Проф.др Горан Матић

ОСНОВЕ ОБРАДЕ И ЗАШТИТЕ ПОДАТАКА

ПРИРУЧНИК

САДРЖАЈ

НАПОМЕНЕ

„Непоштовање и неимплементација Закона о тајности података представља кршење националне безбедности и наношење штете интересима Републике Србије“

Приручник је написан на основу потребе приближавања проблематике штићених података, а пре свега тајних података органима јавне власти и свима онима којима је то неопходно ради имплементације Закона о тајности података и представља радни материјал намењен подизању безбедносне културе и свести и тиме заштити националне безбедности Републике Србије.

Поред тога, овај материјал представља и основ за даље усавршавање у овој области.

Приручник је написан на основу анализе јавних извора, прописа, праксе, стандарда, научних и стручних текстова, медија, интернет извора, као и искустава у раду са штићеним подацима.

Едукације из области рада са тајним подацима одржавају се у Канцеларији Савета за националну безбедности и заштиту тајних података Владе Републике Србије на основу члана 87. Закона о тајности података.

ТЕМЕ

- УВОДНА РАЗМАТРАЊА
- ИНФОРМАЦИОНА БЕЗБЕДНОСТ
- ПРИВАТНОСТ
- НОРМАТИВНО УРЕЂЕЊЕ ПОДАТАКА
- КАТЕГОРИЈЕ И КЛАСИФИКАЦИЈА ПОДАТАКА
- ТАЈНИ И ЛИЧНИ ПОДАЦИ
- КОМПРОМИТАЦИЈА ПОДАТАКА
- ОБРАДА ПОДАТАКА
- АСПЕКТИ ЗАШТИТЕ ПОДАТАКА
- ПРОБЛЕМИ У ПРАКСИ
- ПИТАЊЕ ТЕСТА
- НА КРАЈУ

УВОДНА РАЗМАТРАЊА

ПРИЗМА ПОСМАТРАЊА

- **РЕФОРМА ДРЖАВНЕ УПРАВЕ**
- **РЕФОРМА СЕКТОРА БЕЗБЕДНОСТИ**
- **У СУСРЕТ ИНФОРМАЦИОНИМ ТЕХНОЛОГИЈАМА...**
- **ПРЕГОВАРАЧКА ПОГЛАВЉА СА ЕУ - КЛАСТЕРИ (10, 23, 24 и 31)**

АСПЕКТИ РАЗМАТРАЊА ПРОБЛЕМА:

- **ТЕХНОЛОШКИ**
- **ПРАВНИ**
- **БЕЗБЕДНОСНЕ ПОЛИТИКЕ И СТРАТЕГИЈЕ**

ИНФОРМАЦИОНО ДРУШТВО

Информационо друштво (енгл. Information society) је друштво у коме стварање, дистрибуција и манипулација информацијама постаје значајна културна и економска активност. Заснива се на „економији знања”
јер профит генерише експлоатацијом знања, а у мањој мери природних ресурса.

Централно место у овим друштвима заузимају информационе технологије које директно утичу на производњу и економију. Сматрају се наследником индустријских друштава.

АСПЕКТИ ЗАШТИТЕ САЈБЕР ПРОСТОРА

САЈБЕР БЕЗБЕДНОСТ (CYBER SECURITY) – КРОВНИ КОНЦЕПТ

САЈБЕР ОДБРАНА (CYBER DEFENCE) – ОДНОСИ СЕ НА КРИТИЧНУ ИНФРАСТУКТУРУ КОЈА МОЖЕ БИТИ У ЈАВНОЈ И ПРИВАТНОЈ СВОЈИНИ

INFORMATION ASSURANCE – ОДНОСИ СЕ НА ЗАШТИТУ САЈБЕР ПРОСТОРА КОЈИ КОРИСТЕ ДРЖАВНИ ОРГАНИ У СВОМЕ РАДУ

INFOSEC – ОДНОСИ СЕ НА РАД СА ТАЈНИМ ПОДАЦИМА У ДРЖАВНИМ ОРГАНИМА У МРЕЖАМА И СЛИЧНО

ПРОБЛЕМИ: ПОЈМОВИ, ПРЕВОД И НЕУРЕЂЕНОСТ...

