

Лични подаци у дигиталном добу

**Да ли се твоји лични подаци налазе на Интернету, а да ти то не знаш?
Зашто су лични подаци „нафта“ новог доба?**

Сматра се да лични подаци данас имају највећу вредност на тржишту јер су основна „сировина“ за многе компаније. Да поменемо само Facebook, Google i Amazon, као и многе друге које нам нуде толико бесплатних алата и садржаја. Ако сте мислили да сте „срећници“ што користите бесплатне алате, знајте да сте их скупо платили. Јер платили сте их својим личним подацима, тј. својом приватношћу, подацима које су ове компаније касније скупо наплатиле. И не само компаније, већ и многе владе широм света, све чешће задиру у нашу приватност пратећи оно што радимо, кога знамо и куда идемо. Тако су присутне многе нелегалне активности, почевши од наивног рекламирања производа, преко унапред креираних услуга осигурања и кредита са већом ценом, па до утицаја на јавно мњење и изборне резултате. Методе и сврхе прикупљања података се и даље шире, мењају облике и тешко им се стаје на пут.



Због тога је Европска унија 2016. године донела Општу уредбу о заштити података о личности, односно *GDPR (General Data Protection Regulation)*, а она је ступила на снагу 21. маја 2018. По узору на ову уредбу наша држава је 2018. донела *Закон о заштити података о личности*, чија је примена почела у августу 2019. године.

Па хајде да видимо шта су то подаци о личности и која су наша права у вези са обрадом ових података.

Шта су то лични подаци?

Лични подаци су сви подаци који се односе на једну особу, а чијом се употребом може утврдити идентитет те особе. Обично се ради о подацима које свакодневно користимо у својим активностима на Интернету, у тровини, у школи, у банци, на послу...

Примери личних података

Име и презиме, адреса, имејл адреса, бројеви телефона, подаци о здравственом стању, ЈМБГ, оцене у школи, подаци о образовању, подаци о чланствима у организацијама и удружењима, историја прегледа на Интернету, биометријски подаци (скенирање зенице или отисак прста), број личне карте или број пасоша, фотографија особе, видео запис особе, тонски запис особе, ДНК, подаци о локацији и кретању, висина зараде, брачни статус, рачуни у банкама, пореске пријаве, кредитна задуженост...

Како без нашег знања дајемо личне податке?



Постоје многе твоје активности које одају личне податке, а ниси их уопште свестан. Колико пута си кликнуо и прихватио одређене падајуће прозоре на појединим сајтовима не читајући обавештења о “колачићима”, где је наведено за шта се користе наши лични подаци односно подаци о нашој ИП адреси. На пример, уколико желиш да купиш гитару и на Интернету тражиш понуде, иако ниси уписао ни један лични податак, на већини страница инсталирани су колачићи који прате твоје понашање и

самим тим стварају твој профил – скуп твојих карактеристика. Понуђач прати шта ти тражиш и кад се одлучиш за жељени датум и затражиш *on-line* понуду, алгоритам који је одредио твоје понашање обавештава понуђача и онда се теби може приказати већа цена за жељену гитару. Ово спада у примере непримерене обраде података која се санкционише ГДПР уредбом и нашим Законом о заштити података о личности.

Постављање личних података на огласним таблама и бацање у корпу за смеће штампаних биографија кандидата за посао, само су још неки од примера.

Видео-надзор се често поставља у фирмама без претходне процене ризика и плана обезбеђења и без процене утицаја на заштиту података о личности, што је обавеза по закону. Закон третира слике лица као специјалну категорију података са посебним ограничењем коришћења.

Свака база, односно збирка података са личним подацима у фирмама мора бити евидентирана и заштићена, па је тако, на пример, забрањено да путем имејла круже табеле са списком деце која треба да добију пакетиће за нову годину, затим списак запослених који су се пријавили за добровољно давање крви или за куповину неког производа на рате и сл. јер је тиме нарушена приватност и увећан ризик одавања података о личности.



Информације о болестима су посебно осетљив податак и са њима треба поступати на посебан начин, а одавање ових података треба одмах пријавити лицу за заштиту података о личности.

Приликом куповине, продавци често од нас траже личне податке да би нас придобили картицама лојалности и да би сазнали наше навике и тако повећали своју зараду, али и да би продали те податке другим фирмама. Често се таква комуникација остварује слањем писама поштом, контактирањем путем телефона, али и путем електронске поште, СМС-ом, искачућим прозорима на Интернету и на многе друге начине. За све ово мора да постоји законска основа и твој пристанак.

Често се дешава на нам неко тражи ЈМБГ и то је у реду када је у питању полиција, суд, куповина стана и сл. Али када то чини продавац, или неко други, поготово када одмах иза тебе у реду чека неколико људи, онда то свакако није безбедан поступак.

С обзиром да се већ уводе напредни видео надзори на саобраћајницама, аеродромима, аутобуским станицама, и другим критичним местима, а ви ћете ускоро бити пунолетни, имаћете моралну и цивилизацијску одговорност да учествујете у одређивању равнотеже између сврхе прикупљања података и нарушавања приватности.

Такође, када се будеш запослио, можда ћеш радити у фирми која ће стално имати податке о твојој локацији и кретању, о мобилним бројевима особа са којима си комуницирао, о подацима са RFID картице (за електронске браве, контролу уласка и сл.), о историји IP адреса твојих приступа итд. Уколико оваква контрола није правно регулисана, онда је твоја приватност нарушена.



