

Росана Лемут-Стрле
Невена Ружић

**АНАЛИЗА
ЗАШТИТЕ ПОДАТАКА
У РАДНИМ ОДНОСИМА**
Одабране теме

Београд, 2023.

Издавач

Повереник за информације од јавног значаја и заштиту података о личности у сарадњи са пројектом "Подршка јачању владавине права у Србији", заједнички финансираним од стране Европске уније и немачког Савезног министарства за економску сарадњу и развој (BMZ), за чије спровођење је задужен Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ)

Ауторке:

Росана Лемут-Стрле
Невена Ружић

Дизајн и прелом:

Арт Спот, Горњи Милановац

Штампа

Финеграф, Београд

Тираж

150 примерака

ISBN-978-86-82712-02-2

**ПОВЕРЕНИК**

ЗА ИНФОРМАЦИЈЕ
ОД ЈАВНОГ ЗНАЧАЈА
И ЗАШТИТУ ПОДАТАКА
О ЛИЧНОСТИ



**#ЕУ
ЗА ТЕБЕ**

Израда публикације подржана је од стране пројекта „Подршка јачању владавине права у Републици Србији“, заједнички финансираног од стране Европске уније и Савезног министарства за економску сарадњу и развој Савезне Републике Немачке (BMZ), а који спроводи Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). Њен садржај не одражава нужно ставове Европске уније, немачког Савезног министарства за економску сарадњу и развој (BMZ), нити GIZ-а.

Садржај

Уводна реч	5
Сажетак.....	7
О обради података о личности у радним односима.....	9
Заснивање радног односа	29
Правни оквир	29
Из праксе Повереника	32
Правни оквир и пракса Савета Европе и Европске уније	39
Општи захтеви заштите података о личности у поступку запошљања	39
Питање обраде осетљивих података о личности с друштвених мрежа	42
Коришћење средстава за аутоматско доношење одлука у поступку запошљања.....	44
Вагање између интереса послодавца и основног права на поштовање приватности у поступку избора кандидата за посао	45
Препоруке за усклађивање	46
Узбуњивање	49
Правни оквир.....	49
Из праксе Повереника	51
Правни оквир и пракса Савета Европе и Европске уније.....	53
Препоруке за усклађивање	55
Видео надзор.....	57
Правни оквир.....	57
Из праксе Повереника	59
Правни оквир и пракса Савета Европе и Европске уније.....	68
Препоруке и ограничења при употреби видео-надзора у радним просторијама	68
Допуштеност видео-надзора са аспекта права на поштовање приватног живота запослених у пракси Европског суда за људска права.....	72
Препоруке за усклађивање	75
Употреба информационих-комуникационих технологија.....	77
Правни оквир.....	77
Из праксе Повереника	79
Правни оквир и пракса Савета Европе и Европске уније.....	97
Праћење активности запослених на службеним уређајима за електронску комуникацију	97
Надзор над употребом службеног аутомобила (GPS подаци)	103
Право на приватност и нове праксе рада на даљину односно рада од куће	106
Препоруке за усклађивање	108
Изабрани извори.....	109

Уводна реч

Скоро читав један олимпијски циклус од четири године протекао је од истека рока (31.12.2020. године) за усклађивање одредаба свих закона које се односе на обраду података о личности са одредбама Закона о заштити података о личности, што је као обавеза прописано у члановима 2. и 100. овог закона. Рок за испуњење ове обавезе, нажалост, упркос бројним апелима од стране Повереника, није промењен али то не значи да је обавеза усклађивања закона престала да постоји. Напротив. Срећом, пројекат „Подршка јачању владавине права у Републици Србији“, уз подршку Европске уније и Савезног министарства за економску сарадњу и развој (БМЗ) Савезне Републике Немачке а који спроводи Немачка организација за међународну сарадњу (ГИЗ), препознао је изузетан значај који усаглашавање законских одредаба о обради података о личности са Законом о заштити података о личности, као крунским у овој области људских права, има за заштиту овог, како време протиче све актуелнијег, права грађана. Тако је настала и ова публикација чије ауторке су доказане експерткиње у материји заштите података о личности. И добро је што се анализа из ове публикације односи управо на област рада и радних односа и то из два разлога: прво, зато што су бројни закони и други прописи у овој области који садрже одредбе о обради података о личности и који би морали да буду усклађени са Законом о заштити података о личности, и друго, обрада података о личности у области рада је посебно осетљива како због обима тако и због врсте података који се обрађују. При овоме, нарочито треба имати у виду да између послодаваца, и потенцијалних послодаваца када се ради о поступку запошљавања, и запослених, односно кандидата за посао, не постоји равнотежа снага и моћи, пошто је запослени у незавидном положају у односу према послодавцу код којег остварује егзистенцију. Управо из тог разлога потребно је посебну пажњу посветити заштити приватности и података о личности запослених и радно ангажованих лица, нарочито у времену у којем живимо, о будућем и да не говоримо, које послодавцима пружа све софистициранија средства за обраду података о личности, нарочито оних података који су посебно осетљиви. Из свих наведених разлога, могу са задовољством да констатујем да је ова публикација урађена у правом тренутку и да ће њен садржај бити од изузетне користи приликом вршења анализе од стране органа надлежних за измене појединих закона у циљу њиховог усаглашавања са Законом о заштити података о личности и топло је препоручујем свим заинтересованима.

*Повереник
Милан Мариновић*

Сажетак

Заштита података о личности тема је која се прожима кроз све друштвене односе. Усвајање Опште уредбе о заштити података о личности Европске уније, а посебно имајући у виду њене одредбе које се односе на примену правила и ван територије ЕУ, односно њених држава чланица, као и висину управних мера које се могу изрећи, имало је за резултат да су прописи других земаља писани по узору на Општу уредбу, али и да тема заштите података о личности добије на значају.

Готово **идентично** као и Општа уредба о заштити података о личности, Закон о заштити података о личности Републике Србије посебно издваја обраду података о личности у области рада и запошљавања. Како је то прописано чланом 91. Закона, на обраду података о личности у овој области примењују се одредбе закона којима се уређује рад и запошљавање и колективни уговори уз примену Закона. Посебно је истакнуто да ови прописи (дакле, закони и колективни уговори) морају, поред одредаба које се односе на обраду података, да садрже и посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на, између осталог, систем надзора у радној средини.

Чланом 100. Закона прописана је обавеза усклађивања других закона са овим законом у делу који се односи на обраду података о личности до краја 2020. године. Ипак, многи закони нису усклађени са Законом о заштити података о личности до краја писања ове анализе. Ова опсервација се односи и на прописе у области радних односа. Већина њих усвојена је више година пре усвајања овог закона, па се оцена усклађености може односити и на лексичко питање будући да се у многим прописима користи термин лични податак, а не податак о личности.

Прописа у области радних односа има на претек. Поред прописа који се у базама прописа групишу у оне који се односе на радне односе, и други прописи дотичу ове односе. Такав је пример са законима који уређују различите области друштвеног живота, а садрже одредбе о условима које треба да испуњава лице за обављање тих послова.

Стога, имајући у виду обим радног права, као и појединачних тема које се тичу радних односа, за потребе приказа заштите података о личности у области радних односа определиле смо за поједине теме као што су обрада података о кандидатима за запослење, затим обрада

података у вези са узбуњивањем, као и обрада података употребом видео надзора и информационих технологија, а уз сагласност Повереника за информације од јавног значаја и заштиту података о личности. У оквиру ове публикације приказани су и случајеви из праксе Повереника у вези са одабраним темама. „ У погледу одабраних тема усвојен је јединствен приступ – да се релевантни домаћи прописи, пракса Повереника, као и правни оквир и смернице усвојене Савету Европе, Европској унији, и праксу ових организација, као и препоруке које се односе на потребну измена појединих прописа.

Усклађивање са правним тековинама Европске уније у области заштите података у радним односима, превасходно се односи на усаглашавање са Општом уредбом о заштити података, али и мишљењима и препорукама Европског одбора за заштиту података, као тела успостављеног ради усклађивања примене Опште уредбе у свим државама чланицама. Директиве Европске уније у непосредној везу са радним правом не уређују питања заштите података. Имајући у виду чланство Републике Србије у Савету Европе, с једне, као и однос Европске уније са овим организацијом с друге стране, за усклађивање прописа значајни су и акти Савета Европе, и то Конвенција о људским правима, укључујући и тумачење члана 8. Европског суда за људска права, Конвенција о заштити лица у односу на аутоматску обраду личних података, сви протоколи, Препорука Комитета министара о обради личних података у контексту запошљавања, као и други акти.

О обради података о личности у радним односима

Закон о заштити података о личности уређује начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, као и, између осталог, надлежност Повереника, правна средства, одговорност и казне у случају повреде права. Овај закон прописује правила обраде, и само у изузетним случајевима и сам представља основ за обраду података о личности. Обрада података о личности у радним односима уређена је низом других прописа, а Закон о заштити података о личности се, на конкретне обраде, примењује заједно са другим законима.

Закон о раду¹ као кровни закон за радне односе уређује питања која се тичу права, обавезе и одговорности из радног односа. Додатно, и закони као што су Закон о волонтирању² или Закон о агенцијском запошљавању³ уређују питања и односе који су значајни како за радне односе, тако и за обраду података о личности волонтера или уступљених запослених, као и улоге и обавезе различитих актера са становишта обраде података о личности. Даље, Закон о евиденцијама у области рада⁴ прописује обавезу послодавца која се односи на вођење различитих евиденција за појединачно запослено лице, а које садрже бројне податке о личности. На радне односе, а значајно за обраду података о личности, се примењују и, између осталог, Закон о пензијском и инвалидском осигурању,⁵ Закон о запошљавању и осигурању за случај незапослености⁶, као и Закон о здравственом осигурању.⁷

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

2 Закон о волонтирању ("Сл. гласник РС", бр. 36/2010).

3 Закон о агенцијском запошљавању ("Сл. гласник РС", бр. 86/2019).

4 Закон о евиденцијама у области рада ("Сл. лист СРЈ", бр. 46/96 и "Сл. гласник РС", бр. 101/2005 - др. закон и 36/2009 - др. закон).

5 Закон о пензијском и инвалидском осигурању ("Сл. гласник РС", бр. 34/2003, 64/2004 - одлука УСРС, 84/2004 - др. закон, 85/2005, 101/2005 - др. закон, 63/2006 - одлука УСРС, 5/2009, 107/2009, 101/2010, 93/2012, 62/2013, 108/2013, 75/2014, 142/2014, 73/2018, 46/2019 - одлука УС, 86/2019, 62/2021, 125/2022, 138/2022 и 76/2023).

6 Закон о запошљавању и осигурању за случај незапослености ("Сл. гласник РС", бр. 36/2009, 88/2010, 38/2015, 113/2017, 113/2017 - др. закон и 49/2021).

7 Закон о здравственом осигурању ("Сл. гласник РС", бр. 25/2019 и 92/2023).

Поред ових прописа, за обраду података о личности значајни су и закони који уређују права и дужности службеника у државним органима, односно органима аутономних покрајина и јединицама локалне самоуправе, као и намештеника у овим органима или функционера. У зависности од органа, односно службе, примењиваће се, примера ради Закон о државним службеницима,⁸ Закон о запосленима у аутономним покрајинама и јединицама локалне самоуправе⁹ или Закон о запосленима у јавним службама.¹⁰ За спровођење интерног и јавног конкурса за попуњавање извршилачких радних места и положаја, а посебно начин провере компетенција и критеријуми и мерила за избор на радна места у органима државне управе, стручним службама управних округа и службама Владе, од значаја је Уредба о интерном и јавном конкурсима за попуњавање радних места у државним органима.¹¹

Поједини прописи се примењују у случајевима активирања механизма који уређују, а који претпостављају обраду података о личности, као што је то случај са Законом о заштити узбуњивача.¹² Примена прописа може да има за последицу да се обрађују посебне врсте података о личности – као што су подаци којима се открива расно или етничко порекло неког лица, политичко мишљење, верско или филозофско уверење или чланство у синдикату тог лица, односно генетски подаци, биометријски подаци у циљу јединствене идентификације лица, или подаци о здравственом стању или подаци о сексуалном животу или сексуалној оријентацији физичког лица. Ови подаци, са изузетком података о сексуалном животу (уколико се подаци о осуђиваности неког лица за кривична дела из групе кривичних дела против полне слободе не сматрају подацима који се односе на сексуални живот лица) и података о сексуалној оријентацији неког лица, обрађују се у контексту радних односа у зависности од околности конкретног односа. Примера ради, податак о верском уверењу неког лица обрађује се на основу Закона о државним и другим празницима у Републици Србији,¹³ а сврха обраде је омогућавање лицу да остварује уставом

8 Закон о државним службеницима („Сл. гласник РС”, бр. 79/2005, 81/2005 - испр., 83/2005 - испр., 64/2007, 67/2007 - испр., 116/2008, 104/2009, 99/2014, 94/2017, 95/2018, 157/2020 и 142/2022).

9 Закон о запосленима у аутономним покрајинама и јединицама локалне самоуправе („Сл. гласник РС”, бр. 21/2016, 113/2017, 95/2018, 114/2021, 113/2017 - др. закон, 95/2018 - др. закон, 86/2019 - др. закон, 157/2020 - др. закон и 123/2021 - др. закон).

10 Закон о запосленима у јавним службама („Сл. гласник РС”, бр. 113/2017, 95/2018, 86/2019, 157/2020 и 123/2021).

11 Уредба о интерном и јавном конкурсима за попуњавање радних места у државним органима („Сл. гласник РС”, бр. 2/2019 и 67/2021).

12 Закон о заштити узбуњивача („Сл. гласник РС”, бр. 128/2014).

13 Закон о државним и другим празницима у Републици Србији („Сл. гласник РС”, бр. 43/2001, 101/2007 и 92/2011).

зајемчену слободу вероисповести. Чланство у синдикату је значајан податак за послодавца код утврђивања репрезентативности синдиката, као и код случаја избора запосленог на функцију у синдикату ради мировања радног односа. Ова потоња ситуација односи се и на податак којим се открива политичко мишљење лица у смислу избора, односно именовања на функцију тог лица у некој политичкој организацији (чл. 79. Закона о раду).

Додатно, и други закони, који иако не уређују директно односе између послодавца и запосленог, могу бити од значаја за утврђивање примене правила о заштити података како је то у случају Закона о оглашавању¹⁴ и учешћа запослених у огласним порукама послодавца. Употреба видео надзора у просторијама послодавца подразумева и примену Закона о приватном обезбеђењу.¹⁵

Код заснивања радног односа законодавац је направио разлику између заснивања радног односа у једном државном органу и у једном субјекту приватног права, а која се тиче се и обраде података о личности у вези са кривичним пресудама и кажњивим делима. Док је општи услов за заснивање радног односа у државним органима да лицу раније није престајао радни однос у државном органу због теже повреде дужности из радног односа, као и да није осуђивано на казну затвора од најмање шест месеци, без обзира на врсту послова које ће то лице обављати, могућност условљавања заснивања радног односа у једном привредном субјекту приватног сектора увидом у податак о (не)осуђиваности лица могуће је само уколико је то прописано законом. Примера ради, Законом о безбедности саобраћаја на путевима прописано је да правно лице лиценцирано за оспособљавање кандидата за возаче мора да обрађује податке о осуђиваности у вези са делима која су тешка дела против безбедности јавног саобраћаја, или из групе дела против живота и тела, као и против службене дужности, које се односе на предаваче теоријске обуке, инструкторе вожње или испитиваче. Однос ових лица са правним лицем лиценцираним за оспособљавање кандидата за возаче је у домену радног права. У конкретном случају, реч је подацима о неосуђиваности лица, али и овај податак се односи на кривичне пресуда, кажњива дела и мере безбедности, без обзира што се у том случају података састоји од информације да одређено лице није осуђивано.

Стога, треба имати у виду да Закон о заштити података о личности није једини пропис који ће се применити на неку појединачну ситуацију, а посебно уколико је реч о радним односима.

Одредбе појединих Закона прописују обавезу послодавца која резултира обрадом података о личности, или прописују додатне услове

14 Закон о оглашавању („Сл. гласник РС”, бр. 6/2016 и 52/2019 - др. Закон).

15 Закон о приватном обезбеђењу („Сл. гласник РС”, бр. 104/2013, 42/2015 и 87/2018).

одраде или чак експлицитно забрањују обраду података о личности, искључујући на тај начин могућност послодавца, као руковооца, да обраду заснива на, примера ради, легитимном интересу или чак пристанку лица. Пример за прву групу прописа свакако су Закон о раду и Закон о евиденцијама у области рада, док је пример за додатне услове Закон о приватном обезбеђењу, у случају увођења физичко-техничке заштите као обезбеђења лица и имовине применом физичке заштите (вођење евиденције приликом уласка у просторије послодавца) и коришћењем средстава техничке заштите (видео надзор просторија послодавца). С тим у вези, важно је напоменути да, иако се у пракси догађа да послодавац самостално успостави видео надзор, а у циљу заштите лица, имовине или пословања, те послове може да самостално води само уколико обавља самозаштитну делатност, а која претпоставља лиценцу за вршење тих послова коју издаје Министарство унутрашњих послова. У свим другим случајевима мора да буде ангажован лиценцирани правни субјект који ће са апекта заштите података о личности јавити у улози обрађивача података. На крају, Закон о раду садржи изричиту забрану обраде података који се односе на податке о породичном, односно брачном статусу или планирању породице, као и обраду оних података који нису од непосредног значаја за обављање послова за које заснива радни однос.

Начела обраде података

Начела обраде података прописаних Законом примењују се у радним односима. Тако, према члану 5. Закона подаци се морају обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе, се морају прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама, морају бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде, као и тачни и, ако је то неопходно, ажурирани, морају се чувати у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде и обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера. А руковалац као одговоран за примену наведених захтева мора бити у могућности да предочи њихову примену.

Дакле, свих седам начела обраде података (начело законитости, поштења и транспарентности; начело ограничености сврхе; начело минимизације података; начело тачности података; начело ограни-

ченог чувања података; начело безбедности података и начело одговорности) односе се на обраду података у радним односима и тичу се сваког послодавца, односно руковођа. С тим у вези треба имати у виду да начела обраде података заправо представљају испреплетену мрежу обавеза конкретизованих другим одредбама Закона.

Начело законитости, поштења и транспарентности претпоставља постојање правног основа за обраду података о личности. Према члану 12. Закона, обрада је законита само ако је испуњен један од следећих услова: 1) лице на које се подаци о личности односе је пристало на обраду својих података о личности за једну или више посебно одређених сврха; 2) обрада је неопходна за извршење уговора закљученог са лицем на које се подаци односе или за предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора; 3) обрада је неопходна у циљу поштовања правних обавеза руковођа; 4) обрада је неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица; 5) обрада је неопходна у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења руковођа; 6) обрада је неопходна у циљу остваривања легитимних интереса руковођа или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се подаци односе који захтевају заштиту података о личности, а посебно ако је лице на које се подаци односе малолетно лице.

Ипак, нису сви ови основи једнако примењиви на радне односе. Примера ради, обрада података у циљу обављања послова у јавном интересу или извршењу законом прописаних овлашћења по својој природи се не односи на радне односе, тачније на појединачног послодавца, већ се односи на овлашћење неког органа власти да води посебне регистре. Такви регистри се могу односити на сва запослена лица, као што је то примера ради случај са Централним регистром обавезног социјалног осигурања. Дакле овај правни основ обраде података није примењив у случајевима непосредног односа између послодавца и запосленог, јер је обавеза послодавца да лице пријави у овај регистар његова обавеза прописана законом. Дакле, за послодавца основ обраде података о запосленима је правна обавеза, а Централни регистар обавезног социјалног осигурања податка обрађује на основу овлашћења прописаног законом.

Даље, случајеви када је обрада података о личности неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица су изузетни, и треба их тумачити рестриктивно. Свакако, може се замислити ситуација неке опасности, несреће или повреде на раду, када је неопходно да послодавац достави податак о здравственом стању запосленог или податак о његовој крвној групи

(напомена: овај податак послодавац иначе не обрађује) или какав други податак о запосленом. У тим случајевима, јасно је да превагу има право на живот лица, па се податак о личности може обрађивати.

На крају, пристанак лица на које се подаци односе, као запосленог, такође није, по правилу, ваљан правни основ за обраду података о личности. Наиме, да би пристанак био адекватан правни основ обраде, он мора да буде добровољно, одређено, информисано и недвосмислено изражавање слободне воље лица. У радним односима неретко изостаје елемент добровољности, као и изражавање слободне воље лица. Отуда није изненађујуће што су на мањкавост овог правног основа у области радних односа указивала тела Европске уније још 2001. године,¹⁶ као и на значај свих елемената пристанка који у радним односима изостају¹⁷. Да би се, у оним изузетним случајевима, обрада могла заснивати на пристанку лица, треба посебно установити да ли је однос послодавца и запосленог у некој конкретној ситуацији заиста однос једнаких снага и обрада у корист запосленог, и то готово искључиво у његову корист. Дакле, да би пристанак лица на обраду података у контексту радних односа био ваљан правни основ, морају се узети у обзир све околности случаја. Примера ради, организација неке прославе послодавца и објављивање слика лица, уз претпоставку да нису испуњени услови примена Закона о оглашавању, може бити засновано како на легитимном интересу, тако и на пристанку. Пример за први основ јесте да се догађај фотографише без активног учешћа појединца, док би пример за други основ био уколико се објављују слике само оних запослених који су активним позирањем фотографу и уз знање да ће фотографије бити касније објављене. Који год да је правни основ у питању, лице треба да буде претходно обавештено о обради.

Уобичајени правни основи обраде података у контексту радних односа су: уговор, правна обавеза руковаоца и легитимни интерес руковаоца или треће стране. Међутим, да би руководилац могао да обрађује податке позивајући се на неки од ових основа, и они морају да испуњавају додатне критеријуме. Наиме, уговор као основ обраде тиче се оних података о личности који су неопходни за извршење уговора управо са лицем на које се подаци односе или, за случају да је реч о обради која претходи закључењу, оних података које се односе на радње које захтева (иницира) лице на које се подаци односе. Дакле, није довољно да су подаци садржани у уговору као акту који ће потписати послодавац и запослени како би се испунила ова форма. Треба

16 Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, стр. 3.

17 European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, стр. 9.

имати у виду да овај акт може уређивати различита питања, од елемената који су обавезни према Закону о раду до оних који се односе на поједине повластице које запослени могу да имају, као што је додатно здравствено осигурање чак и чланова породице. Управо у вези са обавезним елементима које прописује Закон о раду, може се рећи да се, имајући у виду листу података о личности чија је обавезност прописана одредбама тог закона, чини да ова обрада као основ има пре правну обавезу руковођа, пре него уговор са лицем на које се подаци односе.

Према члану 33. Закона о раду, уговор о раду садржи следеће податке о личности запосленог: лично име запосленог, место пребивалишта, односно боравишта запосленог; врсту и степен стручне спреме, односно образовања запосленог, који су услов за обављање послова за које се закључује уговор о раду; назив и опис послова које запослени треба да обавља; место рада; врсту радног односа (на неодређено или одређено време); трајање уговора о раду на одређено време и основ за заснивање радног односа на одређено време; дан почетка рада; радно време (пуно, непуно или скраћено); новчани износ основне зараде на дан закључења уговора о раду; као и податке, за случај да нису утврђени законом, колективним уговором, правилником о раду или другим актом послодавца у складу са законом, које се односе на елементе за утврђивање основне зараде, радног учинка, накнаде зараде, увећане зараде и друга примања запосленог; рокове за исплату зараде и других примања на која запослени има право; или трајање дневног и недељног радног времена. Ови подаци су уједно неопходни за закључење уговора са лицем, с једне стране, и прописани су као обавезни, с друге. Избор између ова два основа у случају самог закључења радног односа не би требало да има последице по правилну примену Закона о заштити података о личности, а у погледу значаја за појединца, може се говорити о обиму права лица – па ће право на преносивост података лице имати у случају да је обрада заснована на уговору. Ипак, ово право није специфично за радне односе, а лице свакако има право на увид и копију података.

Закључење уговора о раду само је један пример примене Закона о заштити података о личности и могућег ослањања на правну обавезу руковођа као основа обраде података о личности. Законодавац је обавезао све послодавце да воде евиденције о запосленима у складу са Законом о евиденцијама у области рада.¹⁸ Према члану 5. Закона, послодавац има обавезу да води евиденцију о запосленим лицима у којој, између осталих, обрађује и податке који се односе на заинтересованост

¹⁸ Закон о евиденцијама у области рада ("Сл. лист СРЈ", бр. 46/96 и "Сл. гласник РС", бр. 101/2005 - др. закон и 36/2009 - др. закон).

лица за промену посла. Ову евиденцију послодавац мора трајно да чува (чл. 7.) Такође, послодавац је дужан да води и евиденцију о зарадама запослених (чл. 24.), и то за појединачно лице. И ову евиденцију је у обавези да чува трајно (чл. 25.). Јасно је да је вођење ових евиденција са становишта заштите података о личности правна обавеза руковођаца. Послодавац има правну обавезу обраде података ради испуњавања обавеза прописаних и другим законима. Примера ради, према Закону о безбедности и здрављу на раду¹⁹, послодавац је дужан да води, између осталог, евиденцију о повредама на раду и професионалним болестима, или о запосленима који су изложени карциногенима или мутагенима, хемијским материјама и азбесту, као и о здравственом стању и изложености лица, или евиденцију о издатој личној заштитној опреми.

Према Закону о заштити података о личности, законом којим се утврђује правна обавеза руковођаца треба да се одреде и сврха обраде. Ипак, у пракси су ретки закони који садрже одредбе о сврси обраде података, па се она често претпоставља. Примера ради, наведени Закон о евиденцијама у области рада последњи пут је измењен 2009. године, и упућује на примену савезног закона о заштити података о личности, те је овај закон потребно ревидирати.

На крају, и свакако не мање важан, је легитимни интерес послодавца, као руковођаца подацима, или треће стране, као могући правни основ обраде података. Ипак, овај правни основ подразумева документовање процене легитимног интереса, а које подразумева да се пре одлуке о обради процени да ли је обрада неопходна да се овај интерес оствари као и да ли су, у односу на тај интерес, претежнији интереси или основна права и слободе лица на које се подаци односе (запослених) који захтевају заштиту података о личности. Повереник за информације од јавног значаја и заштиту података о личности објавио је Модел акта о процени легитимног интереса као правног основа за обраду података о личности као необавезујуће форме документа који служи као помоћ руковођаца у поступку процене да ли би позивање на овај правни основ у некој конкретној ситуацији било адекватно.

Легитимни интерес послодавца биће правни основ у случају обраде података уколико је процена послодавца да је неопходно да се уведе видео надзор у појединим просторијама послодавца ради заштите имовине, лица и/или пословања. Поред Закона о заштити података о личности, у случају видео надзора послодавац је дужан да примењује и Закон о приватном обезбеђењу. Такође, легитимни интерес може бити правни основ обраде података када је реч о обради података о запосленима - корисницима електронских уређаја или службених возила који имају уграђен систем сателитског праћења возила

19 Закон о безбедности и здрављу на раду ("Сл. гласник РС", бр. 35/2023).

(GPS). У потоњем примеру, треба правити разлику да ли се код сателитског праћења возила ради о фабрички уграђеном систему, јер је у том случају потпуно искључена примена Закона о приватном обезбеђењу у складу са чланом 30. тог закона.

Без обзира на основ обраде података о личности, руковалац је дужан да запослене обавести о обради података. Ова обавеза се односи и на ситуације када обрада произлази из правне обавезе руковаоца. Може се замислити да је лице већ упознато са неким информацијама, па су могуће ситуације када послодавац као руковалац нема обавезу да их пружи. Међутим, будући да је руковалац обавезан да испуњење обавезе предочи на захтев Поверенику, то подразумева да послодавац треба да сачини обавештење о обради у складу са одредбама Закона о заштити података о личности. Друго питање је како ће послодавац, као руковалац, поступити да упозна свако запосленог о обради података. Начин испуњавања ове обавезе зависи од саме организације рада код послодавца, уобичајеног начина комуникације међу запосленима и слично. То се најчешће чини у папирном облику приликом закључења уговора о раду, односно у електронском облику у оним случајевима када лица комуницирају на овај начин, односно коришћењем различитих канала комуникације у оквиру саме организације послодавца. Без обзира на то који начин обавештавања ће послодавац одабрати, исти је дужан да такво обавештавање и документује.