Рачунарска безбедност, сајбер безбедност, дигитална безбедност или безбедност информационих технологија (ИТ безбедност)

- представљају заштиту рачунарских система и мрежа од напада злонамерних актера који могу довести до неовлашћеног откривања информација, крађе или оштећења хардвера, софтвера или података, као нпр. као и због ометања или погрешног усмеравања услуга које пружају

КОНСТАТАЦИЈА

НЕ ПОСТОЈИ САВРШЕНА ЗАШТИТА ИНФОРМАЦИЈА У САЈБЕР ПРОСТОРУ, НИ У БИЛО КОЈЕМ ПРОСТОРУ

SECURITY: Морамо заштити наше компјутере и податке на исти начин како обезбеђујемо објекте, просторије, врата на нашим домовима

SAFETY: Морамо се понашати на начин да се заштитимо од ризика и претњи које долазе са развојем технологије

БЕЗБЕДНОСТ – ЉУДСКА ПРАВА

ТРАНСПАРЕНТНОСТ – ТАЈНОСТ

ЈАВНОСТ - ПРИВАТНОСТ

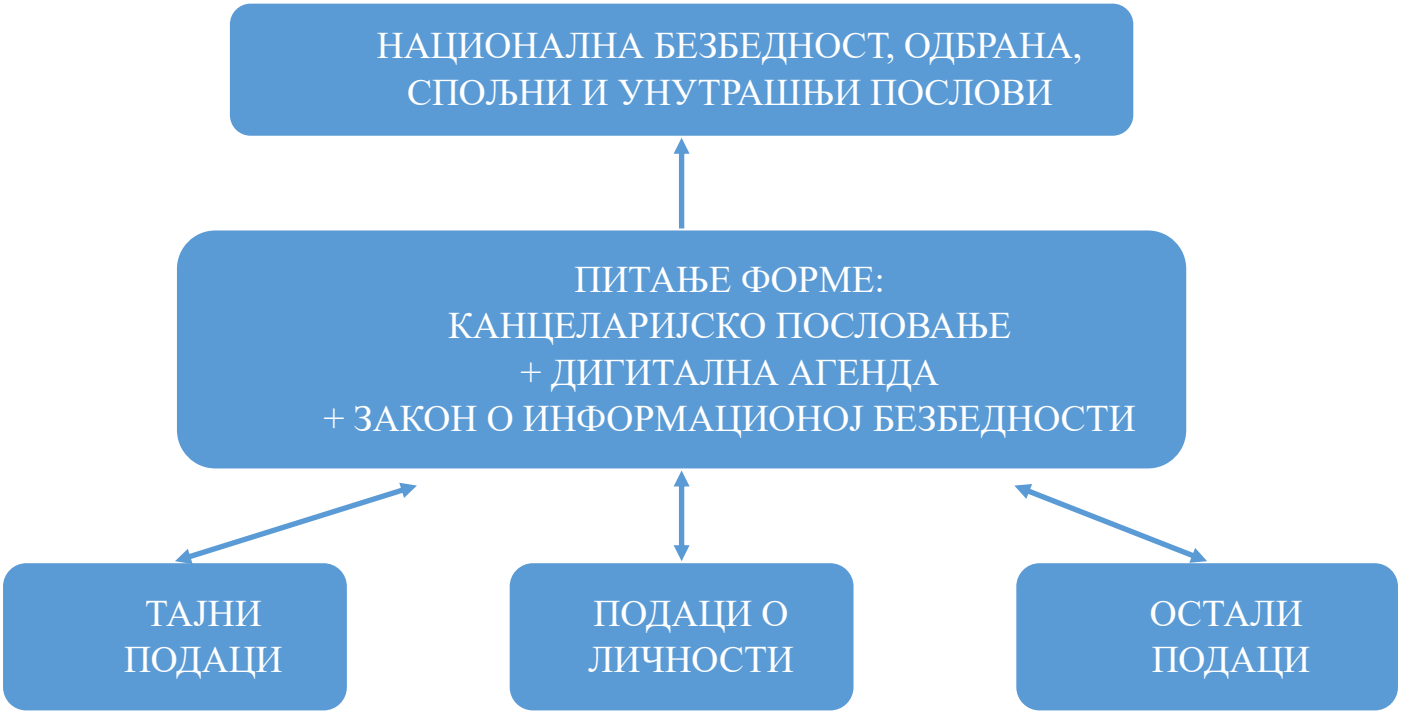
КОЈЕ СУ ГРАНИЦЕ ДО КОЈИХ СЕ МОЖЕ ИЋИ У УСПОСТАВЉАЊУ СИСТЕМА ЗАШТИТЕ?

