95 „Службени гласник РС", број 40/2019.
96 „Службени гласник РС", број 40/2019.
97 „Службени гласник РС", број 61/2019.
98 „Службени гласник РС", број 45/2019.
99 „Службени гласник РС", број 5/2020.

3.2. Усклађеност Закона о заштити података о личности са Општом уредбом о заштити података (GDPR)

За нови Закон о заштити података о личности може се рећи да је усвојен са намером унапређења домаћег правног оквира и његовог прилагођавања новим друштвеним околностима, са једне, односно испуњења обавеза Републике Србије проистеклих из процеса придруживања Европској унији, са друге стране. Ова обавеза предвиђена је чланом 81. у оквиру наслова VII Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије са друге стране (Споразум)[100], а у коме се наводи да ће „Србија ускладити своје законодавство које се односи на заштиту личних података са комунитарним законодавством и осталим европским и међународним прописима о приватности"[101]. Тако је у образложењу Предлога Закона о заштити података о личности предлагач оценио да наведени Предлог (касније усвојен без значајнијих измена) у потпуности испуњава обавезе Србије преузете потписивањем Споразума. Међутим, у процени усклађености Закона о заштити података о личности са правним оквиром Европске уније, а пре свега Општом уредбом о заштити података, треба узети у обзир да Уредба садржи две категорије одредаба:

а) одредбе које су обавезујуће и директно примењиве у државама чланицама;
б) отворене одредбе (енгл. *opening clauses*), које остављају простор државама чланицама да детаље самостално регулишу у складу са својим националним прописима.

Наш Закон дословно преноси и поједине отворене одредбе, које још увек нису даље уређене посебним законима. Такође, додатне потешкоће у процени усклађености, али и тумачењу појединих појмова, представља и чињеница да интегрални део нове европске регулативе чини Преамбула која се састоји од чак 173 тачке које додатно разрађују правне норме и појашњавају циљ свих одредаба Уредбе, почев од тачке 1), која дефинише заштиту података о личности као фундаментално људско право. Преамбула је стога не само корисна, већ представља неопходно полазиште за тумачење прописа. Међутим, ЗЗПЛ није преузео Преамбулу Уредбе.

Коначно, низ одредаба Уредбе непреносив је у наш правни систем, с обзиром на то да те одредбе утврђују обавезе држава или њихових надлежних органа које директно произлазе из чланства у ЕУ, па самим тим не могу бити обавезујуће за Србију као земљу кандидата за чланство.

100 „Службени гласник РС", број 83/2008.
101 Члан 81. Споразума.

Поједине одредбе ЗЗПЛ, иако су у потпуности усклађене или су делимично усклађене са *GDPR*-ом, нису јасно дефинисане, па тако остављају отворен простор за различита тумачења. То се, пре свега, односи на следеће одредбе:

а) У оквиру одредаба којима се регулишу начела, приметно је да, иако Полицијска директива искључује начело транспарентности у погледу обраде података коју врше надлежни органи, ЗЗПЛ ово начело прописује и за општи и за посебан режим обраде.[102] Такође, не прави се разлика у погледу примене начела минимизације података за општи режим обраде и онај предвиђен за надлежне органе предвиђен Полицијском директивом.[103] Нису прецизно одређени појмови „послова у јавном интересу" и „законом прописана овлашћења руковаоца".[104] Старосни узраст за законитост пристанка малолетног лица у вези са коришћењем услуга информационог друштва је 15 година, док Општа уредба предвиђа да је то узраст од 16 година, уз могућност да државе чланице одреде другачије, али да тај узраст не може бити испод 13 година.[105]

б) У оквиру одредаба које се односе на права лица на које се подаци односе, члан 40. ЗЗПЛ је делимично усклађен са *GDPR*-ом и у вези са њим изостављена је обавеза предвиђена Уредбом да ограничења права лица морају бити прописана законом.

в) Код одредаба које се односе на пренос података о личности у друге државе и међународне организације, ЗЗПЛ, у односу на Уредбу, предвиђа шири круг земаља које обезбеђују примерен ниво заштите података о личности, односно предвиђа да се сматра да примерен ниво заштите постоји у земљама и међународним организацијама које су чланице Конвенције 108 Савета Европе.[106] Такође, не прецизира се да ли Повереник одобрава само обавезујућа пословна правила у случају да мултинационална компанија или група привредних друштава имају седиште у Републици Србији, или би Повереник био надлежан за одобравање правила и уколико би чланица групе била компанија са територије РС.[107]

г) У погледу одредаба којима су прописана правна средства, одговорност и казне, није прецизирано да ли је обавезан процесни корак да се, пре обраћања Поверенику, лице на које се подаци односе обрати руковаоцу или обрађивачу, а у сврхе остварења права.[108] Када је реч о заштити права лица, ЗЗПЛ предвиђа два паралелна механизма заштите (пред Повереником и пред надлежним судом)[109], што у пракси може довести до конфликтних одлука два органа.

---

102 Видети: члан 5. став 1. тачка 1. ЗЗПЛ.
103 Видети: члан 5. став 1. тачка 3) ЗЗПЛ.
104 Видети: члан 12. став 1. тачка 5) ЗЗПЛ.
105 Видети: члан 16. ЗЗПЛ.
106 Видети: члан 64. став 2. ЗЗПЛ.
107 Видети: члан 67. ЗЗПЛ.
108 Видети: члан 82. ЗЗПЛ.
109 Видети: члан 84. ЗЗПЛ.

3.3. Основне измене које доноси Закон о заштити података о личности

Основни циљ Закона о заштити података о личности је да свакоме обезбеди заштиту података о личности ради несметаног остваривања права и слобода успостављањем јасног правног оквира у области заштите података о личности у Републици Србији.[110] Новину представља *одредба којом је указано на значај овог закона као системског закона* у области заштите података о личности, као и потреба да посебни закони (обзиром на то да се законом морају уредити прикупљање, држање, обрада и коришћење података о личности) када уређују обраду података морају бити усклађени са овим законом, јер он ову област целовито и најдетаљније уређује.

Већина основних *начела обраде података* која су успостављена новом европском регулативом и која су уграђена у нов Закон о заштити података о личности није новина, међутим новост је у томе што су та начела *добила изричиту примену на промет робе и услуга на интернету*, а такође је отворено и спорно питање регулисања *аутоматизоване обраде података*. Новим правним оквиром у области заштите података о личности *проширена је одговорност људи и организација* које прикупљају и обрађују податке и детаљно су разрађени инструменти и процедуре спровођења прописа. Пописани су и *нови услови за пристанак* на обраду података, тако да више неће бити могуће давати бланко сагласност, нити ће се прихватање компликованих и просечном кориснику неразумљивих политика приватности сматрати валидним пристанком. Такође, без обзира на то да ли се формално поштују обавезе из Закона, могуће је утврдити одговорност уколико начин на који су те обавезе спроведене није у складу са неким од прописаних начела.

Нови правни режим заштите података о личности *строже дефинише одговорност лица која у различитим улогама долазе у додир са подацима о личности*. То могу бити руковаоци, заједнички руковаоци, обрађивачи, примаоци и трећа страна. Међутим, главни актери у обради података о личности су руковалац и обрађивач, чија се права и обавезе разликују. По угледу на *GDPR*, нови Закон уводи читав низ обавеза за обрађивача, док за руковаоца предвиђа обавезу законите обраде података о личности, што значи да руковалац има право да врши обраду само уколико је она утемељена, заснована на једном од Законом прописаних правних основа. Према Закону, а у складу са *GDPR*-ом, расположиви правни основи су: пристанак лица на које се подаци односе, закључење и извршење уговора, поштовање правних обавеза, заштита животно важних интереса, обављање послова у јавном интересу и легитимни интерес руковаоца.

110 Видети: члан 2. ЗЗПЛ.

Једна од најважнијих новина у Закону о заштити података о личности је увођење лица овлашћеног за заштиту података о личности (*DPO*). Законом је предвиђена могућност да руковалац, односно обрађивач одреде лице овлашћено за заштиту података о личности. То је особа у државном органу или компанији која прати обраду података о личности и комуницира са Повереником, као и са корисницима. У складу са Законом, лице овлашћено за заштиту података о личности се обавезно мора одредити: (1) ако се обрада врши од стране органа власти, осим ако се ради о обради коју врши суд у сврху обављања својих судских овлашћења; (2) ако се основне активности руковаоца или обрађивача састоје у радњама обраде које по својој природи, обиму, односно сврхама захтевају редован и систематски надзор великог броја лица на које се подаци односе и (3) ако се основне активности руковаоца или обрађивача састоје у масовној обради посебних података о личности. Оно у свом раду мора бити независно, што значи да може бити запослено код руковаоца или обрађивача или може обављати послове на основу уговора. Овлашћено лице одговара највишем органу управе и не може се позвати на одговорност за обављање свог посла. Руковалац или обрађивач дужни су да објаве контакт податке лица овлашћеног за заштиту података о личности и доставе их Поверенику, који води евиденцију лица овлашћених за заштиту података о личности, на један или више од прописаних начина: 1) у писаном облику, непосредно, 2) путем поште или 3) на електронску адресу: *licezazastitu@poverenik.rs*.[111]

У складу са европском регулативом, ЗЗПЛ предвиђа и *обавезу процене утицаја на заштиту података о личности*. Наиме, руковалац је у обавези да пре започињања обраде изврши процену утицаја радњи обраде на заштиту података о личности, уколико је вероватно да ће нека врста обраде проузроковати висок ризик за права и слободе физичких лица.

Такође, једна од новина је и *велики спектар надлежности Повереника*, као надзорног органа који обезбеђује примену ЗЗПЛ. У оквиру својих овлашћења, Повереник се стара о подизању нивоа свести јавности о ризицима, мерама заштите и правима у вези са обрадом података о личности, као и о подизању нивоа свести руковалаца и обрађивача у вези са њиховим законским обавезама; пружа информације о законским правима за захтев лица на које се подаци односе; поступа по притужбама лица на које се подаци односе и утврђује да ли је дошло до повреде ЗЗПЛ; сарађује са надзорним органима других држава у вези са заштитом података о личности, у размени информација и пружању узајамне правне помоћи; сачињава и јавно објављује на својој интернет страници листу врста радњи обраде за које се мора извршити процена утицаја на заштиту података о личности; води евиденцију лица овлашћених за заштиту података о личности, чије контакт податке му доставља руковалац или обрађивач и томе слично. Такође,

111 Видети: Правилник о обрасцу и начину вођења евиденције лица за заштиту података о личности („Службени гласник РС”, број. 40/2019).

Повереник врши и инспекцијска овлашћења, па је тако овлашћен да, између осталог, наложи руковаоцу и обрађивачу, односно њиховим представницима да му пруже све потребне информације, да од њих добије приступ свим подацима о личности и осталим информацијама потребним за вршење овлашћења, као и приступ свим просторијама, средствима и опреми руковаоца и обрађивача, да обавештава руковаоца и обрађивача о могућим повредама Закона итд.

3.4. Нови правни институти

ЗЗПЛ уводи неколико нових правних института саморегулације по угледу на *GDPR* и то: могућност израде кодекса понашања, могућност сертификације (издавање сертификата о заштити података о личности), као и примену тзв. обавезујућих пословних правила. С обзиром на то да су ово потпуно нови правни институти, пракса Повереника и осталих актера у вези са њима ће се тек развијати у будућности.

Кодекс понашања – ЗЗПЛ предвиђа да удружења и други субјекти који представљају групе руковалаца или обрађивача могу усвојити кодекс понашања ради ефикасније примене Закона. Пошто је израда кодекса понашања само могућност, ЗЗПЛ утврђује обавезу Повереника да подстиче и промовише израду оваквих кодекса. Удружења и други субјекти који намеравају да израде кодекс понашања или да измене постојећи, према ЗЗПЛ дужни су да предлог кодекса, односно његових измена доставе Поверенику на мишљење. ЗЗПЛ предвиђа да контролу примене кодекса врши „правно лице које је акредитовано за вршење контроле у складу са законом који уређује акредитацију". У случају да руковалац или обрађивач повреде кодекс понашања, акредитовано правно лице може, између осталих мера, привремено или трајно искључити руковаоца односно обрађивача из примене кодекса, а дужно је да о предузетим мерама обавести Повереника. Мере које је акредитовано правно лице предузело не утичу на овлашћења Повереника, нити на право лица на које се подаци односе да поднесе притужбу Поверенику или затражи судску заштиту.

Сертификација заштите података о личности – ЗЗПЛ уводи могућност установљавања поступка за издавање сертификата о заштити података о личности с циљем доказивања да руковалац и обрађивач поштују одредбе Закона. Поступак сертификације је добровољан и транспарентан. Руковалац и обрађивач који захтевају издавање сертификата дужни су да сертификационом телу, односно Поверенику, омогуће приступ радњама обраде и пруже све информације о обради података које су неопходне за спровођење поступка сертификације. Сертификат се издаје руковаоцу и обрађивачу на период који не може бити дужи од три године, а може се обновити ако они и даље испуњавају исте прописане услове и

критеријуме за сертификацију. Сертификат се може поништити ако сертификационо тело, односно Повереник утврди да руковалац, односно обрађивач више не испуњава прописане критеријуме за издавање сертификата. Повереник прописује критеријуме за сертификацију[112], проверава испуњеност услова за сертификацију и спроводи периодично преиспитивање издатих сертификата. Поседовање сертификата не утиче на прописана права и обавезе руковалаца у вези са обрадом података о личности. С обзиром на то да једном издати сертификат може истећи или бити одузет, руковалац, односно обрађивач који је прибавио сертификат и даље мора да води рачуна да, приликом обраде података, поступа у складу са ЗЗПЛ-ом.

Обавезујућа пословна правила – Интерна правила о заштити података о личности Закон сматра обавезујућим пословним правилима. Њих усваја и примењује руковалац, односно обрађивач са пребивалиштем или боравиштем, односно седиштем на територији Републике Србије, у сврху регулисања преношења података о личности руковаоцу или обрађивачу у једној или више држава унутар мултинационалне компаније или групе привредних субјеката. Обавезујућа пословна правила одобрава Повереник, уколико испуњавају законом прописане услове.[113] Уколико обавезујућа пословна правила испуњавају законске услове, Повереник их одобрава у року од 60 дана од дана подношења захтева за њихово одобрење. У вези са овим институтом постоје многа отворена питања која нису регулисана законом, а за која ће се пронаћи решење кроз праксу у будућности.

3.5. Разлике у односу на Општу уредбу о заштити података (*GDPR*)

Поједине одредбе ЗЗПЛ се разликују у односу на Општу уредбу о заштити података, а то се пре свега односи на *одредбе којима се регулише надлежност домаћих органа* у погледу заштите права лица и *одредбе којима се прописују казне и одговорност*. Према ЗЗПЛ, постоје паралелни механизми заштите права лица (пред Повереником и пред надлежним судом), као и разне врсте казни и мера које могу да изрекну Повереник односно суд, што у пракси може довести до конфликтних одлука ова два органа.

а) Заштита пред Повереником: Лице на које се подаци односе има право да *Поверенику* поднесе *притужбу*, уколико сматра да обрада његових података о личности није у складу са Законом, при чему искоришћавање права на подношење

112 Критеријуми Повереника за сертификацију тек треба да буду развијени у пракси. Док се критеријуми не усвоје, отворено је питање које све услове један руковалац, односно обрађивач мора да испуни да би му се сертификат издао, као и која је његова мотивација да се упусти у поступак сертификације.

113 Видети: члан 67. ЗЗПЛ.

притужбе не спречава то лице да покрене друге управне или судске поступке. Повереник је дужан да подносиоца притужбе обавести о току и резултатима поступка по притужби, као и о његовом праву да тужбом против одлуке Повереника покрене управни спор у року од 30 дана од дана пријема одлуке. Лице на које се подаци односе, дакле, има право покретања управног спора против одлуке Повереника која се на њега односи, а покретање управног спора не утиче на његово право да покрене и неки други поступак правне заштите.

У вршењу својих овлашћења, Повереник може да покрене поступак пред судом, а суд врши контролу аката Повереника које он донесе у вршењу својих инспекцијских надлежности.

Повереник може да предузме и одређене *корективне мере, односно неновчане санкције*, попут изрицања опомене руковаоцу односно обрађивачу у случају да се обрадом крше одредбе Закона, да им наложи да поступе по захтеву лица на које се подаци односе у вези са остваривањем права тог лица, да наложи руковаоцу и обрађивачу да ускладе радње обраде са ЗЗПЛ-ом на тачно одређени начин и у одређеном року, да наложи руковаоцу да обавести лице на које се подаци односе да је дошло до повреде његових података о личности, да изрекне привремено или трајно ограничење вршења радње обраде и забрану обраде, да изрекне новчану казну на основу прекршајног налога ако је приликом инспекцијског надзора утврђено да је дошло до прекршаја итд.