Иако је у овом делу акценат био на правном основу обраде података у контексту радних односа, као и на обавези обавештавања запослених, као лица на која се подаци односе, о обради, не умањује се значај других начела. Дакле, сва начела обраде података морају бити испуњена. Начело ограничености сврхе посебно је значајно у ситуацијама када послодавац намерава да се позове на легитимни интерес као основ обраде података. Сврха мора бити јасна, одређена и дозвољена. Даље, не смеју се прекомерно обрађивати подаци, односно могу се обрађивати само они који су неопходни ради остваривања сврхе. И закон који прописује правну обавезу руковаоца би требало да се тумачи на начин да се обрађују само они подаци који су неопходни за сврху обраде. Начела тачности података и ограниченог чувања примењују се током трајања обраде података, дакле од прве радње прикупљања до последње радње, као што је брисање или уништавање података. Трајање обраде је, за поједине видове обраде, одређено као трајно законом. Такође, начело безбедности претпоставља конкретне обавезе руковаоца, а које се односе на примену мера – техничких, организационих и кадровских – које обухватају широк спектар поступања, од припрема аката, преко обуке запослених до набавке опреме и софтвера.

На крају, и никако мање важно, је начело одговорности руковаоца који не може да се пренесе на неко друго лице. И у оним случајевима

када руковаоци имају обавезу именовања лица за заштиту података о личности, одговорност за примену Закона о заштити података о личности сносиће руковалац подацима. Одговорност руковаоца не може да се пренесе на другог и у оним случајевима када поједине радње обраде руковалац повери другом лицу као обрађивачу података. Руковалац је тај који је одговоран за обраду података, дакле и избор обрађивача. У односу на права лица поводом обраде података, руковалац поступа по захтевима. У случају штете поводом обраде, руковалац је одговоран у односу на запослене. Ипак, овде треба напоменути да ће и обрађивач бити одговаран лицу за штету у случају да није поступао у складу са налозима или је поступао изван налога послодавца руковаоца, односно за примену обавеза прописаних Законом о заштити података о личности. Када податке обрађује мимо налога руковаоца, обрађивач поступа у улози руковаоца, а који, по природи односа, нема правни основа за обраду, дакле у улози незаконитог руковаоца.

Права лица на које се подаци односе

Поред ових начела, сваки послодавац, дакле руковалац, независно од величине или начина обраде, има обавезу поступања по захтевима лица у односу на права лица на које се подаци односе према Закону о заштити података о личности. Ова права треба разумети у складу са Законом о раду који се односи на заштиту личних података.

Према члану 83. Закона о раду, запослени има право увида у документе који садрже личне податке²⁰ који се чувају код послодавца и право да захтева брисање података који нису од непосредног значаја за послове које обавља, као и исправљање нетачних података. Даље, лични подаци који се односе на запосленог не могу да буду доступни трећем лицу, осим у случајевима и под условима утврђеним законом или ако је то потребно ради доказивања права и обавеза из радног односа или у вези са радом. На крају, личне податке запослених може да прикупља, обрађује, користи и доставља трећим лицима само запослени овлашћен од стране директора

Права лица поводом обраде података зависе од основа обраде података о личности, па самим тим нису увек сва права наведена у глави III Закона о заштити података о личности примењива у неком конкретном случају. Свако лице има право да буде обавештено о обради података, што уједно представља и испуњење начела законитости, поштења и транспарентност. Даље, лице има право на приступ подацима који се на то лице односе, као и на копију податка. Такође, лице

20 Закони нису термилошки усаглашени, и термин „лични подаци“ уместо „Подаци о личности“ није неуобичајен у прописима.

има право на исправку и допуну податка, као и право на брисање податка о личности или на ограниченост обраде. Право на преносивост података, како је описано у Преамбули Опште уредбе о заштити података, по природи, неће бити примењиво у радним односима. Право на приговор је посебно значајно у радним односима имајући у виду учесталост примена легитимног интереса послодавца или треће стране као правног основа обраде. Додатно, примена технологије у свим сферама живота, па и радних односа, огледа се у праву лица да се на њега/њу не примењује одлука донета искључиво на основу аутоматизоване обраде. На крају, за оне ретке ситуације када је основ обраде података пристанак запосленог, лице има право и на опозив пристанка.

Важно је напоменути да ова права нису апсолутна. Могу да се ограниче, наравно, у условима прописаним Законом. На послодавцу је, као руковоацу, да образложи ограничење права лица у неком конкретном случају. У појединим случајевима право лица ограничено је самом природом податка. Примера ради, у случају захтева за остваривање права на исправку податка који се односи на годишњу евалуацију запосленог коју је дао његов претпостављени, ово право није могуће остварити – јер податак који се тиче нечијег мишљења о неком лицу је уједно и податак који се односи на лице које је то мишљење изразило. Дакле, није могућа исправка податка који се односи на нечије мишљење о неком лицу. Додатно, по природи ствари није могуће мењати податак који представља саму евалуацију од стране лица чији је рад оцењен. Као напомена, важно је истаћи да ово право на задира у право запосленог да преиспитује адекватност евалуације и не искључује право запосленог да оспори вредновање рада. Даље, како је наведено, поједини закони предвиђају трајно чување података, па њихово брисање, иако са становишта начела ограниченог чувања података у потпуности целисходно, није могуће без обзира на квалитет података и њихов значај за сврху обраде.

Иако није наведено у посебној одредби у оквиру дела Закона који се односи на права лица, лице има право на заштиту својих права и то пред Повереником за информације од јавног значаја и заштиту података о личности, као и пред вишим судом. На поступак пред Повереником примењују се правила управног поступка, а на поступак пред судом правила парничног поступка, а према Закону о заштити података о личности ревизија правноснажне одлуке је увек допуштена. Овај механизам заштите права лица на које се подаци односе не задира у право лица према општим условима права на накнаду штете према Закону о облигационим односима, такође наведеним у члану 86. Закона о заштити података о личности.

Друге обавезе послодавца

Начела обраде података представљају испреплетену мрежу различитих обавеза. Ипак, Закон о заштити података о личности прописује различите појединачне обавезе које су руковаоци дужни да испуне, а које зависе како од врсте руковаоца, тако од броја запослених, врста података о личности, начина обраде података, постојања обрађивача и томе слично.

Данас је готово незамисливо да све радње обраде руковалац може самостално да предузме. Може се сматрати уобичајеним да неке од њих, као што је одржавање програма за управљање процесима или интернет презентације послодавца, вођење корисничког центра и слично компанија повери неком другом лицу. У односу на обраду података, ова лица су обрађивачи података о личности, а то подразумева посебан, најчешће уговорни, однос између руковаоца и обрађивача. Без обзира да ли је пословни однос руковаоца и обрађивача преточен у писани уговор, Закон намеће обавезу постојања писаног уговора о обради којим послодавац у својству руковаоца и обрађивач уређују права и обавезе у вези са повереним радњама обраде података о личности. Посебну ситуацију представља примена Закона о агенцијском запошљавању, односно сложени односи које једно лице има са различитим послодавцима. У односу на поједине радње обраде, агенција за привремено запошљавање ради уступања на привремени рад и послодавац корисник, како га назива Закон о агенцијском запошљавању, поступају као самостални руковаоци подацима, а у другим као заједнички руковаоци. Утврђивање улога у обради података о личности је важно и за утврђивање обавеза према лицима на које се односе подаци према Закону о заштити података о личности.

Послодавци, односно они руковаоци који су уједно органи власти у широј дефиницији органа власти према Закону (јер је према законима послодавац у неким случајевима Република Србија), као и они чије основне активности захтевају редован и системски надзор великог броја лица на које се подаци односе, или се основне активности састоје у обради посебних врста података или података у вези са кривичним пресудама и кажњивим делима у великом обиму имају обавезу да одреде лице за заштиту података о личности (чл. 56.).

Послодавци који имају 250 и више запослених, имају обавезу вођења евиденција радњи обраде. Ове евиденције не треба доводити у везу са евиденцијама које послодавац води по другим законима. Међутим, ову обавезу имају и они са мањим бројем запослених, дакле мање од 250, уколико је реч о обради која може да проузрокује висок ризик по права и слободе лица, или обради које није повремена, или се тиче обраде посебних врста података или података у вези са кривичним пресудама и кажњивим делима. Имајући у виду да се већина

обрада података о личности које послодавци врше у контексту обраде података о личности запослених одвија континуирано или периодично, примера ради, обрада која се односи на исплату зараде, обрада која се односи на употребу уређаја, затим обрада података о верском уверењу, обавеза вођења евиденције се ипак примењује. Вођење евиденција радњи обраде уједно је корисна активност која помаже да се установе у које се (све) сврхе обрађују подаци и могу послужити као алат руковоаца да преиспита поједине обраде, односно основе обраде или обим података о личности који се обрађују.

У случају да дође до тзв. компромитације, односно до повреде података о личности, као случајног или намерног, а незаконитог, уништења, губитка, измене, или неовлашћеног откривања или приступа подацима, руковалац је дужан да о томе обавести Повереника (чл. 52. Закона) или чак и лица на које се подаци односе (чл. 53.), према Обрасцу обавештења о повреди података о личности који је усвојио Повереник.²¹ Примера ради, у случају да се подаци о зарадама свих запослених, чак и грешком, пошаљу неким другим лицима, реч је о повреди података о личности. Шта је повреда података о личности која ће резултирати обавезом руковоаца да обавести Повереника, па и лица на које се подаци односе, зависиће од околности појединачног случаја. Дакле, није само питања броја лица, већ и осетљивости података који не упућују само на оне податке одређене Законом као посебна врста података, као што је примера ради постојање административне забране на плату. У том случају потребно је спровести процену ризика учињене повреде података о личности по права и слободе запослених, те у случају да повреда може произвести ризик по права и слободе запослених обавестити Повереника, а евентуално и саме запослене уколико је реч о високом ризику који повреда може да произведе. Важно је напоменути да ова обавеза постоји независно од мера које је руковалац предузео.

Уколико послодавац одлучи да обрађује биометријске податке запослених у циљу јединствене идентификације или да податке о личности запослених обрађује употребом апликација или система за праћење њиховог рада, кретања, комуникације и слично, обавезан је да изврши процену утицаја обраде на заштиту података о личности (чл. 54. Закона). Реч је радњама обраде које су према Одлуци Повереника утврђене на листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности.²²

21 Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности ("Сл. гласник РС", бр. 40/2019).

22 Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника ("Сл. гласник РС", бр. 112/20).

Поједини послодавци у Републици Србији део су мултинационалних корпорација које имају интересе да људским ресурсима управљају на глобалном нивоу. Ово је само један пример када постоји потреба да се подаци деле са другим лицима (чланицама групе компанија) и када постоји потреба да се исти износе из наше земље. У тим случајевима, свакако је важно установити природу односа и утврдити евентуално постојање других руковаца који могу бити са послодавцем у односу заједничких руковаца. Додатно, поред основа обраде података, а који укључује дељење података, потребан је и основ за пренос података о личности у друге земље. Овај пренос може да подразумева и испуњење других услова из Закона о заштити података о личности, као што је, примерично, постојање одлуке Повереника којима се дозвољава пренос података (чл. 65.) или одобрење обавезујућих пословних правила (чл. 67.). У вези са потоњим, важно је истаћи да обавезујућа пословна правила које је, у складу са Општом уредбом о заштити података, одобрио орган за заштиту података неке државе чланице Европске уније нису довољан основ за пренос података о личности из Републике Србије у друге земље, већ је, у оквиру важећег правног оквира, потребно да Повереник одобри посебна обавезујућа пословна правила. Ово стога што је Законом прописана садржина обавезујућих пословних правила, а што укључује и успостављање надлежности Повереника за информације од јавног значаја и заштиту података о личности Републике Србије.

Међународни правни оквир

Србија је потписница Европске конвенције о људским правима, чији члан 8. уређује право на поштовање приватног и породичног живота: „Свако има право на поштовање свог приватног и породичног живота, дома и преписке.” У складу са судском праксом Европског суда за људска права, појединци имају одређена разумна очекивања приватности чак и на радном месту, и у том смислу морају бити заштићени од мешања послодавца. Право на поштовање приватног живота на радном месту није апсолутно, јер његов обим може бити предмет одмеравања у односу на легитимне интересе послодавца. Послодавац има оправдан интерес да спроводи надзор над запосленима, њиховим коришћењем радног времена, употребом службених уређаја и аутомобила итд. Надзор ове врсте мора бити строго сразмеран жељеним циљевима, тј. усредсређен на неопходне информације, да што мање задире у приватну сферу запослених и задовољава критеријуме из судске праксе ЕСЉП (рецимо, у погледу обавештавања запослених и интерног уређења потенцијалног ванредног надзора над коришћењем службених средстава).

Србију у предметној области обавезује и Конвенција Савета Европе о заштити лица у односу на аутоматску обраду личних података („Конвенција 108+”), усвојена 1981. године као први правно обавезујући међународни инструмент у погледу заштите података, која је последњи пут модернизована 2018. године. Конвенција 108+ уређује основне и опште принципе обраде података, као што су законитост, транспарентна, поштена, наменска обрада података о личности, минимизација прикупљених података и ограничење трајања њиховог чувања, а не садржи (изричито) обавезе уговорних страна у погледу обраде података о личности у радном односу. Посебна правила о заштити личних података у односима послодаваца и запослених су наведена у Препоруци Савета Европе у вези са личним подацима у контексту запослења, која је објављена 1989. године и последњи пут ревидирана 2015. године. У њој је разматрана обрада личних података у циљу запослења у приватном и јавном сектору. Обрада мора да буде у складу с неким принципима и ограничењима, као што су принцип транспарентности и консултације с представницима запослених пре него што се на радном месту успоставе системи надзора. На основу Препоруке СЕ о запослењу, запослени морају да буду обавештени о сврси обраде њихових података о личности, врсти личних података који се прикупљају, субјектима којима се ови подаци редовно прослеђују и сврси и правној основи оваквих обелодањивања. Појединачна упутства из Препоруке СЕ су по темама укључена у доња поглавља (прикупљање података кандидата за запослење, видео-надзор над запосленима, надзор електронских комуникација на радном месту).

Као додатни правни извор међународног права, за питања обраде личних података на раду меродаван је и документ Међународне организације рада – МОР, чија је чланица и Србија, и то Кодекс поступања за заштиту личних података запослених (Кодекс МОР). Наведени кодекс из 1997. године је резимиран и унесен у модерно окружење у радном документу под насловом Заштита личних података запослених: Општи принципи, који је објављен и стављен на расправу 2022. године.

Иако Србија није држава чланица Европске уније, правила ЕУ о заштити података о личности се од усвајања Опште уредбе о заштити података примењују и на предузећа и друге субјекте који нису основани у ЕУ ако нуде робу и услуге појединцима унутар ЕУ односно прате њихово понашање, на пример, обрадом података о њиховој интерној активности за креирање профила. Несумњиво је да ће обавезе које право ЕУ намеће послодавцима у погледу заштите података о личности запослених бити релевантне за чланство Републике Србије у Европској унији. На крају, али не и мање важно, Општа уредба се заснива на Конвенцији 108 и додатно је уређују, при чему су за разлику

од конвенције која обавезује државе уговорнице директно делотворне за правна или физичка лица (руковаоце и обрађиваче). Корисни су ставови Суда правде Европске уније, који у поступцима претходних питања образлаже обавезе држава чланица онако како проистиче из појединачних одредби Опште уредбе односно примарног права, прецизније члана 7. (поштовање приватног и породичног живота) и члана 8. (заштита личних података) Повеље ЕУ о основним правима.

Већ на овом месту треба напоменути да Општа уредба обавезе поводом обраде података у радном односу директно помиње (само) у члановима 9. (обрада посебних врста података о личности) и 88. (обрада у оквиру запослења). У Општој уредби су, дакле, односи послодаваца и запослених изричито наведени у члану 9(2), који уређује да се посебне врсте личних података, између осталих података о чланству у синдикату, о здрављу, о политичком уверењу, етничком пореклу итд., могу обрађивати у циљу испуњавања обавеза и спровођења посебних права руковаоца и предметног појединца у области радног права, уз постојање једне од правних основа за обраду. Наравно, послодавце као руковаоце подацима о личности запослених иначе обавезују све одредбе Опште уредбе. У складу са чланом 88. Опште уредбе, државе чланице одређују детаљнија правила за осигурање заштите права и слобода запослених у вези с њиховим личним подацима у оквиру запослења, при чему у складу са судском праксом Суда правде морају да поштују захтеве и ограничења из става 2. наведеног члана.

Даље, корисна упутства за успостављање високог стандарда заштите личних података пружају детаљне анализе и конкретне одлуке институција ЕУ, које су основане за имплементацију Опште уредбе, као што је Европски одбор за заштиту података (енг. European Data Protection Board – EDPB) односно његова претходница, Радна група за заштиту података из члана 29. (енг. *Article 29 Working Party*), основана Директивом 95/46/ЕЗ. За поступање с подацима запослених на раду још увек је актуелно Мишљење бр. 2/2017 о обради података на раду, које је усвојила Радна група из члана 29. и бави се многим и данас осетљивим питањима о границама послодавчевог надзора у контексту модерних технологија.

Пошто се европски стандарди за заштиту података о личности заснивају на Конвенцији 108+, инструментима ЕУ, првенствено Општој уредби за заштиту података и предметној судској пракси Европског суда за људска права и Суда Европске уније, Агенција ЕУ за основна права у сарадњи са Саветом Европе и канцеларијом Европског надзорника за заштиту података 2018. године усвојили су Приручник о европском праву заштите података о личности. У њему су јасно представљени сви кључни принципи, важећа правила и тренутни изазови европског права о заштити података о личности, у које спада и питање

законског обима праћења електронских комуникација запосленог на радном месту.

Усаглашавање са прописима Европске уније

Поред наредних одредаба Опште уредбе о заштити података које се односе на обраду података о личности у области радних односа, други прописи Европске уније који уређују поједина питања права лица у радним односима не уређују и питања обраде података. Ови прописи се тичу организације радног времена, као што је Директива 2003/88/ЕЗ о одређеним видовима организације радног времена Директива 2003/88/ЕЗ Европског Парламента и Савета од 4.11. 2003. о одређеним видовима организације радног времена,²³ Директива 2000/78/ЕЗ о успостави општег оквира за једнако поступање при запошљавању и обављању занимања²⁴ или Директива 2010/18/ЕУ која се односи на родитељско одсуство,²⁵ као и други акти ЕУ.²⁶ Из тог разлога, јасне инструкције законодавцу у погледу прописа у области рада и радних односа изостају, те се усклађивање са правним тековинама своди на правилну примену одредби Закона о заштити података о личности које су преузеле дикцију Опште уредбе. Отуда је усклађивање других закона са Законом о заштити података о личности први, и основни, корак ка усаглашавању правног система Републике Србије.

Закључак

Свака обрада података у радним односима, односно у вези са радним односима, мора да буде усклађена са Законом о заштити података о личности. Поред тога, треба да буде у складу са Конвенцијом 108+, као и смерницама тела Савета Европе.

Послодавац, као руковалац, треба да има у виду сва начела обрада података. Дакле, потребно је да утврди правни основ обраде података о личности, сврху обраде, обим података о личности, као и мере безбедности. У пословању, може се замислити ситуација да привредни

23 Директива 2003/88/ЕЗ Европског Парламента и Савета од 4.11. 2003. о одређеним видовима организације радног времена.

24 Директива 2000/78/ЕЗ од 27.11. 2000. о успостављању општег оквира за једнако поступање при запошљавању и обављању занимања.

25 Директива Савета 2010/18/ЕУ од 8.3.2010. о спровођењу ревидираног Оквирног споразума о родитељском одсуству који су закључили BUSINESSEUROPE, UEAPME, СЕЕР и ETUC и стављању ван снаге Директиве 96/34/ЕЗ.

26 Више о томе на European Parliament, „The scope of EU labour law - Who is (not) covered by key directives?“, October 2020.

субјект у оквиру неког процеса рада, примера ради управљање имовином, у погледу истих врста података о личности примењује различите основе, као и сврхе обраде. Ипак, важно је разграничити сврху обраде од процеса рада. Даље, свака обрада података подразумева и обавезу поступања руковођа према захтевима лица на које се подаци односе. Појединачне обраде података могу да подразумевају и посебне обавезе руковођа, које се могу односити на вођење евиденције, израду процене утицаја на заштиту података, уговора о преносу података и сл. Све ове обавезе подразумевају документовање одлука, мера и активности, као и укључивање запослених, па и других лица у примени Закона.

Као посебно значајно, треба истаћи и то да, иако су неке обраде постале свакодневица у пословном свету, не треба извући закључак да су ове обраде увек дозвољене у складу са правилима заштите података о личности. Случајеви из праксе других држава, а посебно имајући у виду праксу Европског суда за људска права, управо указују на недозвољено ограничење права појединца на заштиту података о личности, па тиме и на недозвољеност појединих обрада података, упркос њиховој учесталости у примени. Иако Република Србија није чланица Европске уније, Споразумом о стабилизацији и придруживању се обавезала да усклади своје прописе, а посредно и праксу, те су одредбе Опште уредбе о заштити података, мишљења радног тела овог прописа, као и пракса Европског суда правде у погледу тумачења Опште уредбе, значајнија за разумевање обраде података, па и обраде података у контексту радних односа.

Развој технологија биће све више корака испред правне регулативе њихових утицаја на различите аспекте нашег живота. У радним односима све више се брише граница између приватног и службеног. Наше улоге се преплићу више него икада. Сандуче електронске поште је отворено и након завршетка радног времена. Мобилни телефон звони у свако доба. GPS у службеном аутомобилу који запослени сме да користи и у приватне сврхе ради све време. Питање је да ли и колико ефикасно запослени може да га искључи. При коришћењу штампа, и корисничка подешавања приказују корисничко име запосленог и исписују и адресу штампаног документа. Слично је при употреби апарата за фотокопирање са системом корисничких имена. Видео-надзор на радном месту постаје уобичајен. Тражење равнотеже између права на приватност и заштите података о личности и интереса послодавца постаје све већи изазов.

Усклађивање са правним тековинама Европске уније у области заштите података у радним односима, превасходно се односи на усаглашавање са Општом уредбом о заштити података, али и мишљењима и препорукама Европског одбора за заштиту података, као тела успо-

стављеног ради усклађивања примене Опште уредбе у свим државама чланицама, као и актима Савета Европе, и то Конвенцијом о људским правима, укључујући и тумачење члана 8. Европског суда за људска права, Конвенцијом о заштити лица у односу на аутоматску обраду личних података као и других аката ове организације чије је Република Србија чланица.

Заснивање радног односа

Правни оквир

Заснивање радног односа, у зависности од послова који се обављају, као природе послодавца, условљено је испуњавањем одређених критеријума. Утврђивање да ли лице испуњава услове за заснивање радног односа има за последицу обраду података о личности. Са становишта заштите података о личности, у оквиру ових обрада обрађују се и они подаци о личности који се претпостављају. Примера ради, то су подаци у вези са доказима о испуњености услова за рад у погледу школске спреме, или они који се неопходни да послодавац измири основне обавезе према запосленом, али и држави, као што су идентификациони подаци, порески број лица (у случају Републике Србије јединствени матични број грађана је уједно и порески број физичког лица) или пребивалиште (према којем се обрачунавају доприноси за пензијско осигурање) или број банковног рачуна, уколико се плата исплаћује на тај начин.

Услови за рад могу бити утврђени законом, али и правилником о организацији и систематизацији послова, за случај да послодавац има више од 10 запослених (чл. 24. Закона о раду). За поједине послове законодавац је прописао посебне услове, а који се могу односити и на обраду посебних врста података о личности. Треба имати у виду да услови за заснивање радног односа, без обзира на постојање правилника о организацији и систематизацији послова, не смеју бити одређени на начин да дискриминишу неко лице. Према члану 18. Закона о раду забрањена је свака дискриминација, како непосредна, тако и посредна, лица која траже запослење, с обзиром на пол, рођење, језик, расу, боју коже, старост, трудноћу, здравствено стање, односно инвалидност, националну припадност, вероисповест, брачни статус, породичне обавезе, сексуално опредељење, политичко или друго уверење, социјално порекло, имовинско стање, чланство у политичким организацијама, синдикатима или неко друго лично својство. Додатно, према истом закону, потенцијални послодавац нема право, тачније има забрану, да од кандидата захтева податке о породичном, брачном статусу или планирању породице, нити може да тражи од кандидата да достави исправе или неке друге доказе који нису од непосредног значаја за обављање послова за које заснива радни однос. Даље, сем у случају послова код којих постоји знатан ризик за здравље жене и

детета утврђен од стране надлежног здравственог органа, послодавац не може да условљава заснивање радног односа тестом трудноће (чл. 26. Закона о раду).

Дакле, уколико услови нису прописани самим законом који ближе уређује делатност коју послодавац врши, послодавац може да обрађује само оне податке о личности које сматра да су од непосредног значаја за обављање послова за које се заснива радни однос. Обрада података о личности кандидата за запослење може резултирати обрадом која је заснована на неколико правних основа – примера ради, правне обавезе руковоаца, легитимног интереса или уговора са лицем на које се подаци односе.

Поред примера из Закона о безбедности саобраћаја на путевима (чл. 211. ст. 4. т. 7)) на основу којег је правно лице лиценцирано за оспособљавање кандидата за возаче у обавези да обрађује податке о (не) осуђиваности предавача теоријске обуке, инструктора вожње или испитивача са којим је успоставио радни однос у вези са делима која су тешка дела против безбедности јавног саобраћаја, или из групе дела против живота и тела, као и против службене дужности, и други закони прописују посебне услове које кандидати за запослење треба да испуњавају у моменту подношења пријаве, односно запослења. Треба напоменути да је значајна разлика између обраде ових података у јавном и приватном сектору, те се подаци о осуђиваности кандидата у јавном сектору обрађују за свако лице, док се у приватном сектору они могу обрађивати само уколико је реч о услову прописаном законом, а што се у законима односи само на посебна радна места.

Закон о основама система образовања и васпитања²⁷ прописује да лице може бити примљено у радни однос уколико, поред одговарајућег образовања, између осталог, има психичку, физичку и здравствену способност за рад са децом и ученицима, није осуђивано правноснажном пресудом за кривично дело за које је изречена безусловна казна затвора у трајању од најмање три месеца, као и за кривична дела насиље у породици, одузимање малолетног лица, запуштање и злостављање малолетног лица или родоскврнуће, за кривична дела примање или давање мита; за кривична дела из групе кривичних дела против полне слободе, против правног саобраћаја и против човечности и других добара заштићених међународним правом, без обзира на изречену кривичну санкцију, и за које није, у складу са законом, утврђено дискриминаторно понашање (чл. 139). Дакле, лице које намерава да заснује радни однос у установи образовања или васпитања треба да прође процену психичке, физичке и здравствене способности за рад

²⁷ Закон о основама система образовања и васпитања ("Сл. гласник РС", бр. 88/2017, 27/2018 - др. закон, 10/2019, 27/2018 - др. закон, 6/2020, 129/2021 и 92/2023).

са децом и ученицима. Ову процену не може да врши сам послодавац, а увид у податке о личности послодавац може имати само у случају да лице испуњава овај услов, док је обим података о личности ограничен само на коначну процену способности, а не на појединости и податке о личности обрађене током процењивања способности. их (чл. 139.) Са становишта обима обраде, није јасна сврха обраде и ових података о личности за послове који нису у директној вези са надлежностима овог министарства.

У погледу легитимног интереса и уговора као основа обраде података о личности кандидата за запослење, важно је истаћи да у оба случаја обрада мора да буде неопходна за извршење уговора, односно за остваривања легитимних интереса руковооца или треће стране. У вези са уговором, имајући у виду формулацију основа, то значи да би се то односило на ситуацију када је готово извесно да ће се уговор закључити. Уговор као основ обраде постојаће и у случају предузимања радњи пре закључења уговора са лицем на које се подаци односе, али се овај случај, према Закону о заштити података о личности односи када је та обрада на захтев тог лица, а не потенцијалног послодавца.

Начин ангажовања, односно организовање конкурса за неко радно место, спровођење конкурса, као и различити видови утврђивања испуњавања услова за запослење, међу којима могу бити различити тестови, отварају низ посебних питања поштовања свих начела обраде података. Употреба психолошких тестова у пракси није реткост и с тим у вези треба правити разлику између обавезности провере способности неког лица да обавља одређене послове утврђене прописом, као што је то случај са наставним особљем, и жеље послодавца да ангажује лице које се може сматрати поузданим сарадником, иницијатором или типом личности који према неким другим проценама значи карику која недостаје за успешно пословање. Ови тестови се примењују и у јавном сектору. Тако према Уредби о интерном и јавном конкурсима за попуњавање радних места у државним органима,²⁸ облици провере понашајних компетенција су: психометријски тестови, узорци понашања, интервју базиран на компетенцијама и упитник које спроводе психолози (чл. 44.). Имајући у виду домаћа ових тестова, питање је да ли овај вид тестирања неопходан за сва радна места, а Уредбом нису прописане мере безбедности података.