АСПЕКТИ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

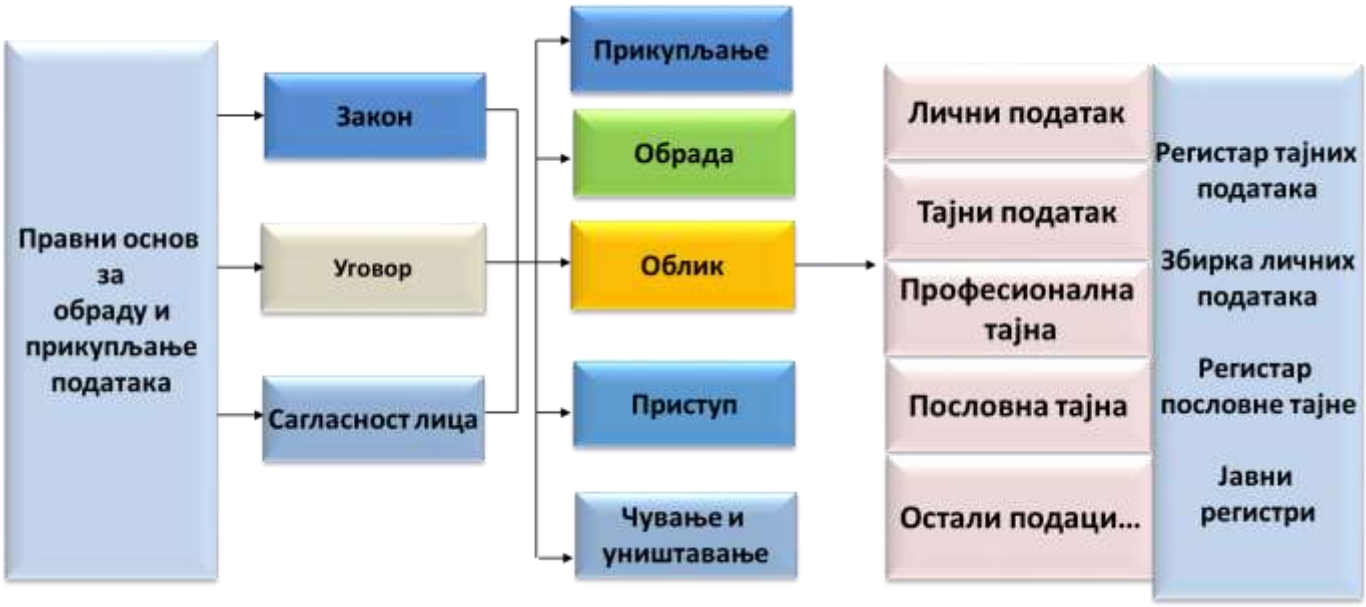
- РЕГИСТАРСКИ СИСТЕМ
- ПЕРСОНАЛНУ БЕЗБЕДНОСТ
- АДМИНИСТРАТИВНУ БЕЗБЕДНОСТ
- ФИЗИЧКУ И ТЕХНИЧКУ БЕЗБЕДНОСТ
- ИНФОРМАТИЧКУ БЕЗБЕДНОСТ (**infosec – information assurance**)
- ИНДУСТРИЈСКУ БЕЗБЕДНОСТ (ПОВЕРЉИВЕ НАБАВКЕ ВЕЗАНЕ ЗА ДРЖАВУ)