С друге стране, *прекршајне казне* предвиђене домаћим законом знатно су ниже од казни из европске регулативе. Највиши износ новчане казне која се у прекршајном поступку против руковаоца може изрећи је 2.000.000 динара, а најмањи 50.000 динара. У случају стицаја више прекршаја, највиша казна би могла износити чак до 4.000.000 динара. Још једна врста санкције коју Повереник може изрећи руковаоцу је *прекршајни налог* у износу од 100.000 динара. Међутим, с обзиром на то да пословање руковаоца може бити предмет и *GDPR* (сем ЗЗПЛ), то се на њихове прекршаје примењују административне казне које могу износити и до 20.000.000 евра. Према ЗЗПЛ, Повереник може да изрекне казну у односу на шест врста повреда, а оне се састоје у томе да руковалац правно лице (1) настави са обрадом с циљем директног оглашавања, а лице на које се подаци односе је поднело приговор на такву обраду; (2) не води прописане евиденције о обради и (3) не објави контакт податке лица овлашћеног за заштиту података о личности и не достави их Поверенику (када је ово лице именовано). Наш ЗЗПЛ предвиђа сличне критеријуме за одређивање висине казне као *GDPR* (врста података, постојање намере или непажње итд.).

б) Заштита пред судом – парнични поступак: Друга могућност јесте да се грађани за повреду својих права обрате и суду у парничном поступку. „ЗЗПЛ, по узору на Општу уредбу, предвиђа да особа која је претрпела материјалну или нематеријалну штету због повреде одредаба прописа о заштити личних података, има *право на новчану накнаду штете* од руковаоца који је штету проузроковао. Дакле, уколико физичко лице сматра да је такву штету претрпело због одређеног

незаконитог поступања руковаоца, може у парничном поступку пред судом доказивати и доказати постојање и висину такве штете. С друге стране, руковалац се може ослободити одговорности за штету ако докаже да за њен настанак није одговоран ни на који начин. Тужбени захтев за надокнаду штете подноси се по општим правилима из Закона о облигационим односима, док ЗЗПЛ у том смислу не регулише додатне захтеве. Према облигационим прописима, штета чија се накнада захтева може бити материјална и нематеријална, а у сваком случају се мора доказати да би била надокнадива. Што се тиче нематеријалне штете, важно је нагласити да се не може свака повреда приватности, односно повреда личних података, сматрати нематеријалном штетом која мора да се надокнади. Накнада се, према Закону о облигационим односима, може досудити само за претрпљене физичке болове, за претрпљене душевне болове због умањења животне активности, наружености, повреде угледа, части, слободе или права личности, смрти блиског лица, као и за страх. Дакле, лице може захтевати да му се, поред материјалне штете и независно од ње, утврди и нематеријална штета која је настала незаконитом обрадом, ако је то довело до повреде неког од личних права. Такође, прописано је да суд приликом одлучивања о захтеву за накнаду нематеријалне штете и о висини њене накнаде, води рачуна о значају повређеног добра и циљу коме служи та накнада, али и о томе да се њоме не погодује тежњама које нису спојиве са њеном природом и друштвеном сврхом[114].

У области заштите података о личности од посебног значаја је могућност да се велики број лица укључи у поступак. У таквом случају укупан износ штете за сва лица чије су појединачне штете мале може бити значајно већи од прекршајних казни (бар што се тиче прекршајне одговорности према српским прописима)".

в) Заштита пред судом – кривични поступак: „Кривични законик Србије прописује новчану казну или казну затвора до једне године уколико неко (1) неовлашћено прибави, саопшти другом или употреби у сврху за коју нису намењени податке о личности који се прикупљају, обрађују и користе на основу закона, као и када (2) противно закону прикупља податке о личности грађана или тако прикупљене податке користи. Квалификовани облик овог кривичног дела, које се кажњава затвором до три године, постоји ако дело учини службено лице у вршењу службе. Круг радњи обухваћених овим кривичним делом је веома широк, те се може односити на било коју ситуацију незаконите обраде личних података. На основу правила из ЗЗПЛ, може се закључити да свака обрада података која је супротна начелима обраде представља радњу овог кривичног дела. С друге стране, постоје нека законска правила из ЗЗПЛ чије кршење вероватно не би могло довести до кривичне одговорности, јер због своје формалне природе суштински не угрожавају права и интересе лица на које се подаци односе, као што су формална правила о вођењу евиденција радњи обраде.

114 Видети: *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR Tumačenje novog pravnog okvira*, Share fondacija, Beograd, 2019, стр. 92.

Пракса домаћих парничних и кривичних судова је у овој области још увек неразвијена. С обзиром на околност да текст новог Закона практично уводи Општу уредбу у Србију, може се очекивати да се пракса развија у складу са релевантном праксом европских судова. Према јавно доступној пракси српских судова, кривични поступци су ретки, док је постојање кривичне одговорности, на пример, утврђено у случају извоза личних података из Србије без валидног правног основа за пренос. Пракса европских судова је по правилу много лакше и ажурније доступна на одговарајућим интернет страницама самих институција."[115]

115 Видети: *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR Tumačenje novog pravnog okvira*, Share fondacija, Beograd, 2019, стр. 93.

4. ОДНОС ПРАВА НА ПРИСТУП ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА И ПРАВА НА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ

4.1. О праву на слободан приступ информацијама од јавног значаја

Право на слободан приступ информацијама је право новије генерације и проистекло је из слободе изражавања, гарантоване најзначајнијим међународним документима, попут Међународног пакта о грађанским и политичким правима[116] и Европске конвенције за заштиту људских права и основних слобода. Члан 10. став 1. ЕКЉП предвиђа да слобода изражавања „*укључује слободу поседовања сопственог мишљења, примања и саопштавања информација и идеја без мешања јавне власти и без обзира на границе.*"[117] Дакле, у изворном облику, слобода изражавања подразумевала је само право грађана на пријем и ширење информација. Међутим, кроз праксу Европског суда за људска права даје се шири аспект овом праву па оно почиње да обухвата и *право на тражење информација*.[118] На нивоу Европске уније, члан 42. *Повеље о основним правима ЕУ* успоставља право на приступ документима органа Уније, док је исто право гарантовано и чланом 15. *Лисабонског уговора*.

Полазна основа права на слободан приступ информацијама јесте да су грађани носиоци суверенитета, те као такви имају право да буду обавештени о раду носилаца јавних овлашћења. Међутим, као и већина људских права, право на слободан приступ информацијама од јавног значаја није апсолутно право и његово

116 Члан 19. став 2. Међународног пакта о грађанским и политичким правима наводи да „свако има право на слободу изражавања; то право подразумева слободу тражења, примања и ширења обавештења и идеја сваке врсте, без обзира на границе, било усмено, писмено, путем штампе или у уметничком облику, или ма којим другим средством по свом избору."

117 Члан 10. став 1. Европске конвенције о људским правима, доступно на: *https://www.echr.coe.int/Documents/Convention_SRP.pdf*.

118 Видети предмете: *Матки против Чешке* (Пресуда од 10. јула 2006), *Тарсасаг против Мађарске* (Пресуда од 14. априла 2009), *Кенеди против Мађарске* (Пресуда од 26. маја 2009), *Magyar Helsinki Bizottság против Мађарске* (Пресуда од 8. новембра 2016).

остваривање и заштита увек се посматрају у корелацији са неким другим правом и/или интересом.

У нашој земљи право на слободан приступ информацијама од јавног значаја први пут је регулисано 2004. године, усвајањем *Закона о слободном приступу информацијама од јавног значаја*.[119] Овим законом успостављена је и институција *Повереника за информације од јавног значаја*, којој се од 2008. године у мандат додаје и заштита података о личности.

Године 2006. право на приступ информацијама ставља се у категорију уставом загарантованих људских права у нашој земљи. Наиме, члан 51. Устава Републике Србије гарантује право на обавештеност, и наводи:

Свако има право да истините, потпуно и благовремено буде обавештаван о питањима од јавног значаја и средства јавног обавештавања су дужна да то право поштују.

Свако има право на приступ подацима који су у поседу државних органа и организација којима су поверена јавна овлашћења, у складу са законом.

Према ЗСПИЈЗ, право на слободан приступ информацијама односи се на *све информације којима располажу органи јавне власти*, под условом да су *настале у раду или у вези са радом ових органа,* те *опредмећене у одређеном документу.* Да би се нека информација сматрала информацијом од јавног значаја није битно да ли је извор информације орган јавне власти или неко друго лице, није битан носач информација (папир, трака, филм, електронски медијум и сл.) на коме се налази документ који садржи информацију, датум настанка информације, начин сазнавања информације, нити су битна друга слична својства информације.[120]

Орган јавне власти је *сваки орган који врши јавна овлашћења* – државни орган, орган територијалне аутономије, јединица локалне самоуправе, правно лице које оснива или финансира државни орган. Ту, дакле спадају и јавна предузећа, али и друштва капитала која имају форму акционарског друштва или друштва са ограниченом одговорношћу, а чији су оснивачи органи власти, као и други носиоци јавних овлашћења, попут јавних извршитеља.

119 „Службени гласник РС", бр. 120/2004, 54/2007, 104/2009 и 36/2010.
120 Члан 2. ЗСПИЈЗ.

4.2. Како се остварује право на слободан приступ информацијама од јавног значаја?

Механизам којим се право остварује подразумева да тражилац подноси *писани захтев* органу власти, или се може остварити усменим захтевом датим на записник, а којим тражилац може тражити:

а) обавештење о томе да ли орган власти поседује одређену информацију од јавног значаја, односно да ли му је она доступна;
б) увид у документ који садржи информацију од јавног значаја или
в) издавање копије документа који садржи информацију.[121]

Право на приступ информацијама гарантовано је без дискриминације у погледу тражилаца, од којих се не тражи да доказују постојање интереса да траже информације нити разлоге због којих то чине. Остваривање права на приступ информацијама у начелу је бесплатно, могу се наплатити само нужни трошкови умножавања и упућивања докумената, а у привилегованим случајевима (нпр. захтеви медија, новинара и организација за заштиту људских права) чак ни то.

Према ЗСПИЈЗ, важи претпоставка да у погледу свих информација којима располажу органи јавне власти постоји оправдани интерес јавности да зна. *Тражилац информација не мора да доказује да има интерес да зна неку информацију или да је његов интерес оправдан, нити орган јавне власти може захтевати од тражиоца да захтева навођење разлога за подношење захтева.* Међутим, иако се интерес јавности претпоставља, Закон прави разлику између две групе информација:

- информације које се односе на угрожавање, односно заштиту здравља становништва и животне средине, у односу на које је претпоставка постојања интереса јавности да зна *необорива* и
- друге информације, у односу на које је претпоставка постојања интереса јавности да зна *оборива*, односно посматра се у корелацији са другим интересима.

Дакле, у првом случају обавеза органа власти да тражиоцу достави информације је апсолутна, док у другом, уколико орган јавне власти ускраћује или ограничава тражиоцу приступ одређеној информацији, обавезан је да докаже да је у конкретном случају оправдано да то учини ради заштите претежнијег интереса, попут интереса безбедности земље или приватности других лица.

Орган власти дужан је да на захтев тражиоца информације одговори без одлагања, а најкасније у законском *року од 15 дана*.[122] Закон предвиђа две могућности за одступање од овог рока:

121 Члан 5. ЗСПИЈЗ.
122 Члан 16. ЗСПИЈЗ.

- уколико се захтев односи на информацију за коју се може претпоставити да је од значаја за заштиту живота или слободе неког лица, односно за угрожавање или заштиту здравља становништва и животне средине, орган власти мора одговорити тражиоцу *у року од 48 сати* од пријема захтева;
- уколико орган власти није у могућности, из оправданих разлога, да у року од 15 дана одговори на захтев тражиоца, дужан је да о томе, најкасније у року од седам дана од пријема захтева, обавести тражиоца и да одреди додатни рок за одговор, који *не може бити дужи 40 дана*, рачунајући од дана пријема захтева.

За разлику од права поводом заштите података о личности, која су лична и гарантована су лицима на која се подаци односе, тражилац информација на основу Закона о слободном приступу информацијама од јавног значаја може бити било које лице, без обзира на то да ли је на било који начин у вези са информацијама које захтева.

Тражилац информације има право да уложи жалбу Поверенику уколико орган власти:

- не одговори у наведеним роковима (тзв. ћутање управе),
- захтев одбије у целини или делимично,
- условљава издавање копије документа уплатом накнаде која превазилази износ нужних трошкова,
- не стави на увид документ који садржи тражену информацију коришћењем сопствене опреме, или опреме тражиоца, уколико он то захтева,
- не стави на увид документ који садржи тражену информацију, односно не изда копију документа на језику на коме је поднет захтев, а орган располаже документом на том језику,
- на други начин отежава или онемогућава тражиоцу остваривање права на слободан приступ информацијама од јавног значаја, супротно одредбама закона.[123]

Од надлежности Повереника, законом је *изузет круī највиших државних орīана* – Народна скупштина, председник Републике, Влада Републике Србије, Врховни суд Србије (односно, Врховни касациони суд), Уставни суд и Републички јавни тужилац, против чијих одлука се директно може покренути управни спор.

Одлуке Повереника по захтевима за приступ информацијама од јавног значаја су *коначне, извршне и обавезујуће*, а против ових одлука се може водити управни спор у поступку који је хитан.

За вршење надзора над спровођењем ЗСПИЈЗ надлежан је Управни инспекторат у саставу Министарства државне управе и локалне самоуправе. У пракси, то подразумева да Повереник обавештава Управни инспекторат о решењима која органи власти нису извршили или по којима нису обавестили Повереника

123 Члан 22. ЗСПИЈЗ.

да су поступили по налогу из решења[124], а Управни инспекторат спроводи инспекцијски надзор у складу са овлашћењима и поступком прописаним Законом о инспекцијском надзору[125] и Законом о управној инспекцији.[126] Такође, Повереник нема овлашћење да иницира покретање прекршајног поступка за прекршаје прописане ЗСПИЈЗ, већ ова овлашћења имају Управни инспекторат и оштећени (тражилац информације)[127], било да се ради о физичком или правном лицу.[128]

Прекршај у смислу Закона о слободном приступу информацијама од јавног значаја, постоји ако орган јавне власти:

1. приступ информацијама условљава доказивањем оправданог или другог интереса;
2. не означи носач информације, где је и када тражена информација објављена;
3. не саопшти, односно не омогући увид у истиниту и потпуну информацију, а оспорава истинитост и потпуност објављене информације;
4. одбије да прими захтев тражиоца;
5. не поступи по захтеву за приступ информацијама у складу са Законом, односно достави непотпуне или нетачне информације;
6. приступ информацијама условљава уплатом трошкова у износу већем од прописаног;
7. не изда информацију у траженом облику, а има техничких могућности за то;
8. неосновано одбије да изда копију документа са информацијом на језику на којем је поднет захтев;
9. на било који други начин, супротно одредбама Закона, онемогућава остваривање права на слободан приступ информацијама од јавног значаја[129];
10. не поступи по решењу Повереника[130];
11. не одржава носач информације у складу са овим Законом;
12. спречи управног инспектора у вршењу инспекцијског надзора и не изврши решење управног инспектора[131].

124 M. Stefanović, K. Kalajdžić, *Primena zakona o slobodnom pristupu informacijama od javnog značaja u Srbiji – Analiza postupanja Upravnog inspektorata i prekršajnih sudova*, Beograd, 2019, доступно на: *http://www.partners-serbia.org/wp-content/uploads/2019/09/analiza-postupanja.pdf*, стр. 28.

125 „Службени гласник РС", бр. 36/2015, 44/2018 – др. закон и 95/2018.

126 „Службени гласник РС", број 87/2011.

127 *Primena zakona o slobodnom pristupu informacijama od javnog značaja u Srbiji – Analiza postupanja Upravnog inspektorata i prekršajnih sudova*, стр. 22.

128 *Ibid.*, стр. 40.

129 Члан 22. став 1. тачка 6) ЗСПИЈЗ.

130 Члан 28. став 1. ЗСПИЈЗ.

131 Члан 45. став 2. ЗСПИЈЗ.

4.3. Заштита података о личности као основ за ограничење приступа информацијама од јавног значаја

Закон о слободном приступу информацијама од јавног значаја предвиђа опште услове за ограничење права гарантованих законом и то:

- да су та ограничења прописана ЗСПИЈЗ;
- да је ограничење права неопходно у демократском друштву;
- да се ограничење права врши ради заштите од озбиљне повреде претежнијег интереса заснованог на уставу или закону.[132]

Тако, према члану 9. ЗСПИЈЗ, орган власти неће тражиоцу омогућити остваривање права на приступ информацијама од јавног значаја, ако би тиме:

- угрозио живот, здравље, сигурност или које друго важно добро неког лица;
- угрозио, омео или отежао спречавање или откривање кривичног дела, оптужење за кривично дело, вођење преткривичног поступка, вођење судског поступка, извршење пресуде или спровођење казне, или који други правно уређени поступак, или фер поступање и правично суђење;
- озбиљно угрозио одбрану земље, националну или јавну безбедност, или међународне односе;
- битно умањио способност државе да управља економским процесима у земљи или битно отежао остварење оправданих економских интереса;
- учинио доступним информацију или документ за који је прописима или службеним актом заснованим на закону одређено да се чува као државна, службена, пословна или друга тајна, односно који је доступан само одређеном кругу лица, а због чијег би одавања могле наступити тешке правне или друге последице по интересе заштићене законом који претежу над интересом за приступ информацији.