Када је реч о конкурсима у јавном сектору, примера ради Закон о државним службеницима уређује право на жалбу кандидата који су учествовали у изборном поступку (нпр. чл. 59), а што за последицу има да је орган који спроводи конкурс у обавези да чува документа

²⁸ Уредба о интерном и јавном конкурсима за попуњавање радних места у државним органима ("Сл. гласник РС", бр. 2/2019 и 67/2021).

настала у поступку спровођења конкурса, најмање до окончања рока за подношење жалбе. Међутим, Закон не уређује ово питање посебно, нити мере безбедности података. У овим случајевима примењују се опште одредбе о поверљивости података. Поред тога, рок чувања ових података може бити и дужи у случајевима покретања поступка по притужби Поверенику за заштиту равноправности.

Из праксе Повереника

Питање: Да ли банка приликом запошљавања, може да тражи доставање доказа о неосуђиваности и да се не води кривични поступак, посебно имајући у виду одредбу чл. 102. став 4. Кривичног законика, као и шта је потребно да се обезбеди (пристанак и сл.) у смислу Закона о заштити података о личности, да би такав податак могао бити тражен од кандидата са којима банка намерава да закључи уговор о раду?

Број предмета: 073-14-2317/2021-02

Послодавац, као руковалац подацима, у сврху закључења уговора о раду, односно у сврху радног ангажовања одређеног лица, може прикупљати и даље обрађивати само оне податке који се односе на то лице чија обрада представља обавезу или овлашћење послодавца предвиђено законом којим се уређује рад, односно запошљавање.

Сагласно одредбама чл. 12. Закона обрада података о личности је законита само ако је испуњен један од следећих услова: 1) лице на које се подаци о личности односе је пристало на обраду својих података о личности за једну или више посебно одређених сврха; 2) обрада је неопходна за извршење уговора закљученог са лицем на које се подаци односе или за предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора; 3) обрада је неопходна у циљу поштовања правних обавеза руковаоца; 4) обрада је неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица; 5) обрада је неопходна у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења руковаоца; 6) обрада је неопходна у циљу остваривања легитимних интереса руковаоца или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се подаци односе који захтевају заштиту података о личности, а посебно ако је лице на које се подаци односе малолетно лице.

Сагласно одредбама члана 19. став 1. поменутог закона, обрада података о личности који се односе на кривичне пресуде, кажњива

дела и мере безбедности може се вршити на основу члана 12. став 1. тог закона, али само под надзором надлежног органа или, ако је обрада допуштена законом, уз примену одговарајућих посебних мера заштите права и слобода лица на које се подаци односе.

Обрада података о личности у области рада и запошљавања, међутим, представља један од посебних случајева обраде, па је тако у члану 91. став 1. Закона прописано да се на обраду у тим областима примењују одредбе закона којима се уређује рад и запошљавање и колективни уговори, уз примену одредаба тог закона.

Сагласно цитираним одредбама Закона, послодавац, као руковолац, у сврху закључења уговора о раду, односно у сврху радног ангажовања одређеног лица, може прикупљати и даље обрађивати само оне податке који се односе на то лице чија обрада представља обавезу или овлашћење послодавца предвиђено законом којим се уређује рад, односно запошљавање.

Ово значи да, од шест могућих правних основа за обраду података о личности који су предвиђени чланом 12. став 1. Закона, послодавац, у сврху закључења уговора о раду, односно у сврху радног ангажовања одређеног лица, може вршити обраду која је неопходна у циљу поштовања правних обавеза руковолаца, у смислу тачке 3), или обраду која је неопходна у циљу извршења законом прописаних овлашћења руковолаца, у смислу тачке 5) наведеног члана Закона.

Питање: Да ли је обрада податка о јединственом матичном броју грађанина (ЈМБГ) у процесу регрутације кандидата за пријем у радни однос неопходна ради предузимања радњи пре закључења уговора са лицем чији се подаци о личности обрађују, тако да је правни основ за обраду тог податка о личности „уговор у настајању“?

Број предмета: 073-14-2576/2021-02

У складу са одредбом члана 90. Закона о заштити података о личности, на обраду јединственог матичног броја грађана примењују се одредбе закона којим се уређује јединствени матични број грађана, односно другог закона, уз примену одредби овог закона које се односе на заштиту права и слобода лица на које се подаци односе.

Овом приликом, начелно указујемо на то да Закон о заштити података о личности („Сл. гласник РС“, бр. 87/2018), на системски начин, уређује опште принципе и правила обраде којих се руковоаци и други субјекти који учествују у обради података о личности морају придржавати, док се обрада података о личности у одговарајућим областима друштвеног живота уређује посебним прописима. Тако на

примену посебних прописа упућују и одредбе чл. 90. и 91. Закона, које се односе на обраду јединственог матичног броја грађана и на обраду у области рада и запошљавања.

Наиме, у складу са одредбом члана 90. Закона, на обраду јединственог матичног броја грађана, примењују се одредбе закона којим се уређује јединствени матични број грађана, односно другог закона, уз примену одредби овог закона које се односе на заштиту права и слобода лица на које се подаци односе. Одредбама члана 11. ст. 1. и 2. Закона о јединственом матичном броју грађана („Сл. гласник РС“, бр. 24/2018) прописано је да се матични број уписан у евиденцију о матичним бројевима уписује у јавне исправе и друге евиденције, а да матични број грађана служи за вођење евиденције података о личности и повезивање с другим евиденцијама државних органа и корисника који имају законски основ за коришћење матичног броја.

Сагласно одредби члана 91. Закона, на обраду у области рада и запошљавања првенствено се примењују одредбе закона којима се уређује рад и запошљавање и колективни уговори, уз примену одредби овог закона. Према томе када је у питању обрада података о личности у области рада и запошљавања, овлашћење руковооца за такву обраду треба да произлази из одговарајућих одредаба прописа у овој области, уз примену начела обраде и других општих правила утврђених Законом.

Сагласно члану 5. став 1. Закона, подаци о личности морају: 1) се обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе („законитост, поштење и транспарентност“). Законита обрада је обрада која се врши у складу са овим законом, односно другим законом којим се уређује обрада; 2) се прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама („ограничење у односу на сврху обраде“); 3) бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде („минимизација података“); 4) бити тачни и, ако је то неопходно, ажурирани. Узимајући у обзир сврху обраде, морају се предузети све разумне мере којима се обезбеђује да се нетачни подаци о личности без одлагања избришу или исправе („тачност“); 5) се чувати у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде („ограничење чувања“); 6) се обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера („интегритет и поверљивост“). У ставу 2. истог члана Закона је прописано да је руковалац одговоран за примену одредаба става 1. овог члана и мора бити у могућности да предочи њихову примену („одговорност за поступање“).

Одредбама члана 12. Закона прописано је да је обрада података о личности законита само ако је испуњен један од следећих услова: 1) лице на које се подаци о личности односе је пристало на обраду својих података о личности за једну или више посебно одређених сврха; 2) обрада је неопходна за извршење уговора закљученог са лицем на које се подаци односе или за предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора; 3) обрада је неопходна у циљу поштовања правних обавеза руковоаца; 4) обрада је неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица; 5) обрада је неопходна у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења руковоаца; 6) обрада је неопходна у циљу остваривања легитимних интереса руковоаца или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се подаци односе који захтевају заштиту података о личности, а посебно ако је лице на које се подаци односе малолетно лице.

Када је у питању обрада у области рада треба водити рачуна и о томе да, иако је један од 6 могућих правних основа обраде предвиђених одредбама члана 12. став 1. Закона и случај када је одређена обрада неопходна за извршење уговора закљученог са лицем на које се подаци односе или предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора (тачка 2), наведени правни основ се не може применити на обраду података о личности коју послодавац врши у сврху закључења уговора о раду или другог вида радног ангажовања.

Наиме, Законом о раду ("Сл. гласник РС", бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - одлука УС, 113/2017 и 95/2018 - аутентично тумачење) прописано је да се радни однос заснива уговором о раду који закључују послодавац и запослени, при чему је тим законом прописана и обавезна садржина уговора о раду.

Сагласно томе, послодавац, у сврху закључења уговора о раду, односно у сврху радног ангажовања одређеног лица, може вршити обраду која је неопходна у циљу поштовања правних обавеза руковоаца, у смислу тачке 3), или обраду која је неопходна у циљу извршења законом прописаних овлашћења руковоаца, у смислу тачке 5) става 1. члана 12. Закона.

Имајући у виду све наведено, обрада податка о ЈМБГ коју би послодавац вршио у сврху закључења уговора о раду са одређеним лицем, а како Законом о раду исти није прописан као обавезан елемент тог уговора, не би се могла сматрати законитом обрадом, у смислу члана 12. Закона.

Свакако да се овим не задире у обавезу послодавца да води евиденцију о запосленим лицима која садржи прописане податке о личности,

а у сврху остваривања права по основу рада и социјалног осигурања и друге сврхе изричито прописане Законом о евиденцима у области рада („Сл. лист СРЈ“, бр. 46/96 и “Сл. гласник РС“, бр. 101/2005 - др. закон и 36/2009 - др. закон), и на начин прописан тим законом.

Овакво поступање приликом обраде података о личности од стране послодаваца као руковаоца, произлази и из начела обраде утврђених чланом 5. Закона, посебно начела „ограничење у односу на сврху обраде“, и начела „минимизација података“.

С друге стране, када је у питању обрада података о личности, укључујући и ЈМБГ и друге прописане податке, у случајевима када је за рад на одређеним радним местима код одређених категорија послодаваца, за које је законом прописана обавеза спровођења безбедносних провера, а која се спроводи од стране надлежних органа сагласно Закону о полицији односно другим посебним прописима, иста се може вршити на начин и под условима утврђеним тим прописима, док у погледу такве обраде својство руковаоца има орган надлежан за спровођење безбедносне провере, а не привредно друштво-послодавац.

Питање: На који начин *послодавац* може да прикупља и даље обрађује податке о здравственом (психофизичком) стању запослених - возача, у циљу спречавања ризика од настанка повреда или изненадне смрти због лошег здравственог стања, као и да ли постоји законит правни основ за такву обраду, уз могућност примене аутоматизованих софтверских система који служе да би се одредило да ли је сваки конкретни запослени спреман за наредни рад на основу медицинских мерења и за израду закључка о способности/неспособности запосленог у облику записа у електронском дневнику лекарских прегледа?

Број предмета: 073-14-1854/2021-02

Са становишта примене Закона о заштити података о личности, указујемо на то да је за закониту обраду података о личности најпре потребно да руковалац, у зависности од околности конкретног случаја, обезбеди одговарајући правни основ, у смислу одредбе члана 12. Закона, при чему је за обраду података о здравственом стању или других података који спадају у посебну врсту података о личности додатно потребно да се ради о неком од случајева из члана 17. став 2. овог закона, затим да је иста у складу са посебним прописима који уређују предметну област/делатност, као и да се иста врши у складу са наче-

лима обраде из члана 5. Закона о заштити података о личности и другим одговарајућим правилима и обавезама прописаним тим законом.

Обрада посебних врста података о личности из члана 17. став 1. Закона о заштити података о личности, у које спадају и подаци о здравственом стању, начелно је забрањена тим законом, односно допуштена је само као изузетак до кога може доћи у случајевима који су таксативно наведени у члану 17. став 2. истог закона.

С тим у вези, указујемо на то да се обрада података о личности не уређује само Законом о заштити података о личности већ и другим тзв. посебним законима, при чему када је у питању обрада података о личности у области радних односа, потребно је имати у виду да се сагласно одредби члана 91. Закона о заштити података о личности, примењују примарно одредбе закона којима се уређује рад и запошљавање и колективни уговори, уз примену начела и правила из Закона о заштити података о личности.

Сходно наведеном, уколико је потребно да прибавите мишљење о примени прописа којима се уређује рад и запошљавање и колективни уговори, можете се обратити Министарству за рад, запошљавање, борачка и социјална питања.

Такође, указујемо и на то да је материја која се односи на обављање здравствене делатности уређена посебним прописима из предметне области, те се ради добијања мишљења о примени тих прописа може обратити Министарству здравља.

Додатно, а како сте у достављеном допису навели да у планираној обради постоји „могућност примене аутоматизованих софтверских система“, указујемо на то да није прецизирано да ли руковалац намерава да доноси одлуке од значаја за правни положај запосленог или одлуке које на сличан начин значајно утичу на њега, искључиво на основу аутоматизоване обраде података о личности, која би се вршила употребом предметних софтверских система, у ком случају би морали бити испуњени услови прописани одредбама члана 38. Закона о заштити података о личности.

Такође, посебно указујемо на одредбу члана 54. Закона о заштити података о личности којом је предвиђено да је руковалац дужан, у случају када је вероватно да ће нека врста обраде, посебно употребом нових технологија и узимајући у обзир природу, обим, околности и сврху обраде, проузроковати висок ризик за права и слободе физичких лица, да пре него што започне са обрадом изврши процену утицаја предвиђених радњи обраде на заштиту података о личности.

Повереник је донео 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 („Сл. гласник РС“

број 45/2019 и 112/2020), којом је у тачки 2. предвиђено да се процена утицаја на заштиту података о личности мора вршити у случају: 1) систематске и свеобухватне процене стања и особина физичког лица која се врши помоћу аутоматизоване обраде 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; 2) обраде посебних врста података о личности, односно података којима се открива расно или етничко порекло, политичко мишљење, верско или филозофско уверење или чланство у синдикату, као и обраде генетских података, биометријских података у циљу јединствене идентификације лица, података о здравственом стању или података о сексуалном животу или сексуалној оријентацији физичког лица или података о личности у вези са кривичним пресудама и кажњивим делима и мерама безбедности, у великом обиму; 3) систематског надзора над јавно доступним површинама у великој мери; 4) обраде података о личности деце и малолетника у сврху профилисања, аутоматизованог одлучивања или за маркетиншке сврхе; 5) употребе нових технологија или технолошких решења за обраду података о личности или са могућношћу обраде података о личности који служе за анализу или предвиђање економске ситуације, здравља, склоности или интересовања, поузданости или понашања, локације или кретања физичких лица; 6) обраде података о личности на начин који укључује праћење локације или понашања појединца у случају системске обраде података о комуникацији насталих употребом телефона, интернета или других средстава комуникације; 7) обраде биометријских података у циљу јединствене идентификације запослених од стране послодавца и у другим случајевима обраде података о личности запослених од стране послодавца употребом апликација или система за праћење њиховог рада, кретања, комуникације и сл; 8) обраде података о личности укрштањем, повезивањем или провером подударности из више извора; 9) обраде посебних врста података о личности у сврху профилисања или аутоматизованог одлучивања.

Сагласно члану 55. Закона, руковалац је дужан да затражи мишљење Повереника пре започињања радње обраде, ако процена утицаја на заштиту података о личности, која је извршена у складу са тим законом, указује да ће намеравање радње обраде произвести висок ризик ако се не предузму мере за умањење ризика, односно у случајевима када ниво ризика, након предузимања мера и даље остаје висок.

Дакле, са становишта примене Закона о заштити података о личности, указујемо на то да је за закониту обраду података о личности најпре потребно да руковалац, у зависности од околности конкретного случаја, обезбеди одговарајући правни основ, у смислу одредбе члана 12. Закона, при чему је за обраду података о здравственом стању или

других података који спадају у посебну врсту података о личности додатно потребно да се ради о неком од случајева из члана 17. став 2. овог закона, затим да је иста у складу са посебним прописима који уређују предметну област/делатност, као и да се иста врши у складу са начелима обраде из члана 5. Закона о заштити података о личности и другим одговарајућим правилима и обавезама прописаним тим законом.

Правни оквир и пракса Савета Европе и Европске уније

Општи захтеви заштите података о личности у поступку запослења

У поступку тражења кандидата односно избора кандидата за слободно радно место путем конкурса, послодавци заузимају улогу руковоаца личним подацима кандидата јер одређују сврхе и средства обраде прикупљених података. На основу података о стеченом образовању, кандидати се класификују по академској успешности, помоћу података из психолошких тестова процењује се њихова могућност сарадње с колективом итд., а све да би се одредило који је кандидат најпогоднији за запослење. Као руковоаци личним подацима, послодавци морају да узму у обзир све принципе права заштите података и с обзиром на сврху, средства обраде, трајање чувања података и друге аспекте обраде према кандидатима се понашају што транспарентније.

Конвенција 108+ у члану 5. одређује принципе заштите личних података ради осигуравања легитимности обраде и квалитета личних података које државе чланице морају да обезбеде у националном законодавству и да се побрину за њихово ефикасно спровођење у пракси. Обрада података мора да буде сразмерна легитимном циљу коме тежи и у свим фазама обраде мора да одражава поштену равнотежу свих укључених интереса, како јавних тако и приватних, као и предметних права и слобода. Принцип сразмерности треба поштовати током свих фаза обраде, укључујући почетну фазу, дакле, при одлучивању да ли спровести обраду или је не спровести.

Свака држава уговорница мора да обезбеди да се подаци обрађују на основу добровољног, специфичног, информисаног и недвосмисленог пристанка појединца чији су подаци предмет обраде, или на основу друге законски одређене основе. Ради се о кључном аспект правне основе за обраду података, која је у Конвенцији 108* одређена алтернативно, или пристанку субјекта података или на основу другог права из националног права државе уговорнице. Лични подаци морају да буду обрађени законито, а тај услов је испуњен ако су:

- обрађени поштено и на транспарентан начин,

- прикупљени за изричите, прецизно одређене и законите сврхе и нису обрађени на начин који није у складу с овим сврхама;
- одговарајући, релевантни и не превазилазе сврхе због којих се обрађују;
- тачни и, када је потребно, редовно ажурирани;
- сачувани у форми која омогућава идентификацију појединаца којих се тичу, и то само онолико времена колико је потребно за сврхе због којих се ови подаци обрађују.

Конвенција 108+ у члану 6. уређује посебне категорије података (осетљиви подаци), у које спадају: генетски подаци; лични подаци у вези с кривичним делима, кривичним поступцима и пресудама и повезаним безбедносним мерама; биометријски подаци који јединствено идентификују особу и подаци о личности који обелодањују информације у вези са расним или етничким пореклом, политичким мишљењима, чланством у синдикату, верским или другим уверењима, здрављем или сексуалним животом. Обрада наведених података је дозвољена само уз предуслов да национално право за њих одређује одговарајуће механизме заштите за заштиту од ризика обраде оваквих осетљивих података за основна права и слободе појединаца, првенствено ризик дискриминације.

У складу с чланом 8. Конвенције 108+ државе уговорнице морају да обезбеде прегледност обраде података тако да у национално законодавство унесе обавезу руковооца да појединце обавести о свом идентитету и седишту, правној основи и сврхама обраде података, о категоријама прикупљених података, о лицима којима ће подаци бити прослеђени (ако постоје) и о могућностима појединаца да остваре права која им припадају по члану 9. Конвенције 108+. У њих спада право да за њих не важи одлука донесена на основу аутоматске обраде података без могућности њихове сарадње; право на приступ прикупљеним подацима; право да добију образложење о обради својих података; право на приговор против обраде; право на брисање незаконито прикупљених података и право на одштету.

Као што је наведено у уводу, Конвенција 108+ директно се не тиче обраде података запослених односно кандидата за запослење, а одбор министара Савета Европе усвојио је Препоруку СЕ о личним подацима о запослењу, која у вези с кандидатима за запослење одређује:

- послодавци треба да прикупе личне податке директно од кандидата за радно место; када је потребно да се ти подаци, прикупљени од стране трећих лица обраде, на пример, за стицање стручних референци, и зато постоји законска основа, кандидат о томе треба да буде адекватно и благовремено обавештен;
- лични подаци које послодавци прикупљају у циљу запослења треба да буду релевантни и не претерано опсежни, поштујући врсту запослења;

- послодавци треба да избегну да траже од кандидата за запослење приступ информацијама које деле с другима на мрежи, посебно преко друштвених мрежа;
- здравствени подаци смеју да буду прикупљени само у сврхе наведене у принципу 9 ове препоруке.
- чување личних података у циљу запослења дозвољено је само ако су подаци били прикупљени у складу са захтевима Конвенције 108+ и само у временском року који је неопходан за праћење законитог циља обраде; (т. 5)
- личне податке прикупљене у поступку запослења послодавци могу да обрађују само у те сврхе;
- послодавци треба да усвоје политике заштите података и друге инструменте о интерној употреби личних података у складу с принципима Препоруке СЕ; (т. 6)
- обрада осетљивих података из члана 6. Конвенције 108+ дозвољена је само у посебним случајевима, када се сматра неопходним за запослење на одређено радно место и унутар је граница одређених домаћим законодавством; поред тога, обрада се мора спроводити у складу с одговарајућим безбедносним мерама које допуњавају оне дефинисане у Конвенцији 108+; (т. 9)
- у складу с националним законодавством, послодавци од кандидата могу да добију податке о његовом здрављу или да траже прегледу циљу утврђивања његове погодности за будуће запослење или како би задовољили захтеве превентивне медицине, при чему генетски подаци не смеју да се обрађују у циљу утврђивања професионалне погодности кандидата, чак и ако би на то пристао; (т. 9.2 и 9.3.)
- личне податке који су део пријаве за слободно радно место, послодавац мора да избрише чим констатује да понуда запослења неће бити дата односно када понуда није прихваћена од стране кандидата; ако се чување ових података настави због евентуалне будуће могућности за запослење, о томе треба обавестити кандидата, а на његов захтев треба избрисати податке; (т. 13.2)
- послодавци могу да наставе да чувају податке кандидата за запослење у циљу започињања парничног поступка или у његовој одбрани или за други законити интерес, али само док не постигне ту сврху; (т. 13.3.)
- употреба психолошких тестова, анализа и сличних процедура које спроводе специјализовани стручњаци и предмет су здравствене поверљивости и осмишљени су за процену карактера или личности кандидата за запослење, треба да буде дозвољена само ако је законска и неопходна за тип радног места (садржај радних задатака), и ако национално законодавство обезбеђује одговарајуће механизме заштите;

- кандидат за посао претходно треба да буде обавештен о сврси коришћења резултата ових тестова и затим и о њиховој садржини како би се осигурала транспарентност; (т. 19) кандидату у вези с оваквом обрадом треба да се обезбеди и право на приступ, исправку и приговор. (т. 11)

Питање обраде осетљивих података о личности с друштвених мрежа

Често послодавци желе да створе ширу слику о кандидатима прегледањем њихових профила на друштвеним мрежама, (LinkedIn, Facebook, Instagram и сл.), интернет претраживачима и сличним изворима. Уколико се ради о јавно објављеним подацима и на основу околности је евидентно да их је појединац објавио управо с циљем да буду што доступнији (рецимо, подаци о образовању и радном искуству на профилу *LinkedIn*), њихова обрада ће у принципу бити дозвољена што не важи аутоматски за сваки случај објаве кандидата на његовим (приватним) друштвеним мрежама.

Лични профили кандидата могу да обелодане бројне личне податке који су у смислу права заштите личних података осетљиве природе (нпр. о ентитчкој, политичкој припадности, сексуалној оријентацији кандидата) и уживају квалификовану заштиту пре обраде. И кад би овакви подаци технички били јавно доступни на отвореном профилу, то још не значи да појединац узимајући их у обзир нема разумно очекивање приватности јер и у том случају ужива право на поштовање приватног живота. Пракси *background screening* дакле треба приступити опрезно и неизбежно је проценити и у перспективи забране дискриминације при запошљавању на основу личних околности.

Коришћење друштвених мрежа од стране појединаца је проширено и релативно често су кориснички профили јавно доступни, зависно од подешавања које одабере власник рачунара. Радна група у Мишљењу 2/2017 наглашава да послодавци не смеју да претпостављају да само зато што је профил појединаца на друштвеним мрежама јавно доступан податке могу обрађивати у сопствене сврхе ван домаћег Опште уредбе о заштити података.²⁹ Информације на друштвеним мрежама сматрају се „псеудо-јавним“ (*quasi-public data*),³⁰ јер појединац дели своје податке на платформи друштвених мрежа у одређене сврхе друштвених мрежа и у кругу (очекиваних) корисника. Иако су

29 Радна група за заштиту података из члана 29, Мишљење бр. 2/2017 о обради података на раду, WP 249, Брисел, 8.6.2017., стр. 11.

30 Kira Vrist Rønn & Sille Obelitz Søre (2019) Is social media intelligence private? Privacy in public and the nature of social media intelligence, *Intelligence and National Security*, 34:3, стр. 362-378.

информације објављене јавно, нису нужно увек намењене општој јавности већ појединац може у погледу њих уживати одређено очекивање приватности, која је заштићена основним људским правима на поштовање приватног живота по члану 8. ЕКЉП односно члану 7. Исправе ЕУ о основним правима. Чињеница да су неки подаци јавно доступни на друштвеним мрежама не значи да не постоје ограничења у погледу њиховог коришћења. Принципи ОПШТЕ УРЕДБЕ о заштити личних података, рецимо, сматрају се личним подацима без обзира на подешавања видљивости платформе (нпр. подаци су увек видљиви само другим корисницима, пријатељима, целокупној јавности итд.).

Да би послодавац могао да у складу с правом приступа подацима с друштвених мрежа потенцијалног кандидата и да их обрађује, мора да поступа у складу с принципима права заштите података о личности и у првом реду покаже да за то има одговарајућу правну основу, као што је законски интерес или претходно добијање пристанка предметног кандидата. У овом контексту послодавац пре прегледања профила на друштвеној мрежи мора да узме у обзир да ли је профил тражиоца запослења повезан с пословним или приватним сврхама јер то битно може да утиче на правну дозволу у погледу података. Поред тога, Радна група из члана 29. у Мишљењу 2/2017 предвиђа да послодавци смеју да прикупљају и обрађују осетљиве личне податке у вези с тражиоцима запослења само у обиму који је неопходан и релевантан за обављање посла за који се пријављују.³¹ Овај услов ће, на пример, бити испуњен ако информације треба прикупити за процену специфичних ризика у вези с кандидатима за одређену функцију.³²

Подаци прикупљени током поступка запослења морали би да буду по правилу избрисани чим постане јасно да понуда посла неће бити дата или није прихваћена од стране укљученог појединца. Појединац мора да буде исправно обавештен о било каквој сличној обради пре укључивања у поступак запослења, тј. у објави о слободном радном месту односно у случају директног контактирања потенцијалног кандидата у првој поруци од стране послодавца. Радна група још наглашава да не постоји правна основа која би послодавцу омогућила да од кандидата тражи да прихвати његов захтев за пријатељство на друштвеној мрежи или на било који други начин омогући приступ садржају његовог профила.

31 Радна група за заштиту података из члана 29, Мишљење бр. 2/2017 о обради података на раду, WP 249, стр. 11.

32 Исто.

Коришћење средстава за аутоматско доношење одлука у поступку запошљања

Посебни захтеви за послодавца могу да се појаве у случајевима конкурса када има много пријављених кандидата, при чему послодавац користи средство за аутоматско доношење одлука за сужење круга кандидата (на пример, програм вештачке интелигенције за прегледање и класификацију биографија), а тек након прве селекције затим долази до завршне евалуације о одабраном будућем запосленом или чак препуштања одлуке потпуно аутоматском процесу прикупљања личних података кандидата (*AI Recruitment*). Аутоматско одлучивање праћено је додатним правима субјеката прикупљених података, као што су право на приговор и право да не буду предмет одлуке донесене само на основу аутоматске обраде. Ако је послодавац добио изричито пристанак кандидата на искључиво аутоматску обраду приложених података, мора да прихвати одговарајуће мере за заштиту права и слобода и законских интереса појединца на кога се односе лични подаци, барем право на лично посредовање руковооца, на изражавање сопственог става и одбацивање одлуке.