ЖИВОТНИ ЦИКЛУС У РАДУ СА БИЛО КОЈИМ ПОДАТКОМ ОБУХВАТА

- НАСТАНАК (ПРОВЕРА И ИЗНОШЕЊЕ ПОДАТКА У ОДГОВАРАЈУЋОЈ ФОРМИ + УНОШЕЊЕ У ОДГОВАРАЈУЋУ ЗБИРКУ ПОДАТАКА)
- КОРИШЋЕЊЕ И ДИСТРИБУЦИЈУ (ПРИСТУП, ИНФОРМАЦИЈА, АНАЛИЗА, КРИВИЧНА ПРИЈАВА, УПРАВНИ АКТ, СУДСКИ АКТ…)
- ПРЕНОШЕЊЕ (ДИГИТАЛНА АГЕНДА, КУРИРИ…)
- ЧУВАЊЕ И СКЛАДИШТЕЊЕ
- АРХИВИРАЊЕ ИЛИ УНИШТАВАЊЕ



ШЕМАТСКИ



ОБАВЕЗА ИМПЛЕМЕНТАЦИЈЕ

- НА ОСНОВУ ЗАКОНА – ЗТП и ЗЗПЛ (Закон о одбрани, Закон о полицији, Закон о спољним пословима, Закон о БИА, Закон о ВБА и ВОА...)
- НА ОСНОВУ СТАТУСА – ОРГАН ЈАВНЕ ВЛАСТИ (ЗТП и ЗЗПЛ)
- УГОВОРНИ ОДНОС СА ОРГАНОМ ЈАВНЕ ВЛАСТИ (ЗТП)
- На основу регистроване делатности у АПР – ЗЗЛП
- Уговорни однос са физичким лицима – ЗЗЛП

ПРИМЕРИ ИЗ ПРАКСЕ

- **Регистар страних тајних података** – Централни регистар и подрегистри ЕУ, НАТО, на основу билатералних споразума – Закон о тајности података
- **Регистар тајних података** – ПЛАН ОДБРАНЕ – прописи о одбрани
- **Збирке личних података** – евиденције које води МУП – прописи о полицији
- **Регистар пословне тајне** – приватни и јавни сектор – Закон о пословној тајни и закон о привредним друштвима
- **Јавни регистри** – АПР: привредна друштва, предузетници, финансијски извештаји, медији, удружења... – Закон о агенцији за привредне регистре РС
- **Јавни регистри** – Министарство правде: регистар судских вештака, регистар правних лица која обављају послове вештачења, именик извршитеља, списак јавнобележничких канцеларија – правосудни прописи

ПОДИЗАЊЕ БЕЗБЕДНОСНЕ СВЕСТИ И КУЛТУРЕ

ПОДИЗАЊЕ БЕЗБЕДНОСНЕ СВЕСТИ И КУЛТУРЕ

- **БЕЗБЕДНОСНА КУЛТУРА И СВЕСТ**
- **ИНФОРМАЦИОНА КУЛТУРА И СВЕСТ**
- **ИНФОРМАЦИОНО БЕЗБЕДНОСНА КУЛТУРА И СВЕСТ**
- **ОРГАНИЗАЦИОНА КУЛТУРА И СВЕСТ**
- **САЈБЕР ХИГИЈЕНА**

Безбедносна култура и свест

- безбедносна активност која изражава спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима. Огледа се у препознавању опасности, реаговању на њих избегавањем опасности, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати и сачувати угрожене вредности.
- знање и став који чланови организације имају у погледу заштите одређених вредности – националне безбедности, одбране, унутрашњих и спољних послова, људских слобода и права, као и физичке и интелектуалне имовине, а посебно информација и података којима располаже организација (орган јавне власти, правно лице или комапнија).