Такође, орган власти неће омогућити остваривање права тражиоцу:

- уколико се ради о информацији која је већ објављена и доступна у земљи или на интернету[133];
- уколико тражилац злоупотребљава права на приступ информацијама од јавног значаја, нарочито ако је тражење неразумно, често, када се понавља захтев за истим или већ добијеним информацијама или када се тражи превелики број информација[134];

132 Члан 8. став 1. ЗСПИЈЗ.
133 Члан 10. став 1. ЗСПИЈЗ.
134 Члан 13. став 1. ЗСПИЈЗ.

- уколико би тиме повредио право на приватност, право на углед или које друго право лица на које се тражена информација лично односи, уз одређене изузетке који су представљени у наставку.[135]

Са аспекта заштите података о личности важан је последњи разлог за ограничење права на слободан приступ информацијама од јавног значаја. Као што је случај и са другим основима за ограничење права на приступ информацијама, уколико орган власти намерава да одбије или ограничи захтев тражиоца, на њему је терет доказивања да би приступ информацијама повредио право на приватност неког лица. Оно што овај посао често отежава јесте чињеница да наш правни систем експлицитно не дефинише појам приватности. Како заштита података о личности несумњиво јесте један од елемената права на приватност, за потребе ове публикације фокус ће бити на односу права на заштиту података о личности и права на приступ информацијама од јавног значаја.[136]

ПРИМЕР

ЈМБГ, адресни подаци, бројеви банковних рачуна, приватни бројеви телефона, фотографије и видео-материјали из приватног живота, подаци о здравственом стању и сл. спадају у податке који се сматрају личним подацима и који би требало да буду изостављени приликом одговарања на захтеве.

Такође, напомињемо да је у Прегледу одредаба које се мењају у ЗСПИЈЗ, а који је новембра 2019. године објавило Министарство државне управе и локалне самоуправе као надлежно за процес измена и допуна овог закона, предложено додатно прецизирање члана 14, у смислу да се тражиоцу информација остваривање права *може* ограничити ако би се тиме повредило право на приватност, *право на заштиту података о личности*, право на углед или које друго право лица на које се тражена информација лично односи.[137] Дакле, уз посебно навођење права на заштиту података о личности као могућег основа за ограничење права на слободан приступ информацијама од јавног значаја, предлогом се јасније упућује на чињеницу да примена овог основа представља могућност (а не обавезу) за орган власти, те да сваки случај треба засебно ценити.

135 Члан 14. став 1. ЗСПИЈЗ.

136 О елементима права на приватност видети више у оквиру главе *О праву на заштиту података о личности* у овој публикацији.

137 Више информација доступно је на страници: *http://mduls.gov.rs/javne-rasprave-i-konsultacije/informacija-o-radu-na-izmenama-i-dopunama-zakona-o-slobodnom-pristupu-informacijama-od-javnog-znacaja/*.

ПРИМЕР

Приступ информацијама садржаним у списковима корисника личне инвалиднине
Удружење инвалида је захтевом за слободан приступ информацијама од јавног значаја од градске управе затражило фотокопије спискова корисника личне инвалиднине за ратне војне и мирнодопске инвалиде, као и за кориснике породичне инвалиднине, ради сравњивања евиденције.
По жалби Удружења због непоступања органа власти, Повереник је нашао да захтев тражиоца треба одбити. Имајући у виду да је жалилац у овом случају тражио фотокопије спискова корисника личне инвалиднине за ратне војне и мирнодопске инвалиде и корисника породичне инвалиднине ради сравњивања евиденције, Повереник је нашао да се, у конкретном случају, ради о таквим информацијама које имају карактер података о личности у смислу Закона о заштити података о личности и то оних из категорије нарочито осетљивих података138, који се могу обрађивати искључиво на основу изричите сагласности лица на које се односе или када је то законом прописано, те да, с обзиром на то да не постоје услови за примену изузетака из члана 14. Закона о слободном приступу информацијама од јавног значаја, приступ овим информацијама не треба дозволити.
У решењу Повереника такође се наводи да оваква одлука не би довела у питање право тражиоца на приступ информацијама које би се односиле на износе средстава која се из буџета исплаћују по основу инвалиднина и сл., тј. на деперсонализоване спискове за износима исплата, што у конкретном случају, очигледно није било предмет интересовања жалиоца, већ лични подаци о корисницима, за потребе евиденције.[139]

Међутим, треба нагласити да *свако објављивање података о личности не конституише увек повреду приватности*, у смислу члана 14. ЗСПИЈЗ, већ да повреду приватности треба тумачити тако да она може наступити објављивањем личних података који се односе на околности или детаље из приватног живота.[140]

ПРИМЕР

Име и презиме судије или министра несумњиво јесу подаци о личности, али ти подаци треба да буду доступни када се објављују судске одлуке или када се објављују акти које донесе министар.[141]

Као што је већ поменуто у одељку посвећеном Закону о заштити података о личности, обрада података о личности ради спровођења ЗСПИЈЗ представљена

138 Односно посебне врсте података, према Закону о заштити података о личности (2018).
139 Видети: *https://повереник.срб/sr-yu/pristup-informacijama2/praksa/odluke-i-mišljenja-poverenika/mišljenja-poverenika/povreda-privatnosti/1040-pristup-informacijama-sadranim-u-spiskovima-korisnika-line.html.*
140 A. Toskić, dr J. Kleut, U. Mišljenović i K. Kalajdžić, *Analiza o granicama privatnosti javnih funkcionera – Javna funkcija privatna stvar*, Partneri Srbija, Beograd 2018, доступно на *http://www.partners-serbia.org/wp-content/uploads/2018/04/jfps-publikacija.pdf, стр. 13.*
141 *Ibid.*

је као један од посебних видова обраде. Наиме, члан 98. ЗЗПЛ наводи да „информације од јавног значаја које садрже податке о личности могу бити учињене доступним тражиоцу информације од стране органа власти на начин којим се обезбеђује да се право јавности да зна и право на заштиту података о личности могу остварити заједно, у мери прописаној законом којим се уређује слободан приступ информацијама од јавног значаја и овим законом." Објављивање података о личности представља, дакле, радњу обраде података, а у случају објављивања података о личности на основу ЗСПИЈЗ, овај закон представља правни основ за обраду података.

Тако, уколико документ који садржи информацију затражену на основу Закона о слободном приступу информацијама од јавног значаја садржи и податке о личности неког физичког лица, *орган јавне власти треба да процени које је од два права – право на приватност или право јавности да зна – претежније*, узимајући у обзир околности конкретног случаја. Ова процена подразумева примену тзв. *теста јавног интереса*.[142]

Тест јавног интереса састоји се из три дела, односно три питања на које орган јавне власти треба да одговори у ситуацијама када може постојати неко друго право које ограничава право на слободан приступ информацијама од јавног значаја:

1. Да ли се тражене информације ускраћују ради неког од Законом побројаних интереса (чл. 9, 13. и 14) и, уколико се утврди да је то случај,
2. Да ли би достављањем информација тражиоцу тај интерес био озбиљно повређен?
3. Да ли је по мерилима демократског друштва неопходно ускратити информацију?[143]

Уколико је супротстављени интерес у конкретном случају заштита приватности, те се применом теста јавног интереса процени да примат треба дати праву јавности да зна, на посредан начин креира се правни основ за обраду података, у смислу да законски основ за обраду података представља ЗСПИЈЗ. У таквим околностима законски основ за обраду података постоји, те није потребно прибавити пристанак лица за обраду података.

142 *Ibid.*

143 Одређивање критеријума и процена неопходности ограничења права у демократском друштву спада међу најкомплексније задатке приликом одлучивања у сваком појединачном случају. Европски суд за људска права дао је, кроз своју праксу, опште смернице за примену овог правног стандарда, уз напомену да се морају разматрати околности и чињенице сваког појединачног случаја. Тако Суд наводи да ограничење права (тј. мешање државе) мора бити оправдано „хитном друштвеном потребом" која се односи на остварење једног или више легитимних циљева. Као кључне карактеристике демократског друштва, Суд издваја слободу изражавања, плурализам, толеранцију и отвореност, као и потребу за заштитом права на правично суђење. Према ставу Суда, демократија не подразумева једноставно преовлађивање ставова већине, већ правилан и праведан третман мањина и избегавање доминантног положаја. Више о томе: *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*, Steven Greer, University of Bristol, доступно на: *https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf*, стр. 14.

Међутим, чак и када се ради о истом лицу у истом конкретном случају, тест јавног интереса не мора да дâ исте резултате у односу на све информације. Иако процену да ли ће нека информација која садржи и личне податке бити дата и у којој мери треба вршити од случаја до случаја и не постоје универзална правила, може се направити груба класификацију које *врсте података* треба да да буду уклоњене или сакривене поступком анонимизације приликом одговарања на захтеве. Док, са друге стране, треба нагласити и које врсте информације не потпадају под домен заштите података о личности.

ПРИМЕР

Интерес јавности да зна може да превагне у погледу информација о висини прихода одређеног функционера, али право на приватност може да превагне у погледу информације о броју банковног рачуна тог функционера на који је извршена уплата.[144]
Међутим уколико су предмет интересовања јавности, на пример, информације о здравственом стању високог функционера, како би се испитало да ли је лице и даље способно да обавља своју функцију, поставља се питање да ли ће право на заштиту приватности превагнути у односу на право на слободан приступ информацијама од јавног значаја.

ПРИМЕР

Информације о образовању судија
Предмет захтева упућен једном суду биле су информације о одређеним судијама, и то: датум и место рођења, када и где су уписали и завршили правни факултет, са којим просеком, као и основни моменти у развоју каријере. Суд је одбио захтев тражиоца с позивом на кршење права на приватност прописаног у члану 14. ЗСПИЈЗ, са образложењем да не постоји сагласност судија чији су подаци тражени. Након тога, тражилац информације се обратио Поверенику жалбом. Суд је у одговору на жалбу која је изјављена против њега као аргумент за одбијање захтева навео да је тражилац странка у поступку пред истим судом те да би достављање евентуално могло да доведе до ометања судских поступака или би утицало на фер поступање и правично суђење. Повереник је поводом овог случаја донео занимљиву одлуку, која илуструје како се приликом одговарања на захтев може постићи баланс између права јавности да зна и права на приватност, тако да ни једно од права не буде угрожено. Наиме, Повереник је утврдио да је захтев тражиоца основан у делу у коме се тражи приступ информацијама о томе када су одређене судије уписале и завршиле правни факултет, са којим просеком и о „основним моментима у развитку њихове каријере" (радне биографије), а да су захтев, односно жалба неосновани у делу којим се захтева достављање информација о датуму и месту рођења, где су уписали и завршили факултет. Повереник је своју одлуку образложио на следећи начин: *Повереник налази да тражене информације о томе када су одређене судије уписале и завршиле правни факултет, са којим просеком и њихове радне биографије јесу од значаја за утврђивање мерила за оцену стручности судија, као једног од услова за њихов избор и у вези су са судијском функцијом коју врше, а не у вези са њиховим приватним животом, те да је, у конкретном случају, испуњен услов из одредбе члана 14. тачка 2. Закона о слободном приступу информацијама од јавног значаја, за примену изузетка од права на приватност.*

144 *Analiza o granicama privatnosti javnih funkcionera – Javna funkcija privatna stvar.*

ПРИМЕР

Повереник је одбио жалбу у делу која се односи на приступ информацијама о датуму и месту рођења судија, као и о томе где су уписали и завршили правни факултет, закључујући да ови подаци нису прописани као мерила за оцену стручности лица која обављају судијску функцију, односно нису услов за њихов избор на судијску функцију, те да у односу на ове податке не постоји преовлађујући интерес јавности да зна у односу на право на приватности и право на заштиту података о личности, јер није испуњен ниједан услов за примену изузетака од права на приватност из члана 14. Закона.[145]

За адекватно балансирање два права/интереса, ЗСПИЈЗ предвиђа *могућност раздвајања информација*. Наиме, члан 12. ЗСПИЈЗ предвиђа да, уколико је могуће издвојити тражену информацију од осталих информација у које орган власти није дужан да тражиоцу да увид, орган власти ће омогућити увид тражиоцу у део документа који садржи само издвојену информацију. Раздвајање информација може се спровести на један од следећих начина:

а) *физичко раздвајање* страна одређеног документа тако што би се јавности ставиле на увид само оне стране тог документа у односу на чији садржај претеже интерес јавности да зна, а уколико је то физички изводљиво у конкретном случају;

б) *анонимизација података* у односу на које претеже право на приватност. „Анонимизација је радња обраде података о личности садржаних у одређеном документу или збирци података, којом лице на које се подаци односе престаје да буде одредиво (енгл. *identifiable*). Анонимизација се спроводи тако да осујети повратну идентификацију (реидентификацију) лица чији се подаци анонимизују, чак и уколико се предузму одређене мере попут укрштања или спајања информација са информацијама доступним из других извора."[146] Када се спроводи анонимизација, потребно је имати на уму њену двојаку сврху: да се уклоне могућности идентификације лица, а да остале информације пружене у документацији задрже изворно значење и смисао, те да документација буде лако читљива и контекстуално разумљива. У супротном, садржај документације неће бити разумљив, чиме може бити ускраћено право јавности да зна.

Анонимизација се може спровести *изменом података* (применом техника генерализације или шифрирања) или *изостављањем података* (интервенцијом у електронској или штампаној верзији документа). У случају када се изостављање података спроводи помоћу рачунара, најчешће се подаци које треба заштити

145 За више видети: *Слободан приступ информацијама: Ставови и мишљења Повереника*, Повереник за информације од јавног значаја и заштиту података о личности, Београд 2018, стр. 47–48.

146 *Transparentnost i privatnost u sudskim odlukama*, Ana Toskić i Uroš Mišljenović, Partneri Srbija, Beograd 2016, *http://www.partners-serbia.org/wp-content/uploads/2016/03/Transparentnost-i-privatnost-u-sudskim-odlukama.pdf*, стр. 7.

прекривају црном бојом или се уместо текста уносе тачке или линије у низу. Уколико се интервенише у штампаном документу, најчешће се подаци прекривају коректором или црним непрозирним фломастером. Техника генерализације подразумева да се подаци редукују на ознаке које задржавају директну везу са податком, али тако да указују на више лица и онемогуће идентификацију лица на која се подаци односе (на пример, означавање иницијалима, уместо пуним именом и презименом). У случају да се примени ова техника, треба посебно водити рачуна о контексту самог документа и околности конкретног случаја како идентификација лица не би била могућа укрштањем са другим информацијама доступним у документу.[147] У случају шифрирања, а уколико се жели анонимизирати информација о идентитету физичког лица, име и презиме лица замениће се одговарајућом шифром са унапред формиране листе шифара (на пример: Петар Петровић – АА, Марко Марковић – ББ итд.). Додељену шифру потребно је користити кроз читав документ, како не би било могуће идентификовати лице.[148]

ПРИМЕР

Приступ информацијама из уговора општине и закупца пословних просторија

Општина је од Повереника затражила мишљење о поступању по захтеву за приступ информацијама од јавног значаја у случају када се захтев односи на информације из уговора у вези са располагањем пословним простором општине будући да уговори садрже податке о закупцима, те да ли је неопходно да се претходно прибавља њихова сагласност за достављање података тражиоцима, као и то да ли се уговори морају фотокопирати обзиром на то да их има на десетине, односно на који начин треба поступити да би се испоштовао Закон о слободном приступу информацијама од јавног значаја и Закон о заштити података о личности.

У вези с тим, Повереник је дао начелан став о овом питању, наводећи да се конкретно ради о информацијама о располагању пословним простором општине, тј. о располагању јавним ресурсима, за које увек постоји јак интерес јавности да зна, укључујући и имена лица са којима органи власти закључују правне послове. У том смислу, тешко да би орган власти могао доказивати супротно, под видом заштите права на приватност, с обзиром на то да су овакве ситуације, односно догађаји обухваћени изузецима од права на приватност из члана 14. став 1. тачка 2) ЗСПИЈЗ и да лица која послују са државом не могу имати очекивања заштите приватности у мери у којој то очекују тзв. обични грађани.

Према ставу Повереника, ако се има у виду да уговори о закупу пословног простора садрже и друге податке о личности у погледу којих јавност не треба да има интерес да зна и чија би обрада била прекомерна, тј. несразмерна сврси, то је код поступања по захтеву за приступ потребно претходно заштитити и учинити недоступним оне податке о личности из уговора чијом општом доступношћу би се могло повредити право на приватност, као што су нпр. подаци о адреси становања, ЈМБГ, бр. личне карте и сл., а у складу са чланом 12. ЗСПИЈЗ.[149]

147 На пример, уколико се користе иницијали лица са назнаком његовог места пребивалишта, те уколико се ради о мањем насељеном месту, идентификовање лица би било би значајно олакшано.

148 *Transparentnost i privatnost u sudskim odlukama*, стр. 16.

