Сузана Лежаић*

Брига о заштити података о личности као обележје одговорног пословања

Заштита података о личности данас је битна тема за свако пословање, без обзира на његову величину. Закон у Србији не прави разлику између великих ИТ компанија и малих предузетника: ако имате макар једног запосленог, сарађујете са књиговођом или користите видео-надзор, постајете обвезник Закона о заштити података о личности.[1] Надлежни орган у Србији је Повереник за информације од јавног значаја и заштиту података о личности, који прати примену закона и објављује смернице које помажу организацијама да ускладе своје поступке са прописима.[2]

Свака законита обрада почиње јасном сврхом. Пре него што почнете да прикупљате податке, морате знати због чега их тражите, колико дуго ће се чувати и коме ће бити доступни. Типичне сврхе у пословању укључују вођење кадровске евиденције, испуњење уговорних обавеза, као што су слање робе или издавање рачуна, као и обезбеђење имовине путем видео-надзора. Важно је да сврха обраде не буде „шира од нужног“ - обрада „за било коју пословну сврху“ није законита.[3]

Правни основ обраде је следећи кључни елемент. Закон препознаје неколико основних правних основа: сагласност испитаника, извршење уговора, испуњење законске обавезе, заштиту животно важних интереса, извршење задатака у јавном интересу и легитимни интерес руковаоца или трећег лица. Легитимни интерес је често практичан, на пример за заштиту имовине, али захтева спровођење претходне процене. Пре него што се обрада заснива на легитимном интересу, потребно је проверити да ли је сврха обраде јасно дефинисана и оправдана, те да ли користи које фирма има од обраде надмашују потенцијалне ризике по права и слободе лица чији се подаци обрађују. Такође, важно је документовати сврху обраде и врсту података, те осигурати да се обрада спроведе на начин на који би минимално могла да угрожава приватност. Ако се утврди да су права испитаника угрожена, обрада на основу “легитимног интереса није дозвољена”.[4]

Грађани имају низ права која руковалац мора омогућити: Право на информисање о обради, приступ сопственим подацима, исправку, брисање, ограничење обраде, преносивост података и право на приговор, нарочито код обраде засноване на легитимном интересу или у сврху

---

[1] Закон о заштити података о личности, *“Службени гласник РС”*, бр. 87/2018.
[2] https://www.poverenik.rs/sr/, 01. октобар 2025. године.
[3] Денис Тул и Тадија Митић, *Приручник „Заштита података о личности“*, КЕЦ Група, Нови Сад, 2023.
[4] Приручник, исто.

маркетинга. Руковалац је дужан да захтеве обради у законским роковима и води евиденцију о таквим захтевима. Уколико лице процени да су му права повређена, може поднети притужбу Поверенику. Повереник тада има овлашћења да спроведе надзор и изрекне мере.[5]

У свакодневном пословању често се праве грешке које изгледају „ситне“, али су законски значајне и ризичне. На пример, видео-надзор је дозвољен искључиво у сврху заштите људи и имовине високе вредности и не сме служити за сталну процену учинка запослених. Камере постављене како би се стално пратила продуктивност запослених прелазе границу законитости и представљају непримерену обраду. Снимање звука је у принципу забрањено, па је важно да микрофон не хвата разговоре запослених или посетилаца. Повереник је више пута указивао на неадекватне праксе видео-надзора и наглашавао потребу за јасним обавештавањем и ограничењем приступа снимцима.[6]

Не смеју се чувати осетљиви финансијски подаци у неуобичајеном формату. Скениране платне картице са троцифреним ЦВЦ кодом, на пример, не би требало да буду део интерне евиденције фирме, јер представљају директан ризик од злоупотребе. Уколико је потребан број текућег рачуна запосленог због уплате зараде, таква информација се може преписати у електронску евиденцију или водити у папирном облику, у зависности од организационих могућности фирме или институције. Копије личних докумената, попут личних карата, пасоша или здравствене документације, треба чувати само ако постоји законски основ или јасна пословна потреба која захтева такво чување или достављање копије документа. „За сваки случај“ није довољан разлог. Чување докумената без ваљаног основа може довести до санкција и угрозити репутацију фирме, тако да свака вођена евиденција треба претходно бити проверена и да се води у мери, обиму и у складу са прописима из те области рада.

Маркетинг и електронске комуникације захтевају посебну пажњу. Слање промотивних имејлова или објављивање фотографија запослених без сагласности сматра се злоупотребом и може резултирати новчаним санкцијама и жалбама. Јасна могућност за приговор и одјаву или брисање мора бити доступна у свакој комуникацији.