У складу са чланом 9. Конвенције 108+, појединци имају право да за њих не важи одлука која ће на њих значајно утицати и заснива се само на аутоматској обради а притом се не узимају у обзир њихови ставови. Исту одредбу специјално у контексту радног односа садржи Препорука СЕ.³³ Захтев да се узму у обзир ставови појединца на кога се односе лични подаци када се одлуке заснивају искључиво на аутоматској обради значи да ови појединци имају право да оспоре овакве одлуке и да им треба дати прилику да укажу на све нетачне податке о личности које користи руковалац и оспоре релевантност било ког профила употребљеног за њих.³⁴ Међутим, појединац не може остварити ово право ако је аутоматска одлука дозвољена националним законом који се примењује на руковооца и који такође предвиђа одговарајуће мере за заштиту права, слобода и легитимних интереса појединаца на које се лични подаци односе. У складу са Конвенцијом 108+ и Препорукама СЕ,³⁵ при сваком случају употребе аутоматског одлучивања, државе морају да обезбеде одговарајуће заштитне мере, које треба да обухвате конкретне податке о појединцу на кога се лични подаци односе, као и право на лично посредовање, право да изнесе своје ставове, право да добије образложење одлуке донесене након такве оцене и право да оспори одлуку.

33 11.4. тачка Препорука СЕ.

34 Образложење Конвенције 108+, тачка 75.

35 21. тачка Препорука СЕ.

Аутоматско доношење одлука често укључује процену личних околности дотичне особе и креирање профила, посебно због анализе или предвиђања учинка на послу, економске ситуације, здравља, личног укуса или интересовања, поузданости или понашања, на пример, у контексту онлајн запошљавања, без интервенције људи. Усвајање одлука на основу овакве обраде представља озбиљан ризик за (прикривену) дискриминацију, ако коришћени алгоритам не садржи адекватне механизме заштите, на пример, ако се процедуре запослења паралелно не контролишу од стране физичког лица послодавца. Наведено је посебно важно у вези с правом појединца да тражи образложење о аутоматском процесу одлучивања који утиче на њега.³⁶ Радна група из члана 29. у својим Смерницама о аутоматском доношењу појединачних одлука и профилисању за потребе Уредбе (ЕУ) 2016/679,³⁷ нагласила је да због сложености обраде као такве руковацац не би смео да буде спречен да појединцима на које се односе лични подаци обезбеди јасна појашњења у погледу циљева обраде личних података и коришћене аналитике, што је могуће пренети и на обавезе послодавца да поједине кандидате за посао унапред обавесте о евентуалним системима аутоматског одлучивања који су укључени у њихов поступак запослења, а истовремено интерно брину о разумевању ангажованих алгоритама у случају молбе кандидата за појашњење.

Међународна организација рада је у Кодексу МОР-а нагласила да аутоматске процедуре не ослобађају послодавце обавезе да испитају све неопходне податке за исправну процену резултата аутоматске обраде података запослених. Послодавци не би требало да се мешају у потпуно аутоматске процесе доношења одлука, већ би требало да их користе искључиво као помоћно средство да се запосленима обезбеди да имају право на одговарајући индивидуални третман у сваком случају.³⁸

Вагање између интереса послодавца и основног права на поштовање приватности у поступку избора кандидата за посао

Право на поштовање приватног живота појединаца из члана 8. Европске конвенције за заштиту људских права није апсолутно, већ се може задржати у њега под условима одређеним у ставу 2. наведеног члана: (i) ако је то у складу са законом и (ii) неопходно у демократском друштву у интересу (iii) државне безбедности, јавне безбедности или

³⁶ 11.5. тачка Препорука СЕ.

³⁷ Радна група за заштиту података из члана 29, Смернице о аутоматизованом доношењу појединачних одлука и профилисању за потребе Уредбе (ЕУ) 2016/679, WP251, 3.10.2017, стр. 14.

³⁸ Коментар Кодекса МОР-а, стр. 14.

економског благостања државе зато да се спречи неред или кривично дело, због заштите здравља или морала, или да се заштите права и слободе других.

У области процедура запослења је занимљив случај ЕСЉП у случају *Леандер против Шведске*.³⁹ Господин Леандер се запослио у музеју шведске морнарице (*Naval Museum*), који је лоциран крај самог подручја и обухвата одређене објекте унутар подручја државне војне базе. После мање од две недеље отпуштен је зато што није прошао тестирање контроле особља, спроведено у складу с одредбама националног закона, и у оквиру кога је особље војног руководства приступило тајној фасцикли полиције која садржи личне податке о г. Леандру. Могућност задирања је одређена законом, што у судској пракси ЕСЉП значи да се заснивала на националном праву које је било доступно и имало је предвидљива дејства за предметног појединца. Суд је објаснио да предвидљивост у посебном контексту тајних контрола особља у секторима који утичу на националну безбедност не може бити иста као у другим областима, али је довољно да је закон довољно јасан у погледу услова да се појединцима омогући бар да донесу закључке (индиција) о околностима и условима под којима државни органи имају овлашћење да користе ову врсту тајног задирања у приватни живот. Суд је донео пресуду да тајни надзор кандидата за радна места која су важна за државну безбедност сам по себи није у супротности с условом неопходности у демократском друштву. Узимајући у обзир посебне заштитне мере утврђене у националном закону због заштите интереса појединца на кога се односе подаци, као што је надзор од стране парламента и омбудсмана, утврдио је да шведски систем надзора над запосленима испуњава услове из члана 8. став 2. ЕКЉП. Узимајући у обзир широко поље слободне процене које јој је на располагању, тужена држава је с правом сматрала да су у случају подносиоца тужбе интереси националне безбедности превладали над интересима појединца. Суд је констатовао да није дошло до повреде члана 8. ЕКЉП.

Препоруке за усклађивање

У погледу испуњавања услова за заснивање радног односа потребно је размотрити одредбе закона којима се прописује обрада података о личности који се односе на кривичне пресуде, кажњива дела и мере безбедности. Имајући у виду различите законе којима се пропи-

³⁹ Пресуда ЕСЉП у предмету Леандер против Шведске од 26.3.1987, представка бр. 9248/81.

сује обрада ових података, као примери се могу навести обрада података прописана чланом 139. Закона о основама система образовања и васпитања у погледу заснивања радног односа у средњој школи унутрашњих послова.

Одредбу чл. 45. Закона о државним службеницима која се односи на општи услов за заснивање радног односа у државним органима - да лицу раније није престајао радни однос у државном органу због теже повреде дужности из радног односа, као и да није осуђивано на казну затвора од најмање шест месеци, без обзира на врсту послова које ће то лице обављати, потребно је размотрити. Исти коментар односи се и на одредбу члана 80. Закона о запосленима у аутономним покрајинама и јединицама локалне самоуправе. Одредбе је потребно преиспитати и са становишта целисходности обраде, без обзира на дело, како је то случај са условима за обављање других послова, у односу на које је законодавац утврдио групу дела у односу на које се подаци обрађују. Поред тога, потребно је размотрити да ли овај услов, податак о осуђиваности, може бити основан и код заснивања радног односа код послодавца ван ових случајева, под условима који би посебно били прописани законом, а који би прописао и мере заштите права и интереса лица не које се подаци односе. Ово стога што у пракси није неубичајено да кандидат достави податке из казнене евиденције, као потврду о неосуђиваности. Тиме би се адекватно уредила ова обрада и отклонила неадекватна пракса уз поштовање права лица, али и, у појединим случајевима, уз поштовање интереса послодавца.

У току поступка испитивања кандидата, употреба тестова није неубичајена. Уредба о интерном и јавном конкурс за попуњавање радних места у државним органима прописује обавезу примене, примера ради, психометријских тестова или које спроводе психолози (чл. 44.). Имајући у виду домаћај ових тестова, питање је да ли овај вид тестирања неопходан за сва радна места без изузетка. Уједно, Уредбом нису прописане мере безбедности података. Стога је потребно преиспитати неопходност обраде сваког кандидата и уредити одредбе о безбедности података.

Узбуњивање

Правни оквир

Закон о заштити узбуњивача усвојен је 2014. године, и није био предмет каснијих измена или допуна. Како је у дефиницији појма наведено, узбуњивање је откривање информација о кршењу прописа, кршењу људских права, вршењу јавног овлашћења противно сврси због које је поверено, опасности по живот, јавно здравље, безбедност, као и ради спречавања штете великих размера. Иако узбуњивач може бити и лице које није у радном односу код послодавца, у пракси се најчешће овај појам везује за радне односе. У вези са заштитом података о личности, код узбуњивања она се односи како на податке о лицу које врши узбуњивање, дакле о узбуњивачу, уколико узбуњивање није анонимно, тако и на податке који се односе на лица у односу на које се врши узбуњивање, у оним случајевима када се узбуњивање односи не само на догађај, него и могуће виновнике.

Према Закону, могуће је да лице анонимно достави информацију о неком кажњивом, односно штетном делу. Уколико се одлучи да то учини у личном својству, Закон прописује обавезу у вези са чувањем података о личности и обавештавањем лица о могућим примаоцима података. Према члану 10. Закона о заштити узбуњивача, лице које је овлашћено за пријем информације дужно је да штити податке о личности узбуњивача, односно податке на основу којих се може открити идентитет узбуњивача, осим ако се узбуњивач не сагласи са откривањем тих података, а у складу са законом који уређује заштиту података о личности. Обавеза чувања поверљивости ових података односи се и на друга лица којима су подаци откривени или су остварили увид у њих. Истим чланом прописана је обавеза да лице овлашћено за пријем информације приликом пријема информације, обавести узбуњивача да његов идентитет може бити откривен надлежном органу, ако без откривања идентитета узбуњивача не би било могуће поступање тог органа, као и да га обавести о мерама заштите учесника у кривичном поступку. Такође, ако је у току поступка неопходно да се открије идентитет узбуњивача, лице овлашћено за пријем информације дужно је да о томе, пре откривања идентитета, обавести узбуњивача.

Подаци који се односе на идентитет узбуњивача не смеју се саопштити лицу на које се указује у информацији, ако посебним законом није другачије прописано. Ова одредба уједно је и одредба о ограничењу

права тог лица на које се подаци односе према члану 40. Закона о заштити података о личности. Основ за ограничење права лица на које се указује у информацији може бити заштита лица на које се подаци односе, дакле право на заштиту података о личности који се односе на узбуњивача. Такође, основ ограничења може бити и права и слободe других лица, као што то може бити случај са другим правима лица које се сматра узбуњивачем, примера ради слобода изражавања, али и безбедност тог лица.

Међутим, овај закон не прописује мере заштите података у односу на лице на које се указује у информацији коју узбуњивач пружа. У том погледу, Закон треба допунити одредбама о заштити података у односу на ово лице, односно лица.

Начин на који је послодавац организовао систем узбуњивања може имати утицај на примену других института из Закона о заштити података о личности. У великим системима, где је непосредан однос између запослених у различитим секторима, деловима или јединицама, може се замислити ситуација да је начин пријаве дигитализован, у смислу да се врши кроз информационе и комуникационе технологије. Самим тим, овај начин обраде може резултирати стварањем ризика по права и слободe лица, као што то може бити случај са ризиком по право на приватност (као бојазан лица да ће његов идентитет бити откривен другим лицима) или слободу изражавања (чињеница да лице сматра да због технологије не може анонимно да изврши узбуњивање може да спречи лице да пријави информације). У тим случајевима ће послодавац бити у обавези да изврши процену утицаја на заштиту података о личности.

Из праксе Повереника

Обрада података о личности ББ, запосленог у Министарству унутрашњих послова, од стране лица овлашћеног за пријем информација и вођење поступка у вези са унутрашњим узбуњивањем у Управи криминалистичке полиције Министарства унутрашњих послова Републике Србије у току поступка унутрашњег узбуњивања.

Број предмета: 072-04-741/2021-07

Увод

Поверенику је, од стране Управног инспектората, на даље поступање прослеђена представка, којом је пред Управним инспекторатом покренута иницијатива за вршење инспекцијског надзора над применом Закона о заштити узбуњивача, од стране лица овлашћеног за пријем информација и вођење поступка у вези са унутрашњим узбуњивањем у Управи криминалистичке полиције Министарства унутрашњих послова Републике Србије. У представци се, између осталог, наводи да је лице овлашћено за пријем информација и вођење поступка у вези са унутрашњим узбуњивањем у Управи криминалистичке полиције Министарства унутрашњих послова Републике Србије, сачинило Извештај Овлашћеног лица, при чему није заштитило податке узбуњивача, односно податке на основу којих се може открити идентитет узбуњивача, чиме је повредио члан 10. став 1. Закона о заштити узбуњивача.

Из одговора Повереника:

Чланом 2. ставом 1. Закона о заштити узбуњивача („Службени гласник РС“, бр. 128/2014) прописано је да је узбуњивање откривање информације о кршењу прописа, кршењу људских права, вршењу јавног овлашћења противно сврси због које је поверено, опасности по живот, јавно здравље, безбедност, животну средину, као и ради спречавања штете великих размера, а ставом 2. истог члана прописано је да је узбуњивач физичко лице које изврши узбуњивање у вези са својим радним ангажовањем, поступком запошљавања, коришћењем услуга државних и других органа, носилаца јавних овлашћења или јавних служби, пословном сарадњом и правом власништва на привредном друштву.

Чланом 10. истог закона прописано је да је лице које је овлашћено за пријем информације дужно да, штити податке о личности узбуњивача, односно податке на основу којих се може открити идентитет узбуњивача, осим ако се узбуњивач не сагласи са откривањем тих података, а у складу са законом који уређује заштиту података о личности. Свако лице које сазна податке из става 1. овог члана, дужно је да штити те податке. Лице овлашћено за пријем информације дужно је да приликом пријема информације, обавести узбуњивача да његов идентитет може бити откривен надлежном органу, ако без откривања идентитета узбуњивача не би било могуће поступање тог органа, као и да га обавести о мерама заштите учесника у кривичном поступку. Ако је у току поступка неопходно да се открије идентитет узбуњивача, лице овлашћено за пријем информације дужно је да о томе, пре откривања идентитета, обавести узбуњивача. Подаци из става 1. овог члана не смеју се саопштити лицу на које се указује у информацији, ако посебним законом није другачије прописано.

Чланом 14. став 5. Закона о заштити узбуњивача прописано је да је послодавац дужан да одреди лице овлашћено за пријем информације и вођење поступка у вези са узбуњивањем, док је чланом 15. став 1. истог закона прописано да поступак унутрашњег узбуњивања започине достављањем информације послодавцу. Ставом 2. истог члана закона прописано је да је послодавац дужан да поступи по информацији без одлагања, а најкасније у року од 15 дана од дана пријема информације, а ставом 3. и 4. да је послодавац дужан да обавести узбуњивача о исходу поступка по његовом окончању, у року од 15 дана од дана окончања поступка из става 1. овог члана и да је дужан да, на захтев узбуњивача, пружи обавештења узбуњивачу о току и радњама предузетим у поступку, као и да омогући узбуњивачу да изврши увид у списе предмета и да присуствује радњама у поступку.

Чланом 7. став 2. Правилника о начину унутрашњег узбуњивања, начину одређивања овлашћеног лица код послодавца, као и другим питањима од значаја за унутрашње узбуњивање код послодавца који има више од десет запослених („Службени гласник РС“, бр. 49/2015 и 44/2018-др.закон) прописано је да се у циљу провере информације у вези са унутрашњим узбуњивањем, предузимају одговарајуће радње, о чему се обавештава послодавац, као и узбуњивач, уколико је то могуће на основу расположивих података.

Увидом у Извештај Лица овлашћеног за пријем информације и вођење поступка у вези са унутрашњим узбуњивањем у Министарству унутрашњих послова број: хх од 22.12.2021. године, утврђено је да је ово лице при провери навода у вези са примљеном информацијом надлежним службама указало да је при предузимању свих радњи из њихове надлежности, потребно штитити податке о личности узбуњивача, у

складу са чланом 10. став 5. Закона о заштити узбуњивача. Додатно, из изјашњења Руковаоца, утврђено је да се овлашћено лице није обраћало лицу на које се информација односила, нити је податке садржане у информацији учинило доступним другим лицима, осим организационим јединицама пред којима се вршила провера навода узбуњивача и достављене информације.

Како је одредбама члана 36. Закона о заштити узбуњивача, прописано да надзор над спровођењем овог закона врши управна инспекција, уколико је у самом поступку унутрашњег узбуњивања било пропуста, исте ће утврдити управна инспекција.

Правни оквир и пракса Савета Европе и Европске уније

Кључни аспект који омогућава примену шема за пријаву неправилности јесте и очување поверљивости узбуњивача и заштита идентитета наводног прекршиоца током истражног поступка. Функционисање интерног система пријава прекршаја зависи од обраде података о личности (тј. од прикупљања, чувања, обелодањивања и уништавања података у вези с одређеном или особом која се може идентификовати), што значи да се примењују правила о заштити података. На почетку, с обзиром на садржај релевантне публикације, треба истаћи да широка употреба технологија надзора на радном месту као таква може имати одбојан ефекат на спремност запослених да обавештавају послодавца о неправилностима или незаконитим радњама својих надређених или других запослених, јер отежава очување анонимности узбуњивача. Радна група из члана 29. упозорава да у оваквом случају успостављена средства за интерне узбуњиваче могу да постану неефикасна.⁴⁰

Савет министара у Препоруци СЕ наглашава да послодавци морају да обезбеде заштиту података о личности свих укључених страна када су по закону или интерним правилима дужни да спроводе интерне механизме за извештавање, као што су отворене телефонске линије. Послодавци би нарочито морали да обезбеде поверљивост запосленог који извештава о незаконитом или неетичком поступању (*whistleblower*). Личне податке укључених лица треба искористити искључиво у сврхе одговарајућих интерних поступака у вези с пријавом и као што траже прописи односно као што је потребно за евентуалне касније судске поступке.⁴¹ Интерне истраге се не би смеле спроводити само

40 Радна група за заштиту података из члана 29, Мишљење бр. 2/2017 о обради података на раду, WP 249, Брисел, 8.6.2017., стр. 10.

41 17.1. тачка Препорука СЕ.

на основу анонимне пријаве, осим ако су прописно утемељене и односе се на тешке повреде домаћег законодавства, дакле, само у изузетним случајевима.⁴²

Што се тиче заштите података о личности у системима за пријаву прекршаја, користан правни извор је директива Европске уније о заштити лица која пријављују повреде права уније.⁴³ Наведена директива уређује да свака обрада података о личности за функционисање интерног механизма пријаве повреда треба да буде извршена у складу с правилима, а посебно су наглашени принципи сразмерности и минимизације. Подаци о личности који очигледно нису релевантни за обраду конкретне пријаве не прикупљају се или, ако су прикупљени грешком, бришу се без непотребног одлагања.⁴⁴

Државе чланице имају обавезу чувања поверљивости, у складу с којом морају да обезбеде да се идентитет узбуњивача не открије без изричите сагласности ове особе никоме осим овлашћеном особљу надлежном за пријем пријава или даље предузимање мера на основу пријава. То важи и за све друге информације на основу којих је могуће посредно или непосредно донети закључак о идентитету узбуњивача.⁴⁵ У изузетним случајевима се идентитет узбуњивача може обелоданити онда када је то неопходна и сразмерна дужност према националном праву у вези с истрагама националних органа или судским поступцима и у циљу заштите права лица којег се пријава тиче. У оваквим случајевима обелодањивања, у складу с националним правом, примењују се адекватне заштитне мере. Посебно узбуњиваче треба обавестити пре него што се њихов идентитет обелодани, осим у случају да овакво обавештење угрози повезане истраге или судске поступке. При обавештавању пријављивача, надлежни орган им шаље писмено појашњење о разлозима обелодањивања предметних поверљивих података.⁴⁶

При очувању поверљивости идентитета узбуњивача који пријављује повреде не треба заборавити и на право приватности и интегритета наводног прекршиоца. Радна група из члана 29. наглашава да шеме узбуњивања представљају веома озбиљан ризик од стигматизације и виктимизације пријављеног запосленог у организацији којој

42 17.2. тачка Препорука СЕ.

43 Директива (ЕУ) 2019/1937 Европског парламента и Савета од 23.10. 2019. о заштити лица која пријављују повреде права ЕУ.

44 Члан 17 Директиве (ЕУ) 2019/1937.

45 Члан 16 Директиве (ЕУ) 2019/1937.

46 Члан 16 Директиве (ЕУ) 2019/1937.

припада.⁴⁷ Наводни прекршилац ће бити изложен оваквим ризицима чак и пре него што буде свестан да је инкриминисан и пре него што се испитају наводне чињенице како би се утврдило да ли су оптужбе оправдане или нису. С тим у вези, радна група препоручује да се посебна пажња посвети појединцу који је оптужен, али и даље има права која су му дата у складу са међународним и националним прописима о заштити података о личности.⁴⁸

Препоруке за усклађивање

У погледу узбуњивања, односно заштите података о личности насталих применом Закона о заштити узбуњивача потребно је ревидирати Закон у делу који се односи на заштиту података који се односе и на лица у односу на која се врши узбуњивање.

47 Радна група за заштиту података из члана 29, Мишљење 1/2006 о примени правила ЕУ о заштити података код интерних шема за пријаву неправилности у области рачуноводства, интерног рачуноводственог надзора, послова ревизије, борбе против корупције, банкарског и финансијског криминала, WP 117, Брисел, 1.2.2006, стр. 6.

48 Исто.

Видео надзор

Правни оквир

Видео надзор није посебно уређена радња обраде података о личности. Закон о заштити података о личности упућује на могући видео надзор управо у одредби која се односи на обраду у области рада и запошљавања. Према члану 91. Закона, ако закон који уређује рад и запошљавање или колективни уговор садрже одредбе о заштити података о личности, морају се прописати и посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини. Дакле, и из ове законске одредбе може се извести закључак да је надзор, па и видео-надзор, запослених дозвољена обрада података. То не значи да је сваки видео-надзор дозвољен, већ се морају поштовати пре свега општа правила ограничавања права, према члану 18. Устава Републике Србије, законом се може прописати начин остваривања ових права само ако је то Уставом изричито предвиђено или ако је то неопходно за остварење појединог права због његове природе, при чему закон ни у ком случају не сме да утиче на суштину зајемченог права.

Приликом успостављања система видео-надзора, поред Закона о заштити података о личности, примењиваће се и Закон о приватном обезбеђењу, којим приватно обезбеђење, у смислу тог закона, обухвата пружање услуга, односно вршење послова заштита лица, имовине и пословања физичком и техничком заштитом. Иако би се могло оспоравати да ли је сваки видео-надзор у радном окружењу у функцији заштите лице, имовине и пословања, треба имати у виду да су послови приватног обезбеђења условљени постојањем лиценце Министарства унутрашњих послова. Један од примера таквог видео-надзора, односно снимања лица, могло би бити снимање испита кандидата за одређено радно место. Екстензивним тумачењем „у функцији заштите пословања“ и за овај видео надзор могло би да се тврди да је у функцији заштите пословања.

Међутим, ни Закон о приватном обезбеђењу не садржи детаљније одредбе о видео-надзору. Према члану 30. Закона, видео-обезбеђење сматра се техничком мером, и као таква може уследити тек након, и на основу, извршене процене ризика у заштити лица, имовине и пословања

(чл. 34.). Стога у процесу увођења видео-надзора у радном окружењу, према законима Републике Србије, успостављена је надлежност је како Повереника за информације од јавног значаја и заштиту података о личности у домену обраде података, односно примене начела обраде, права лица на које се подаци односе и појединачних обавеза руковалаца, тако и Министарства унутрашњих послова, у домену услуга приватног обезбеђења, односно постојање адекватне лиценце како оног пружаоца услуга приватног обезбеђење које је израдило процену ризика, тако и оног који пружа услугу ове техничке мере заштите. Послодавац би могао самостално да успостави систем видео-надзора у случају обављања лиценциране самозаштитне делатности у складу са чланом 45. Закона о приватном обезбеђењу.

Видео-надзор као радња обраде података може бити у функцији различитих сврха обраде података о личности. Примера ради, камера инсталирана на једном месту може уједно да служи и за контролу уласка у просторије послодавца, као и за бележење времена доласка појединачног запосленог на радно место, али и за континуиран надзор запослених. Ово последње у изузетним случајевима. С обзиром на то да су у питању различите сврхе обраде, ради се о различитим обрадама и свака од њих мора да буде у складу са Законом о заштити података о личности. У погледу основа обраде, правни основ ће углавном бити легитимни интерес послодавца или трећег лица, а што такође подразумева процену и документовање. Међутим, за разлику од процене ризика према Закону о приватном обезбеђењу чија је сврха да се установе ризици по послодавца, а тиме и мере (начин) смањивања ризика, процена легитимног интереса према Закону о заштити података о личности мора бити извршена тако да се узму у обзир, између осталог, права и слободе лица на које се односе подаци који ће се обрађивати овим путем.

Обавештење о видео надзору прописано је чланом 32. Закона о приватном обезбеђењу уколико је реч о објектима или просторима који се користе за јавну употребу. И ови објекти и простори могу уједно да буду радно окружење за запослена лица у тим објектима и просторима. Ипак, садржина овог обавештења не одговара у потпуности садржини обавештења о обради према Закону о заштити података о личности. Стога, обавештење о обради података, у овом случају обавештење о обради путем видео-надзора, је обавеза руковаоца који је дужан да лица на које се подаци односе обавести пре прве радне обраде података о томе обавести лица.

Избор врсте уређаја, односно техничких могућности камере, као и место постављања и угао снимања или опсег, такође су значајни. Тај визуелни угао треба да снима само онај простор који је неопходан за остварење сврхе и, с тим у вези, је значајна примена начела минимизације података. Није исто да ли камера обухвата искључиво простор послодавца који се односи на руковање новцем или и друге делове,

као ни да ли су камере постављене у просторима ограниченог приступа или свим просторијама послодавца, или просторијама где је очекивана неформална интеракција лица. Такође, иако је један систем успостављен за различите сврхе, рокови чувања, а тиме и коришћење података о личности насталих снимањем, може да буде различити. Подужа је листа питања које треба имати у виду да би обрада података овим начином била у складу са законима, уз поштовање права и слободе лица. Није исто да ли снимак може да се користи за обраду биометријских података, као што је лик лица, у циљу јединствене идентификације лица добијен посебном техничком обрадом, или не. У првом случају примењиваће се и додатни услови будући да је реч о посебној врсти података о личности у смислу Закона о заштити података о личности. На крају, посебан изазов би представљао видео надзор са могућношћу аудио снимања.

Из праксе Повереника

Питање: Да ли би послодавац могао да имплементира камере које снимају звук у пулту послодавца, као месту где се налази каса и новац? Разлог за овакво поступање би пре свега било награђивање и исплата стимулације запосленима, а које би могло касније да се користи и за утврђивање повреде радне обавезе. У питању је руковалац истакао и питање одређивања групе лица за послове „слушања разговора“, као и питање да ли би „у том случају сврсисходније било да се у реалном времену слушају запослени, и с тим у вези да записе не чувамо, или можемо да снимамо разговоре и потом их овај тим људи преслушамо“. На крају је наведено да би обавештење о аудио запису био део уговора о раду.

Број предмета: 073-14-1018/2022-02

Са становишта заштите података о личности указујемо да обрада података о личности употребом система видео или аудио надзора може значајно да угрози приватност појединаца, али и друга права и слободе физичких лица чији подаци о личности се овим путем обрађују, те се у сваком конкретном случају најпре мора размотрити неопходност и сразмерност такве обраде, а имајући у виду начела обраде из члана 5. Закона о заштити података о личности.

Најпре указујемо на то да Закон о заштити података о личности („Сл. гласник РС“, бр. 87/2018) не садржи посебне одредбе о видео и аудио надзору.

Међутим, обрада података о личности путем видео и/или аудио надзора представља радњу обраде у смислу одредбе члана 4. тачка 3. Закона, и на исту се примењују општа начела обраде из члана 5. овог закона, као и друга одговарајућа правила и обавезе за руковооце прописана овим законом, у зависности од околности у сваком конкретном случају.

Сагласно члану 5. став 1. наведеног закона, подаци о личности морају: 1) се обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе („законитост, поштење и транспарентност“). Законита обрада је обрада која се врши у складу са овим законом, односно другим законом којим се уређује обрада; 2) се прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама („ограничење у односу на сврху обраде“); 3) бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде („минимизација података“); 4) бити тачни и, ако је то неопходно, ажурирани. Узимајући у обзир сврху обраде, морају се предузети све разумне мере којима се обезбеђује да се нетачни подаци о личности без одлагања избришу или исправе („тачност“); 5) се чувати у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде („ограничење чувања“); 6) се обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера („интегритет и поверљивост“). У ставу 2. истог члана Закона је прописано да је руковалац одговоран за примену одредаба става 1. овог члана и мора бити у могућности да предочи њихову примену („одговорност за поступање“).