149 Видети: *https://www.poverenik.rs/index.php/sr-yu/pristup-informacijama2/praksa/odluke-i-mišljenja-poverenika/mišljenja-poverenika/povreda-privatnosti*.

ЗСПИЈЗ прави разлику и када је реч о *категоријама лица* на које се могу односити подаци или другим елементима приватности садржаним у документима у поседу органа јавне власти. Па тако, према члану 14. став 2. ЗСПИЈЗ, чак и када би остваривањем права на приступ информацијама од јавног значаја могло доћи до повреде права на приватност, права на углед или неког другог права лица на које се тражена информација лично односи, орган власти може омогућити остварење права на приступ информацијама:

- ако је лице на које се информација односи на то пристало;
- ако се ради о личности, појави или догађају од интереса за јавност, а нарочито ако се ради о носиоцу државне и политичке функције и ако је информација важна с обзиром на функцију коју то лице врши;
- ако се ради о лицу које је својим понашањем, нарочито у вези са приватним животом, дало повода за тражење информације.

У погледу захтева који се односе на носиоце државне и политичке функције, поставља се питање која лица улазе у ову категорију, с обзиром на то да не постоји јединствен акт који таксативно набраја ко се све сматра носиоцем јавне функције. У том смислу, треба указати на дефиниције појма *функционер* које дају неки од релевантних прописа за локалне самоуправе. Тако члан 3. став 2. Закона о запосленима у аутономним покрајинама и јединицама локалне самоуправе[150] наводи да је *функционер изабрано, именовано, односно постављено лице (осим службеника на положају) у органима аутономне покрајине и јединице локалне самоуправе, односно у органима градске општине, као и у службама и организацијама које они оснивају према посебном пропису.* Такође, Закон о Агенцији за борбу против корупције[151] у члану 2. предвиђа да је функционер *свако лице изабрано, постављено или именовано у органе Републике Србије, аутономне покрајине, јединице локалне самоуправе и органе јавних предузећа и привредних друштава, установа и других организација чији је оснивач, односно члан Република Србија, аутономна покрајина, јединица локалне самоуправе и друго лице које бира Народна скупштина.* Додатно, исти закон дефинише јавну функцију као функцију *у органима Републике Србије, аутономне покрајине, јединице локалне самоуправе, органима јавних предузећа и привредних друштава, установа и других организација, чији је оснивач, односно члан Република Србија, аутономна покрајина, јединица локалне самоуправе, као и функција других лица које бира Народна скупштина, а подразумева овлашћења за руковођење, одлучивање, односно доношење општих или појединачних аката.*

Дакле, *приватност носилаца државних функција ужа је у односу на приватност других лица*; међутим, то свакако не значи да је њихова приватност суспендована, већ да се може јемчити само у „односу на информације и активности које

150 „Службени гласник РС", бр.. 21/2016, 113/2017, 95/2018 и 113/2017 – др. закон.

151 „Службени гласник РС", бр. 97/2008, 53/2010, 66/2011 – одлука УС, 67/2013 – одлука УС, 112/2013 – аутентично тумачење и 8/2015 – одлука УС.

су у вези са њиховим приватним животима, док информације које су релевантне за посао који те особе обављају у име јавности и за потребе јавности треба да буду доступне јавности."[152]

Са друге стране, *приватност службеника и других лица запослених у јавним институцијама заштићенија је у односу на функционере*. Међутим, пракса Повереника потврдила је да и у односу на информације о овим лицима може превагнути интерес јавности да зна, пре свега када се ради о информацијама о обављању њихових дужности.[153] Дакле, околности сваког случаја треба сагледати и треба проценити да ли претеже интерес права јавности да оствари увид у рад јавног службеника или пак претеже интерес да се заштити приватност тог лица.

ПРИМЕР

Подаци из казнене евиденције одборника

Захтевом за слободан приступ информацијама од јавног значаја тражени су подаци из казнене евиденције одборника скупштине града, тј. носиоца политичке функције у јединици локалне самоуправе, који је, према наводима тражиоца, и претендент са изгледним шансама за место градоначелника. Орган јавне власти од којег су информације тражене, у овом случају надлежно Министарство, одбио је решењем захтев тражиоца, позивајући се на члан 9. тачка 5. Закона о слободном приступу информацијама од јавног значаја и члан 102. Кривичног законика. Тражилац је изјавио жалбу Поверенику, који је утврдио да подаци из казнене евиденције представљају податке о личности, те да се објављивањем свих података из казнене евиденције одређеног лица (лични подаци о учиниоцу кривичног дела, правним последицама осуде, подаци о издржавању казне, поништењу евиденције о погрешној осуди и др.) озбиљно задире у његову приватност и права на заштиту података о личности, Повереник је донео решење којим је потврдио одлуку првостепеног органа – Министарства. У образложењу одлуке Повереника стоји: *„Чињеница да је лице, за које се траже све информације из казнене евиденције, носилац политичке функције у јединици локалне самоуправе, тј. одборник скупштине града, а према наводима жалиоца и 'претендент са изгледним шансама на место градоначелника', по оцени Повереника, није довољан разлог који би, у одсуству сагласности лица из члана 14. став 1. тачка 1. Закона о слободном приступу информацијама од јавног значаја, оправдавао примену преостала два изузетка од права на приватност из члана 14. став 1. тач. 2. и 3. овог закона. Повереник је код оваквог става ценио чињеницу да информације тј. подаци из казнене евиденције нису законски услов за избор лица за одборника, као и друге објективне околности случаја, попут јавне моћи одборника, компетенција за одлучивање, одговорности за располагање јавним средствима и слично. Такође, у поступку нису предочени докази, нити је опште познато да би доступност предметних информација у овом тренутку била важна за доношење одлуке од интереса за јавност у односу на лице о чијим подацима се ради, нпр. за избор на одређену државну или јавну функцију, нити да је лице својим понашањем, изјавама и слично дало повода за објављивање његових података из казнене евиденције."*[154]

152 *Analiza o granicama privatnosti javnih funkcionera – Javna funkcija privatna stvar*, стр. 15.

153 *Ibid*., стр. 16.

154 За више видети: *Слободан приступ информацијама: Ставови и мишљења Повереника*, Повереник за информације од јавног значаја и заштиту података о личности, Београд 2018, стр. 44-45.

ПРИМЕР

Статистички подаци као информације од јавног значаја

Захтевом који је упућен једном центру за социјални рад тражени су подаци о броју притужби против запослених, против којих запослених су поднете притужбе и информације о томе које мере је центар за социјални рад предузео тим поводом.

Центар за социјални рад је одбио захтев тражиоца уз образложење да је област рада социјалних центара уређена Породичним законом и другим законима из области социјалне заштите и да се у смислу тих закона информације у вези са радом центара сматрају поверљивим, те да због заштите права малолетног детета и др. тражени подаци не могу бити достављени. Повереник није уважио став Центра за социјални рад и наложио је достављање информација тражиоцу, уз образложење:

…поднетим захтевом за приступ информацијама тражени статистички подаци, тј. информације о броју поднетих притужби и других аката на рад запослених у центру за социјални рад, против којих запослених су поднете, и шта је предузето по притужбама на рад тих лица, а нису тражени никакви подаци о малолетним лицима и другим корисницима социјалне заштите, који подаци би задирали у њихову приватност.[155]

ПРИМЕР

Подаци о дисциплинском поступку

Тражилац информација је у захтеву затражио податке о дисциплинском поступку против секретара једног суда. Суд је одбио да достави тражена документа са образложењем да информације представљају нарочито осетљиве податке о личности и да подносилац захтева није поднео доказ о испуњености услова за примену законских изузетака од заштите права на приватност из члана 14. Закона о слободном приступу информацијама од јавног значаја. Тражилац се након тога обратио Поверенику наводећи да тражилац информације није у обавези да подноси доказе о разлозима за захтев, нити о основаности тог захтева, као и да се суд неосновано позива на приватност секретара суда, с обзиром на то да је он државни службеник, те су информације о његовом раду доступне јавности сходно одредби члана 8. Закона о државним службеницима. Повереник је оценио да је суд погрешно применио право када је одбио захтев тражиоца информација. Повереник у својој одлуци наводи да тражилац: *„... има право да му се тражене информације учине доступним, али на начин да се, у складу са одредбом члана 12. Закона, учине недоступним – заштите сви подаци о личности, осим имена службених лица. У конкретном случају, тражене информације односе на секретара суда, државног службеника, чији је послодавац, према одредби члана 3. став 1. Закона о државним службеницима („Службени гласник РС", бр. 79/05 ... и 94/17), Република Србија и који, према члану 6. став 1. истог закона, одговара за законитост, стручност и делотворност свог рада, због чега у односу на предметне информације постоји појачан интерес јавности да буде упозната са њиховом садржином, јер говоре о законитости рада државног службеника, па је у односу на њега испуњен услов из члана 14. тачка 2. Закона о слободном приступу информацијама од јавног значаја за примену изузетка од права на приватност."*

155 За више видети: *Слободан приступ информацијама: Ставови и мишљења Повереника*, Повереник за информације од јавног значаја и заштиту података о личности, Београд 2018, стр. 60.

ПРИМЕР

Међутим, то не значи да лицу треба да буду достављене све информације и документи у изворном стању, већ пре достављања информација тражиоцу треба учинити недоступним све личне податке, сем имена и презимена службеника – адресни подаци, лични матични број и сл., јер би њихово достављање представљало прекомерну обраду података о личности супротну основном начелу пропорционалности односно сразмерности из члана 8. Закона о заштити података о личности. „Такође, Повереник налази да се јавности не могу учинити доступним подаци о именима и презименима других физичких лица (која нису службена), као ни њихови други лични подаци уколико су они садржани у траженим документима, из разлога заштите права на приватност тих лица, с обзиром на то да у погледу њих нису испуњени услови за изузетак од права на приватност прописани одредбама члана 14. тач. 1, 2, и 3. Закона о слободном приступу информацијама од јавног значаја."[156]

156 За више видети: *Слободан приступ информацијама: Ставови и мишљења Повереника*, Повереник за информације од јавног значаја и заштиту података о личности, Београд 2018, стр. 57–58.

5. АНАЛИЗА КАПАЦИТЕТА ЈЕДИНИЦА ЛОКАЛНЕ САМОУПРАВЕ ЗА УСКЛАЂИВАЊЕ СА НОВИМ ПРАВНИМ ОКВИРОМ ЗА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ

5.1. Циљеви и методологија анализе

Анализа капацитета јединица локалне самоуправе за примену прописа у области заштите података о личности спроведена је у периоду од 10. септембра до 20. новембра 2019, са следећим циљевима:

- да се утврди постојеће стање у јединицама локалне самоуправе у области заштите података о личности;
- да се испитају постојећи капацитети јединица локалне самоуправе у области заштите података о личности, те
- да се утврди потреба за унапређењем капацитета јединица локалне самоуправе у овој области.

Анализа је заснована на прикупљању информација директно од представника узоркованих локалних самоуправа. У припремној фази, извршено је узорковање локалних самоуправа, при чему се водило следећим критеријумима:

а) територијална покривеност, тј. равномерна заступљеност региона према административно-територијалној подели и номенклатури статистичких територијалних јединица (ниво 2),
б) врста јединице локалне самоуправе (град или општина),
в) степен развијености ЈЛС, а према Уредби о утврђивању јединствене листе развијености региона и јединица локалне самоуправе за 2014. годину, објављеној у „Службеном гласнику РС", број 104/2014.

Упитник је достављен контакт особама у 20 узоркованих јединица локалне самоуправе, а одговоре је доставило 14 јединица локалне самоуправе, дајући репрезентативни узорак за реализацију анализе.

Структура ЈЛС које су учествовале у анкети дата је у табели у наставку, док је списак јединица локалне самоуправе доступан у Прилогу 2.

а) Структура учесника анкете према регионалној распрострањености:

Регион	Београд	Шумадија и Западна Србија	Војводина	Јужна и Источна Србија
	2	4	5	3

б) Структура учесника анкете према врстама јединица локалне самоуправе:

Врста ЈЛС	Град	Општина
	4	10

Напомињемо да су међу 10 општина и две градске општине.

в) Структура учесника анкете према степену развијености ЈЛС:

Степен развијености	I	II	III	IV
	5	2	3	4

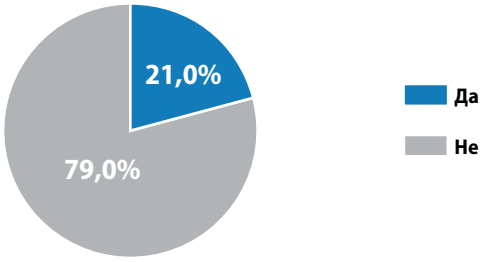
За прикупљање података, коришћен је упитник са 24 питања који је електронским путем достављен представницима узоркованих јединица локалне самоуправе, и то контакт лицима задуженим (формално или неформално) за питања заштите података о личности. Електронска форма изабрана је због ефикасности и економичности, с обзиром на намеру да се обухвате ЈЛС из свих региона Републике Србије. Упитник је доступан у Прилогу 1 ове публикације.

Упитник је обухватао затворена и отворена питања, међу којима су била и питања са дихотомним (два алтернативна понуђена одговора) и вишеструким избором одговора.

5.2. Резултати

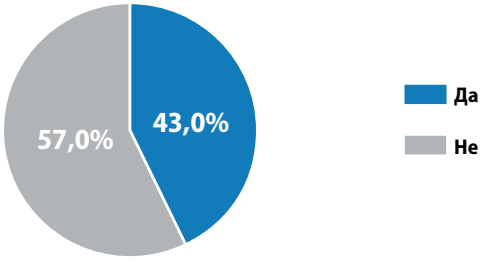
Од 14 ЈЛС које су доставиле одговоре на упитник, само њих три, односно *21%, регулисало је област заштите података неким интерним актом*, и то углавном актом који регулише и неке друге области, попут поступања по захтевима за слободан приступ информацијама од јавног значаја. Такође, *мање од половине испитаних ЈЛС*, односно њих 43%, у време спровођења истраживања *није испунило своју законску обавезу именовања лица овлашћеног за заштиту података о личности*. Међу онима које нису формално именовале лице овлашћено за заштиту података су и три ЈЛС у оквиру којих постоји лице које је задужено за питања заштите података. Ради се о лицима која обављају и друге послове, попут оних у области слободног приступа информацијама од јавног значаја или послова у области информационих технологија. *Већина ЈЛС (71%) не води евиденције радњи обраде података*.

Питање:
Да ли је неким интерним актом ЈЛС уређена област заштите личних података?



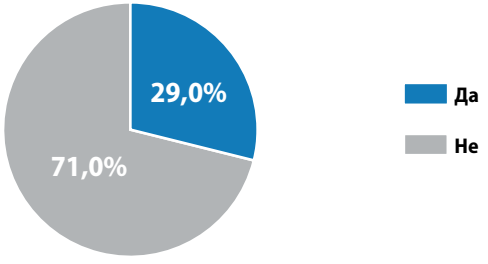
01

Питање:
Да ли је Ваша ЈЛС именовала лице за заштиту података о личности?



02

Питање:
Да ли Ваша ЈЛС води евиденцију радњи обраде података о личности?



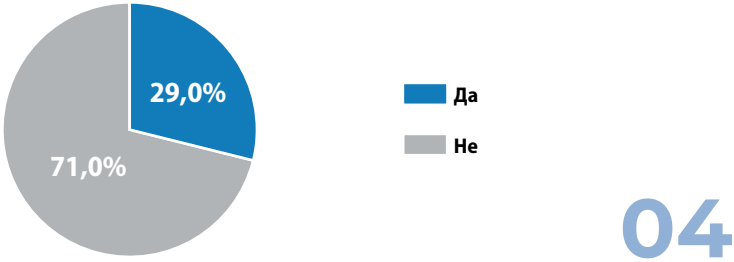
03

У погледу *спремности ЈЛС за поступање по захтевима за остварење права лица за заштиту података о личности*, *ниједна од анкетираних ЈЛС нема развијене интерне процедуре за поступање по овим захтевима, нити се до сада сусретала са захтевима лица чији се подаци обрађују.* Једна ЈЛС до сада је била предмет надзора Повереника на основу Закона о заштити података о личности, док ниједна није била предмет поступка по правним лековима пред Повереником, нити судског поступка у овој области. Запослени у 36% анкетираних ЈЛС су на друге начине били у контакту са институцијом Повереника, и у 80% таквих случајева су добили одговоре на постављена питања.

Интерне процедуре у области *безбедност података о личности* дефинисане су посебним актима у мање од трећине (29%) анкетираних ЈЛС, и углавном се ради о актима који регулишу питања безбедности информационо-комуникационих система ЈЛС. Са друге стране, ниједна од анектираних ЈЛС не поседује неки од сертификата у овој области (нпр. ИСО 27000 или ИСО 27001), а запослени у анкетираним ЈЛС нису преузели обавезу чувања поверљивости података потписивањем посебних изјава.