Практични примери додатно илуструју последице непоштовања правила. Француска национална комисија за информатичке и грађанске слободе изрекла је казну компанији *Google* због недовољне транспарентности и недостатка валидних сагласности за персонализацију огласа.[7]

---

[5] *https://www.poverenik.rs/sr-yu/za%C5%A1tita-podataka/%D0%BA%D0%B0%D0%BA%D0%BE-%D0%BE%D1%81%D1%82%D0%B2%D0%B0%D1%80%D0%B8%D1%82%D0%B8-%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D1%83-%D0%BF%D1%80%D0%B0%D0%B2%D0%B02.html*, 01. октобар 2025. године.

[6] *https://www.poverenik.rs/sr-yu/saopstenja/2162-video-nadzor-qsiva-zonaq.html*, 01. октобар 2025. године.

[7] CNIL vs Google, *https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc*, 01. октобар 2025. године.

Национална канцеларија за заштиту података санкционисала је *Budapest Bank* због аутоматизоване анализе позива без одговарајућег правног основа.[8] Италијанска *Garante* казнила је *TIM* због незаконите праксе маркетинга и неправилне обраде података великог броја лица.[9] *Clearview AI* и друге компаније у ЕУ и Великој Британији такође су кажњене због прикупљања биометријских података без законског основа.[10][11][12] Ови примери показују да регулаторне агенције озбиљно приступају контроли обраде података, а финансијске последице и јавне кампање указују на потребу за доследним спровођењем мера усклађености.

Поред законске стране, важно је размишљати и о дигиталној сигурности. Редовно ажурирање софтвера, антивирус, енкрипција и бекап података нису само технички детаљи, они су саставни део законите и сигурне обраде. Лозинке треба чувати сегментирано, а приступ подацима ограничити само на овлашћена лица. У фирмама где се користи Облак или екстерни сервери, уговори са провајдерима морају јасно регулисати одговорност за заштиту података.

Практична примена у фирми захтева низ корака. Корисне су мапе тока података (где се бележе све тачке прикупљања, обраде и прослеђивања информација, од обрачуна плата и пријава за посао до база купаца и видео-надзора), пожељно је одређивање одговорног лица или тима који је задужен за заштиту података (ДПО). За обраду високог ризика, као што су стална видео-аналитика, аутоматизоване одлуке или биометрија, потребно је спровођење процене утицаја на заштиту података (ДПИА) и документовање резултата.

Уговори са обрађивачима, попут књиговођа, ИТ подршке или агенција за надзор, морају садржати клаузуле о заштити података и одговорности. Јасно обавештавање и сагласност запослених, кандидата и клијената су неопходни, док техничке мере укључују енкрипцију, редован бекап, ажурирање софтвера, антивирус, јаке лозинке и сегментацију приступа подацима. Потребан је план за инциденте, са процедуром откривања, извештавања и санације инцидената, а обука запослених о безбедном руковању подацима и реакцији у случају инцидента додатно смањује ризик.[13]

Осим овога, фирме могу укључити и интерне смернице које конкретно регулишу чување и обраду података, као што су ограничење приступа финансијским и личним документима, забрана

---

[8] NAIH, Budapest Bank fined for AI analysis: *https://www.lewissilkin.com/en/insights/budapest-bank-stung-with-fine-for-carrying-out-emotional-ai-analysis-incorrectly,* 01. октобар 2025. године.

[9] Garante (Italija) vs TIM: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486,* 01. октобар 2025. године.

[10] CNIL, Clearview AI fined: *https://www.cnil.fr/en/facial-recognition-clearview-ai-fined-20-million-euros,* 01. октобар 2025. године.

[11] Garante, Clearview AI fines in Italy: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10634329,* 01. октобар 2025. године.

[12] EU/UK regulator press releases on biometry & GDPR: *https://www.eugdpr.org,* 01. октобар 2025. године.

[13] чл. 50. Закона о заштити података о личности.

фотографисања или скенирања докумената без одобрења и обавезно брисање застарелих података. Ове интерне мере нису формално обавезне, али су снажан показатељ одговорног приступа и смањују ризик од прекршаја.

Усклађивање са Законом о заштити података о личности није само правна обавеза, већ и пословна предност. Брига о заштити података о личности све више се препознаје као важан део одговорног и ефикасног пословања. Компаније које систематски приступају управљању подацима грађана често уживају веће поверење клијената, мањи ризик од непријатних ситуација и лакше усклађују своје интерне процесе.

Датум објаве: 03.10.2025. године

*Текстови објављени на страници Правне теме на сајту Асоцијације судијских помоћника не представљају правне савете, већ личне ставове аутора, који не морају нужно одражавати ставове Асоцијације судијских помоћника.