Одредбама члана 12. Закона утврђено је да је обрада података о личности законита само ако је испуњен један од следећих услова: 1) лице на које се подаци о личности односе је пристало на обраду својих података о личности за једну или више посебно одређених сврха; 2) обрада је неопходна за извршење уговора закљученог са лицем на које се подаци односе или за предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора; 3) обрада је неопходна у циљу поштовања правних обавеза руковооца; 4) обрада је неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица; 5) обрада је неопходна у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења руковооца; 6) обрада је неопходна у циљу остваривања легитимних интереса руковооца или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе

лица на које се подаци односе који захтевају заштиту података о личности, а посебно ако је лице на које се подаци односе малолетно лице.

Дакле, да би обрада података о личности била дозвољена најпре је потребно да сврха обраде буде конкретно одређена, изричита, оправдана и законита, да је обрада у складу са посебним прописима који уређују предметну област/делатност, да постоји одговарајући правни основ, у смислу члана 12. Закона, да се иста врши у складу са начелима обраде из члана 5. овог закона, а посебно начелима „ограничење у односу на сврху обраде“ и „минимизација података“, као и у складу са другим одговарајућим правилима и обавезама прописаним овим законом, у зависности од чињеница и околности у сваком конкретном случају. Уколико наведени услови нису испуњени, таква обрада података о личности била би недозвољена.

Такође, указујемо и на то да се, у складу са одредбама члана 91. Закона, на обраду података о личности у области рада и запошљавања примењују одредбе закона којима се уређује рад и запошљавање и колективни уговори, уз примену одредби овог закона.

Према томе када је реч о обради података о личности запослених од стране послодавца, првенствено се примењују одредбе Закона о раду и других закона којима су уређена питања рада и запошљавања.

Сагласно одредби члана 1. став 1. Закона о раду („Сл. гласник РС“, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - одлука УС, 113/2017 и 95/2018 - аутентично тумачење) права, обавезе и одговорности из радног односа, односно по основу рада, уређују се овим законом и посебним законом, у складу са ратификованим међународним конвенцијама па се, сагласно наведеном, ради добијања мишљења о примени наведених прописа, можете обратити Министарству за рад, запошљавање, борачка и социјална питања.

Са становишта заштите података о личности указујемо да обрада података о личности употребом система видео или аудио надзора може значајно да угрози приватност појединаца, али и друга права и слободе физичких лица чији подаци о личности се овим путем обрађују.

Када је у питању обрада података о личности запослених путем видео, аудио надзора или употребом других система за праћење њиховог рада, кретања и сл, мора се имати у виду да запослени имају право на приватност у свом радном окружењу, и да се у сваком конкретном случају најпре мора размотрити неопходност и сразмерност такве обраде, а имајући у виду начела обраде из члана 5. Закона.

Овом приликом указујемо и на обавезу за руковооце, утврђену одредбом члана 54. Закона. Наиме, у случају када је вероватно да ће нека врста обраде, посебно употребом нових технологија и узимајући у обзир природу, обим, околности и сврху обраде, проузроковати висок ризик за права и слободе физичких лица, руковалац је дужан да

пре него што започне са обрадом изврши процену утицаја предвиђених радњи обраде на заштиту података о личности.

Повереник је донео 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 („Сл. гласник РС“ број 45/2019 и 112/20).

Између осталог, једна од радњи обраде за коју се мора извршити процена утицаја на заштиту података о личности, прописана тачком 7) наведене одлуке, је обрада биометријских података у циљу јединствене идентификације запослених од стране послодавца и у другим случајевима обрада података о личности запослених од стране послодавца употребом апликација или система за праћење њиховог рада, кретања, комуникације и сл.

Такође указујемо да сагласно одредби члана 82. став 1. Закона, лице на које се подаци односе има право да поднесе притужбу Поверенику ако сматра да је обрада података о његовој личности извршена супротно одредбама овог закона, а може затражити и одговарајућу судску заштиту, подношењем тужбе надлежном вишем суду, сагласно одредби члана 84. Закона о заштити података о личности.

Сагласно члану 5. став 2. Закона, одговорност за поступање је на руковоацу, стога руковалац је тај који мора бити у могућности да предочи, односно докаже извршавање Законом предвиђених обавеза у вези са обрадом података.

Питање: Да ли је законита обрада података о личности путем видео надзора у малопродајном објекту који продаје робу велике вредности – златари

Број предмета: 072-21-614/2023-07

Увод

Пуномоћник М.С. је доставио представку у којој наводи да његова клијенткињу ради у малопродајном објекту (у златари), у којем се непрекидно врши видео надзора целог продајног простора. На основу притужби других запослених да М.С. не проводи све време у продајном простору, већ у другој просторији, Руковалац је на основу снимљеног материјала утврдио тачност ових навода.

На основу сазнања добијених од других запослених, власника малопродајних објеката у близини и других лица, а са материјалним доказом који је прикупљен видео надзором, Руковалац упозорава С.М.

да не испуњава радне обавезе, између осталог да није стално пристуна у продајном простору у којем се налази имовина велике вредности и каса са новцем.

Даље је у представци пуномоћника наведено да је М.С. „дала изричиту забрану да је снимају док је на свом радном месту“, а да пуномоћник М.С. сматра да „оправдан разлог за угрожавање и ограничавање права личности није заштита имовине послодавца у ситуацији када послодавац може да запосли обезбеђење и тиме постигне и већи степен безбедности и заштите.“

Утврђено чињенично стање:

- Руковалац врши обраду података о личности путем система видео надзора који чине 5 камера које се налазе у продајном простору и једна која се налази у просторији са сефом.
- Систем видео надзора инсталиран је од стране предузећа „ХХ д.о.о“, које је израдило Процену ризика у заштити лица, имовине и пословања за златару.
- Приступ снимљеним подацима има директорка, такође и администратор система, у случају да неко из продајног простора притисне аларм због угрожавања безбедности имовине и лица.
- М.С. запослена у продајном објекту, према пријави запослених и других лица која су то приметили, није проводила време у продајном простору, чиме је каса и изложена имовина остављана без надзора. Имајући у виду да је на тај начин долазило до угрожавања безбедности имовине златаре, извршен је увид у видео снимке чиме су ове сумње потврђене.
- Подаци прикупљени путем видео надзора чувају се 30 дана.

Закључак

Имајући у виду да је Руковалац видео надзор поставио у сврху заштите имовине и пословања, да је видео надзор инсталиран у складу са одредбама Закона о приватном обезбеђењу (“Сл. гласник РС”, бр. 104/2013, 42/2015 и 87/2018) којим је уређена област видео надзора, и то од стане лиценциране фирме која је израдила Процену ризика у заштити лица, имовине и пословања за Руковаоца, да је надзор инсталиран у сврху заштите имовине и пословања, те да се напуштањем продајног простора роба велике вредности као и каса излажу ризику од крађе, то обрада података путем видео надзора није у супротности са начелима обраде ЗЗПЛ.

Питање: Да ли је дозвољен видео надзор запосленог за време рада на уређају велике финансијске вредности, са радиоактивним материјалом?

Број предмета: 072-04-2592/2021-07

Из одговора:

Поверенику за информације од јавног значаја и заштиту података о личности (у даљем тексту: Повереник), доставили сте представку поводом постављања видео надзора у Лабораторији за деструктивну карактеризацију радиоактивног отпада, која припада Сектору за управљање радиоактивним отпадом. Тим поводом, Повереник је преко овлашћеног лица, у циљу прикупљања података од значаја за евентуално вршење ванредног инспекцијског надзора актима од 09.11.2021. 25.11.2021 године, упутио ЈП Нуклеарни објекти Србије захтев да се изјасни на наведене околности, као и да наведе правни основ и сврху предметне обраде података о личности.

Руковалац се изјаснио дописима од 23.11.2021. и 26.11.2021. године, у којима је наведено, да је Влада Републике Србије оснивањем доделила Предузећу објекте на управљање на сигуран и безбедан начин, те да је пројектовање и имплементација мера радијационе и нуклеарне сигурности и безбедности једна од основних делатности предузећа. Такође, да је цео процес управљања радиоактивним отпадом, између осталог, покривен системом видео надзора у сврху обезбеђивања целог тока кретања радиоактивних материјала. Лабораторија за деструктивну карактеризацију радиоактивног отпада је, према наводима, део интегралне акредитоване и сертификоване по ISO 9001:2015 стандарду Лабораторије на нивоу Предузећа, а једано од основних захтева стандарда је да се у лабораторијски простор имплементирају мере безбедности како би се спречило неовлашћено коришћење опреме и како би комплетан процес рада био покривен и са безбедносног аспекта. Део лабораторијског простора, према наводима из изјашњења, биће коришћен за деструктивну карактеризацију радиоактивног отпада и ту ће долазити радиоактивни узорци.

Као правни основ за имплементацију система видео надзора у ЈП Нуклеарни објекти Србије наведене су одредбе следећих прописа:

- Закон о радијационој и нуклеарној безбедности (“Сл. гласник РС”, бр. 95/2018 и 10/2019), члан 188.
- Уредба о мерама безбедности нуклеарних објеката и нуклеарних материјала (“Сл. гласник РС”, бр. 39/2014), члан 11.
- Закон о приватном обезбеђењу (Сл. гласник РС бр. 104/2013, 42/2015 и 87/2018), чл. 30,31,32, и 45.

– Правилник о начину и вршењу послова техничке заштите и коришћења техничких средстава („Сл. гласник РС“ бр. 91/2019), члан 6.

У прилогу изјашњења Руковалац је доставио Решење од 05.08.2021. године којим се ЈП Нуклерани објекти Србије издаје Лиценца за рад нуклеарног постројења за безбедно складиштење извора јонизујућих зрачења БС, као и Решење од 13.09.2021. године којим се овом предузећу издаје лиценца за рад нуклеарног постројења за складиштење радиоактивног отпада ХЗ.

Имајући у виду наведено, у наставку, детаљније указујемо на законски оквир конкретне обраде података.

Чланом 42. Устава Републике Србије („Сл. гласник РС“, број 98/06) зајемчена је заштита података о личности, а истовремено је прописано да се прикупљање, држање, обрада и коришћење података о личности уређују законом, да је забрањена и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом, као и да свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом, и право на судску заштиту због њихове злоупотребе.

Сагласно одредбама члана 4. став 1. тач. 3) и 8) обрада података о личности је свака радња или скуп радњи које се врше са подацима о личности као што су прикупљање, бележење, разврставање, груписање, односно структурисање, похрањивање, уподобљавање или мењање, откривање, увид, употреба, откривање преносом, односно достављањем, умножавање, ширење или на други начин чињење доступним, упоређивање, ограничавање, брисање или уништавање, док руковалац података може бити физичко или правно лице, односно орган власти који самостално или заједно са другима одређује сврху и начин обраде.

Одредбама члана 5. став 1. ЗЗПЛ прописана су и утврђена начела обраде података о личности, односно да се подаци о личности морају: обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе, те да је законита обрада она обрада која се врши у складу са овим законом, односно другим законом којим се уређује обрада ("законитост, поштење и транспарентност"); прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама ("ограничење у односу на сврху обраде"); бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде ("минимизација података"); бити тачни и, ако је то неопходно, ажурирани, те да се морају предузети све разумне мере којима се обезбеђује да се нетачни подаци о личности без одлагања избришу или исправе ("тачност"); чувати у облику који омогућава идентификацију лица само

у року који је неопходан за остваривање сврхе обраде ("ограничење чувања"); обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера ("интегритет и поверљивост"). сагласно ставу 2. овог члана 33ПЛ руковалац је одговоран за примену одредаба из става 1. овог члана и мора бити у могућности да предочи њихову примену („одговорност за поступање“).

Такође, указујемо да је чланом 12. став 1. 33ПЛ прописано да је обрада података о личности законита само ако је испуњен један од следећих услова: 1) лице на које се подаци о личности односе је пристало на обраду својих података о личности за једну или више посебно одређених сврха; 2) обрада је неопходна за извршење уговора закљученог са лицем на које се подаци односе или за предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора; 3) обрада је неопходна у циљу поштовања правних обавеза руковоаца; 4) обрада је неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица; 5) обрада је неопходна у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења руковоаца; 6) обрада је неопходна у циљу остваривања легитимних интереса руковоаца или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се подаци односе који захтевају заштиту података о личности, а посебно ако је лице на које се подаци односе малолетно лице.

Обрада података о личности путем видео надзора и других техничких средстава уређена је одредбама Закона о приватном обезбеђењу ("Сл. гласник РС", бр. 104/2013, 42/2015 и 87/2018), док је начин вршења послова техничке заштите и коришћења техничких средстава у обављању послова приватног обезбеђења, укључујући и видео обезбеђење, ближе уређен Правилником о начину вршења послова техничке заштите и коришћења техничких средстава ("Сл. гласник РС", бр. 91/2019).

Чланом 31. Закона о приватном обезбеђењу прописано је да се техничка заштита спроводи на подручју штићеног објекта или простора, приликом обезбеђења штићених лица, имовине и пословања, или приликом обезбеђења транспорта новца и вредносних пошилики, као и да техничка средства која се користе у обављању послова приватног обезбеђења није дозвољено користити на начин којим се нарушава приватност других.

Даље, члан 32. наведеног закона прописује да, када се послови заштите објекта или простора који се користе за јавну употребу врше уз употребу уређаја за снимање слике, правно лице и предузетник за

приватно обезбеђење дужни су да на видљивом месту истакну обавештење да је објекат или простор заштићен видео обезбеђењем, а корисник услуга је обавезан да то прихвати и архивирани снимке чува најмање 30 дана и да их, на захтев, стави на увид овлашћеном полицијском службенику, да се подаци из става 1. тог члана могу користити само у сврху за коју су прикупљени и да је забрањено уступање трећим лицима и јавно објављивање података из става 1. тог члана, осим у случајевима предвиђеним законом.

Члан 33. став 2. Закона о приватном обезбеђењу прописује да ближи начин вршења послова техничке заштите и коришћења техничких средстава утврђује министар.

Члан 45. истог закона прописује да правна лица и предузетници, ради организовања самозаштитне делатности, односно ради заштите своје имовине, пословања, објеката, простора и лица у њима и организовања своје унутрашње (редарске) службе обезбеђења за одржавање реда могу добити лиценцу за самозаштитну делатност, ако испуњавају услове из члана 10. став 1. тач. 2)-6) овог закона и ако имају најмање два службеника обезбеђења са лиценцом за вршење послова службеника обезбеђења са или без оружја. На поступак и начин издавања лиценце, из става 1. овог члана, као и на начин вршења послова приватног обезбеђења, ако овим законом није друкчије уређено, сходно се примењују одредбе овог закона којима се одговарајућа питања уређују за правна и физичка лица која послове приватног обезбеђења обављају за кориснике услуга. Правно лице и предузетник из става 1. овог закона могу за своје потребе обављати послове процене ризика у заштити лица имовине и пословања и послове техничке заштите, ако имају запослене службенике обезбеђења који поседују одговарајућу лиценцу за обављање ових послова.

Одредбама члана 188. став 1. и 2. Закона о радијационој и нуклеарној сигурности и безбедности („Сл. гласник РС“, бр. 95/201/ и 10/2019) прописано је да је носилац лиценце дужан да обезбеди и одржава мере физичко - техничке заштите и друге мере безбедности извора зрачења и повезаних постројења укључујући и транспорт. Такође, дужан је да предузме све прописане мере у оквиру својих одговорности и капацитета усклађених са Проценом основне безбедносне угрожености у циљу спречавања крађе, саботаже или губитка извора зрачења као и у циљу умањења штетних последица таквог догађаја.

Такође, одредбама члана 11. Уредбе о мерама безбедности нуклеарних објеката и нуклеарних материјала („Сл. гласник РС“, бр. 39/2014) прописано је да се ограђени простор на коме се налазе објекти, опрема и уређаји носиоца лиценце за обављање нуклеарне активности сматра зоном са ограниченим приступом. Истим чланом су прописане мере безбедности које се спроводе у зони са ограниченим

приступом су: 1) периодична физичка контрола зоне; 2) визуелни надзор; 3) контрола кретања робе, возила и људи; 4) провера идентитета лица која улазе у зону и обавезно ношење идентификационе картице на видном месту.

Имајући у виду садржај представке поводом обраде података о личности путем система видео надзора, као и све претходно наведено, Повереник је проценио да нема разлога за покретање поступка ванредног инспекцијског надзора по службеној дужности.

Правни оквир и пракса Савета Европе и Европске уније

Препоруке и ограничења при употреби видео-надзора у радним просторијама

Видео-надзор у радним просторијама представља обраду података о запосленим и спада у делокруг Конвенције 108+ и одговарајуће Препоруке СЕ о обради података о личности у радном окружењу. У данашњем свету напредних технологија, послодавци су у погледу спровођења надзора суочени са дилемом да ли да користе, на пример, аутоматизовано препознавање лица за регистрацију радног времена, или да прате кретање запослених унутар радних просторија, да ли да користе камере за надзор њихове продуктивности или чак за утврђивање њиховог односа према раду (на тај начин утврђују како се запослени осећају при обављању радних задатака). Најрелевантније промене које се односе на употребу „паметних“ технологија видео-надзора јесу једноставна могућност приступа прикупљеним подацима на даљину (нпр. преко паметног телефона); смањење величине камера (заједно с повећањем њихових перформанси, нпр. висока резолуција), које више не раде превентивно јер их запослени и не примећују; и прецизна обрада слика и других карактеристика запослених на снимцима које послодавци могу да изведу користећи нову видео-аналитику.⁴⁹

С правног аспекта, горе описани надзор запослених по правилу значи задирање у поље њихове приватности, које се протеже и на професионалну сферу живота и коју запослени уживају на радном месту. Задирање у њу је дозвољено само када је у складу с важећим прописима у области заштите података о личности, при чему се као кључни у овој области показују принципи законитости, сразмерности и транспарентности обраде података о личности.

Препорука СЕ о обради података у домену радног односа на више места односи се на коришћење видео-надзора односно осталих

⁴⁹ Радна група за заштиту података из члана 29, Мишљење бр. 2/ о обради података на раду, WP 249, стр. 19.

информационих технологија за надзор запослених од стране послодаваца. Основна смерница је да не би смело да се дозволи увођење и примена информационих система и технологија на такав начин да главни циљ њихове употребе буде праћење делатности и понашања запослених. Када је њихово увођење и коришћење оправдано другим легитимним сврхама, као што је, на пример, заштита производње (укључујући пословну тајну), здравље и безбедност запослених или обезбеђивање ефикасног функционисања организације, послодавци би прво требало да воде рачуна о одређеним мерама које такву употребу чине сразмерном – нарочито би требало да се консултују с представницима запослених.⁵⁰ Примена видео-надзора за праћење просторија које спадају у најличнију област живота запослених није дозвољена ни у ком случају.⁵¹ Уколико дође до спора или правних поступака, запослени би требало да имају могућност да добију копије евентуалних снимака у складу с националним законодавством. Чување снимака мора да буде временски ограничено.⁵² Послодавци нарочито треба да буду уздржани приликом прикупљања и обраде биометријских података, добијених путем видео-надзора. За заштиту биометријских података требало би да уведу додатне безбедносне мере.⁵³

Уопште, Препорука СЕ за обраду података о запосленима, у мери у којој превазилази пуке податке за закључивање радног односа, захтева од послодаваца да:

- a) обавесте запослене пре увођења информационих система и технологија које омогућавају праћење њихових активности; обавештење треба да садржи све тражене информације у складу с принципом транспарентности, укључујући посебно јасни и потпуни опис категорија прикупљених личних података у циљу обраде добијених снимака, периодом чувања и постојањем сигурносних копија и поуком о правима запослених на приступ и исправке; наведене информације морају да остану на располагању запосленима све време док траје надзор;
- b) доносе одговарајуће интерне мере у вези са обрадом ових података (и с аспекта безбедности) и запослене о њима унапред обавештавају;
- c) консултују се с представницима запослених у складу с националним законодавством или праксом, пре него што се уведе било који надзорни систем односно у околностима где се планира

50 15.1. тачка Препорука СЕ.

51 15.2. тачка Препорука СЕ.

52 15.3. Препорука СЕ.

53 18. тачка Препорука СЕ.

промена надзорног система; ако поступак консултација обелодани могућност повреде права запослених на приватност и људског достојанства, треба добити сагласност представника запослених;

- d) у складу са националним законодавством консултују се с националним надзорним органом надлежним за контролу обраде података о личности (на пример, с Повереником за информације).

Конкретан став Савета Европе о прихватљивости видео-надзора на радном месту произилази из Извештаја с водећим принципима за заштиту појединаца у контексту прикупљања и обраде података путем видео-надзора из 2003. године.⁵⁴ Једна од препорука садржи захтев да се ограничи употреба система видео-надзора на радном месту, јер сврха таквих система не би требало да буде систематска контрола квалитета и квантитета рада појединца на радном месту.⁵⁵ Сличан став проистиче из Водича о видео-надзору за европске институције, који је издао Европски надзорник за заштиту података (*European Data Protection Supervisor*). Циљеви, као што су управљање продуктивношћу на радном месту, обезбеђивање контроле квалитета, спровођење политика послодавца или обезбеђивање доказа за решавање спорова, сами по себи, у принципу, не оправдавају видео-надзор запослених у оквиру рада послодавца.⁵⁶

У пракси, видео-надзор је углавном дозвољен тамо где постоји велика вероватноћа да ће предмети бити отуђени (на пример, имовина послодавца или имовина трећих лица за коју је послодавац одговоран) или нанесена већа штета, на пример, у продавницама, складиштима, на местима у производњи, на шалтерима банака, изнад каса у угостиољским објектима и продавницама, на радним местима где се послује с готовином, на улазима у системске (ИТ) просторије и административне интерне просторе, на местима где се чувају тајни или други поверљиви подаци и др., при чему камере морају да буду усмерене на носиоце таквих података, а не на запослене. Обухват камера мора да буде што више усредсређен на предмет заштите и да не обухвата целокупну радну просторију уколико то није неопходно.⁵⁷

54 European Committee on Legal Co-operation, Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, 2003.

55 Исто. тачка 11.

56 European Data Protection Supervisor, The EDPS Video-Surveillance Guidelines, Брисел, март 2010., стр. 22.

57 Poverenik za informacije Republike Slovenije, Smernice u kontekstu sprovođenja video-nadzora, април 2023.

У складу са Мишљењем 4/2004 радне групе из члана 29. о обради личних података путем видео-надзора,⁵⁸ такав надзор не би смео да обухвата просторије које су резервисане за приватну употребу запослених или нису намењене обављању радних задатака – као што су тоалети, туш-кабине, кабине за гардеробу и просторије за рекреацију. Снимци прикупљени искључиво ради заштите имовине и/или откривање, спречавање и надзор озбиљних прекршаја не би требало да се користе за оптужбу запосленог за мање дисциплинске прекршаје. Радна група још додаје да запосленима увек треба омогућити да поднесу противтужбе или захтеве користећи садржај прикупљених снимака.⁵⁹ Мишљење 4/2004 садржи препоруку да запослени и сва друга лица која раде у просторијама које су предмет видео-надзора морају бити обавештени о овом надзору. Морају да буду обавештени о идентитету руковођа, сврси надзора и другим аспектима неопходним да би се обезбедила поштена обрада у односу на појединца на кога се односе лични подаци, на пример, у којим случајевима би снимке прегледао менаџмент компаније, временско трајање снимања и када је снимак обелодањен органима гоњења. Обезбеђивање информација о видео-надзору коришћењем симбола не може се сматрати довољним информисањем у контексту запослења.⁶⁰

Кодекс Међународне организације рада условљава увођење видео-надзора над запосленима двома околностима. Прво, може се извршити само ако су предметни запослени унапред обавештени о намерама послодавца. Због тога запослени пре почетка спровођења надзора морају да буду упознати с циљевима надзора и морају имати јасно представу о временском трајању. Друго, послодавци не могу да изаберу слободно начин и средства надзора, за које сматрају да су најпогоднији за њихове циљеве јер строго морају да поштују последице за приватност запослених и да дају предност најмање наметљивим начинима надзора. Према закључцима стручне групе, непрекидно праћење може узроковати сталну забринутост која код запослених може да изазове физичка обољења као и психичку анксиозност. Због тога га треба ограничити на случајеве када је надзор неопходан за решавање посебних проблема који су повезани са здрављем и безбедношћу запослених или заштитом имовине.⁶¹ Кодекс МОР-а такође се бави питањем тајног видео-надзора, и то на такав начин да је тајно

58 Радна група за заштиту података из члана 29, Мишљење бр. 4/2004 о обради личних података путем видео надзора, WP 89, Брисел, 8.2. 2004.

59 Радна група за заштиту података из члана 29, Мишљење бр. 4/2004 о обради личних података путем видео надзора, WP 89, Брисел, 8.2. 2004., стр. 25.

60 Исто.

61 Коментар Кодекса МОР-а, стр. 18 и 19.

праћење прихватљиво ако је предвиђено посебним одредбама националног законодавства. Неизбежно може бити у вези с истрагама у вези с криминалним делатностима или осталим озбиљним прекршајима. Међутим, Кодекс наглашава да само сумња у такву делатност или прекршај нису довољни. Послодавац може да прибегне тајном праћењу само ако и уколико постоје оправдани разлози за сумњу. Као пример озбиљног прекршаја стручна група наводи сексуално узнемиравање ако већ можда није дефинисано као кривично дело.⁶²

Допуштеност видео-надзора са аспекта права на поштовање приватног живота запослених у пракси Европског суда за људска права

Концепт приватног живота заштићен чланом 8. ЕКЉП није ограничен на интерни круг у коме појединац може да живи свој лични живот без спољног мешања, већ укључује и право на „приватни друштвени живот“, тј. могућност успостављања и развоја односа са другима и спољним светом.⁶³ У овом контексту обухвата и професионалне делатности или делатности које се одвијају у јавном животу. Стога, постоји област интеракције особе с другима, чак и ако је то у јавности, која може да спада у област приватног живота. Да би се проценило да ли се радње трећих лица које се обављају ван куће или приватних просторија појединца тичу његовог приватног живота по овој дефиницији, према судској пракси Европског суда за људска права важно је више елемената. Пошто се људи свесно и намерно баве активностима које су или би могле бити јавно праћене или о којима се извештава, где се потенцијално спроводи надзор ради јавне безбедности итд. суд у својој процени узима у обзир разумна очекивања особе у погледу приватности у конкретном окружењу.⁶⁴ По природи ствари, очекивање запосленог у погледу приватности на радном месту биће ниже него у приватним стамбеним просторијама, али и даље постоји очекивање запосленог о приватности у одређеној мери и на радном месту, диференцирано по различитим типовима радних просторија (рецимо, трпезарија, просторија тоалета, одвојена канцеларија) и у зависности од садржаја радних активности (да ли запослени долази у контакт са јавношћу – клијентима и у којој мери).

⁶² Исто, стр. 19.

⁶³ На пример, пресуда ЕСЉП у случају Барбулеску (Bărbulescu) против Румуније од 5.9.2017, бр. пред. 61496/08, пасус 70.

⁶⁴ На пример, Пресуда ЕСЉП у случају П.Г. и Ј.Х. против Уједињеног Краљевства („P.G. and J.H. v. UK“) од 25. 9. 2001, бр. пред. 44787/98, пасус 56.

Где су границе надзора послодавца над запосленима односно границе прихватљивости коришћења камера видео-надзора у односу на право појединаца на поштовање приватног живота на радном месту, Европски суд за људска права се већ неколико пута осврнуо у својој пракси. О основном питању постојања задирања у право из члана 8. ЕКЉП, суд је донео одлуку у случају *Антовић и Мирковић против Црне Горе*⁶⁵. Жалбу на кршење приватности уложила су два професора Математичког факултета Универзитета у Црној Гори пошто је постављен видео-надзор у слушаоницама у којима су држали предавања. Снимци су се чували месец дана и били су доступни на увид декану факултета. Подносиоци тужбе су навели да нису имали ефективан надзор над прикупљеним информацијама и да је надзор незаконит. Домаћи судови су одбацили њихов захтев за накнаду штете јер су сматрали да се овде уопште не ради о питању приватног живота, јер су слушаонице у којима су два подносиоца тужбе предавала биле јавне површине. Суд је прво одбацио аргумент владе да је случај неприхватљив јер није била у питању никаква приватност. С тим у вези, Суд је посебно упозорио на то да у складу с устаљеном судском праксом важи да приватни живот може да укључи професионалне делатности, о чему се радило и у предметном случају, иако су просторије обављања посла биле јавно доступне. Универзитетске слушаонице су радне просторије професора где су, поред предавања, у контакту са студентима, развијају односе и граде свој друштвени идентитет.⁶⁶ У вези са садржином предмета, Суд је затим констатовао да је надзор помоћу камере значио задирање у права подносилаца тужбе на приватност и да су надзором повређене одредбе националног законодавства, јер није следио ниједан циљ предвиђен законом.⁶⁷ Наиме, домаћи судови се нису упуштали у тражење правне основе за оправданост надзора пошто су још од почетка погрешно пресудили да није било никаквог задирања у приватност.