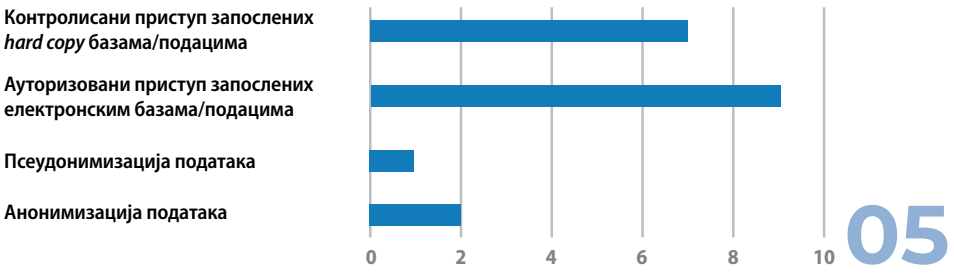
Анкетиране ЈЛС *најчешће примењују организационе мере заштите података о личности*, и то ауторизацију приступа електронским збиркама података (64% анкетираних ЈЛС), односно контролисани приступ запослених штампаним (*hard copy*) збиркама података (50% анкетираних ЈЛС). Друге мере заштите, попут анонимизације или псеудономизације података о личности, ЈЛС спроводе у мањој мери (у 14%, односно 7% случајева). Такође, у нешто више од трећине испитаних ЈЛС (36%) води се евиденција о томе која лица имају приступ одређеним збиркама података, и то се најчешће чини путем система електронског пријављивања корисника.

Питање:
Да ли су неким интерним актом ЈЛС прописане мере заштите података о личности од злоупотреба, уништења, губитка, неовлашћених промена или приступа?



04

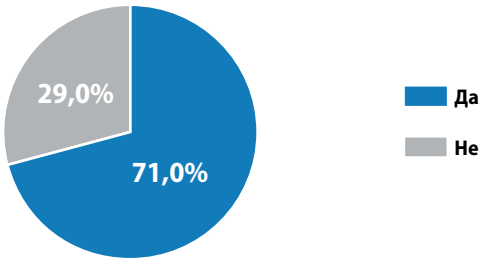
Питање:
Да ли Ваша ЈЛС примењује неке од следећих мера заштите података о личности (могућ избор више одговора)?



05

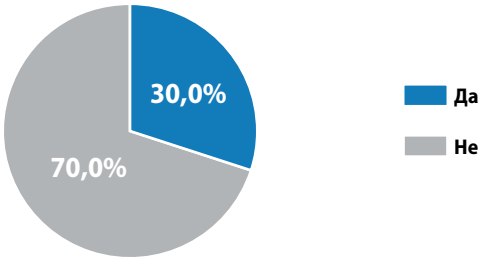
Велика већина (71%) *испитаних ЈЛС врши обраду података путем видео-надзора*, али само у трећини ЈЛС које спроводе видео-надзор интерним актом је прецизирано на који начин се користи снимљени материјал. Приступ видео-записима имају углавном лица задужена са послове информационих технологија, док дужина рокова чувања записа (у случајевима када су се представници ЈЛС о томе изјаснили) варира од 48 сати до 30 дана. Одржавање рачунарских система ЈЛС поверавају по правилу интерним ИТ стручњацима, а подаци настали у раду ЈЛС чувају се на серверима у Републици Србији.

Питање:
Да ли Ваша ЈЛС користи опрему за видео-надзор?



06

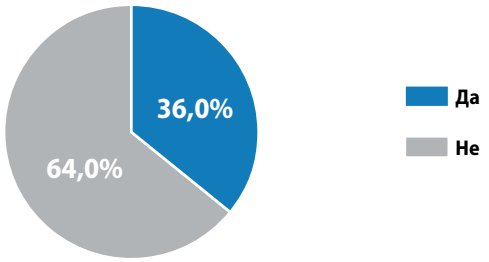
Питање:
Да ли је неким интерним актом прецизирано на који начин се снимљени материјал користи?



07

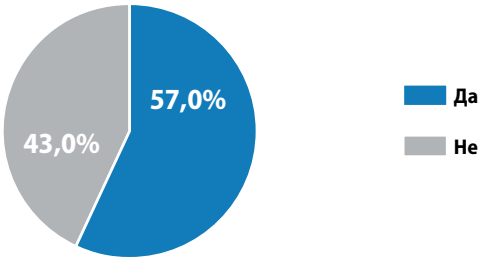
У погледу *интерних капацитета* ЈЛС за заштиту података о личности, запослени у већини (64%) од анкетираних ЈЛС нису прошли ниједну обуку у области заштите података. Сви анкетирани упознати су са чињеницом да је у Србији усвојен нови Закон о заштити података о личности, а информисање запослених о новинама Закона о заштити података о личности ЈЛС су углавном вршиле преко информативних брошура или простим ослањањем на чињеницу да је нови Закон објављен на интернету, те да је запосленима у опису посла да прате измене релевантних прописа.

Питање:
Да ли су запослени у ЈЛС учествовали на обукама у области заштите података о личности?



08

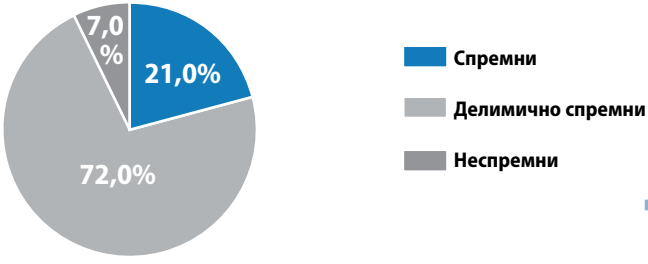
Питање:
Да ли су запослени у ЈЛС на други начин упознати са обавезама и правима из ЗЗПЛ (обавештења, промотивне брошуре, и сл.)?



09

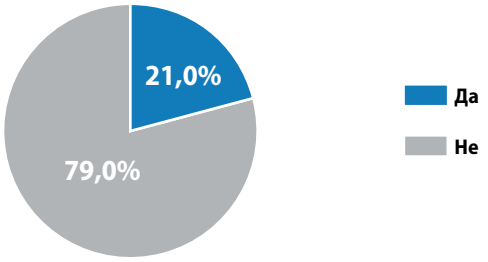
Само у свакој петој од анкетираних ЈЛС (21%) *буџетима су предвиђена средства за унапређење капацитета* за заштиту података. Исти проценат анкетираних ЈЛС сматра се спремним, 72% делимично спремним, а 7% њих неспремним за примену новог Закона. Све анкетиране ЈЛС сматрају да им је потребна подршка за унапређење капацитета у области заштите података о личности, и то пре свега кроз обуке лица овлашћених за заштиту података, и обуке запослених о техничким, односно правним аспектима заштите података.

Питање:
Молимо оцените спремност Ваше ЈЛС за примену новог Закона о заштити података о личности.



10

Питање:
Да ли су у буџету Ваше ЈЛС опредељена средства за унапређење капацитета за заштиту података?



11

Питање:
Молимо наведите каква врста подршке би била потребна запосленима у Вашој ЈЛС (можете изабрати више од једног одговора):

12

5.3. Закључак

На основу прикупљених одговора, може се закључити да јединице локалне самоуправе, иако свесне постојања новог правног оквира, *нису у довољној мери испуниле своје законске обавезе у области заштите података о личности, нити поседују довољно капацитета за примену новог Закона о заштити података о личности.*

Иако би се могло претпоставити да би развијеније ЈЛС требало да имају и више стандарде заштите података, на основу прикупљених података овим истраживањем није се могао донети такав закључак. Такође, разлике у погледу (не) испуњености законских обавеза не постоје ни између ЈЛС које припадају различитим регионима.

Тако, на пример, већина ЈЛС није именовала лице овлашћено за заштиту података о личности, нити је успоставила евиденције радњи обраде података, иако према новом ЗЗПЛ, а чија је примена већ започела у време спровођења истраживања, неиспуњење ових обавеза представља прекршај.

У већини ЈЛС недостају интерне процедуре за заштиту података о личности, а тамо где оне постоје, односе се углавном на општу безбедност података (дакле, не искључиво података о личности) у оквиру информационо-комуникационих система ЈЛС. Са друге стране, похвална је чињеница да је већина ЈЛС препознала значај неких од мера заштите података о личности.

Забрињавајућа је, међутим, чињеница, да *ниједна од анектираних ЈЛС нема развијене процедуре за остварење права лица чији се подаци обрађују*, као и то да су ЈЛС углавном спремне да *предузимају инванзивније радње обраде података* (попут видео-надзора), али да нису унапред дефинисале правила о коришћењу сачињених садржаја.

Запослени у ЈЛС нису до сада имали довољно прилика за унапређење знања из области заштите података о личности, док *буџети ЈЛС не препознају у довољној мери потребу за унапређењем капацитета* у овој области. Међутим, значајно је што су све ЈЛС свесне да им недостаје капацитет у области заштите података о личности, и што препознају потребу за даљом обуком запослених о обавезама предвиђеним Законом.

6. ПРЕПОРУКЕ ЗА УСКЛАЂИВАЊЕ РАДА ЈЛС СА НОВИМ ЗАКОНОМ О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ

Ради усклађивања рада јединица локалне самоуправе са новим Законом о заштити података о личности, неопходно је спровести низ регулаторних, али и конкретних измена у пракси ЈЛС. У том смислу, препоруке за усклађивање груписане су у предлоге активности које би требало да предузму органи на националном нивоу, саме јединице локалне самоуправе, као и Стална конференција градова и општина.

6.1. Препоруке за органе на националном нивоу за потребе усклађивања рада ЈЛС са новим Законом о заштити података о личности

У погледу иницијатива и активности органа на националном нивоу у сврхе усклађивања рада ЈЛС са новим Законом, најзначајнију улогу требало би да има Министарство државне управе и локалне самоуправе (МДУЛС), и то кроз:

- иницирање и учешће у спровођењу анализе секторских закона релевантних за ЈЛС, посебно имајући у виду да Република Србија до краја 2020. године треба да усклади свој правни оквир са новим ЗЗПЛ;
- иницирање регулаторних измена у делу који се односи на заштиту података о личности, а у погледу надлежности и овлашћења ЈЛС;
- праћење, у сарадњи са СКГО, даљег развоја правног оквира у ЕУ у области заштите података, а који је релевантан за надлежности и активности ЈЛС, са посебним осврtом на појединачна решења и примере добре праксе из држава чланица;
- иницирање и подстицање, у сарадњи са СКГО и Националном академијом за јавну управу, унапређења капацитета ЈЛС за адекватну примену прописа и стандарда у области заштите података о личности;

- подстицање јединица локалне самоуправе да буџетирају средства за примену прописа у области заштите података о личности, а посебно за спровођење техничких мера заштите података.

6.2. Препоруке за активности СКГО са циљем усклађивања рада ЈЛС са новим Законом о заштити података о личности

Даље, значајну улогу у процесу у усклађивању рада ЈЛС са новим Законом може пружити и *Стална конференција градова и општина (СКГО)*, и то:

- умрежавањем ЈЛС и омогућавањем прилика за размене искустава у овом процесу, оснивањем тематских одбора или других тела;
- организацијом стручних скупова и едукација намењених представницима ЈЛС, те специјализованим едукацијама за лица овлашћена за заштиту података именована у оквиру ЈЛС;
- учешћем у анализи секторских закона и подзаконских аката релевантних за ЈЛС, те предлозима за њихове измене у делу који се односи на заштиту података о личности;
- иницирањем и/или подршком при усвајању модела аката у области заштите података о личности прилагођених потребама ЈЛС, уз могућност да се на нивоу Сталне конференције градова и општина усвоји и Кодекс понашања с циљем ефикасније и уједначеније примене ЗЗПЛ од стране јединица локалне самоуправе;
- сарадњом и комуникацијом са Повереником за информације од јавног значаја и заштиту података о личности, кроз иницијативе за давање мишљења Повереника о питањима од значаја за примену ЗЗПЛ у јединицама локалне самоуправе.

6.3. Препоруке за активности ЈЛС за потребе усклађивања са новим Законом о заштити података о личности

Иако нови Закон о заштити података о личности уноси низ нових обавеза за ЈЛС у својству руковалаца или обрађивача података о личности, основне смернице приликом спровођења процеса усклађивања треба да буду начела обраде података. Кључни захтеви за сваког руковаоца и обрађивача, па тако и за ЈЛС, које нови правни режим поставља јесу да *ЈЛС обрађују само оне податке о личности који су им неопходни (начела минимизације и ограничења у односу на сврху обраде), уз примену мера заштите података, одређивање рока њиховог чувања и предузимање свих расположивих мера које им омогућавају да документују*

своје активности поводом обраде података о личности (начела транспарентности и одговорности).

Процес усклађивања са новим Законом може се представити у неколико практичних корака, појашњених у тексту у наставку. Напомињемо да списак корака и активности за усклађивање може бити и шири, у зависности од комплексности система и специфичности руковаоца, као и да се ради о процесу који не мора имати ограничено временско трајање, већ подразумева стално унапређење и преиспитивање процедура.

При спровођењу процеса усклађивања, ЈЛС треба да се руководе и *Контролном листом за руковаоце који су органи власти*, коју је израдио и објавио Повереник[157] за потребе планирања инспекцијског надзора над применом ЗЗПЛ. Контролна листа има сврху и да руковаоцима омогући самопроцену испуњености обавеза предвиђених Законом, те ризика у погледу заштите података лица чије податке обрађују.

Слика 3. Кораци за усклађивање са новим Законом о заштити података о личности

Корак 1: Именовање лица овлашћеног за заштиту података и формирање тима за усклађивање са ЗЗПЛ

- *Лице овлашћено за заштиту података* именује се одлуком органа ЈЛС. О именовању овог лица ЈЛС су дужне да обавесте Повереника, а његове контакт податке треба објавити на веб презентацији ЈЛС или другом видљивом месту (нпр. огласна табла).
- Како процес усклађивања са новим обавезама подразумева анализу радних процеса у свим јединицама/секторима руковаоца, препоручује се формирање *интерног тима* који ће спроводити овај процес. У тиму, којим би требало да руководи лице овлашћено за заштиту података, учешће би требало да узму представници различитих сектора (људски ресурси, финансије, правни послови), а посебно и стручњак или администратор за информационе технологије.

157 Контролне листе за руковаоце доступне су на страници: *https://www.poverenik.rs/sr/заштита-података/контролне-листе.html.*

Корак 2: Идентификовање и анализа збирки података

- За потребе адекватне процене стања и нивоа заштите података у оквиру ЈЛС, неопходно је *идентификовати постојеће збирке података и извршити њихову анализу*. Уколико ЈЛС раније није пријављивала евиденције радњи обраде у централни регистар, овај процес може бити временски најзахтевнији, али представља неопходан предуслов за предузимање свих даљих радњи усклађивања. Процесом руководи лице овлашћено за заштиту података, али се информације прикупљају од запослених у свим секторима који треба да идентификују (попишу): које збирке података о личности воде, који подаци се у тим збиркама налазе, по ком правном основу се подаци обрађују, да ли ЈЛС у датом случају има улогу руковаоца или обрађивача, који су рокови чувања података, да ли се подаци уступају трећим лицима, да ли се износе из земље, по ком правном основу, да ли се предузимају мере заштите података и које мере су у питању, као и да евидентирају све друге чињенице које могу бити од значаја за дате радње обраде или поједине збирке. Адекватно спроведено идентификовање збирки и њихова анализа представљаће основ за успостављање и вођење евиденција радњи обраде.

Корак 3: Преглед постојећих интерних процедура ЈЛС

- На основу резултата идентификовања збирки података, и њихове анализе, ЈЛС треба да ревидира и постојеће интерне процедуре за заштиту података о личности. Пре свега, ЈЛС треба да утврди да ли постоје *интерни акти* који регулишу питања заштите података, попут интерних правилника, одлука и сл. који могу прописивати поделу послова и одговорности запослених у погледу обраде и заштите података, права и обавезе у том погледу, мере заштите које се примењују итд. Такође, уколико ЈЛС има веб презентацију, потребно је ревидирати и ускладити *политику приватности сајта*. Коначно, ЈЛС треба да утврди да ли је до сада, за потребе спровођења појединих радњи обраде, ангажовала обрађиваче података, те да изврши *анализу постојећих уговора са обрађивачима* у делу у коме они уређују обавезе заштите података.

Корак 4: Имплементација промена у оквиру ЈЛС

- Имплементација промена у оквиру ЈЛС може обухватити следеће кораке:
  - *Успостављање и редовно ажурирање евиденција радњи обраде*, у складу са чланом 47. ЗЗПЛ. У овом поступку, потребно је и избрисати све податке за које не постоји правни основ обраде (односно обезбедити правни основ за њихову обраду), који нису више неопходни за остварење сврхе обраде података од стране ЈЛС, или за које је протекао рок чувања; такође, ЈЛС треба да одреди рокове чувања података за оне податке за које то није прописано законом или раније одређено;

- *Измена постојећих или усвајање нових интерних аката* којима се утврђују права, обавезе и подела одговорности запослених у погледу заштите података о личности, као и други релевантни аспекти заштите података о личности; обавештавање запослених о новим стандардима и политикама заштите података у оквиру ЈЛС;
- *Израда интерне процедуре за остварење права лица* на основу заштите података о личности;
- *Измене постојећих или потписивање нових уговора са обрађивачима* у складу са чланом 45. ЗЗПЛ, те обавештавање обрађивача о новим стандардима и политикама заштите података у оквиру ЈЛС;
- *Измене постојећих или потписивање нових уговора са спољним сарадницима* у делу утврђивања права и обавеза заштите података о личности, као и обавештавање о новим стандардима и политикама заштите података у оквиру ЈЛС;
- *Израда интерних правила/смерница* којима се остварује *баланс између права на слободан приступ информацијама од јавног значаја и заштите података о личности*, пре свега у погледу стандарда анонимизације и псеудонимизације података о личности.