Казне

Казне прекршаја GDPR-а су изузетно високе и иду и до 20 милиона евра или четири одсто укупног годишњег прихода компаније. Тај износ од 4% може да буде невероватно висок. Да се подсетимо да је Француска агенција за заштиту личних података казнила Google са 50 милиона евра. Домаћи Закон предвиђа казне у распону од 50.000 – 2.000.000 динара за правно лице, односно 20.000 - 500.000 за фирме.

Савети за побољшање ваше Интернет приватности

Ево како да побољшате своју приватност на мрежи:

1. Проверите подешавања приватности за друштвене мреже (Facebook, Twitter, LinkedIn, Instagram, Snapchat...).
2. Не користите јавна складишта за приватне информације (Google drive, Dropbox, OneDrive...).
3. Избегавајте праћења на Internetu (користите алате за ову заштиту).
4. Нека ваша главна адреса е-поште и телефонски број буду приватни (креирајте додатни налог за е-пошту и купите додатну СИМ картицу коју бисте користили за куповину на мрежи и друге ситуације за које је потребно дељење података са непознатим особама).
5. Користите апликације за размену података са шифрирањем „од краја до краја“ (користите апликацију за ту намену).
6. Користите сигурне лозинке (12 знакова и више, једну главну, а другу лозинку за сваку услугу).
7. Прегледајте дозволе за мобилне апликације и за додатке прегледача Интернета (да ли вам је заиста потребно да нека апликација користи камеру, микрофон, геолокацију и др.).
8. Осигурајте свој телефон и рачунар лозинкама у комбинацији са другим начином (шестоцифрени ПИН-ови, биометријску аутентификацију и сл.), а не само једно од овог.
9. Ономогућите обавештења кад је закључан екран (подесите да вам не „искачу“ поруке и сл. када је телефон закључан).
10. Останите приватни на Wi-Fi мрежама (избегавајте их, али ако морате да их користите, употребите VPN заштиту).
11. Ограничите оно што делите на друштвеним мрежама (престаните да делите толико личних података на мрежи).
12. Будите свесни преваре (застаните и размислите пре него што одговорите на „алармантни“ е-mail, или када непозната апликација тражи „кликни овде“).

Упознајмо се са још неким терминима важним за личне податке

Обрада података о личности је поседовање и употреба, односно свака радња која укључује личне податке – копирање, уступање, прикупљање, чак и увид у здравствени картон представља обраду података о личности. **Руковалац (обрађивач)** је особа или фирма која обрађује податке о личности и имају одређену сврху зашто прикупљаја и обрађује, али је важно да сврха обраде података није супротна законима. Поред овакве врсте обраде



податка, она се може вршити и на основу **пристанка лица** за прикупљање и обраду података. Пример таквог пристанка је улазак у тржни центар на чијим вратима је наглашено да се унутрашњост објекта снима. Уласком унутра, обавештени смо и тако дали свој пристанак да будемо снимани. Још један пример дате сагласности је и већ чувено чекирање *ascept*

(прихватам) приликом преузимања апликација на Интернету. Већина вас не чита текст који је повезан са квадратићем где обележавамо да се слажемо са условима под којима компанија послује или апликација ради. Ту се заправо налазе информације које се односе и на употребу наших личних података. Па тако, неке од тих апликација захтевају приступ галерији са фотографијама, контактима у нашем телефонском именуку итд.

Даћемо примере само неких важних информација о томе који услови морају да постоје, у супротном не прихватајте понуђено:

- која је сврха обраде и да ли је заснована на закону;
- информације да ли ће руковалац делити податке са неким другим у земљи или ван земље (обично под појмом „third party“);
- рок колико ће подаци о личности бити чувани;
- да се твоји подаци неће користити за аутоматско стварање твог профила – скупа твојих карактеристика.

Права лица чији се подаци о личности обрађују – ТИ ИМАШ ПРАВА:

- да будеш обавештен ко обрађује твоје податке;
- да ти подаци буду достављени на увид (преглед, читање, слушање);
- да ти се достави копија тих података;
- да захтеваш исправку, допуну, ажурирање, брисање података, као и прекид и привремену обуставу обраде;
- да се подаци пренесу другом лицу (на пример да се из банке у којој си клијент изврши пренос твојих личних података у другу банку);
- да повучеш сагласност коју си дао;
- да поднесеш притужбу, али најпре *Поверенику за информације од јавног значаја и заштиту података о личности*. Повереник је самосталан (независан) државни орган, који врши послове заштите података о личности. Ако тако не оствариш своја права, можеш поднети тужбу пред основним судом.

**За потребе наставе, материјал припремио:
наставник Информатике и рачунарства, Г. Н.**

Теме за пројекат:

- 1. Чување личних података**
- 2. Права детета у дигиталном добу**
- 3. Угроженост деце на Интернету**
- 4. Ризици злоупотребе личних података о деци**
- 5. Савети за побољшање ваше Интернет приватности**
- 6. Заштита личних података на Интернету**

У тексту је коришћен материјал из следећих извора:

https://www.unicef.org/serbia/media/10366/file/Deca_u_digitalnom_dobu.pdf

https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

<https://www.blic.rs/vesti/drustvo/otkrivamo-ko-sme-a-ko-ne-da-koristi-vase-licne-podatke-i-na-koji-nacin/rr07xy6>

<https://otvorenavratapravosudja.rs teme/ustavno-pravo/pravo-na-privatnost-i-zastitu-licnih-podataka>

<https://www.kaspersky.com/blog/privacy-ten-tips-2018/23022/>

Илустрације су преузете са следећих сајтова (по редоследу):

www.medium.com; www.hostpapa.blog; www.novosti.rs; www.novimagazin.rs;
www.nbgcreator.com