Суд је више пута пресуђивао и о сложеним питањима спровођења тајног видео-надзора над запосленима, и коришћења овако прибављених доказа за престанак радног односа. У случају *Копке против Немачке*⁶⁸ је подносиатељка жалбе, благајница у супермаркету, отпуштена због крађе пошто је послодавац уз помоћ приватне детективске агенције две недеље (прибл. 50 сати) спроводио прикривени видео-надзор. Отказ није успешно оспорила пред домаћим судовима. Суд је

65 Пресуда ЕСЉП у случају Антовић и Мирковић против Црне Горе од 28. 11. 2017, бр. пред. 70838/13.

66 Исто.

67 Исто.

68 Одлука ЕСЉП у случају Копке (Körke) против Немачке од 5. 10. 2010, бр. пред. 420/07.

жалбу подносиоце тужбе прогласио неприхватљивом и очигледно неоснованом са становишта члана 8. ЕКЉП, јер је утврдио да су национални органи успоставили правичну равнотежу између права раднице на поштовање њеног приватног живота, интереса послодавца за заштиту његових имовинских права и јавног интереса по правилном спровођењу правосуђа. Суд је посебно утврдио да се послодавац побринуо да ограничи видео-надзор само на неопходан обим за обезбеђење имовине. Мера је била временски ограничена (две недеље) и односила се само на подручје око благајне. Добијене визуелне податке је обрадио ограничени број особа које су запослене у детективској агенцији и службеника послодавца. Коришћени су само у вези с престанком радног односа и поступком пред радним судом. Суд је закључио да је задирање у приватни живот подносиоце жалбе ограничен на то што је било неопходно за постизање циљева којима се тежи видео-надзором. На крају је Суд упозорио да се наведено образложење заснива на процени свих околности случаја и да га убудуће не треба генерализовати, посебно имајући у виду све инвазивније технологије надзора.⁶⁹

Случај *Лопез Рибалда и други против Шпаније*⁷⁰ односио се на тајно праћење запослених, осумњичених за крађу, а стечени докази су били основа за раскид њиховог уговора о запослењу. Подносиоци тужбе су оспорили отпуштање због тајног видео-надзора и коришћења прибављених података од стране шпанских судова који су утврдили да је њихов раскид уговора о запослењу био правичан и законит. Суд је констатовао да у вези с подносиоцима жалбе није дошло до повреде члана 8. ЕКЉП. Национални судови су пажљиво размотрили права подносилаца тужби – запослених у робним кућама који су осумњичени за крађу – и права послодавца да заштити своју имовину, и детаљно испитали оправданост видео-надзора, посебно његовог ограниченог трајања (10 дана), доступности и наменске употребе. Кључни аргумент подносиоца жалбе пред Судом је био да, упркос законском захтеву, претходно нису били обавештени о надзору. Суд је потврдио да у међународном праву постоји консензус да пре спровођења надзора запослене о томе треба обавестити, али постоји изузеће од ове обавезе, када је то неопходно за заштиту важних јавних или приватних интереса (као што је имовина послодавца).⁷¹ У недостатку овог услова, други критеријуми заштите приватности су утолико важнији. За легалну уградњу тајног видео-надзора од стране послодавца не би била довољна само блага сумња да је запослени починио прекршај,

69 Исто.

70 Пресуда ЕСЉП у предмету Лопез Рибалда (López Ribalda) и други против Шпаније од 17.10.2019, бр. пред. 1875/13 и 8567/13.

71 Исто. пасус 133.

али основана сумња на озбиљни прекршај, узимајући у обзир обим губитака за послодавце у овом случају, може представљати легитиман разлог за тајно праћење.⁷² Ово се још више односи на сумњу у сарадњу више запослених код послодавца. Суд је додао да су подносиоци тужбе имали на располагању друге правне лекове као што су жалба органу за заштиту података или тужба на суду због наводне повреде њихових права из Закона о заштити података о личности, али их нису искористили.⁷³ Суд је пресудио да је мера јасно оправдана због основане сумње у озбиљни прекршај и релевантне губитке (штете) послодавца у последњих 5 месеци пре постављања. У предметном случају домаћи судови нису, дакле, прекорачили своје поље процене (*margin of appreciation*), када су констатовали да је праћење било сразмерно и законито.⁷⁴

Препоруке за усклађивање

Као општа оцена Закона о приватном обезбеђењу може се навести да је овај закон неопходно посебно размотрити, и то не само са становишта обраде података у контексту радних односа.⁷⁵ Потребно је размотрити могућност посебног уређивања видео-надзора, којим би се уредило не само питање дозвољености успостављања видео надзора у неком посебном окружењу, укључујући и у контексту радних односа, него и посебне обавезе руковалаца, а нарочито у вези са правима лица и безбедношћу обраде. Појединачне одредбе о употреби видео-надзора у контексту радних односа могу бити садржане и у, примера ради, Закону о раду или Закону о заштити података о личности. У случају допуне Закона о раду, потребно је да одредбе садрже и мере у складу са чланом 91. Закона о заштити података о личности.

Препорука Савета Европе, као и други документи Савета Европе, Међународне организације рада и Европске уније наведени у тексту могу заједно с праксом Суда за људска права и Суда правде Европске уније представљати користан алат.

Као добар пример уређивања видео надзора у, између осталог, радном окружењу, може се истаћи Закон о спроведби Опће уредбе о

72 Пресуда ЕСЉП у предмету Лопез Рибалда (López Ribalda) и други против Шпаније од 17. 10. 2019, бр. пред. 1875/13 и 8567/13, пасус 134.

73 Исто. пасус 135.

74 Исто. пасус 137.

75 Видети нпр. Анализу прописа који уређују сектор безбедности из аспекта заштите података о личности (Н. Ружић и А. Тоскић Цветиновић), Мисија ОЕБС у Србији, 2020.

заштити података Републике Хрватске.⁷⁶ Према члану 30. овог закона, подаци о личности запослених путем система видео-надзор могу се обрађивати уколико су, поред Закона, испуњени и других прописи који се односе на заштиту на раду и уколико су запослени унапред обавештени о обради. Поред тога, истим чланом је забрањено успостављање видео надзора у просторије за одмор, хигијену или пресвлачење.

76 Zakon o provedbi Opće uredbe o zaštiti podataka („Narodne novine“ br. 42/18)

Употреба информационо-комуникационих технологија

Правни оквир

Употреба технологија одавно је уобичајена у радним односима и тешко је замислити неки садашњи процес рада без њих. Према истраживању Републичког завода за статистику за 2023. годину, преко 85% предузећа има веб-сајт, а преко преко 53%, предузећа користи друштвене мреже (Facebook, LinkedIn, Xing, Yammer), а већина користи услуге клауд сервиса (чување у облаку).⁷⁷

Према Закону о раду обавеза је послодавца да обезбеди средства рада, и у складу са чланом 179. ст. 2. т. 3), може да откаже уговор о раду уколико запослени користи средства рада нецелисходно и неодговорно. У случају да се радни однос заснива за обављање послова ван просторија послодавца, послодавац је дужан да набави, инсталира и одржава средства за рад за обављање послова, а уговор о раду садржи и одредбе у вези са коришћењем и употребу ових средстава, као и накнаду трошкова за њихову употребу (чл. 42.). Примера ради, запосленима ће бити омогућено да користе телефонске уређаје, укључујући и мобилне телефоне.⁷⁸ Очекивано је да послодавац, водећи рачуна о средствима рада, врши неку контролу употребе средстава, те је обрада података о личности последична. С тим у вези, на ову обраду података, као и неке друге, примењује се Закон о заштити података о личности. Запослени морају да буду обавештени о обради података на адекватан начин.

Који ће се подаци обрађивати зависиће од сврхе обраде, односно од природе послодавца и послова који се обављају. Између осталог на то упућују и случајеви Европског суда за људска права, као и Препорука која је описана у наставку овог дела, а који се односи и на оне ситуације када је запосленима јасно предочено да средства не могу да се користе

77 Републички завод за статистику, Употреба информационо-комуникационих технологија у Републици Србији, 2023., доступно на: <https://publikacije.stat.gov.rs/G2023/Pdf/G202316018.pdf>, стр. 75-77.

78 На пример, Одлука о коришћењу службених телефона у Служби Повереника за информације од јавног значаја и заштиту података о личности, бр. 021-02-16/2022-04 од 9.5.2022. године, доступна на https://www.poverenik.rs/images/stories/dokumentacija-nova/akti-o-radu-sluzbe/2022/odluka_o_kori%C5%A1%C4%87enju_sl_telefona.pdf.

у приватне сврхе, а да их запослени користи у те сврхе. Имејл кореспонденција може бити предмет строже контроле у оним радним срединама у којима је уобичајено да се обавезе у име послодавца преузимају на овај начин, или је реч о затвореном систему. Приступ интернету, уколико је дозвољен, такође може бити под надзором послодавца. Исто се односи и на приступ мрежи послодавца и кад се тиче приступа бежичној мрежи (Wi-Fi) преко личног уређаја запосленог. Иако ова публикација не обухвата питања синдикалног организовања запослених код послодавца, важно је истаћи да начин контроле употребе ИКТ опреме не задире у слободу синдикалног организовања запослених.

Поред средстава комуницирања употреба ИКТ опреме може да се односи и на возила. У случају да није реч о употреби фабрички уграђених ГПС и других техничких уређаја у возилима без услуге одржавања, надгледања и повезивања на систем техничке заштите, примењује се и Закон о приватном обезбеђењу. На ове услуге примењује се наведено у делу који се односи на видео надзор.

Праћење процеса рада омогућено је разним алатима, програмима. Према наведеном истраживању, на територији Републике Србије, 22,4% предузећа користи ERP - софтвер за планирање ресурса предузећа, CRM - софтвер за управљање односима са клијентима користи 10,7 % предузећа, а док пословно обавештавање (софтвери за BI) користи 5,1% предузећа.⁷⁹ Ови алати, поред праћења процеса, усклађености са роковима или повезивање различитих организационих јединица послодавца, могу да се користе и за надзор над радом запослених. Такав надзор може имати вишеструку сврху, а коју је сваку понаособ неопходно утврдити и одредити у складу са примењивим законима, другим правним основама обраде података, као и свим начелима обраде података.

Примера ради, органи државне управе, као и други одређени органи, поступају у складу са правилима канцеларијског пословања.⁸⁰ Додатно, ова програмска решења могу да бележе приступ, као и разлог приступа систему, или предузете радње. У случају да послодавац нема правну обавезу обраде ових података, односно нема правну обавезу обраде ових података у сврху контроле приступа, односно контроле запослених, послодавац може да обрађује податке о личности само уколико та обрада испуњава услове из Закона о заштити података о личности, као и других прописа уколико је примењиво.

79 Републички завод за статистику, Употреба информационо-комуникационих технологија у Републици Србији, 2023., стр. 81.

80 Уредба о канцеларијском пословању органа државне управе ("Сл. гласник РС", бр. 21/2020, 32/2021 и 14/2023).

На крају, важно је напоменути да уколико послодавац користи апликације или систем за праћење њиховог рада, кретања, комуникације и слично има обавезу да изради акт о процени утицаја на заштиту података о личности.

Из праксе Повереника

Питање: Да ли послодавац може (уз претходно обавештење и прибављање писане сагласности запослених) у службене аутомобиле уградити GPS систем ради контроле и заштите своје имовине, или је пак пре отпочињања ових радњи потребно извршити Процену утицаја обраде на заштиту података о личности и прибавити претходно мишљење Повереника?

Број предмета: 073-14-1525/2022-02

Запослени имају право на приватност у свом радном окружењу па се у сваком конкретном случају најпре мора размотрити неопходност и сразмерност намеравања обраде, односно да ли би се утврђена сврха обраде могла остварити оним механизмима који су мање интервизивни по приватност лица.

Законом о приватном обезбеђењу ("Сл. гласник РС", бр. 104/2013, 42/2015 и 87/2018) уређују се обавезно обезбеђење и заштита одређених објеката, послови и рад правних и физичких лица у области приватног обезбеђења, услови за њихово лиценцирање, начин вршења послова и остваривање надзора над њиховим радом.

Као једно од могућих средстава техничке заштите предвиђено чланом 30. став 1. Закона о приватном обезбеђењу је и сателитско праћење возила (GPS), а даље је одредбама овог закона прописано на који начин се исто може вршити. Дакле, код употребе GPS система у сврху заштите лица/имовине, као и других начина техничке заштите из члана 30. став 1. Закона о приватном обезбеђењу, примењују се првенствено одредбе овог закона којима је уређено спровођење самозаштитне делатности.

Како је старање о спровођењу Закона о приватном обезбеђењу у надлежности Министарства унутрашњих послова, то се истом органу можете обратити ради добијања мишљења о примени одредби наведеног закона.

Наиме, Законом о заштити података о личности, чије је спровођење у надлежности Повереника, уређују се, на системски начин, начела

обраде података о личности, као и друга општа правила и одређене обавезе за руковооце и друге субјекте, док се обрада података о личности у одговарајућим областима друштвеног живота уређује посебним прописима о чијој се примени старају други органи.

Са становишта примене Закона о заштити података о личности начелно указујемо на то да је за дозвољеност обраде неопходно да постоји одговарајући правни основ у смислу члана 12. Закона, да се намеравана обрада врши у складу са посебним прописима који уређују одређену област/делатност, начелима обраде из члана 5. Закона (укључујући и начело минимизације података), као и другим одговарајућим правилима и обавезама, а у зависности од околности у сваком конкретном случају.

Када је у питању обрада података о личности запослених употребом система за праћење њиховог рада, кретања, комуникације и сл, мора се имати у виду да запослени имају право на приватност у свом радном окружењу, и да се у сваком конкретном случају најпре мора размотрити неопходност и сразмерност такве обраде, односно да ли би се утврђена сврха обраде могла остварити оним механизмима, који су мање инвазивни по приватност лица.

С тим у вези указујемо и на обавезу за руковооце, утврђену одредбом члана 54. Закона о заштити података о личности. Наиме, у случају када је вероватно да ће нека врста обраде, посебно употребом нових технологија и узимајући у обзир природу, обим, околности и сврху обраде, проузроковати висок ризик за права и слободе физичких лица, руковалац је дужан да пре него што започне са обрадом изврши процену утицаја предвиђених радњи обраде на заштиту података о личности.

Случајеви у којима је руковалац обавезан да изврши процену утицаја обраде утврђени су чланом 54. став 4. Закона о заштити података о личности и Одлуком 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 ("Сл. гласник РС", бр. 45/2019 и 112/2020).

Једна од радњи обраде за које се мора извршити процена утицаја, између осталог, је прописана тачком 2. подтачка 7) наведене одлуке, и односи се на обраду података о личности запослених од стране послодавца употребом апликација или система за праћење њиховог рада, кретања, комуникације и сл.

Одредбама члана 54. став 6. Закона о заштити података о личности прописано је да процена утицаја најмање мора да садржи: 1) свеобухватан опис предвиђених радњи обраде и сврху обраде, укључујући и опис легитимног интереса руковооца, ако он постоји; 2) процену нео-

пходности и сразмерности вршења радњи обраде у односу на сврхе обраде; 3) процену ризика за права и слободе лица на које се подаци односе из става 1. овог члана; 4) опис мера које се намеравају предузети у односу на постојање ризика, укључујући механизме заштите, као и техничке, организационе и кадровске мере у циљу заштите податка о личности и обезбеђивања доказа о поштовању одредби овог закона, узимајући у обзир права и легитимне интересе лица на које се подаци односе и других лица.

Одредбама члана 55. став 1. Закона о заштити података о личности предвиђено је да је руковалац дужан да затражи мишљење Повереника пре започињања радње обраде, ако процена утицаја на заштиту података о личности, која је извршена у складу са чланом 54. тог закона, указује да ће намераване радње обраде произвести висок ризик ако се не предузму мере за умањење ризика. Напомињемо да одговорност за поступање у складу са Законом о заштити података о личности лежи на руковаоцу и указујемо на то да Повереник нема обавезу давања мишљења када извршена процена утицаја указује да ниво ризика, после предузимања мера, неће бити висок.

Питање: Послодавац намерава да у постојећи ИТ систем (платформа) који бележи захтев потрошача, као и одговор на његово питање и брзину тог одговора уведе и функцију да у систему буде видљиво име и презиме запосленог који ради на одређеном питању потрошача, која би омогућила један вид контроле рада и понашања запослених, јер би било могуће на основу система видети број решених упита, брзину одговора, начин решавања, а произлази да постоји легитиман интерес послодавца за увођење оваквог система праћења имајући у виду дозвољен рад од куће, те потребу послодавца да испрати ефикасност и брзину запослених који раде у директној комуникацији са купцима, па је с тим у вези затражено мишљење о томе „да ли је дозвољена наведена обрада података, а у складу са чланом 12. став 1. тачка 6) (легитиман интерес) Закона о заштити података о личности?“

Број предмета: 073-14-1913/2022-02

У погледу легитимног интереса као правног основа обраде података о личности, напомињемо да је за коришћење тог правног основа за обраду података потребно да су испуњени услови из члана 12. став 1. тачка 6) Закона, тј. да је утврђено: 1) постојање легитимног интереса; 2) неопходност обраде; 3) претежност легитимног интереса руковоаца/треће стране над интересима или основним правима и слободама лица на које се подаци односе. Дакле, није довољно само навести и описати интерес руковоаца, већ је потребно да руковалац изврши процену испуњености сва три напред наведена елемента, како би утврдио да се ради о одговарајућем правном основу за обраду. Извршење наведене обавезе мора бити документовано. Одговоре на најчешће постављена питања у вези са легитимним интересом, као и модел акта о процени легитимног интереса као правног основа за обраду података о личности можете пронаћи на интернет презентацији Повереника www.poverenik.rs, у делу „Заштита података“ – „Легитимни интерес“.

Најпре указујемо на то да је одредбом члана 91. Закона о заштити података о личности („Сл. гласник РС“, бр. 87/2018) прописано да се на обраду у области рада и запошљавања примењују одредбе закона којима се уређује рад и запошљавање и колективни уговори, уз примену одредби овог закона. Стога, када је у питању обрада података о личности запослених, најпре се примењују одредбе Закона о раду и

других прописа из области радних односа, чије спровођење није у надлежности Повереника, па се ради добијања мишљења о примени истих, можете обратити Министарству за рад, запошљавање, борачка и социјална питања.

Међутим, како из одредбе члана 91. Закона о заштити података о личности произлази да руковооци уз примарну примену прописа из области рада и запошљавања морају примењивати и одредбе тог закона, начелно, са становишта надлежности овог органа у области заштите података о личности, указујемо и на следеће.

За сваку обраду података о личности, најпре је потребно обезбедити одговарајући правни основ у смислу одредбе члана 12. Закона о заштити података о личности, уз поштовање начела, правила и обавеза за руковооце, утврђених одредбама Закона, а у зависности од околности сваког конкретног случаја.

Када је у питању обрада података о личности запослених од стране послодавца, правни основ такве обраде треба првенствено да произлази из одговарајућих прописа у области рада, запошљавања и сл.

У погледу легитимног интереса као правног основа обраде података о личности, напомињемо да је за коришћење тог правног основа за обраду података потребно да су испуњени услови из члана 12. став 1. тачка 6) Закона, тј. да је утврђено: 1) постојање легитимног интереса; 2) неопходност обраде; 3) претежност легитимног интереса руковооца/треће стране над интересима или основним правима и слободама лица на које се подаци односе. Дакле, није довољно само навести и описати интерес руковооца, већ је потребно да руковалац изврши процену испуњености сва три напред наведена елемента, како би утврдио да се ради о одговарајућем правном основу за обраду. Извршење наведене обавезе мора бити документовано. Одговоре на најчешће постављена питања у вези са легитимним интересом, као и модел акта о процени легитимног интереса као правног основа за обраду података о личности можете пронаћи на интернет презентацији Повереника www.poverenik.rs, у делу „Заштита података“ – „Легитимни интерес“.

Такође, када је у питању обрада података о личности запослених употребом система за праћење њиховог рада, кретања, комуникације и сл, мора се имати у виду да запослени имају право на приватност у свом радном окружењу, и да се у сваком конкретном случају најпре мора размотрити неопходност и сразмерност такве обраде, односно да ли би се утврђена сврха обраде могла остварити оним механизмима, који су мање инвазивни по приватност лица.

Дакле, за закониту обраду података о личности, потребно је најпре обезбедити одговарајући правни основ, у смислу члана 12. Закона, те да је обрада у складу са посебним прописима који уређују предметну област/делатност, као и да се иста врши у складу са начелима обраде

из члана 5. овог закона и другим одговарајућим правилима и обавезама прописаним тим законом, у зависности од чињеница и околности у сваком конкретном случају.

С тим у вези указујемо и на обавезу за руковооце, утврђену одредбом члана 54. Закона о заштити података о личности. Наиме, у случају када је вероватно да ће нека врста обраде, посебно употребом нових технологија и узимајући у обзир природу, обим, околности и сврху обраде, проузроковати висок ризик за права и слободе физичких лица, руковалац је дужан да пре него што започне са обрадом изврши процену утицаја предвиђених радњи обраде на заштиту података о личности.

Случајеви у којима је руковалац обавезан да изврши процену утицаја обраде утврђени су чланом 54. став 4. Закона о заштити података о личности и Одлуком 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 ("Сл. гласник РС", бр. 45/2019 и 112/2020).

Једна од радњи обраде за које се мора извршити процена утицаја, између осталог, је прописана тачком 2. подтачка 7) наведене одлуке, и односи се на обраду података о личности запослених од стране послодавца употребом апликација или система за праћење њиховог рада, кретања, комуникације и сл. Поступање руковооца сагласно обавези из члана 54. Закона, подразумева доношење посебног акта о извршеној процени утицаја обраде на заштиту података о личности оји треба да садржи све обавезне елементе.

Одредбама члана 54. став 6. Закона о заштити података о личности прописано је да процена утицаја најмање мора да садржи: 1) свеобухватан опис предвиђених радњи обраде и сврху обраде, укључујући и опис легитимног интереса руковооца, ако он постоји; 2) процену неопходности и сразмерности вршења радњи обраде у односу на сврхе обраде; 3) процену ризика за права и слободе лица на које се подаци односе из става 1. овог члана; 4) опис мера које се намеравају предузети у односу на постојање ризика, укључујући механизме заштите, као и техничке, организационе и кадровске мере у циљу заштите податка о личности и обезбеђивања доказа о поштовању одредби овог закона, узимајући у обзир права и легитимне интересе лица на које се подаци односе и других лица.

Одредбама члана 55. став 1. Закона о заштити података о личности предвиђено је да је руковалац дужан да затражи мишљење Повереника пре започињања радње обраде, ако процена утицаја на заштиту података о личности, која је извршена у складу са чланом 54. тог закона, указује да ће намераване радње обраде произвести висок ризик

ако се не предузму мере за умањење ризика. Напомињемо да одговорност за поступање у складу са Законом о заштити података о личности лежи на руковооцу и указујемо на то да Повереник нема обавезу давања мишљења када извршена процена утицаја указује да ниво ризика, после предузимања мера, неће бити висок.

Сагласно члану 5. став 2. Закона, одговорност за поступање лежи на руковооцу, који мора бити у могућности да предочи, односно докаже извршавање свих Законом предвиђених обавеза у вези са обрадом података о личности.

Праћење запослених путем ГПС, рад на даљину, рад од куће

Број предмета: 072-21-1975/2020-07

Увод

Поверенику је достављена представка, у којој се наводи да је Јавно предузеће (даље Руковалац), прописало „Обавезно упутством за запослене при обављању рада од куће“, којим је уређено да запослени морају да користе приватну имејл адресу у пословне сврхе, да увек имају укључену ГПС локацију на службеном телефону, те да ће запосленима који нису укључили ГПС локацију бити изречена санкција предвиђена Законом о раду.

Из диспозитива Опомене

И Јавном предузећу (у даљем тексту: Руковалац), зато што је обрадом податка о локацији запослених путем ГПС, за време рада од куће, повредио:

- одредбе члана 5. став 1. тачка 1. ЗЗПЛ, на тај начин што исти подаци о личности нису обрађивани законито, поштено и транспарентно у односу на лице на које се подаци односе („законитост, поштење и транспарентност”);
- одредбе члана 54. ЗЗПЛ, зато што није извршио процену утицаја предвиђених радњи обраде на заштиту података о личности.

Утврђено чињенично стање

На основу прикупљених информација, аката, документације и писаних изјашњења представника Руковаоца о предмету надзора, у наведеном поступку утврђено је следеће чињенично стање:

- Руковалац је на основу Одлуке о проглашењу ванредног стања (Сл. гласник РС“ број 29 од 15.03.2020. године), и Наредбе о проглашењу епидемије заразне болести Covid -19 („Сл. гласник РС“ бр. 37 од 19.03.2020. године), у складу са препорукама Владе упутио запослене на рад од куће.
- У циљу спречавања злоупотребе овог облика рада и у сврху вршења надзора над радом запослених, Руковалац је вршио проверу локације запослених, тако што је захтевао да му путем Вибера доставе своју тренутну ГПС локацију.
- Руковалац је запослене на рад од куће упућивао на основу донетог решења и Обавезног упутства за запослене при обављању рада од куће. Обавезним упутством је уређено да је надлежно лице Руковаоца овлашћено да периодично врши проверу поштовања услова за рад од куће обиласком запосленог на адреси пребивалишта или провером локације путем апликације за ГПС лоцирање. Према изјашњењу Руковаоца, могућност да се запослени обилазе на место пребивалишта није примењивана.
- Руковалац у свом изјашњењу наводи да су запослени злоупотребљавали рад од куће у циљу одласка на одмор у друго место и за обављање приватних активности ван куће, противно циљу и сврси њиховог упућивања на рад од куће, због чега је уведена провера њихове локације.
- Руковалац је запосленима путем мејла достављао решење о упућивању на рад од куће и Обавезно упутство за запослене при обављању рада од куће. Запослени су били у обавези да писаним путем потврде пријем решења и Упутства, што је Руковалац у свом изјашњењу представио као чин давања сагласности запослених на обраду њихових података о личности. Из изјашњења Руковаоца се може закључити да запослени нису били упознати да потврдом пријема мејла дају сагласност на обраду података о личности, а Руковалац као битну чињеницу истиче да нико од запослених у свом мејлу није навео да не пристаје на нека од права и обавеза која су овим актима утврђена и са којима су запослени упознати.
- Наведене радње – потврда мејла као и одсуство протеста запослених због намеравање обраде података о личности запослених од стране Руковаоца, Руковалац је предочио Поверенику као слободно дат пристанак запослених на обраду њихових података о личности.
- Руковалац није извршио процену утицаја предвиђаних радњи обраде на заштиту података о личности, нити је прибавио мишљење Повереника, у складу са обавезама из члана 54. и 55. ЗЗПЛ. У свом изјашњењу Руковалац наводи да се провера лока-

ције запослених који су били упућени на рад од куће није спроводила континуирано, већ повремено и спорадично. Даље, Руковалац наводи да је провера локације запослених вршена у циљу потврде да ли се запослени „придржава упућивања на рад од куће као правног основа института реализованог у интересу послодавца подједнако као и у интересу запосленог, а као мера које се спроводи у циљу безбедног и здравог рада у доба пандемије вируса Covid – 19“. Из наведених разлога, Руковалац сматра да се на ову врсту обраде података о личности запослених не примењују одредбе члана 54. и 55. ЗЗПЛ.

- Као правни основ обраде података о личности запослених Руковалац наводи члан 12. став 1. тачка 2. ЗЗПЛ, као и додатни основ, пристанак лица у складу са тачком 12. став 1. тачка 1. ЗЗПЛ. Руковалац се позива на члан 42. и члан 16. став 2. Закона о раду („Сл. гласник РС“, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - одлука УС, 113/2017 и 95/2018 - аутентично тумачење), члан 11. и члан 12. тачка 1. Закона о безбедности и здравља на раду („Сл. гласник РС“ бр. 101/2005, 91/2015 и 113/2017 - др. Закон).

У свом изјашњењу Руковалац наглашава да у конкретном случају није реч о раду на даљину, који такође прописује Закон о раду, већ да је реч о раду од куће и напомиње да је локација битан услов за рад од куће, као и да представља битну карактеристику превенције од заразне болести.