Информациона култура и свест

- пракса осигурања информација и управљања ризицима везаним за употребу, обраду, складиштење, пренос и архивирање информација. Информациона култура и свест укључује заштиту интегритета, доступности, аутентичности, неповрешености и поверљивости корисника. Обухвата и дигиталне заштите и физичке технике.
- усвајање адекватног понашања да се пронађу информације, користећи притом било који начин или медијум , који на најбољи могући начин задовољава потребе за информацијама, а које воде мудром и етичком коришћењу информација у друштву (дигитална писменост?).

Информационо безбедносна култура и свест

- Део у развоју информационе безбедности која се фокусира на прикупљање сазнања и искустава у вези са потенцијалним ризицима и претњама које се брзо развијају, у вези са људским понашањем, како корисника ИКТ система, тако и потенцијалних нападача.
- Манифестије се у оквиру организације кроз аспекте безбедности који се односе на: 1) вредности; 2) понашање; 3) ставове; 4) акције; 5) активности руководства (менџмента); и 6) физичко окружење.

Организациона култура и свест

- Систем заједничких значења и симбола.
- Модел основних претпоставки, вредности и норми, које је дата група развила или открила учећи како да решава проблеме екстерне адаптације и интарне интеграције и који функционишу довољно добро да би били пренети новим члановима организације као исправан начин мишљења и осећања у вези са тим проблемима.
- Образац веровања, вредности и научених начина поступања са искуством који су се развили кроз организациону историју и који се манифестују кроз материјалне објекте, као и понашање чланова организације.

Сајбер хигијена

- Реч је о безбедносној пракси која укључује све кориснике интернета, и са интернетом повезаних ствари, сервиса, апликација, и уређаја са циљем заштите сигурности и интегритета штићених података и спречавања сајбер напада.

- Односи се на праксе које имају за циљ спречавање инфекције малициозним софвером (malware), као и сајбер упаде и губљење или корупмирање података и одржавање здравог сајбер окружења.

ТИПОВИ ОБУКА ЗА ШТИЋЕНЕ ПОДАТКЕ:

1. **ОСНОВНА ОБУКА О БЕЗБЕДНОСНОЈ КУЛТУРИ** – посвећена свим запосленима који имају додира са штићеним подацима
2. **ОБУКА О ТЕХНИЧКИМ АСПЕКТИМА БЕЗБЕДНОСТИ** – компатибилна са стандардом СРПС ИСО 27001
3. **ОБУКА О УПРАВЉАЊУ БЕЗБЕДНОСТИ** – посвећена је руководиоцима и менаџерима који би требали да имплеметирају прописе о штићеним подацима
4. **ОБУКА О УСКЛАЂЕНОСТИ БЕЗБЕДНОСНИХ СТАНДАРДА** – односи се на примену Закона о тајности података или Закона о заштити података о личности
5. **Обука за руковаце тајних/личних података**

ЕДУКАЦИЈЕ

могу бити:

1. У учионици директно предавач – полазници
2. Вебинари и видео тренинг
3. Постављене снимљене едукације и презентације
4. Симулације реалних ситуација за потребе едукација

- Програми редовне едукације и тренинга су кључни елементи за подизање безбедносне свести, како код запослених, тако и код менаџмента (руководилаца).
- Запослени морају схватити и разумети зашто је безбедност важна за организацију, као и да је свако од њих одговоран за безбедност у својој сфери, без обзира да ли у свом раду користе штићене податке и информационе технологије или не.
- Програми едукација су од виталног значаја за спровођење безбедносне политике.