Корак 5: Обука запослених о правима и обавезама у погледу заштите података о личности

- Поред иницијалне обуке за запослене, на којој би требало да буду едуковани о новим стандардима заштите података, процедурама, правима и обавезама, потребно је периодично спроводити и додатне едукације, посебно у случајевима измена прописа или ажурирања интерних правила. Обуке за запослене могу спроводити спољни сарадници, а то може бити и један од задатака лица овлашћеног за заштиту података. За потребе организовања обука запослених, ЈЛС се могу обратити и Националној академији за јавну управу, као централној институцији система стручног усавршавања у јавној управи Републике Србије.

7. ДОПРИНОС ИСКУСТАВА ШВЕДСКЕ У ОБЛАСТИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ И ОСНОВНИХ ПРАВА – ПРИСТУП ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ

Дејвид Јанг (*David Young*)

7.1. Преглед

Шведска има дугу традицију интегритета података о личности, имајући у виду да је 1973. године прва у свету донела закон о заштити података. Са чланством у ЕУ, приступ заштити података временом се мењао, најскорије ступањем на снагу Опште уредбе о заштити података (*GDPR*).

Општа уредба о заштити података унела је одређене промене у радној култури локалних власти, где се многи процеси ослањају на обраду података о личности. Потреба за већом пажњом у идентификацији сврхе прикупљања података, утврђивање правног основа, избегавање непотребне обраде, информисање појединаца, вођење детаљне евиденције и слично, представљају знатан административни изазов, који резултира додатним трошковима и периодима неизвесности за многе људе.

Конкретни проблеми са којима се администрација суочила (у поређењу са ситуацијом из претходног периода и применом Директиве о заштити података) укључују, између осталих следеће:

- „правило злоупотребе", којим су електронска пошта и интернет странице биле изузете од режима заштите података, све док не наступи нека злоупотреба, више се не примењује
- службеници за заштиту података сада морају да буду независни, док су раније често били задужени за политике и процедуре заштите података
- ИТ провајдери и други обрађивачи података невољно потписују додатне услове који се захтевају у складу са Општом уредбом о заштити података.

Међутим, уопштено говорећи, ни Општа уредба о заштити података, ни допунски национални прописи не садрже ништа чиме се локалним властима брани да наставе са обрађивањем личних података (уколико су раније то радили на законом дозвољен начин). Можда су и даље присутне једна или две сиве области – на пример, негде је потребно надоградити застарели ИТ систем; такође је сада теже оправдати раније уобичајену праксу чувања биографија неуспешних кандидата за посао. Међутим, све у свему, Општа уредба о заштити података није се показала као препрека за легитимну реализацију циљева локалне политике.

Посебно питање у Шведској представља равнотежа између заштите података и приступа јавним документима, с обзиром на снажну традицију отвореног приступа. Општа уредба о заштити података у основи не мења ову равнотежу, али је држава одлучила да то питање додатно објасни одредбом у комплементарном националном закону о заштити података. Та одредба налаже да се Општа уредба о заштити података неће примењивати у мери у којој би то било у супротности са уставним одредбама о слободи говора, слободи штампе и приступу јавним документима.

Слично случајевима у другим областима законодавства ЕУ (нпр. јавне набавке), шведске власти одлучиле су се за проширење опсега Опште уредбе о заштити података изван онога што ЕУ строго захтева, између осталог, и тако што јавни органи и тела подлежу знатним административним новчаним казнама у случају кршења прописа.

Представници Шведске асоцијације локалних власти и регија (*SALAR*) поздрављају ширу примену ове уредбе у јавном сектору. Они тврде да ће локалне власти имати користи од тога што ће их људи доживљавати као неког ко озбиљно схвата заштиту података, јер пуни потенцијал дигитализације може се реализовати само ако грађани имају поверења у систем.

Влада је уложила знатне напоре у анализирање начина на који би Општа уредба о заштити података утицала на локалне власти, прилагодивши законе где је то било потребно. Овај процес укључио је консултације са *SALAR*-ом и појединим општинама, што је важно нагласити јер, иако је Општа уредба о заштити података пропис који се директно примењује, она ипак садржи неколико аспеката који су „налик директиви", који државама чланицама дају одређени степен флексибилности.

7.2. Скорашњи прописи и друге мере у Шведској

Како се и могло очекивати, кључна скорашња законодавна промена у овој области је ступање на снагу *Опште уредбе о заштити података* (25. маја 2018. године), која је непосредно применљива у Шведској и има предност у односу на шведске прописе.

Национални *Закон о заштити података (2018:218)* допуњује Општу уредбу о заштити података у областима у којима Општа уредба дозвољава изузећа или додатне мере.[158] Кључне одредбе за ову сврху укључују следеће:

- изузеће у случајевима у којима би примена била у супротности са Законом о слободи штампе или Основним законом о слободи изражавања (видети у наставку право на приступ јавним информацијама)
- додатно објашњење правног основа за обраду података (нарочито законске обавезе, као и обављања послова у јавном интересу или вршења законом прописаних овлашћења, што најчешће представља основу за рад локалних власти)[159]
- старосна граница за давање сагласности за обраду података је 13 година
- одредбе које омогућавају обраду осетљивих података у одређеним областима као што су радно право, социјална заштита, здравље и социјална заштита, као и за потребе архивирања и статистике
- ограничење права на приступ подацима, на пример, у случајевима када је обелодањивање података забрањено законом или другим прописом
- кажњавање јавних органа и тела у случају кршења прописа (при чему је максимум 5 милиона евра, у складу са чланом 83. став 4. Опште уредбе о заштити података, односно 10 милиона евра, у складу са чланом 83. став 5. и чланом 83. став 6, тачније половина опште применљивих износа).[160]

Поред наведених, у примени је и *Уредба о заштити података*, која, између осталог, идентификује Шведску агенцију за заштиту података као надзорни

158 *Lag (SFS 2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.* Овим се замењује и ставља ван снаге Закон о заштити података из 1998. године (и Уредба о заштити података), којима је имплементирана Директива ЕУ о заштити података.

159 Закон 2018:218 овде једноставно наводи да се подаци о личности могу обрађивати у складу са чланом 6. став 1. тачка в) Опште уредбе о заштити података „ако руковалац подацима треба да обради податке ради испуњења законске обавезе која проистиче из закона или другог прописа, из колективног уговора или одлуке донесене на основу закона или другог прописа"; или у складу са чланом 6. став 1. тачка д) Опште уредбе о заштити података „ако је обрада неопходна: 1) за обављање послова од јавног интереса који проистичу из закона или другог прописа, из колективног уговора или одлуке донесене на основу закона или другог прописа, или 2) у оквиру вршења јавних овлашћења руковаоца подацима у складу са законом или другим прописом" [незваничан превод]. Предлог Закона 2018:218 (предл. 2017/18:105, од стр. 48) објашњава да се овим испуњава захтев из члана 6. став 3. Опште уредбе о заштити података да законска основа за обраду на основу наведеног почива у закону Уније или државе чланице (што укључује, у смислу шведског модела тржишта рада, законску обавезу из колективног уговора). Нарочито је било потребно (стр. 56) да се изразу „јавни интерес" да шире значење, ако се има у виду да јавни органи не би више могли да се ослањају на „легитимне интересе", као што је био случај у оквиру ранијих прописа..

160 Члан 83. став 7. Опште уредбе о заштити података дозвољава државама чланицама да одреде да ли јавни органи и тела, и до које границе, подлежу административним новчаним казнама. Износи казни утврђени у Шведској представљају половину максималних опште применљивих износа, док су неке друге земље (нпр. Белгија, Француска, Шпанија) изабрале да јавним органима не намећу новчане казне.

орган у складу са Општом уредбом о заштити података и Законом 2018:218.[161] Надлежности Агенције за заштиту података детаљно су описане у Уредби 2007:975 (последњи пут измењена и допуњена 2019. године).[162] Њен општи задатак је да ради на заштити основних људских права и слобода у вези са обрадом података о личности, да омогући слободно кретање тих информација унутар ЕУ и да промовише поштовање добре праксе у кредитном пословању и наплати дуговања. Поред послова дефинисаних у Глави VI Опште уредбе о заштити података и Закону 2018:218, она је и надзорни орган у примени закона о надзорним камерама, закона о обради података о личности од стране безбедносних снага и низа других међународних и инструмената и споразума ЕУ у вези са обрадом и разменом информација.[163]

Постоје још и *сектор̄ски п̄равилници*, који имају предност у односу на Закон о заштити података, али су подређени Општој уредби о заштити података. Они укључују, на пример, Закон о подацима о пацијентима, нови Закон о надзорним камерама (из 2018. године) и велики број прописа којима се уређује евидентирање података о личности код јавних органа (почев од студентских кредита до безбедности крви).

Уопштено говорећи, Општа уредба о заштити података изискивала је минимум промена у другим прописима, бар кад је реч о општинама.[164] У области *образовања*, на пример, држава је анализирала потребе за изменама (на основу званичног упита и одговора од многобројних заинтересованих страна, укључујући *SALAR*, Агенцију за заштиту података и појединачне општине).[165] Донесен је закључак да постојећи прописи омогућавају општинама да као правне основе за обраду података примењују вршење послова у јавном интересу, извршење законом прописаних овлашћења (нпр. у одређивању оцена) или законску обавезу (нпр. информисање родитеља о напредовању деце). У појединим случајевима може се тражити сагласност (нпр. за школске фотографије), мада се шире ослањање на сагласност не саветује због неравнотеже између руковаоца подацима и лица на

161 *Förordning (SFS 2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.*

162 *Förordning (2007:975) med instruktion för Datainspektionen.*

163 Прописи укључују Директиву ЕУ 2016/680 о заштити физичких лица у погледу обраде података о личности коју врше надлежни органи у сврху превенције, истраге, откривања или гоњења кривичних дела или извршења кривичних санкција и о слободном кретању таквих података; Директиву ЕУ 2016/681 о коришћењу података о именима путника (*PNR*) за потребе превенције, откривања, истраге и гоњења кривичних дела тероризма и тешких кривичних дела; споразуме са САД о праћењу финансирања тероризма и спречавања и борбе против криминала; многе друге прописе и одлуке ЕУ о питањима из области Шенгенског информационог система за размену информација о саобраћајним прекршајима. Агенција је такође задужена за испуњавање обавеза из члана 13. Конвенције Савета Европе о заштити појединаца у смислу аутоматске обраде података о личности.

164 Листа допунских предлога прописа може се пронаћи овде (на шведском): *https://www.regeringen.se/regeringens-politik/grundlagar-och-integritet/lagforslag-som-kompletterar-eus-dataskyddsforordning/*.

165 *Behandling av personuppgifter på utbildningsområdet* [Руковање подацима о личности у области образовања], предл. 2017/18:218.

које се подаци односе (Општа уредба о заштити података, члан 43). Свеукупно, мада јавни органи не могу више да користе „легитимни интерес" (Општа уредба о заштити података, члан 6. став 1. тачка ђ) као основу за обраду, локални образовни органи и даље могу да раде оно што је потребно да раде. Измене Закона о образовању су, дакле, биле минималне (нпр. приватне школе су добиле могућност да обрађују осетљиве податке о личности под истим условима као што то могу јавни органи у складу са Законом о заштити података).

Закључак о јавном интересу завређује пажњу јер Општа уредба о заштити података (члан 6. став 3) захтева да јавни интерес има основу у пропису ЕУ или државе чланице. Активности из Закона о образовању јасно имају ту основу. Поред тога, покривене су додатне активности које локалне власти бирају да спроведу, јер Закон о локалној самоуправи наводи да општине могу да делују искључиво у јавном интересу. Ипак, намећу се одређена питања. Општина Стокхолм, на пример, наводи да образовне апликације на бази клауда, које они користе (које су биле предмет заштите података и пре доношења Опште уредбе о заштити података) могу бити у јавном интересу, али да Општа уредба о заштити података ипак од њих захтева да докажу да је обрада ове врсте потребна за постизање њихових циљева.[166]

У области *здравствене заштите*, званичним упитом дошло се до сличног закључка да Општа уредба о заштити података неће ометати обраду података о личности која је и пре била законита. У неким аспектима, Општа уредба о заштити података заиста је флексибилнија у давању изузећа на забрану обраде посебних категорија података о личности (нпр. генетски, биометријски, здравствени подаци) у оквиру система здравствене заштите.[167] Поштовање Опште уредбе о заштити података, наравно, и даље може и јесте административни изазов (видети одељак 1.4), али не би требало да спречи локалне власти да врше обраду података у постизању својих легитимних циљева.

Такође вреди поменути и шведску *Националну стратегију дигитализације*, која позива на већу дигиталну стручност широм јавног сектора, нарочито у социјалним службама.[168] Дигитална безбедност је један од пет циљева, који укључује поменуто прилагођавање националних прописа Општој уредби о заштити података. Влада, као и *SALAR*, подвлачи значај поверења јавности у дигиталне услуге.

---

166 У случају да се ово покаже мање проблематично него што је било очекивано, а Стокхолму је омогућено да настави са коришћењем образовних апликација на бази клауда, под условом да су провајдери из Европске уније. Актуелни спор пред Судом ЕУ о преносу података између ЕУ и САД створио је одређене несигурности у погледу провајдера из САД.

167 Видети следећу интернет страницу, укључујући линкове према званичном упиту и позицији *SALAR*-а: *https://skr.se/ekonomijuridikstatistik/juridik/halsoochsjukvardskolasocialtjanst/halsoochsjukvardsjuridik/halsoochsjukvardsjuridk/dataskyddsforordningenochhalsoochsjukvarden.9501.html.*

168 Министарство за индустрију, *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi* [За одрживо дигитализовану Шведску – стратегија дигитализације], мај 2017. године.

Заштита података и право на приступ јавним информацијама

Поред прописа о заштити података, *Устав Шведске* (члан 6) садржи основно право на заштиту од повреда личне приватности.[169] Такође се примењују релевантне одредбе Европске конвенције о људским правима и Повеље ЕУ о основним правима. Међутим, Уставом се штити и слобода штампе, слобода изражавања и право на приступ званичној документацији. Од приступања ЕУ, Шведска је настојала да осигура да прописи ЕУ о заштити података не буду у супротности са овим уставним правима.[170]

Право на приступ службеним документима је посебно и детаљно уређено у Глави 2 Закона о слободи штампе (и у Уставу). Опште начело је да свако може да приступи документима које поседује и прима јавни орган. Међутим, постоје и одређени изузеци:

- Сматра се да је „скуп информација узетих из материјала евидентираног за аутоматску обраду података" у поседу органа само ако му се може приступити уобичајеним средствима. Даље, не сматра се да је такав скуп у поседу органа власти ако садржи податке о личности (било какве информације које се посредно или непосредно могу повезати са неким појединцем) и орган власти нема законско овлашћење да га учини доступним.
- Други изузетак односни се на тајност. Закон о слободи штампе наводи низ основа за ограничавање приступа званичним документима, ипак само уколико се та ограничења „стриктно наводе" у *Закону о јавном приступу информацијама и тајности података* (или у другом пропису који се позива на овај закон). Међутим, једна од основа је „заштита личних или економских околности појединца", а закон о тајности података заиста наводи велики број ограничења, почев од здравствених услова до списка књига изнајмљених из јавне библиотеке.

Дакле, закон је успоставио равнотежу између права на приступ документима и заштите података о личности. Оно што нови Закон о заштити података (члан 7, став 1) посебно истиче јесте да Општа уредба о заштити података не би требало да оспорава (нити омета) право на приступ службеним документима:

[Општа уредба о заштити података] и овај Закон не примењују се уколико би то било у супротности са Законом о слободи штампе и Законом о слободи изражавања.

Законодавац је сматрао да је ово објашњење важно за пружање сигурности, нарочито ако се има у виду ризик од знатних казнених мера.[171]

---

169 Прописи, који укључују и Устав, доступни су на енглеском језику са коментаром у: *Sveriges Riksdag*, *Ustav Švedske*, 2016.

170 Видети нпр. Patricia Jonason, "The Swedish measures accompanying the GDPR", у: K. Mc Cullagh, O. Tambou i S. Bourton (eds.), *National Adaptations of the GDPR*, Collection Open Access Book, Blogdroiteuropeen, Luxembourg, фебруар 2019. Доступно на: *https://wp.me/p6OBGR-3dP*.