Образложење

Увидом у решење Руковаоца о упућивању запосленог на рад од куће, Повереник је утврдио да је тачком 5. решења уређено да надзор над радом запосленог за време трајања рада од куће спроводи његов непосредни руководиоца, кроз директну комуникацију, писаним путем (мејлом), кроз појединачне извештаје или на други одговарајући начин.

Увидом у Обавезно упутство за запослене при обављању рада од куће, Повереник је утврдио, да је Руковалац овим актом уредио, да надзор над радом запосленог за време трајања рада од куће спроводи његов непосредни руководиоца, кроз директну комуникацију, усменим и писаним путем (мејлом), кроз периодичне извештаје или на други одговарајући начин. Даље, овим упутством је уређено да је надлежно лице Руковаоца овлашћено да периодично врши проверу поштовања услова за рад од куће, обиласком запосленог на адреси пребивалишта или провером локације путем апликације за ГПС лоцирање.

С обзиром на наведено, указујемо да је чланом 42. Устава Републике Србије (“Сл. гласник РС”, бр. 98/06) зајемчена заштита података о личности и прописано је да се прикупљање, држање, обрада и коришћење података о личности уређују законом, да је забрањена и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом, те да свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом, и право на судску заштиту због њихове злоупотребе.

ЗЗПЛ, између осталог, уређује право на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, кодекс поступања, пренос података о личности у друге државе и међународне организације, надзор над спровођењем овог закона, правна средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом података о личности, као и посебни случајеви обраде, сагласно члану 1. став 1. тог закона.

Податак о личности је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета, сагласно члану 4. тачка 1) ЗЗПЛ.

Тачком 2) наведеног члана ЗЗПЛ прописано је да је лице на које се подаци односе физичко лице чији се подаци о личности обрађују, док је тачком 3) истог члана ЗЗПЛ прописано да је обрада података о личности 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 структурисање, похрањивање, уподобљавање или мењање, откривање, увид, употреба, откривање преносом, односно достављањем, умножавање, ширење или на други начин чињење доступним, упоређивање, ограничавање, брисање или уништавање (у даљем тексту: обрада).

Члан 4. тачка 8) ЗЗПЛ прописује је да је руковалац физичко или правно лице, односно орган власти који самостално или заједно са другима одређује сврху и начин обраде, као и да се законом којим се одређује сврха и начин обраде може одредити и руковалац или прописати услови за његово одређивање;

Чланом 5. став 1. ЗЗПЛ прописана су начела обраде података о личности, у складу са којим подаци о личности морају: 1) се обрађивати

законито, поштено и транспарентно у односу на лице на које се подаци односе („законитост, поштење и транспарентност“). Законита обрада је обрада која се врши у складу са овим законом, односно другим законом којим се уређује обрада; 2) се прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама („ограничење у односу на сврху обраде“); 3) бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде („минимизација података“); 4) бити тачни и, ако је то неопходно, ажурирани. Узимајући у обзир сврху обраде, морају се предузети све разумне мере којима се обезбеђује да се нетачни подаци о личности без одлагања избришу или исправе („тачност“); 5) се чувати у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде („ограничење чувања“); 6) се обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера („интегритет и поверљивост“). Руководалац је одговоран за примену одредаба става 1. овог члана и мора бити у могућности да предочи њихову примену („одговорност за поступање“).

Одредбама члана 12. ЗЗПЛ прописано је да је обрада законита, само ако је испуњен један од следећих услова: 1) лице на које се подаци о личности односе је пристало на обраду својих података о личности за једну или више посебно одређених сврха; 2) обрада је неопходна за извршење уговора закљученог са лицем на које се подаци односе или за предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора; 3) обрада је неопходна у циљу поштовања правних обавеза руковоаца; 4) обрада је неопходна у циљу заштите животних важних интереса лица на које се подаци односе или другог физичког лица; 5) обрада је неопходна у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења руковоаца; 6) обрада је неопходна у циљу остваривања легитимних интереса руковоаца или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се подаци односе који захтевају заштиту података о личности, а посебно ако је лице на које се подаци односе малолетно лице.

Следећим ставом наведеног члана ЗЗПЛ прописано је да се став 1. тачка б) тог члана не примењује на обраду коју врши орган власти у оквиру своје надлежности.

Чланом 14. став 1. ЗЗПЛ прописано је да се правни основ за обраду из члана 12. став 1. тач. 3) и 5) овог закона *одређује законом*, док је ставом 2. истог прописано да, ако се ради о обради из члана 12. став 1.

тачка 3) овог закона, *законом* се одређује и *сврха* обраде, а ако се ради о обради из члана 12. став 1. тачка 5) овог закона, законом се прописује да је обрада неопходна у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења руковоаца.

Пре започињања обраде података о личности, обавеза Руковоаца да лицу чије податке обрађује пружи одређене информације прописана је чланом 23. став 1. ЗЗПЛ и то: 1) о идентитету и контакт подацима руковоаца, као и његовог представника, ако је он одређен; 2) контакт податке лица за заштиту података о личности, ако је оно одређено; 3) о сврси намеравање обраде и правном основу за обраду; 4) о постојању легитимног интереса руковоаца или треће стране, ако се обрада врши на основу члана 12. став 1. тачка 6) овог закона; 5) о примаоцу, односно групи прималаца података о личности, ако они постоје; 6) о чињеници да руковалац намерава да изнесе податке о личности у другу државу или међународну организацију, као и о томе да ли се та држава или међународна организација налази на листи из члана 64. став 7. овог закона, а у случају преноса из чл. 65. и 67. или члана 69. става 2. овог закона, о упућивању на одговарајуће мере заштите, као и о начину на који се лице на које се подаци односе може упознати са тим мерама.

Уз информације из става 1. члана 23, а како је то прописано следећим ставом истог члана ЗЗПЛ, руковалац је дужан да у тренутку прикупљања података о личности лицу на које се подаци односе пружи и следеће додатне информације које могу да буду неопходне да би се обезбедила поштена и *транспарентна* обрада у односу на то лице:

1) о року чувања података о личности или, ако то није могуће, о критеријумима за његово одређивање; 2) о постојању права да се од руковоаца захтева приступ, исправка или брисање његових података о личности, односно постојању права на ограничење обраде, права на приговор, као и права на преносивост података; 3) о постојању права на опозив пристанка у било које време, као и о томе да опозив пристанка не утиче на допуштеност обраде на основу пристанка пре опозива, ако се обрада врши на основу члана 12. став 1. тачка 1) или члана 17. став 2. тачка 1) овог закона; 4) о праву да се поднесе притужба Поверенику; 5) о томе да ли је давање података о личности законска или уговорна обавеза или је давање података неопходан услов за закључење уговора, као и о томе да ли лице на које се подаци односе има обавезу да да податке о својој личности и о могућим последицама ако се подаци не дају; 6) о постојању аутоматизованог доношења одлуке, укључујући профилисање из члана 38. ст. 1. и 4. овог закона, и, најмање у тим случајевима, сврсисходне информације о логици која се при томе користи, као и о значају и очекиваним последицама те обраде по лице на које се подаци односе.

Како Руковалац наводи да је као додатну меру обезбеђивања законитости обраде прибавио пристанак запосленог, указујемо да би пристанак био законит, поред цитираних обавеза из члана 23. ЗЗПЛ Руковалац је дужан да примени и одредбе члана 15. тог закона, којим су прописани услови који морају бити испуњени да би се обрада на основу пристанка сматрала законитом, између осталог и то да: руковалац мора бити у могућности да предочи да је лице пристало на обраду својих података о личности, ако се пристанак даје у оквиру писмене изјаве која се односи и на друга питања, захтев за давање пристанка мора бити представљен на начин којим се издваја од тих других питања, у разумљивом и лако доступном облику, као и уз употребу јасних и једноставних речи, да пре давања пристанка лице на које се подаци односе мора бити обавештено о праву на опозив, као и дејству опозива, а опозивање пристанка мора бити једноставно, као и давање пристанка и др. Такође, приликом оцењивања да ли је пристанак за обраду података о личности слободно дат, посебно се мора водити рачуна о томе да ли се извршење уговора, укључујући и пружање услуга, *условљава* давањем пристанка који није неопходан за његово извршење.

Одредбама члана 54. ЗЗПЛ прописана је обавеза Руковаоца да пре него што започне са обрадом изврши процену утицаја предвиђених радњи обраде на заштиту података о личности, ако је вероватно да ће нека врста обраде, посебно употребом нових технологија и узимајући у обзир природу, обим, околности и сврху обраде, проузроковати висок ризик за права и слободе физичких лица.

Истим чланом у ставу 6. је прописано да се процена утицаја најмање мора да садржи: 1) свеобухватан опис предвиђених радњи обраде и сврху обраде, укључујући и опис легитимног интереса руковаоца, ако он постоји; 2) процену неопходности и сразмерности вршења радњи обраде у односу на сврхе обраде; 3) процену ризика за права и слободе лица на које се подаци односе из става 1. овог члана; 4) опис мера које се намеравају предузети у односу на постојање ризика, укључујући механизме заштите, као и техничке, организационе и кадровске мере у циљу заштите податка о личности и обезбеђивања доказа о поштовању одредби овог закона, узимајући у обзир права и легитимне интересе лица на које се подаци односе и других лица.

Одлуком о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника („Службени гласник РС“ број 45/2019), утврђена је листа радњи обраде за које се мора извршити процена утицаја на заштиту података о личности. Таком 2. подтачка 7. наведене Одлуке уређено је да се процена утицаја на заштиту података о личности, између осталог, врши у случају: обраде биометријских

података у циљу јединствене идентификације запослених од стране послодавца и у другим случајевима обраде података о личности запослених од стране послодавца употребом апликација или система за праћење њиховог рада, кретања, комуникације и сл.

Одредбама члана 91. став 1. ЗЗПЛ прописано је да се на обраду у области рада и запошљавања примењују одредбе закона којима се уређује рад и запошљавање и колективни уговори, уз примену одредби тог закона. Ставом 2. наведеног члана ЗЗПЛ прописано је да, ако закон који уређује рад и запошљавање или колективни уговор садрже одредбе о заштити података о личности, морају се прописати и посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини.

Из наведених одредби произилази да је обрада података о локацији запослених путем ГПС као и посета запослених на адресе пребивалишта, представља радњу обраде података о личности, те да иста подлеже начелима обраде података о личности прописаним одредбама члана 5. ЗЗПЛ, законитостима обраде прописаним одредбама члана 12. овог закона, као и одредбама закона којима се уређује рад и запошљавање и колективни уговори.

Одредбама члана 42. став 1. Закона о раду, прописана је могућност заснивања радног односа ван просторија послодавца. Истим чланом, у ставу 2. прописано је да рад ван просторија послодавца обухвата „рад на даљину“ и „рад од куће“. Међутим, ни један од ова два појма није дефинисан, ближе уређен, нити се међу њима у овом закону прави разлика.

Тако је одредбама члана 42. Закона о раду прописано да уговор о раду који се закључује ради обављања послова ван просторија послодавца (рада на даљину и рад од куће), поред одредаба из члана 33. овог закона (*назив и седиште послодавца; лично име запосленог, место пребивалишта, односно боравишта запосленог; врсту и степен стручне спреме, односно образовања запосленог, који су услов за обављање послова за које се закључује уговор о раду; назив и опис послова које запослени треба да обавља; место рада; врсту радног односа (на неодређено или одређено време); трајање уговора о раду на одређено време и основ за заснивање радног односа на одређено време; дан почетка рада; радно време (пуно, непуну или скраћено); новчани износ основне зараде на дан закључења уговора о раду; елементе за утврђивање основне зараде, радног учинка, накнаде зараде, увећане зараде и друга примања запосленог; рокове за исплату зараде и других примања на која запослени има право; трајање дневног и недељног радног времена*); садржи

и: 1) трајање радног времена према нормативима рада; 2) начин вршења надзора над радом и квалитетом обављања послова запосленог; 3) средства за рад за обављање послова које је послодавац дужан да набави, инсталира и одржава; 4) коришћење и употребу средстава за рад запосленог и накнаду трошкова за њихову употребу; 5) накнаду других трошкова рада и начин њиховог утврђивања; 6) друга права и обавезе.

Цитиране одредбе члана 42. Закон о раду, прописују да се уговором о раду који се закључује у смислу обављања послова ван просторија послодавца, уређује и начин надзора над радом запослених. Међутим, како сам закон није уредио начин вршења надзора над радом запослених од куће, треба узети у обзир одредбе овог и других закона којима се штите права запослених на приватност и заштиту података о личности.

Члан 8. Закона о раду прописује да колективни уговор и правилник о раду (у даљем тексту: општи акт) и уговор о раду не могу да садрже одредбе којима се запосленом дају мања права или утврђују неповољнији услови рада од права и услова који су утврђени законом, те да општим актом и уговором о раду могу да се утврде већа права и повољнији услови рада од права и услова утврђених законом, као и друга права која нису утврђена законом, осим ако законом није друкчије одређено.

Када је реч о правима запослених даље указујемо да је одредбама члана 60. Устава Републике Србије прописано, између осталог, да свако има право на поштовање достојанства своје личности на раду, безбедне и здраве услове рада, потребну заштиту на раду, ограничено радно време, дневни и недељни одмор, плаћени годишњи одмор, правичну накнаду за рад и на правну заштиту за случај престанка радног односа.

У свом изјашњењу Руквалац наводи да су запослени злоупотребљавали рад од куће у циљу одласка на одмор у друго место и за обављање приватних активности ван куће, противно циљу и сврси њиховог упућивања на рад од куће. Руквалац такође наглашава да у конкретном случају није реч о раду на даљину, да је локација битан услов за рад од куће, као и да представља битну карактеристику превенције од заразних болести.

У вези са наводима Руковаоца о разлици између рада на даљину и рада од куће, као битном елементу уговора, указујемо на одредбе Закона о раду које се односе на ове видове радног ангажмана. Иако Закон о раду препознаје „рад на даљину“ и „рад од куће“ као различите термине, као што је већ истакнуто, ни један од ова два појма није дефинисан, ближе уређен, нити се међу њима у овом закону прави разлика. Код закључивања уговора, било да је реч о уговору о раду на даљину или уговору о раду од куће, морају се уредити иста питања.

Такође, одредбе овог закона не упућују на сврху која би се остварила тиме што би запослени обављао одређени посао управо од куће или са неког другог места које обезбеђују услове рада као и просторије Послодавца.

Међутим, у недостатку одредби Закона о раду, којима би се на јасан начин дефинисали ови појмови као и начин вршења надзора запослених који су упућени на рад од куће, потребно је водити рачуна о начелима обраде који су прописани чланом 5. ЗЗПЛ; као и о постојећој правној регулативи, према којој се, пре свега, запосленима не могу умањити права прописана законом.

Из образложења предлога измена и допуна Закона о раду из 2014, којим је у правни систем Републике Србије уведен „рад од куће“, каже се између осталог, да се чл. 42, 43, 45. и 46. „уводи рад на даљину као један од флексибилних облика рада. Развој информационих технологија и њена све већа примена на радном месту довели су до промена начина рада код послодавца. Данас све већи број запослених може радити на даљину, далеко од простора свога послодавца користећи нове технологије. Користи за послодавца су, пре свега, смањење трошкова рада, повећање продуктивности уз истовремено лакше запошљавање, а за запосленог комфорнији начин организације властитог радног времена. Због раста ове појаве указала се потреба да се и овај начин рада законски уреди. При томе, обезбеђена је радноправна заштита ове категорије запослених, тако што је прописано да основна зарада ових запослених не може бити мања од основне зараде запослених који раде у просторијама послодавца на истим пословима, као и да остварују права на ограничено радно време, одморе и одсуства и друга права из радног односа. Такође овим одредбама прецизирана је и садржина уговора о раду на даљину и уговора о раду од куће.“ Са садржином овог документа, можете се упознати на интернет страници Народне скупштине РС, на веб адреси: http://www.parlament.gov.rs/upload/archive/files/cir/pdf/predlozi_zakona/2344-14.pdf.

Из свега наведеног произлази да, у начелу, нема основа да се закључи да је законодавац кроз постављање правила у Закону о раду имао за циљ да ограничи „рад од куће“ само на ситуације када запослени обавља посао управо у свом пријављеном пребивалишту/боравишту. То не искључује могућност да у конкретном случају место обављања посла буде заиста битно, и као такво уређено уговором о раду. То би, на пример, могле бити ситуације када је послодавац обезбедио запосленом одређене услове за рад који су везани за конкретну локацију, нпр. заштићену интернет везу у његовом стану, опремање стана тако да задовољи одређене стандарде безбедности чувања документације и слично.

Упоредно право препознаје и појам „радника на даљину“ (*teleworkers*), којем би у контексту прописа Републике Србије највише

одговарао појам „рада од куће“. На европском нивоу ова питања су, између осталог уређена кроз Европски оквирни споразум о раду на даљину из 2002 (European Framework Agreement on Telework – 2002), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ac10131>, на основу којег су поједине чланице ЕУ донеле посебне прописе. У овом Оквирном споразуму се рад који се одвија од куће сматра само једним обликом „рада на даљину“, и у том случају су прописана посебна правила за заштиту приватности.

У оквиру Савета Европе као регионалне међународне организације европских земаља, једно од основних тела је и Комитет министара који, између осталог, одлучује о питањима од интереса свих чланица Савета, а састављен је од министара иностраних послова свих земаља чланица. Препоруком CM/Rec (2015)5 Комитета министара државама чланицама о обради података о личности у контексту запошљавања, <https://www.poverenik.rs/images/stories/dokumentacija-nova/medjunarodna-dokumenta/2019/1224.CMRec2015.5.pdf>, указано је, да опрему која открива локације запослених треба увести само ако се то покаже неопходним за постизање легитимне сврхе коју спроводе послодавци и њихова употреба не треба да води континуираном надзору запослених. Наиме, како истичу, надзор не треба да буде главна сврха, већ само индиректна последица радње која је потребна за заштиту производње, здравља и сигурности, или за осигурање ефикасног вођења неке организације, односно да послодавци треба да осигурају све неопходне гаранције за права на приватност и заштиту података о личности запослених. Овде је наглашено да послодавци треба да осигурају све неопходне гаранције за права на приватност и заштиту података о личности запослених, да обрате посебну пажњу на сврху за коју се такви уређаји користе и на принципе минимализације и пропорционалности те да примене одговарајуће интерне процедуре у вези с обрадом ових података и о њима треба унапред да обавесте предметна лица, тј. запослене.

Имајући у виду утврђено чињенично стање и наведене одредбе ЗЗПЛ, неспорно је да је Руковалац вршио обраду података о личности и то локације запослених путем ГПС апликације као и да је Обавезним упутством за рад од куће уредио да се надзор може вршити и обиласком запослених на место пребивалишта.

Неспорно је да вршење надзора над радом и условима рада запослених обиласком на адресе пребивалишта представља изузетно висок ризик по приватност како запосленог тако и других физичких лица, са којима запослени дели стамбени простор.

Даље, имајући у виду наводе Руковаоца да је обраду података вршио у циљу извршавања уговора о раду закључених са запосленим, у складу са чланом 12. став 1. тачка 2 ЗЗПЛ; указујемо да је одредбама

тог члана прописано да је обрада законита ако је неопходна за извршење уговора закљученог са лицем на које се подаци односе. Међутим, у свом изјашњењу Руковалац није образложио да је обрада локације запослених путем ГПС или посета запослених на адреси пребивалишта неопходна за вршење надзора над радом и квалитетом обављања послова, док је запослени у могућности да одговара на захтеве послодавца, извршава задатке у задатом року и испуњава друге обавезе које су прописане законом и уговором о раду, као и да је рад на месту пребивалишта нужен услов рада од куће. Дакле, неоспорно је да се надзор над радом запослених могао остварити и на други начин који би представљао мањи ризик по приватност лица, те да обрада локације запослених путем ГПС и обилазак запослених на месту боравишта у конкретном случају није била неопходна и није била законита.

Даље, супротно обавезама из члана 54. и 55. ЗЗПЛ, Руковалац није извршио процену утицаја обраде на заштиту података о личности нити је прибавио претходно мишљење Повереника, у поступку којег би, сходно одредбама наведеног члана, изradio процену ризика на права и слободе лица на које се подаци односе као и процену неопходности и сразмерности вршења радњи обраде у односу на сврху обраде.

Такође, имајући у виду наводе из изјашњења Руковаоца да је као додатни правни основ за обраду података о личности прибавио пристанак запослених лица, Повереник указује да пристанак прибављен на начин описан у изјашњењу Руковаоца није законит, односно није прибављен у складу са чланом 15. ЗЗПЛ, као и да Руковалац запосленима није пружио информације из члана 23. ЗЗПЛ, што је неопходан услов да би предметна обрада била транспарентна.

Сходно наведеном, Руковалац обрадом локације запослених путем ГПС или обиласком запослених на место пребивалишта, врши обраду података која није законита, поштена и транспарентна, супротно одредбама члана 5. став 1. тачка 1. ЗЗПЛ, као и обраду без претходно извршене процене утицаја предвиђених радњи обраде на заштиту податка о личности, супротно одредбама члана 54. ЗЗПЛ.

Због свега наведеног, Повереник је изрекао ову Опомену, са налогом Руковаоцу да га обавести о предузетим мерама и активностима за отклањање утврђених повреда одредби ЗЗПЛ, као и мерама и активностима које ће Руковалац предузети да се исте не би поновиле, и то у року од 15 дана од дана пријема овог акта, а како не би дошло до предузимања других корективних мера из надлежности Повереника.

Правни оквир и пракса Савета Европе и Европске уније

Праћење активности запослених на службеним уређајима за електронску комуникацију

Надзор употребе електронских комуникација на радном месту

Запослени с правом очекују одређени ниво приватности на радном месту јер на радном месту развијају значајан део својих односа с другим људима. Ово право мора да буде у равнотежи с правима и интересима послодавца, примера ради, интересу послодавца да ефикасно води своје пословање и да се заштити од одговорности или штете која може бити проузрокована радњама запослених (на пример, одавање пословне тајне, поседовање забрањеног садржаја на службеном рачунару). Под одређеним условима, послодавац има право да контролише професионалну комуникацију запослених, коју запослени, на пример, шаље у име послодавца. На службеним средствима за рад се често налазе и приватне комуникације запослених. Оне су (изричито) заштићене правом на тајност дописивања из члана 8. ЕКЉП.

Одбор министара у Препоруци СЕ о обради личних података у оквиру запослења државама чланицама препоручује да би требало да предузимају мере надзора употребе службених техничких средстава и комуникација, као што су телефон, електронска пошта и интернет, дозвољавају под рестриктивним условима да се спрече неоправдани и неразумни задирања у права запослених на приватни живот. Овај принцип важи за све техничке уређаје и Информационо-комуникационе технологије (*ИКТ*), које запослени користе у склопу обављања радних задатака. Послодавци морају да упознају запослене са редовно ажурираном политиком заштите података о личности за појединачна средства за рад и да у њој дефинишу сврху обраде, чување или период прављења резервних копија саобраћајних података и архивирање професионалних електронских комуникација.

Препоруке у погледу надзора над употребом интернета на радном месту

Превасходно у случају обраде података о личности у вези с интернет или интранет страницама којима запослени приступају, у складу с Препоруком СЕ, приоритет треба дати усвајању превентивних мера, као што је употреба филтера који спречавају одређене операције и ескалацију могућих мера надзора, при чему се препоручује неиндивидуална и насумична провера података који су анонимни или на

неки начин обједињени.⁸¹ Све наведено има приоритет и треба га искористити за остваривање интереса послодавца, тако да је беспотребан над употребом средстава за рад конкретног запосленог. Исти став о значају увођења превентивних механизма за употребу интернета на радном месту заузела је радна група из члана 29. у Радном документу о надзору електронских комуникација на радном месту.⁸² Колико год је могуће, интернет политика послодавца би се морала односити на техничка средства за ограничавање приступа, а не на праћење понашања, тј. блокирање неких интернет сајтова или подешавање аутоматских упозорења о неовлашћеној употреби мреже.⁸³

Брзо обавештавање запослених о откривању сумњиве употребе интернета је важно за спречавање ризика од злоупотребе. Радна група из члана 29. наглашава да се у већини случајева може открити злоупотреба интернета, а да нема потребе за анализом посећених страница. На пример, провера утрошеног времена или провера интернет страница које одређено одељење код послодавца најчешће посећује може бити довољно да се послодавац увери да његови капацитети нису злоупотребљени. Уколико ови општи прегледи открију потенцијалну злоупотребу интернета, послодавац може размислити о могућности додатног надзора (који би морао да буде усредсређен на примећене ризике). Радни документ укључује и предложене информације које треба да буду део минималног садржаја интернет политике послодаваца, између осталог:

- јасно дефинисање услова под којима је дозвољена приватна употреба интернета и навођење материјала који није дозвољено гледати или копирати; притом, радна група упозорава да општа забрана употребе интернета у личне сврхе не изгледа као разумна мера;
- информисање запослених о системима који се примењују за спречавање приступа одређеним интернет страницама за откривање злоупотреба и навода да ли се праћење односи на појединце или одређене делове предузећа, да ли је стално или се активира приликом посебних околности;
- дефинисање сврхе обраде прикупљених података о употреби интернета;
- укључивање представника запослених у спровођење интернет политике и њихова улога у истрази наводних кршења.⁸⁴

81 14.2. тачка Препорука СЕ.

82 Радна група за заштиту података из члана 29, Радни документ о надзор електронских комуникација на радном месту, WP 55, Брисел, 29. 5. 2002.

83 Исто. стр. 24.

84 Радна група за заштиту података из члана 29, Радни документ о надзор електронских комуникација на радном месту, WP 55, Брисел, 29. 5. 2002, стр. 25.

Препоруке у вези с надзором службеног сандучета електронске поште

Према Препоруци СЕ, приступ послодаваца професионалним електронским комуникацијама својих запослених, који су унапред обавештени о постојању ове могућности, требало би да буде могућ само када је то неопходно из безбедносних или других законских разлога. То потврђује и радна група из члана 29. уз образложење да се послодавац не може ослањати на сагласност запосленог за обраду његових личних података у ситуацијама када би одбијање сагласности могло довести до штетних последица по њега због природе радног односа и подређеног положаја запосленог.⁸⁵ У случају одсуства запослених, послодавци су дужни да предузму потребне мере и обезбеде процедуре у циљу омогућавања приступа професионалним електронским комуникацијама само када је тај приступ неопходан за пословање послодавца. Приступ треба извршити на што ненаметљивији начин и тек након обавештавања запослених којих се тиче.⁸⁶ Садржај, слање и пријем *приватних* електронских комуникација на радном месту се ни под којим условом не сме контролисати.⁸⁷

Радна група из члана 29. препоручује послодавцима да запосленима дозволе да на радном месту користе, поред свог службеног налога е-поште и свој приватни налог (у оквиру система послодавца или онлајн) у сврху искључиво личне употребе. На овај начин се поједностављује разлика између професионалне и приватне комуникације и прилагођава очекивање приватности за запослене који су обавештени да у приватне сврхе треба да користе посебно (приватно) сандуче.

Према Препоруци СЕ, по одласку запосленог из организације, послодавац је дужан да предузме неопходне организационе и техничке мере за аутоматско деактивирање службеног електронског налога запосленог. Ако послодавци треба да обнове садржај налога запосленог да би ефикасно водили организацију, нека то ураде пре његовог одласка и, ако је то изводљиво, у његовом присуству.⁸⁸

85 Исто. стр. 21: *“Ослањања на пристанак требало би да буде ограничено на случајеве када запослени има истински слободан избор и може накнадно да повуче сагласност без консеквенци.”*

86 14.3. тачка Препорука СЕ.

87 14.4. тачка Препорука СЕ.

88 14.5. тачка Препорука СЕ.

Заштита приватности телефонских комуникација запослених

Све горе наведене опште препоруке у погледу задирања у телекомуникације запослених на радном месту важе и за телефонске комуникације. На овом месту ваља напоменути и да је у Европској унији успостављена директива о приватности и електронским комуникацијама,⁸⁹ која у члану 7. уређује право претплатника на пријем нерашчлањених рачуна. Државе чланице користе своје националне одредбе да би усагласиле право претплатника који примају рашчлањене рачуне с правом на приватност позивајућих корисника и позваних претплатника, на пример, тако што ће таквим корисницима и претплатницима пружити довољно друкчијих начина да повећају приватност порука или плаћања (као што је прекривање последње три цифре позивног броја). Увођење опције нерашчлањених рачуна нуди се као кључна могућност за послодавце као претплатнике пословних бројева које користе запослени да би избегли прекомерно задирање у приватност запослених.