ПРИМАРНИ ЗАДАТАК ЕДУКАЦИЈА О ШТИЋЕНИМ ПОДАЦИМА

1. Подизање безбедносне свести и културе
2. Имплементација прописа и стандарда у организацију

Кључни сегмент безбедности, у контексту националне и организационе безбедности представља ИНФОРМАЦИОНА БЕЗБЕДНОСТ.

Пет кључних елемената безбедносне културе

1. Култура информисања
2. Култура поверења
3. Култура пријављивања
4. Култура учења
5. Прилагодљива култура

Подизање свести о безбедности штићених података

постиже се кроз:

- Личну одговорност
- Лојалност запослених и
- Активности менаџмента (руководства) организације.

Теме обухваћене едукацијама о безбедносној култури и свести

укључују:

- **Природу штићених података**, осетљивог материјала и физичких средстава са којима могу доћи у контакт, као што су тајни подаци, лични подаци, пословне тајне, професионалне тајне, указујући на националну безбедност и људске слободе и права (приватност)

- **Одговорности запослених** и лица у уговорном односу са организацијом, у руковању штићеним подацима, укључујући преглед безбедносних сертификата за физичка и правна лица, као и уговора о неоткривању података...
- **Захтеве за правилно руковање штићеним подацима** (осетљивим материјалом) у физичком облику, укључујући одређивање, класификацију, обележавање, пренос, чување - складиштење и уништавање, као и архивирање
- **Одговарајуће методе за заштиту штићених података на рачунарским системима**, укључујући посебне процедуре (политику лозинке и коришћење двофакторске аутентификације)
- **Друге проблеме у вези са рачунарском безбедношћу**, укључујући малвер, фишинг, крађе идентитета, друштвени инжењеринг итд.

- **Физичку безбедност на радном месту**, укључујући приступ зградама и безбедносним зонама, административним зонама, ношење идентификационих беџева и електорнских кључева, пријављивање инцидената, уношење забрањених предмета итд.
- **Последице пропуста** да се правилно заштите подаци - информације, укључујући потенцијални губитак запослења, последице по орган јавне власти и националну безбедност, економске последице по организацију, штету појединцима чији су лични подаци (приватни досијеи) откривени, као и могуће кривичне и прекршајне казне, одговорност у дисциплинском поступку и поступке накнаде материјалне и нематеријалне штете у парничном поступку

КЉУЧНИ ПОЈМОВИ

ПОЈМОВИ

- сигурност,
- осигураност,
- обезбеђеност,
- безбедност,
- безопасност,
- безбрижност,
- спокојност,
- заклоњеност и
- заштићеност

СИГУРНОСТ (Речник српског језика Матице српске)

1. Стање, особина оног који је сигуран, онога што је сигурно;
2. Безбедност, обезбеђење: јавна и државна;
3. Увереност, поуздање;
4. Одлучност, чврстина
5. Јасност, одређеност, доследност
6. За сваки случај, евентуално, за сваку;

БЕЗБЕДНОСТ (БЕЗОПАСНОСТ)

У НАЈШИРЕМ СМИСЛУ ПОДРАЗУМЕВА ОДСУСТВО ОПАСНОСТИ (ЗАШТИЋЕНОСТ ОД ПРЕТЊИ) ЗА ФУНКЦИОНИСАЊЕ ИЛИ РАЗВОЈ СУБЈЕКАТА, ПРОЦЕСА, ПОЈАВА, ОДНОСНО СВОЈСТВА ИЛИ СТАЊА (СТАБИЛНОСТ, ПОСТОЈАНОСТ)

ОЗНАЧАВА СТАЊЕ НЕКОГ СУБЈЕКТА (ПОЈЕДИНЦА, ГРУПЕ ЉУДИ, ЗАЈЕДНИЦЕ, ИНСТИТУЦИЈЕ) КОЈЕ КАРАКТЕРИШЕ ОДСУСТВО НЕВОЉА, БРИГА, НЕСРЕЋА, ОПАСНОСТИ И ДРУГИХ ЗЛА.