171 Видети предлог новог државног закона о заштити података (предлог 2017/18:105 – *Ny dataskyddslag*), нарочито стр. 40–44 о слободи информација и изражавања.

Упутство Агенције за заштиту података ипак подсећа јавне власти да су у обавези да поштују правила из Опште уредбе о заштити података уколико одлуче да дигитално објаве службена документа. У том случају, потребно је адекватно заштитити личне податке мерама заштите као што је, на пример, енкрипција података.

Поред тога, разлог за тајност података из Закона о јавном приступу информацијама и тајности података је „руковање супротно прописима о заштити података" (укључујући и Општу уредбу о заштити података). Ако тражени материјал садржи нечије личне податке, можда власти треба да установе како лице које тражи информације намерава да их користи да би одредиле да ли те информације могу бити дате или не. Како су одредбе Опште уредбе о заштити података строже у неком погледу, у теорији може бити случај да информације не могу више да се дају, мада досад још нема много практичног искуства у вези с оваквим случајевима. Међутим, уопште узев, Општа уредба о заштити података не даје изговор за даље ограничавање приступа службеним документима.

Упутство Агенције за заштиту података у овој области каже да јавни орган „може да не поставља инвазивнија или бројнија питања него што је потребно за процену тајности" и да „ако се на питања дају конкретни одговори и изјава подносиоца делује веродостојно, треба је прихватити".[172] Припремне активности на изради новог закона о заштити података такође се позивају на одлуку парламентарног омбудсмана, у којој се каже да органи треба да постављају питања само ако постоје конкретне околности које указују да ће прималац руковати подацима супротно прописима, што може бити (осим нечега што подносилац наведе) да се захтев односи на информације о великом броју људи или о изабраним људима са одређеним особинама (на пример, њихов приход или језичка или политичка припадност).[173]

Један пример (у складу са претходним законодавством) јесте случај у коме је суд подржао одлуку јавног органа да не дâ информације које су се односиле на захтев за списак лица којима је онемогућен увид у резултате пријемног испита за упис на факултет због преписивања. Конкретне околности у овом случају биле су да је сличан списак већ био објављен на једном интернет форуму. Захтев је одбијен, иако је подносилац тврдио да му треба списак за личне потребе и да га не би објавио.[174]

---

172 *https://www.datainspektionen.se/vagledningar/for-myndigheter/*.

173 Предлог 2017/18:105 – *Ny dataskyddslag*, стр. 135–136.

174 Број предмета 8316-16, Стокхолмски административни жалбени суд, 12. април 2017. године. Орган је у овом случају био Шведски савет високог образовања, државна установа. Још један детаљ из овог случаја је да је подносилац тврдио да је становник Норвешке, те да не подлеже претходном Закону о заштити података Шведске. То је одбијено као аргумент јер подносилац није могао да докаже норвешко пребивалиште. Међутим, према ранијој судској пракси, да је доставио писани доказ, његова жалба била би успешна. У том смислу, Општа уредба о заштити података мења ствари, јер се она (и допунски шведски прописи) примењује и на руковаоце подацима у трећим земљама.

Јавни органи већ су били у могућности да одбију захтеве од компанија за спискове адреса електронске поште за потребе директног маркетинга, јер се, у складу са постојећим прописима, за тако нешто тражи сагласност онога на кога се подаци односе.[175] Теоретски пример где Општа уредба о заштити података може да закомпликује процену органа о томе да ли дати податке односи се на децу, јер члан 6. став 1. наводи „нарочито где је лице на које се подаци односе дете" у вези са тим да ли основна права могу бити испред легитимних интереса руковаоца подацима. Можемо замислити сценарио у којем компанија која пружа услуге деци захтева податке од локалних органа не за потребе директног маркетинга, већ ради побољшања квалитета или безбедности.

7.3. Мере за подстицање законодавног усаглашавања локалне самоуправе

Агенција за заштиту података је државни орган надлежан за надзор и информисање, а има и саветодавну улогу код тумачења прописа о заштити података. Основно упутство за јавне органе доступно је на интернет страници Агенције (*datainspektionen.se*). Такође постоје и (плаћени) курсеви и конференције, укључујући и обуке за службенике из јавног сектора задужене за послове заштите података и за службенике за заштиту података из приватног и јавног сектора (у децембру 2019. године максимално испуњени, уз учешће 400 полазника). Правници из Агенције доступни су телефоном за савете, а Агенција има циљ да објави и конкретније смернице о питањима која се јављају у истрагама приликом надзора.

Кључни фактор за подстицање усаглашености јесте то што се Агенција показала вољном да истражи кршење прописа о заштити података о личности у локалним самоуправама, уз ризик од потребе за изрицањем укора или чак знатних новчаних казни (видети одељак 1.5).

SALAR својим члановима обезбеђује опсежна упутства о примени Опште уредбе о заштити података и релевантних домаћих прописа. Једна од страница на интернет презентацији *SALAR*-а садржи следеће:[176]

- кратки филм (минут и по) са прегледом Опште уредбе о заштити података
- дигитални курс о основама Опште уредбе о заштити података; он траје око пола сата и састоји се од низа кратких филмова, текстова и квиза, којима се промовише основна информисаност међу запосленима у локалној самоуправи

175 Број предмета 5553-15, Гетеборшки административни жалбени суд, 2015-11-06.

176 *https://skr.se/ekonomijuridikstatistik/juridik/offentlighetsekretessarkiv/dataskyddsforordningengdpr.13023.html.*

- страницу са питањима и одговорима, коју правни стручњаци *SALAR*-а непрестано ажурирају кроз одговоре на питања која добијају од чланова; ова страница је у време писања овог извештаја садржала око 50 тема, које се крећу од руковања електронском поштом до тога да ли вртићи треба да имају службеника за заштиту података или не
- линкове на десет информативних кампања; они иду дубље у, на пример, улогу службеника за заштиту података (укључујући и контролну листу за ангажовање); специјализоване теме, као што су е-здравље, становање и школски сервиси на бази клауда; мрежа (или дигитални простор за сарадњу) у оквиру које чланови могу да размењују искуства о питањима у вези са Општом уредбом о заштити података.

У оквиру асоцијације и њених друштава, *SALAR* такође управља групом у оквиру које се размењују искуства о *уговорима са обрађивачима података* (нпр. компаније за ИТ подршку у обради или чувању података о личности). *SALAR* је израдио стандардни уговор и контролну листу о томе шта такви уговори треба да садрже (у складу са чланом 28. Опште уредбе о заштити података).

Мада наведене смернице из *SALAR*-а чине знатан материјал, приступ на путу ка ступању на снагу Опште уредбе о заштити података ипак је био селективан – изабрано је да пажња буде усмерена на најважнија питања, а не на покушаје (највероватније узалудне) да се покрије сваки појединачни аспекат.

Из ограниченог броја спроведених разговора, смернице *SALAR*-а су добро примљене. На пример, већи број локалних органа недвосмислено користи контролне листе *SALAR*-а приликом ангажовања службеника за заштиту података (видети уоквирени текст у наредном одељку). У исто време, потреба за обуком јасно превазилази смернице које *SALAR* или Агенција могу да пруже. Неке локалне власти би волеле да *SALAR* понуди више образаца и стандардних процедура.

Правници из *SALAR*-а у радно време дају савете и путем телефона. Овим послом баве се три саветника специјализована управо за ову област, а послови у вези са Општом уредбом о заштити података чине око 20–30% њиховог времена проведеног у телефонским разговорима.

Један од најважнијих фактора у осигурању законодавне усаглашености, који подвлаче стручњаци из *SALAR*-а и Агенције, јесте *укљученост руководства*. Руководство мора схватати сложеност прописа о заштити података и давати јасна упутства запосленима у организацији како би се успоставиле делотворне рутине.

SALAR и *Inera*, друштво у власништву *SALAR*-а које пружа „заједничка дигитална решења" и помаже у усмеравању послова локалних власти, у непрестаним је консултацијама и дијалогу са Агенцијом за заштиту података. Агенција је (у свом извештају за 2018. годину) истакла да дијалог са кључним актерима, као што је овај, види као важан део свог посла на спречавању озбиљних ризика за лични интегритет.

7.4. Припреме на локалном нивоу

Поштовање Опште уредбе о заштити података и релевантних домаћих прописа јасно се показало као знатна административна препрека за многе локалне самоуправе. Оно је довело и до додатних трошкова (нпр. за прилагођавање ИТ система и ангажовање службеника за заштиту података), а често и до периода неизвесности пре обликовања јасних процедура. Без намере да буду исцрпне, у наставку су наведене неке од кључних тема које су се јавиле у разговорима.

- Правни основ. Иако је (као што је већ наведено) држава покушала да разјасни то питање у свом припремном раду, потреба да се унапред одреди правни основ за сваку сврху обраде података још увек изазива забуну. На пример, неки локални званичници се питају да ли се и даље могу позивати на „легитимне интересе" (као у претходном законодавству); Општа уредба о заштити података предлаже да се то не односи на јавне органе, мада то остаје да се испита на суду. За свакодневне активности, као што је администрација особља, јавни интерес остаје одговарајућа правна основа према смерницама *SALAR*-а.
- Прелазак са пасивне на активну заштиту. Руковаоци подацима морају се придржавати не само начела Опште уредбе о заштити података, већ морају и бити у стању да покажу усаглашеност. Један од начина за то је усвајање кодекса понашања, интерних смерница или стандардних процедура. Друго (посебно важно у случају високоризичне обраде) јесте употреба алата наведених у Поглављу IV Опште уредбе о заштити података, укључујући процену утицаја и претходне консултације са надзорним органом.
- Прекид примене „правила злоупотребе" за електронску пошту, интернет странице и слично. Претходно законодавство у Шведској (имплементирајући Директиву о заштити података) дозвољавало је изузеће за обраду података у „неструктурираном материјалу" (као што су електронска пошта или непрекидни текстови објављени на интернету) све док то не нарушава приватност дотичне особе. Другим речима, обрада би подлегала закону само у случају злоупотребе. По Општој уредби о заштити података, то више није случај. За електронску пошту и слично, као и за друге врсте обраде, руковаоци подацима морају бити унапред јасни у навођењу сврхе, правног основа, поступка у случају жалбе и томе слично. Ово је за неке службенике за заштиту података била једна од најтежих области са којом се у пракси сусрећу.
- Уговори са трећим обрађивачима података, као што су пружаоци ИТ услуга. Питања о томе су међу најчешће постављаним питањима саветницима из *SALAR*-а. Они се крећу у опсегу од тога да ли директор ИТ службе може закључити такав уговор за све активности у општини, до тога да ли регион

може приступити подацима о пацијентима из приватних здравствених картона који се чувају у регионалном систему. Посебну главобољу задала је неспремност пружалаца услуге да прихвате услове прописане чланом 28. Опште уредбе о заштити података. Чак и тамо где локалне власти користе обрасце *SALAR*-а, неки пружаоци услуге желе да преговарају о додатним клаузулама како би ограничили своју одговорност или обезбедили додатну накнаду.

- Несигурност у вези са интерним процедурама. Многа питања из делокруга Агенције за заштиту података потичу не од службеника или од координатора за заштиту података, већ од других запослених и тичу се основних аспеката питања „да ли нам је дозвољено да то урадимо?" – што би требало да буде јасно из политике и рутине у заштити података у тој организацији. Од маја 2018. године примећена су одређена побољшања: на пример, многе прве пријаве кршења заштите података односе се на погрешно упућене дописе, који се (све док не откривају ништа осим контакт података) не морају пријављивати. Ипак, ово још више указује на потребу за подизањем нивоа свести и успостављањем јасних процедура у целој организацији.
- Раздвајање улога службеника и координатора за заштиту података (или слично). Према претходном законодавству, службеник за личне податке био је одговоран за праћење поштовања, али често и за мере заштите података у организацији. Строго говорећи, то више није дозвољено Општом уредбом о заштити података, што јасно указује на то да службеник за заштиту података мора бити у стању да делује независно и, мада може имати и друге задатке, они не смеју довести до сукоба интереса. Заправо, неки службеници за заштиту података виде своју улогу више као продужену руку Агенције за заштиту података. *SALAR* препоручује да се одреди посебан координатор, чија ће општа одговорност бити заштита података, што у пракси често значи да службеник за заштиту података мора бити запослен или ангажован по уговору о делу (видети уоквирени текст у наставку).

Ангажовање службеника за заштиту података

SALAR је израдио контролну листу (у форми нацрта огласа за посао) за радно место службеника за заштиту података у локалној власти.[177] Опис посла обухвата проверу да ли се личним подацима рукује на коректан и законит начин, информисање и давање савета о Општој уредби о заштити података и релевантним прописима, као и функцију контакт особе за комуникацију са надзорним органом и регистрованим лицима. Службеник за заштиту података би требало да има независну улогу у организацији и да извештава руководство. Специфични задаци су детаљно описани.

Што се тиче квалификација, Општом уредбом о заштити података захтева се да се службеник за заштиту података „ангажује на основу стручних квалитета, нарочито стручног знања о закону и пракси заштите података, и на основу способности за испуњавање [потребних] задатака." *SALAR*-ова контролна листа наводи диплому правног факултета или еквивалентну универзитетску диплому, вишегодишње искуство у самосталном раду у области права, добро познавање Опште уредбе о заштити података и других прописа, по могућности, са искуством на пословима заштите података или на другој релевантној позицији.

Мада су неки службеници за податке о личности према претходном законодавству били у могућности да наставе у новој улози службеника за заштиту података, Општом уредбом о заштити података, као што је већ речено, ипак се траже посебни координатори за заштиту података (или слично). Стога је јасно да је Општа уредба довела до запошљавања у већини локалних власти. Поједини службеници за заштиту података запослени су у локалним властима, мада се ова улога често дели са другим задужењима (нпр. осим као службеник за заштиту података, ради и као правни саветник, архивар, стручњак за ИТ). Поједини су ангажовани на основу уговора о делу, чак и у општинама средње величине, као што је Лидинго код Стокхолма (где улога службеника за заштиту података узима око 20 сати месечно).

Запошљавање службеника за заштиту података било је тешко у време када је Општа уредба ступила на снагу, посебно тамо где је било потребно ангажовање за само половину радног времена. Неке општине су се одлучиле да деле једног службеника. На пример, седам од осам општина које формирају асоцијацију општина у области Борас одлучило је да именује два заједничка службеника за заштиту података. Чак и Сундсвал (око 99.000 становника) дели једног службеника са још две општине. Мада заједнички службеници могу бити мање упознати са унутрашњом организацијом локалних власти за које раде, једна од предности овог аранжмана је та што они могу да заштити података посвете пуно радно време и да преузму независну улогу ревизора и саветника.

С друге стране, највећим општинама можда је потребно неколико службеника за заштиту података; Гетеборг, на пример, има 13 службеника за различита одељења као што су образовање, саобраћај, животна средина и слично или друштва у власништву општине.

Општа уредба о заштити података по много чему представља позив за буђење локалних власти чије се активности у великој мери ослањају на обраду података о личности. То не значи да је претходно законодавство олако схватано, али

177 *https://skr.se/download/18.2ced2eb215cc46662ca11a03/1498030806732/förslag%20på%20jobbannons%20för%20dataskyddsombud.pdf*

Општа уредба захтева строжи приступ у дефинисању сврхе прикупљања података, ограничавајући га на оно што је неопходно, уз идентификовање правног основа, поштовање права лица на која се подаци односе, вођење регистра о обрадама података и слично.

Разговори сугеришу да је потпуно усаглашавање процеса у току, што можда и није изненађујуће с обзиром на то да неке локалне власти баратају стотинама различитих ИТ система (неке од њих је потребно надоградити) и да се ради о хиљадама запослених. Највећи изазов неких службеника и координатора за заштиту података је уградити ову нову културу у велику организацију и обезбедити да је сви прихвате.

Један једноставан пример: у прошлости је било природно да одељења за људске ресурсе задржавају пријаве за посао, укључујући и оне које доставе кандидати који нису примљени, у случају да се појаве нова слободна радна места. Ступањем на снагу Опште уредбе о заштити података то више није лако оправдати. Приступ у једној локалној власти је да пријаве задржава на рок од две године на основу законске обавезе, у случају покретања спора у вези са дискриминацијом (за који је рок застаревања две године), након чега се подаци бришу.

Међутим, широко говорећи, локалне власти кажу да могу да обављају исте врсте обраде података као и пре Опште уредбе, све док се ради о законитим обрадама и док се поштују горе наведени захтеви.

Што се тиче *координатора за заштиту података* (или представника и слично), типичан аранжман је ангажовање једног координатора у седишту општинске управе са општом одговорношћу, а затим још неколико у различитим оперативним одељењима или друштвима. Ове последње набројане улоге у многим случајевима неће чинити више од 20–25% радног времена запосленог, али то се често додаје на постојеће задатке који већ чине 100%! Неки централни координатори примећују различите степене укључености или интересовања оперативних координатора, као и потешкоће у убеђивању руководства да издвоји довољно времена. Међутим, чак и када би било могуће додатно запошљавање, новоангажовано лице би се морало упознати са четири или пет различитих послова, што би такође могло бити проблематично.