У случају *Халфорд против Уједињеног Краљевства*⁹⁰ Суд је донео одлуку да телефонски позиви како из пословних просторија тако и од куће могу бити обухваћени појмом „приватног живота“ и „дописивања“ у складу са чланом 8. став 1. ЕКЉП.⁹¹ Чињенице случаја су биле следеће. Подносиатељка жалбе је била заменица начелника локалне полиције. Против својих претпостављених и владе Уједињеног Краљевства покренула је судски поступак због сексуалне дискриминације, зато што јој је послодавац ускратио могућности напредовања. У поступку је откривено да су њени претпостављени без судског налога односно другог налога надлежног органа прислушкивали телефон у њеној канцеларији. Имала је своју канцеларију с два телефона, а један од њих је био намењен приватним позивима. У погледу употребе телефона није било никаквих ограничења јер јој је претпостављени дозволио обављање позива приватне природе. Телефони су били део интерне телефонске мреже локалне полицијске станице где се радило о телекомуникационом систему који је одвојен од јавне телефонске мреже. Све позиве је плаћала полиција. Прислушкивањем без судског налога послодавац је придобио информације које је затим користио у поступку против запослене. Велика Британија је до тада само забрањивала прислушкивање јавних телекомуникационих мрежа као не-

89 Директива 2002/58/EZ Европског парламента и Савета од 12.7.2002. о обради података о личности и заштити приватност у области електронских комуникација.

90 Пресуда ЕСЉП у случају Халфорд против Уједињеног Краљевства од 25.6.1997, бр. пред. 20605/92.

91 Исто, пасус 44.

легално, а закон није важио за унутрашње, интерне комуникационе мреже. Влада је сматрала да Халфордова није могла разумно очекивати приватност ових позива јер је послодавац требало да има могућност да прати позиве без претходног упозорења путем уређаја које је сам обезбедио. Суд је констатовао да телефонски разговори које је подносиатељка тужбе обављала на послу и током радног времена (без обзира на то са ког телефона их је обављала) могу спадати у домен њеног приватног живота и да је на основу свих околности подносиатељка тужбе при комуникацији разумно очекивала одређену приватност.⁹² Коначно, након утврђивања критеријума за законитост мешања у право подносиатељке тужбе, суд је закључио да не постоји правни основ за прикривено пресретање њене комуникације, као и да мешање није било сразмерно очекивању приватности коју је подносиатељка тужбе разумно имала, дакле, дошло је до повреде члана 8. ЕКЉП.

Остали случајеви из судске праксе Европског суда за људска права

У случају *Барбулеску против Румуније*⁹³ запослени је био упознат с правилима послодавца о забрани употребе било каквих уређаја послодавца у приватне сврхе (између осталог, да не сме да користи интернет и рачунар, Yahoo Messenger у приватне сврхе), а такође је био обавештен о томе да је послодавац успоставио поступак праћења његове документације. Упркос томе је запослени интернет у Yahoo Messengerу користио у приватне сврхе. Због наведених прекршаја, послодавац је против запосленог покренуо поступак за отказ уговора о раду. Сходно томе, запосленом је престао и радни однос код послодавца. Запослени је оспорио законитост отказа, тврдећи да је надзор његових комуникација био незаконит јер су комуникације које је послодавац пратио приватне природе, имао је и једини лозинку за приступ свом налогу и, због тога што није био обавештен унапред да послодавац чита његову пошту, разумно је очекивао приватност у вези с таквом комуникацијом. Суд је одлучио (након подношења жалбе Великом већу) да, без обзира на ограничења која је послодавац одредио у конкретном случају у погледу употребе опреме за рад, ово право запосленог на приватност на радном месту не може свести на „нулу“ – „нема приватности“.⁹⁴ Право на приватни живот и приватност преписке постоји, чак и ако су права ограничена у мери која је неопходна за осигурање интереса послодавца.

92 Исто, пасус 45.

93 Пресуда ЕСЉП у случају Барбулеску (Bărbulescu) против Romuniје од 5.9.2017, бр. пред. 61496/08.

94 Исто. пасус 80.

Суд је истакао околности које се морају узети у обзир приликом одмеравања легитимних интереса послодавца и права запосленог на приватност:

- да ли је запослени унапред обавештен од стране послодавца о могућности праћења или контроле његове преписке или комуникације и о спровођењу ових мера; (обавештење послодавца о надзору и мерама које се спроводе морало би да буде јасно и дато унапред);
- обим надзорних мера које спроводи послодавац, тј. да ли се прате само подаци о саобраћају, или се евентуално прегледа и садржај порука запосленог; да ли се прегледају све комуникације или само део, временско ограничење праћења, број лица која имају приступ овим подацима;
- да ли је послодавац доказао легитимне разлоге који уређују преглед комуникација; с тим у вези, преглед садржаја комуникација као инвазивније методе захтева веће оправдање за прихватљивост мешања послодавца у право запосленог на приватност;
- да ли би било могуће успоставити надзор коришћењем мање наметљивих метода и мера;
- последице надзора по запосленог и у које сврхе послодавац користи резултате надзора; посебно је потребно проценити да ли резултати надзора и прегледа по садржају могу довести до циља надзора како је дефинисано – да ли су уопште погодни за заштиту легитимних интереса послодавца;
- да ли је запослени имао на располагању довољно заштитних механизма, које првенствено треба да обезбеде да послодавац нема приступ садржају комуникације осим у случају претходног обавештења запосленог о коме је реч.⁹⁵

У конкретном случају, суд је закључио да је дошло до повреде члана 8. ЕКЉП, пошто је национални суд поступио само формалистички и теоријски, те је конкретно мешање у право запосленог на приватност требало да оцени из перспективе свих горе наведених критеријума.

Случај *Либерт против Француске*⁹⁶ односио се на отпуштање службеника француске националне железничке компаније након што је заплена његовог службеног рачунара обелоданила чување порнографских датотека и фалсификованих сертификата. Конкретно, подносилац тужбе је навео да је његов послодавац у његовом одсуству отворио личне датотеке које су биле сачуване на хард-диску његовог службеног рачунара. Подносилац тужбе је сачувао наведене датотеке

⁹⁵ Исто. пасус 121.

⁹⁶ Пресуда ЕСЉП у случају Либерт против Француске од 22. 2. 2018, бр. пред. 588/13.

у општој фасцикли која је намењена службеним датотекама, али је сам у називу подфасцикле обележио да се ради о његовој приватној фасцикли. Политика коришћења службеног рачунара допуштала је приватну употребу рачунара само у изузетним случајевима, при чему би приватне датотеке требало да буду искључиво у широј фасцикли под називом „Приватно“. Суд је донео пресуду да није дошло до повреде члана 8. конвенције, при чему је констатовао да француске власти у овом случају нису прекорачиле поље слободне процене које им је на располагању. Суд је утврдио да је увид послодавца у предметну фасциклу подносиоца тужбе следио легитимни циљ послодавца да обезбеди да његови запослени користе службену рачунарску опрему у складу са својим уговорним обавезама и важећим прописима.⁹⁷ Суд је такође констатовао да француски закон и судска пракса не дозвољавају послодавцу приступ приватним датотекама запослених осим у њиховом присуству, али у конкретном случају подносилац тужбе није правилно обележио датотеку као приватну у складу са правилником послодавца. Наведени механизам раздвајања не би спречио послодавца да приступи предметним фајловима јер нису правилно идентификовани као приватни.⁹⁸ Коначно, Суд је сматрао да су домаћи судови исправно третирали захтев подносиоца жалбе тиме што су га одбацили.

Надзор над употребом службеног аутомобила (GPS подаци)

У складу са Препоруком СЕ, државе уговорнице треба да дозволе уређаје за обелодањивање локације запослених само ако се покаже да је то неопходно за остваривање легитимне сврхе послодавца, а њихово коришћење не сме резултирати сталним праћењем запослених. Пре свега, праћење не би требало да буде главна сврха, већ само индиректна последица мере неопходне за заштиту производње, здравља и безбедности или да би се обезбедило ефикасно функционисање организације. Узимајући у обзир висок ризик од кршења права и слобода радника, послодавци треба да обезбеде све неопходне заштитне механизме да би се заштитила приватност запослених и њихових личних података. При томе послодавци треба да обрате посебну пажњу на сврху коришћења оваквих уређаја и на принципе минимизације и сразмерности у обради података. И у овом случају се сматра да би послодавци морали да успоставе интерну политику у погледу обраде података и да пре увођења надзора о томе обавесте запослене.⁹⁹

⁹⁷ Исто. пасус 46.

⁹⁸ Исто. пасус 52.

⁹⁹ 16. тачка Препорука СЕ.

Конкретнија упутства о обради геолокационих података у оквиру радног односа дала је радна група из члана 29. у Мишљењу 2/2017. Обрада података о локацији може бити оправдана ако се спроводи као део праћења превоза људи или робе или побољшања дистрибуције ресурса за услуге на дисперзованим локацијама (нпр. планирање операција у реалном времену) или ако следи безбедносни циљ у вези са самим запосленим или робом, односно возилима која су под његовим задужењем. Насупрот томе, Радна група сматра да је обрада података претерана када запослени имају слободу да организују своје путне аранжмане онако како желе, или када се то обавља искључиво у сврху праћења рада запосленог, где се то може пратити на други начин.¹⁰⁰

Када послодавац дозволи приватну употребу службеног возила, најважнија мера коју може да предузме да би се обезбедила усклађеност с принципима заштите података о личности је опција: *opt-out*: запослени треба да има могућност да привремено искључи праћење локације у посебним околностима, ако оправда ово искључење, нпр. за посету лекару. На тај начин запослени самоиницијативно може да заштити одређене локацијске податке као приватне. Поред тога, послодавац мора да обезбеди да се прикупљени подаци не користе за незакониту даљу обраду, као што је праћење и процена запослених.¹⁰¹

У случају *Флодиндо де Алмеида Васконселос против Португалије*¹⁰² подносилац жалбе је тврдио да је обрадом геолокационих података добијених од GPS система инсталираног у његовом службеном возилу и коришћењем тих података за оправдање његовог отпуштања повређено његово право на поштовање његовог приватног живота. Жалио се и да су поступци пред домаћим судовима непоштени јер су се одлуке суда заснивале скоро искључиво на незаконитим доказима стеченим помоћу система GPS. У току поступка је утврђено да је подносилац тужбе обавештен да ће његово службено возило бити опремљено GPS уређајем и да је потписао документ на основу кога је јасно да је систем намењен праћењу пређених раздаљина током рада запослених здравствених заступника и да може бити покренут дисциплински поступак против сваког запосленог у случају неусклађености података о пређеној километражи које обезбеди GPS и података које обезбеди запослени. Компанија је дозволила коришћење возила за приватна путовања и путовања ван радног времена, али је требало надокнадити трошкове километраже на приватним путовањима. У

100 Радна група за заштиту података из члана 29, Мишљење бр. 2/2017 о обради података на раду, WP 249, Брисел, 8.6.2017., стр. 20. и 21.

101 Исто.

102 Пресуда ЕСЉП у случају *Флодиндо де Алмеида Васконселос Грамаксо* (Florindo de Almeida Vasconcelos Gramacho) против Португалије од 13. 12. 2022, бр. пред. 26968/16.

дисциплинском поступку против подносиоца тужбе утврђено је да је он у свом професионалном својству повећао пређене раздаљине како би смањιο удео превезених приватних путовања викендом и празницима, чиме је избегао надокнаду одговарајућих износа. Подносилац тужбе је такође оптужен да је манипулисао GPS-ом тако што је уклонио картицу GSM из уређаја. Суд је донео пресуду да није дошло до повреде права на приватност, констатујући да су национални органи испунили своје позитивне обавезе да заштите право подносиоца тужбе на поштовање његовог приватног живота. Суд је узео у обзир да је подносилац тужбе знао да је компанија у његово возило уградила GPS систем за праћење пређених раздаљина у оквиру његове професионалне делатности и, ако је применљиво, на приватним путовањима како би контролисала коришћење средстава послодавца. Такође је утврдио да су, узимајући у обзир геолокационе податке искључиво у вези с превезеним раздаљинама, домаћи судови смањили обим задража у приватни живот подносиоца тужбе на оно што је било апсолутно неопходно за постизање легитимног циља послодавца. Судови су такође проверили да је приступ подацима о превезеним раздаљинама био на располагању само оним запосленима који су организовали пословне посете и израчунавали накнаду трошкова службених путева.

О прихватљивости коришћења података из GPS уређаја који су постављени у службеним аутомобилима је недавно одлучивао и аустријски повереник за информације. Послодавац (руководилац) прво је обрађивао информације из GPS система за одређивање тренутне локације возила, а затим и као алат за вођење евиденције о радном времену, службеним путовањима и за обрачун путних трошкова. Уређај који је постављен на возилима преноси податке на сервер и активира се покретањем мотора аутомобила и деактивира се када се мотор заустави. Међутим, сваки ауто има и прекидач који возачу омогућава ручно деактивирање уређаја. Прослеђени подаци укључују: превезену раздаљину у км, датум и време, почетну тачку, циљ и податке о локацији возила (и стварно пређени пут). Послодавац је свој законски разлог засновао на интересу да тачно обрачуна радне сате и путне трошкове, награђивању запослених и да има интерес да зна њихову локацију у реалном времену уколико би морао спонтано да их пошаље клијенту (узимајући у обзир природу рада послодавца). Повереник за информације је у уводу констатовао да обрада при оправданом интересу руковооца мора да буде строго ограничена на оно што је неопходно за остваривање овог интереса. Увек треба утврдити да ли је исту сврху могуће постићи употребом мање наметљивих средстава. У конкретном случају је повереник за информације проценио да би послодавац могао да утврди локацију запослених у реалном времену и на други начин, тако што би питао интерне координаторе који

су странци били додељени. Поред тога, није нашао ваљан разлог да тврди да је коришћење уређаја за праћење било неопходно да би се материјално олакшала административна обавеза руковооца да евидентира радно време и обрачуна путне трошкове, јер се то лако може урадити без употребе GPS трагача. Као резултат реченог, послодавцу је наложио да обустави обраду спорних података.¹⁰³

Право на приватност и нове праксе рада на даљину односно рада од куће

Нове праксе обављања посла ван области директног надзора послодавца у радним просторијама, рад од куће односно рад на даљину, отварају нова питања оправданих интереса послодавца да повећа надзор над запосленима, а на другој страни бригу о очувању приватности запослених у околностима све већег преплитања посла и приватног живота.

Послодавци у режиму рада од куће или рада на даљину запосленима обично стављају на располагање опрему или софтвер који им после постављања у њиховој кући односно на сопственим уређајима омогућава исти степен приступа мрежи, системима и ресурсима послодавца, које би имали када би били на радном месту. Иако се рад на даљину може схватити као позитиван помак начина обављања радних обавеза, он представља и додатни ризик за послодавца. На пример, запослени који имају даљински приступ послодавчевој инфраструктури нису везани мерама физичког обезбеђења које су можда успостављене у просторијама послодавца. Једноставно речено: без спровођења одговарајућих техничких мера, ризик од неовлашћеног приступа се повећава и може довести до губитка или уништавања информација, укључујући личне податке запослених или клијената које поседује послодавац. Како би умањили описани ризик, послодавци могу сматрати да је оправдано применити софтверске пакете (било у месту употребе или у облаку) који, на пример, снимају притиске тастера и покрете миша, снимају слику тренутног екрана (било насумично или у подешеним интервалима), бележе коришћене апликације (које су коришћене и колико дуго) и, на компатибилним уређајима, активацију веб-камера и прикупљање направљених снимака. Иако су овакве технологије и дан-данас широко доступне, према ставу Радне групе за заштиту података о личности из члана 29, предметна обрада података о личности је несразмерна и послодавац по правилу неће имати правне основе унутар законског интереса, нпр.

¹⁰³ Аустријски орган за заштиту података, одлука од 1.3.2022. у случају бр. пред. 2022-0.021.739.

за снимање притисака тастера и покрета миша запосленог. Кључна је процена ризика који представља рад од куће и рад на даљину, као и строго сразмерно предузимање мера послодавца, нарочито када грађани пословне и приватне употребе нису јасно уређене у политици употребе службених уређаја за комуникацију.¹⁰⁴

Због раста популарности, функција и перформанси електронских уређаја за широку потрошњу, послодавци се могу суочити са захтевима запослених да користе своје уређаје на радном месту за обављање свог посла. Овакав облик употребе приватних уређаја у службене сврхе је познат као политика „донесите свој уређај“ односно „*bring your own device*“ („BYOD“). Организација посла на сопственим уређајима запослених доноси својеврсне изазове, посебно са становишта да је по самој природи ствари такав уређај приватне природе, садржи и приватне датотеке, фотографије, податке о приватном коришћењу интернета, итд. У контексту радног односа, ризици у погледу приватности BYOD-а су обично повезани с технологијама праћења које прикупљају идентификаторе као што су MAC адресе, или у случајевима када послодавац приступа уређају запосленог на основу обављања безбедносне провере, тј. у вези са злонамерним софтвером, али тада може наићи и на многе приватне садржаје запосленог.¹⁰⁵

Праћење локације и саобраћаја приватних уређаја које запослени користи на послу сматра се да се спроводи у легитимном интересу послодавца за безбедност података о личности за које је послодавац одговоран као руковалац података (нпр. података о клијентима). Овакво праћење брзо може постати незаконито ако обухвата и податке у вези с приватним и породичним животом запосленог. Радна група у Мишљењу 2/2017 саветује да послодавци успоставе критеријуме за разликовање приватне и пословне употребе уређаја. Послодавци би морали да уведу и методе којима се њихови подаци у уређају безбедно преносе између тог уређаја и њихове мреже. Послодавац може да конфигурише уређај тако што усмерава сав саобраћај преко VPN-а назад у мрежу послодавца тако да пружа одређени ниво безбедности. Ако користи такву меру, послодавац такође мора узети у обзир да софтвер инсталиран у сврхе праћења представља ризик за приватност током периода личне употребе од стране запосленог. Радна група у овом контексту препоручује употребу алатки које пружају додатну заштиту, као што је „*sandboxing*“ података (чување података унутар одређене апликације).¹⁰⁶ Уколико у конкретном случају није могуће пронаћи

104 Радна група за заштиту података из члана 29, Мишљење бр. 2/2017 о обради података на раду, WP 249, Брисел, 8.6.2017., стр. 16.

105 Исто. стр. 17.

106 Исто.

ефикасно решење за заштиту података о личности за које је одговоран послодавац, препоручује се да послодавац забрани употребу уређаја у приватне сврхе.

Препоруке за усклађивање

У вези са обрадом података о личности запослених у делу који се односи на обраду геолокационих података путем сателитског праћења возила (ГПС), а како је наведено у делу о видео надзору, потребно је ревидирати Закон о приватном обезбеђењу. Поред тога, имајући у виду одредбе Закона о раду, а које се односе на обавезу послодавца да обезбеди средства рада, а посебно када је реч о раду ван просторија послодавца, и с тим повезану обавезу запосленог да средства користи целисходно и одговорно, потребно је прецизирати начин употребе средстава за рад, као и приступа услугама информационог друштва. Ове одредбе, у складу са чланом 91. Закона о заштити података о личности треба да садрже и посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе.

Изабрани извори

Документи међународних организација

Савет Европе

Европска конвенција о људским правима

Конвенција Савета Европе о заштити лица у односу на аутоматску обраду личних података (Конвенција 108+)

Препорука CM/Rec(2015)5 Комитета министара државама чланицама о обради личних података у контексту запошљавања (незваничан превод објављен у публикацији Повереника за информације од јавног значаја и заштиту података о личности бр. 3, 2018)

Приручник за заштиту података о личности Агенције ЕУ за основна права у сарадњи са Саветом Европе и канцеларијом Европског надзорника за заштиту података (доступан на енглеском језику на: https://www.echr.coe.int/documents/d/echr/handbook_data_protection_ENG)

Пресуде Европског суда за људска права

Барбулеску против Ромуније од 5.9.2017, бр. пред. 61496/08.

Флодиндо де Алмеида Васконселос Грамаксо против Португалије од 13. 12. 2022, бр. пред. 26968/16.

Леандер против Шведске од 26.3.1987, бр. пред. 9248/81.

Либер против Француске од 22. 2. 2018, бр. пред. 588/13.

Лопез Рибалда и други против Шпаније од 17. 10. 2019, бр. пред. 1875/13 и 8567/13.

П.Г. и Ј.Х. против Уједињеног Краљевства од 25. 9. 2001, бр. пред. 44787/98

Халфорд против Уједињеног Краљевства од 25.6.1997, бр. пред. 20605/92.

Европска унија

Директива 2002/58/ЕЗ Европског парламента и Савета од дана 12. јула 2002. о обради података о личности и заштити приватности у области електронских комуникација. (доступно на: <http://data.europa.eu/eli/dir/2002/58/oj>)

Директива (ЕУ) 2019/1937 Европског парламента и Савета од дана 23. октобра 2019. о заштити лица која пријављују повреде права уније (доступно на енглеском: <http://data.europa.eu/eli/dir/2019/1937/oj>)

Директива 2003/88/ЕЗ Европског Парламента и Савета од 4.11. 2003. о одређеним видовима организације радног времена (доступно на енглеском на: <https://eur-lex.europa.eu/eli/dir/2003/88/oj>)

Директива 2000/78/ЕЗ од 27.11. 2000. о успостављању општег оквира за једнако поступање при запошљавању и обављању занимања (доступно на енглеском на: <https://eur-lex.europa.eu/eli/dir/2000/78/oj>)

Директива Савета 2010/18/ЕУ од 8.3.2010. о спровођењу ревидираног Оквирног споразума о родитељском одсуству који су закључили BUSINESSEUROPE, UEAPME, СЕЕР и ETUC и стављању ван снаге Директиве 96/34/ЕЗ (доступно на енглеском на: <https://eur-lex.europa.eu/eli/dir/2010/18/oj>)

Европски одбор за заштиту података - European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, (доступно на енглеском: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf)

European Parliament, „The scope of EU labour law - Who is (not) covered by key directives?“, October 2020 (доступно на енглеском на: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/658181/IPOL_IDA\(2020\)658181_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/658181/IPOL_IDA(2020)658181_EN.pdf))

Мишљење о обради података на раду Радне групе за заштиту података из члана 29, бр. 2/2017 (доступно на енглеском: <https://ec.europa.eu/news-room/article29/items/610169/en>)

Мишљење 4/2004 Радне групе из члана 29. о обради личних података путем видео-надзора (доступно на енглеском: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf)

Радни документ о надзору електронских комуникација на радном месту, Радна група за заштиту података из члана 29, мај 2002. (доступно на енглеском: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf)

Мишљење 8/2001 Радне групе из члана 29 о обради података у контексту запошљавања (доступно на енглеском: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf)

Мишљење 1/2006 о примени правила ЕУ о заштити података код интерних шема за пријаву неправилности у области рачуноводства, интерног рачуноводственог надзора, послова ревизије, борбе против корупције, банкарског и финансијског криминала, Радне групе за заштиту података из члана 29, фебруар 2006. (доступно на енглеском: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf)

Извештај Европског комитета за правну сарадњу, који садржи смернице за заштиту појединаца у погледу прикупљања и обраде података путем видео надзора, 2003. (доступно на енглеском: https://www.europarl.europa.eu/doceo/document/TA-5-2004-0141_EN.html)

Смернице Европског надзорника за заштиту података за видео надзор, Брисел, март 2010. (доступно на енглеском: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf)

Смернице Радне групе за заштиту података из члана 29 о аутоматском доношењу појединачних одлука и профилисању за потребе Уредбе (ЕУ) 2016/679, 3. октобар 2017. (доступно на: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en)

Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. о заштити физичких лица у односу на обраду података о личности, и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге (Општа уредба о заштити података) (незваничан превод на српски доступан на интернет презентацији Повереника за информације од јавног значаја и заштиту података о личности)

Други документи

Кодекс поступања за заштиту личних података запослених Међународне организације рада 2022. (доступно на енглеском: https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_107797/lang--en/index.htm)

Informacijski pooblaščenec Republika Slovenija, Smernice glede izvajanja videonadzora, април 2023. (доступно на словеначком: <https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-spl%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/smernice-glede-izvajanja-videonadzora>)

Republika Hrvatska, Закон о provedbi Opće uredbe о zaštiti podataka („Narodne novine“ br. 42/18) (доступно на хрватском на: <https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka>)

Поједини прописи Републике Србије који се односе на обраду података у контексту радних односа:

Закон о агенцијском запошљавању („Сл. гласник РС“, бр. 86/19)

Закону о безбедности и здрављу на раду („Сл. гласник РС“, бр. 35/23)

Закон о безбедности саобраћаја на путевима („Сл. гласник РС“, бр. 41/09, 53/10, 101/11, 32/13 - одлука УС, 55/14, 96/15 - др. закон, 9/2016 - одлука УС, 24/18, 41/18, 41/18 - др. закон, 87/18, 23/19, 128/20 - др. закон и 76/23)

Закон о волонтирању („Сл. гласник РС“, бр. 36/2010)

Закон о државним и другим празницима у Републици Србији („Сл. гласник РС“, бр. 43/01, 101/07 и 92/11)

Закон о државним службеницима („Сл. гласник РС“, бр. 79/05, 81/05 - испр., 83/05 - испр., 64/07, 67/07 - испр., 116/08, 104/09, 99/14, 94/17, 95/18, 157/20 и 142/22)

Закон о евиденцијама у области рада („Сл. лист СРЈ“, бр. 46/96 и „Сл. гласник РС“, бр. 101/05 - др. закон и 36/09 - др. закон)

Закон о заштити података о личности („Сл. гласник РС“, бр. 87/18).

Закон о заштити узбуњивача („Сл. гласник РС“, бр. 128/14)

Закон о запосленима у аутономним покрајинама и јединицама локалне самоуправе („Сл. гласник РС“, бр. 21/16, 113/17, 95/18, 114/21, 113/17 - др. закон, 95/18 - др. закон, 86/2019 - др. закон, 157/20 - др. закон и 123/21 - др. закон).

Закон о запосленима у јавним службама („Сл. гласник РС“, бр. 113/17, 95/18, 86/19, 157/20 и 123/21)

Закон о запошљавању и осигурању за случај незапослености („Сл. гласник РС“, бр. 36/09, 88/10, 38/15, 113/17, 113/17 - др. закон и 49/21)

Закон о здравственом осигурању („Сл. гласник РС“, бр. 25/2019 и 92/2023).

Закон о оглашавању („Сл. гласник РС“, бр. 6/16 и 52/19 - др. закон)

Закон о основама система образовања и васпитања („Сл. гласник РС“, бр. 88/17, 27/18 - др. закон, 10/19, 27/18 - др. закон, 6/20, 129/21 и 92/23)

Закон о пензијском и инвалидском осигурању („Сл. гласник РС“, бр. 34/2003, 64/2004 - одлука УСРС, 84/2004 - др. закон, 85/2005, 101/2005 - др. закон, 63/2006 - одлука УСРС, 5/2009, 107/2009, 101/10, 93/12, 62/13, 108/13, 75/14, 142/14, 73/18, 46/19 - одлука УС, 86/19, 62/21, 125/22, 138/22 и 76/23)

Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података, „Сл. лист СРЈ - Међународни уговори“, број 1/92, „Сл. лист СЦГ - Међународни уговори“, број 11/05 - др. закон и „Сл. гласник РС - Међународни уговори“, бр. 98/2008 - др. закон и 12/10)

Закон о потврђивању Протокола о изменама и допунама Конвенције о заштити лица у односу на аутоматску обраду личних података, „Сл. гласник РС - Међународни уговори“, бр. 4/20)

Закон о приватном обезбеђењу („Сл. гласник РС“, бр. 104/13, 4215 и 87/18).

Закон о раду („Сл. гласник РС“, бр. 24/05, 61/05, 54/09, 32/13, 75/14, 13/17 - одлука УС, 113/17 и 95/18 - аутентично тумачење)

Модел акта о процени легитимног интереса као правног основа за обраду података о личности, доступан на интернет презентацији Повереника за информације од јавног значаја и заштиту података о личности

Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника („Сл. гласник РС“, бр. 45/19 и 112/20)

Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности („Сл. гласник РС“, бр. 40/19)

Уредба о интерном и јавном конкурс за попуњавање радних места у државним органима („Сл. гласник РС“, бр. 2/19 и 67/21)

Уредба о канцеларијском пословању органа државне управе („Сл. гласник РС“, бр. 21/20, 32/21 и 14/23)