Када је реч о *обуци*, јасан закључак из свих разговора и смерница је да особљу на свим нивоима треба непрестано усавршавање, а најчешћи узрок пропуста у заштити података је људски фактор. Службеници за заштиту података имају одређену одговорност за информисање и едукацију колега. Неке локалне власти су уговориле екстерне тренере или прилагодиле електронске курсеве својим потребама. Једно од питања је како пратити које курсеве су запослени похађали, јер службеници за заштиту података треба да имају преглед обука ради осигурања квалитета и доказивања усаглашености. Обуке које су се одржавале пре ступања на снагу Опште уредбе такође су важне. Општина Сундсвал је, на пример, организовала класичну обуку за око 600 запослених, као и проширени интернет курс за око 1000 запослених.

За сада не постоје националне шеме сертификације (било у смислу члана 42. Опште уредбе о заштити података, било другачије). Многе образовне институције и друге организације развиле су курсеве који резултирају сертификацијом службеника за безбедност података (нпр. *IFU* при Економској школи у Стокхолму, или Шведско рачунарско друштво, удружење стручњака за ИКТ). Неколико универзитета такође има курсеве за информациону безбедност. Шведски институт за стандардизацију, између осталог, има обуку за помоћ организацијама у прибављању сертификата *ISO 27000* (нпр. *ISO 27001* за системе управљања информационом безбедношћу, користан за испуњавање захтева из Опште уредбе). Поједини службеници за безбедност података у неким локалним самоуправама стекли су сертификате у другим земљама (нпр. у Канади).

Упитани за савет, практично сви саговорници истичу значај подизања нивоа свести, систематског рада и изградње културе заштите података. Ово захтева време и може бити тешко изводљиво у контексту текућих послова. Заштита података требало би да буде одвојена, и да се њоме бави на исти начин на који се бави буџетом или родном равноправношћу, кроз јасне процесе уграђене у систем. На почетку, замка коју треба избећи је непотребно фокусирање на ИТ системе, што може довести до превида важних аспеката (као што су брига о документацији или информисање лица на које се подаци односе). Пре се треба усредсредити на основна начела Опште уредбе о заштити података. Помоћ споља или искусни координатор са пуним радним временом могу бити непроцењиви у успостављању првих политика и рутина, као и у пружању подршке особљу у раним фазама имплементације. Још један практични савет је престанак коришћења *USB*-ова, који стоје иза многобројних пропуста у заштити података који су се лако могли избећи.

7.5. Примери добре и лоше праксе на локалном нивоу

Тешко је у овој области наћи дефинитивне примере добре праксе, јер је пажња наравно усмерена на прекршаје. Агенција за заштиту података, као ни *SALAR* нису могли да идентификују узорне примере, тако да се морамо задовољити укупним искуством локалних власти наведеним у претходном одељку.

Када је реч о проблематичним примерима, општина Скелефта је у августу 2018. године постала прва у Шведској која је кажњена у складу са Општом уредбом о заштити података у износу од 200.000 SEK (око 20.000 евра). Локална средња школа спровела је пилот-пројекат користећи технологију препознавања лица како би пратила присуство ученика. Мада је локални просветни одбор добио сагласност од ученика који су учествовали у пројекту, Агенција за заштиту података је утврдила да то није валидна правна основа, с обзиром на неравнотежу између руковаоца подацима и лица на која се подаци односе. Други кључни

фактор био је пропуст да се спроведу процена утицаја или претходне консултације са Агенцијом (у складу са члановима 35–36. Опште уредбе у високоризичним случајевима). Општина Скелефта је уложила жалбу на одлуку.

У току је још неколико истрага Агенције за заштиту података у локалним самоуправама:

- Регион Стокхолма, Сормланда и Вармланда о подацима о личности приликом давања здравствених савета (овај случај је покренут након медијских објава да су на интернету јавно доступни снимци 2,7 милиона осетљивих позива према регионалној телефонској служби за давање савета у области здравствене заштите)
- Просветни одбор Стокхолма у вези са правом приступа школског особља личним подацима ученика
- Регион Упсале у вези са преносом података о пацијентима без енкрипције.

Агенција за заштиту података објављује редовне извештаје о *пријављеним кршењима заштите података о личности*. У периоду од јануара до септембра 2019. године, локалне власти су направиле 12% свих пријављених пропуста, здравство 14%, школство 10%, а социјалне службе 9%. Како школе и здравство најчешће припадају општинама и регионима, локалне власти дакле чине до 45% свих пријављених пропуста. Јавни сектор у целини чини готово две трећине укупних пропуста.

Висока учесталост може бити делом приписана релативно марљивом извештавању, мада саговорници сугеришу да још увек постоји одређен степен недовољног извештавања. Многи пријављени пропусти су безначајни (нпр. погрешно адресирана писма). Најважније за локалну спремност јесте то да је више од половине пријављених инцидената (51%) последица људског фактора. Следећи најчешћи узрок су технички проблеми (15%), затим злонамерни напади (13%) и пропусти у организационим рутинама и процесима (12%).

У мају 2019. године, Агенција за заштиту података објавила је свој први *Национални извештај о интегритету*, годину дана након ступања на снагу Опште уредбе о заштити података.[178] Закључено је да су општине и региони прекомерно заступљени међу организацијама који се суочавају са већим изазовима и у мањој су могућности да континуирано и систематски раде на интегритету и заштити података.

Ови налази засновани су делимично на анкетама обављеним са службеницима за заштиту података. Међу највећим изазовима са којима се сусрећу запослени у општинама и регионима су потешкоће у успостављању функционалних рутина и процеса, затим перцепција правила о заштити података као опструкције, и застарели ИТ системи који компликују њихов рад. Седам од десет службеника

178 Datainspektionen, Nationell integritetsrapport 2019. Datainspektionens rapport 2019:2 (Стокхолм, мај 2019).

за заштиту података у општинама и регионима изјавило је да су укључивани у пројекте или друге активности са доношењем одлука са импликацијама за заштиту података никада, ретко или тек понекад. Само три од десет службеника изјавило је да је руководство образовано и стручно у питањима заштите података.

8. ПРИЛОЗИ

8.1. Прилог 1: Упитник за анализу утицаја европских интеграција на локалну самоуправу у Србији у области заштите података о личности и слободног приступа информацијама од јавног значаја (део преговарачког поглавља 23 – правосуђе и основна права)

Стална конференција градова и општина – Савез градова и општина Србије (СКГО) приступила је изради серије студија којима се испитује утицај европских интеграција на локалну самоуправу у Србији. Студије су тематске, према подели материје европског законодавства и политика по преговарачким поглављима у процесу приступања. Циљ је сагледавање надлежности локалне самоуправе у тематским областима, капацитета за спровођење законодавства и политика ЕУ у њима, као и дефинисање препорука за локалну самоуправу, републичке власти и СКГО у процесу преговора. Овај упитник односи се на део материје преговарачког поглавља 23 – област заштите података о личности и слободног приступа информацијама од јавног значаја.

Експерт:
Ана Тоскић
извршна директорка, Партнери за демократске промене Србија

Молимо Вас да упитник попуни особа која је у Вашој општини или граду задужена за послове у области заштите података о личности и приступа информацијама од јавног значаја.
Молимо Вас да електронски попуните овај упитник – „болдирањем" одговора **ДА** или **НЕ**, као и да одговоре на додатна питања откуцате у простору који је за то предвиђен.

ОПШТИНА или ГРАД: _____
Попунио/-ла: _____
(име и презиме, функција)
Датум и место: _____

Скраћенице које се користе у овом упитнику:
ЈЛС Јединица локалне самоуправе
ЗЗПЛ Закон о заштити података о личности
Повереник Повереник за информације од јавног значаја и заштиту података о личности

1. Да ли је неким интерним актом ЈЛС уређена област заштите података о личности?
   а) ДА б) НЕ
   Уколико јесте, молимо Вас да наведете о ком се акту ради_____.

2. Да ли је Ваша ЈЛС именовала лице овлашћено за заштиту података о личности?
   а) ДА б) НЕ
   Уколико је Ваш одговор НЕ, да ли постоји друга особа у оквиру ЈЛС задужена за питања заштите података о личности?
   а) ДА б) НЕ
   Уколико таква особа постоји, молимо наведите њену позицију у систематизацији ЈЛС _____, као и нека од њених задужења: _____
   _____.

3. Да ли су запослени у ЈЛС учествовали на обукама у области заштите података о личности?
   а) ДА б) НЕ
   Уколико јесу, молимо наведите ко је спроводио/организовао обуку _____
   _____.

4. Да ли Ваша ЈЛС поседује неки од сертификата за заштиту података (нпр. сертификат *ISO 27000* или *ISO 27001*)?
   а) ДА б) НЕ
   Уколико поседује, молимо наведите о ком се сертификату ради: _____.

5. Да ли су запослени у ЈЛС на други начин упознати са обавезама и правима из ЗЗПЛ (обавештења, промотивне брошуре и сл.)?
   а) ДА б) НЕ
   Уколико јесу, молимо наведите на који начин су били упознати _____
   _____.

6. Да ли су запослени у Вашој ЈЛС потписали изјаву о поверљивости података са којима долазе у контакт током свог рада?
   а) ДА б) НЕ

7. Да ли је одређеним интерним актом ближе прецизиран начин поступања са пристиглим захтевима за остваривање права у погледу обраде података о личности?
   а) ДА б) НЕ

8. Које лице је у оквиру Ваше ЈЛС задужено за одговоре на захтеве грађана на основу ЗЗПЛ (наведите радно место тог лица)?
   _____.

9. Да ли су Вашој ЈЛС до сада упућивани захтеви грађана за остварење права на основу заштите података о личности?
   а) ДА б) НЕ
   Уколико јесу, молимо Вас наведите број оваквих захтева примљених у 2018. години _____

10. Да ли је Ваша ЈЛС била предмет надзора Повереника за информације од јавног значаја и заштиту података о личности, а у вези са применом Закона о заштити података о личности?
    а) ДА б) НЕ

11. Да ли је Ваша ЈЛС била предмет жалбеног поступка пред Повереником, а у вези са применом Закона о заштити података о личности?
    а) ДА б) НЕ

12. Да ли је Ваша ЈЛС, тј. овлашћено лице у ЈЛС, била предмет судског поступка у вези са применом Закона о заштити података о личности?
    а) ДА б) НЕ

13. Да ли су запослени у Вашој ЈЛС имали прилике да на други начин контактирају са Повереником поводом питања у области ЗЗПЛ?
    а) ДА б) НЕ
    Уколико је одговор на претходно питање ДА, молимо наведите на који начин су запослени у Вашој ЈЛС били у контакту са Повереником: _____
    _____.
    Уколико је одговор на питање бр. 13 ДА, молимо наведите да ли сте од Повереника добили одговоре на постављена питања.
    а) ДА б) НЕ

14. Да ли су неким интерним актом ЈЛС прописане мере заштите података о личности од злоупотреба, уништења, губитка, неовлашћених промена или приступа?
    а) ДА б) НЕ
    Уколико јесу, молимо наведите о ком се акту ради _____.

15. Да ли Ваша ЈЛС примењује неке од следећих мера заштите података о личности:

Анонимизација података[179]	ДА	НЕ
Псеудонимизација података[180]	ДА	НЕ
Ауторизовани приступ запослених електронским базама/подацима	ДА	НЕ
Контролисани приступ запослених *hard copy* базама/подацима	ДА	НЕ

16. Да ли Ваша ЈЛС води евиденцију радњи обраде података о личности?
    а) ДА б) НЕ

17. Да ли Ваша ЈЛС води евиденцију о томе ко је и када имао увид у одређене збирке личних података?
    а) ДА б) НЕ
    Уколико је одговор на претходно питање ДА, молимо наведите на који начин се води ова евиденција приступа (нпр. евидентирање логова на рачунарској мрежи, коришћење електронских картица или потписивање запослених при уласку у просторије у којима се чувају штампане/*hard copy* евиденције итд..).
    _____.

179 Анонимизација је радња обраде података о личности садржаних у одређеном документу или збирци података, којом лице на које се подаци односе престаје да буде одредиво. Анонимизација се спроводи тако да осујети повратну идентификацију (реидентификацију) лица чији се подаци анонимизују, чак и уколико се предузму одређене мере попут укрштања или спајања информација са информацијама доступним из других извора.

180 Псеудонимизација је обрада на начин који онемогућава приписивање података о личности одређеном лицу без коришћења додатних података, под условом да се ови додатни подаци чувају посебно и да су предузете техничке, организационе и кадровске мере које обезбеђују да се податак о личности не може приписати одређеном или одредивом лицу.

18. Да ли Ваша ЈЛС користи опрему за видео-надзор?
    а) ДА б) НЕ
    Уколико користи, да ли је неким интерним актом прецизирано на који начин се снимљени материјал користи:
    а) ДА б) НЕ
    Молимо Вас да наведете лице (наведите назив радног места) које има приступ видео-записима: _____.
    Молимо Вас да наведете који је рок за брисање видео-записа: _____
    _____.

19. Молимо наведите (заокружите 1 од понуђених одговора) ко је одговоран за одржавање рачунарских система Ваше ЈЛС?
    а) интерни ИТ стручњак б) екстерни ИТ стручњак
    ц) друго _____ (наведите)

20. Сервери на којима Ваша ЈЛС похрањује податке налазе се (заокружите 1 од понуђених одговора):
    а) у Републици Србији
    б) у иностранству _____ (молимо наведите земљу)

21. Да ли су у буџету Ваше ЈЛС опредељена средства за унапређење капацитета за заштиту података?
    а) ДА б) НЕ
    Уколико је Ваш одговор ДА, молимо наведите о ком износу средстава се ради
    _____.

22. Да ли сте упознати са чињеницом да је у Србији усвојен нови Закон о заштити података о личности („Службени гласник РС”, број 87/2018)
    а) ДА б) НЕ

23. Молимо Вас, оцените спремност Ваше ЈЛС за примену новог Закона о заштити података о личности.
    1 – у потпуности смо неспремни,
    2 – неспремни смо,
    3 – делимично смо спремни,
    4 – спремни смо,
    5 – у потпуности смо спремни.

24. Да ли сматрате да је запосленима у Вашој ЈЛС потребна додатна подршка за унапређење капацитета у области ЗЗПЛ?
    а) ДА б) НЕ
    Уколико је Ваш одговор ДА, молимо наведите каква врста подршке би била потребна (можете заокружити више од једног одговора):
    а) обуке лица овлашћених за заштиту података
    б) обуке запослених о правним аспектима заштите података
    в) обуке запослених о техничким аспектима заштите података
    г) унапређење техничких мера за заштиту података
    д) услуге саветовања за потребе усклађивања интерних аката са новим ЗЗПЛ
    ђ) друго _____(молимо Вас, наведите)

8.2. Прилог 2: Преглед ЈЛС које су учествовале у анкети за потребе Анализе капацитета јединица локалне самоуправе за усклађивање са новим правним оквиром за заштиту података о личности

РБ	ЈЛС	ВРСТА	РАЗВИЈЕНОСТ (ГРУПА)	РЕГИОН
1	Гроцка	Градска општина	I	Београд
2	Ваљево	Град	I	Шумадија и Западна Србија
3	Вождовац	Градска општина	I	Београд
4	Бачка Паланка	Општина	I	Војводина
5	Суботица	Град	I	Војводина
6	Кикинда	Град	II	Војводина
7	Пирот	Град	II	Јужна и Источна Србија
8	Бољевац	Општина	III	Јужна и Источна Србија
9	Трстеник	Општина	III	Шумадија и Западна Србија
10	Шид	Општина	III	Војводина
11	Бујановац	Општина	IV	Јужна и Источна Србија
12	Тутин	Општина	IV	Шумадија и Западна Србија
13	Љиг	Општина	IV	Шумадија и Западна Србија
14	Опово	Општина	IV	Војводина

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

339.5.012.42(4-672EU)
339.923(4-672EU:497.11)
352(497.11)
342.738(497.11)

ТОСКИЋ, Ана, 1981-
Анализа утицаја процеса европских интеграција на локалну самоуправу у Србији у области заштите података о личности и приступа информацијама од јавног значаја (део преговарачког поглавља 23-правосуђе и основна права) / Ана Тоскић, Маја Стојановић Керић, Дејвид Јанг. - Београд : Стална конференција градова и општина - Савез градова и општина Србије, 2020 (Београд : Досије студио). - 119 стр. : граф. прикази ; 24 cm

Тираж 300. - Abstract. - Напомене и библиографске референце уз текст.

ISBN 978-86-80480-07-7

1. Стојановић Керић, Маја, 1980- [аутор]
а) Европска унија -- Придруживање -- Србија
б) Локална самоуправа -- Србија в) Право на заштиту података о личности -- Србија

COBISS.SR-ID 14050313

Стална конференција
градова и општина

Савез градова и општина Србије

Македонска 22/VIII
11000 Београд
Србија

Тел: 011 3223 446
Факс: 011 3221 215
E-mail: secretariat@skgo.org

www.skgo.org
www.facebook.com/skgo.sctm
www.twitter.com/skgo_sctm

ISBN 978-86-80480-07-7