САЈБЕР ПРОСТОР СЕ ОДРЕЂУЈЕ КАО МЕЂУЗАВИСНА МРЕЖА ИНФОРМАЦИОНИХ ТЕХНОЛОШКИХ ИНФРАСТРУКТУРА, А ОБУХВАТА ИНТЕРНЕТ, ТЕЛЕКОМУНИКАЦИЈСКЕ МРЕЖЕ, КОМПЈУТЕРСКЕ СИСТЕМЕ, УГРАЂЕНЕ ПРОЦЕСОРЕ И РЕГУЛАТОРЕ У РАЗНИМ ДЕЛАТНОСТИМА....

- Не служи само уклањању ризика и претњи
- Не одређује начин пословања
- Омогућавање корисницима информационих технологија да користе погодности и добробити на интернету, у локалној мрежи или код потпуно изолованих рачунарских система
- Поред заштите приватности и неометаног коришћења информационих технологија, обезбеђује и заштиту интелектуалне и материјалне својине корисника

ШТА ЈЕ ТАЈНА

- ОНО ШТО СЕ НИКОМЕ НЕ СМЕ РЕЋИ, САОПШТИТИ
- ОНО ШТО СЕ СКРИВА, ТАЈИ
- ОНО ШТО СЕ НЕ ПРИЧА И НЕ ОБЈАВЉУЈЕ

У ширем смислу – назива се све што је непознато

У ужем смислу – појављује се у међуљудским односима и чине је подаци и информације које уже или шире групе или држава чувају за себе, скривају од других, а посебно од јавности

Приватне тајне – сазнање о одређеним интимним и приватним подацима која се сазнају од других лица на основу родбинског, пријатељског или емотивног односа, као и међусобног поверења.

Јавне тајне – тајни подаци и други штићени подаци који се користе за потребе органа јавне власти и њихов рад (лични подаци, тајни подаци, пословне тајне и професионалне тајне)

Правни аспект материје тајности података – представљају подаци, информације и документи који су прошли процедуре класификације и декласификације у складу за прописима (Закон о тајности података, Закон о заштити пословне тајне, етичке кодексе...)

ШТА ЈЕ ПРИВАТНОСТ

- Заштита достојанства и интегритета сваког појединца остварује се кроз читав каталог људских права, где се као једно од фундаменталних права налази право на приватност.
- ИАКО НЕ ПОСТОЈИ ОПШТЕ ПРИХВАЋЕНА ДЕФИНИЦИЈА - Под правом на приватност подразумева се право једног лица да, од сазнавања чињеница која се тичу лично њега, искључи трећа лица, односно право лица да одређене чињенице задржи само за себе.

ИНФОРМАЦИОНА БЕЗБЕДНОСТ

ИНТЕРНЕ И ЕКСТЕРНЕ ИНФОРМАЦИЈЕ

За доношење правовремених и квалитетних одлука, потребне су интерне и екстерне информације:

- Интерне информације су у оквиру организације и оне омогућавају кретање података између свих запослених у организацији;
- Екстерне информације се добијају споља, од окружења, и везане су најчешће за државне органе, јавна предузећа или приватне компаније
- Интерне и екстерне информације могу бити тајни подаци, пословне тајне, професионалне тајне и могу садржавати личне податке

ПОСТОЈЕЋЕ СТАЊЕ

- УПОТРЕБА ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА У РЕПУБЛИЦИ СРБИЈИ;
- ЈАВНА УПРАВА (E-GOVERNMENT);
- ИКТ СЕКТОР И
- ИНФОРМАЦИОНА БЕЗБЕДНОСТ.

ШТА ЧИНИ ИНФОРМАЦИОНУ СИГУРНОСТ

- ЕТИЧКИ И ПРАВНИ АСПЕКТИ
- МЕТОДЕ ЗАШТИТЕ
- СИГУРНОСНИ МЕХАНИЗМИ, УСЛУГЕ И АЛАТИ

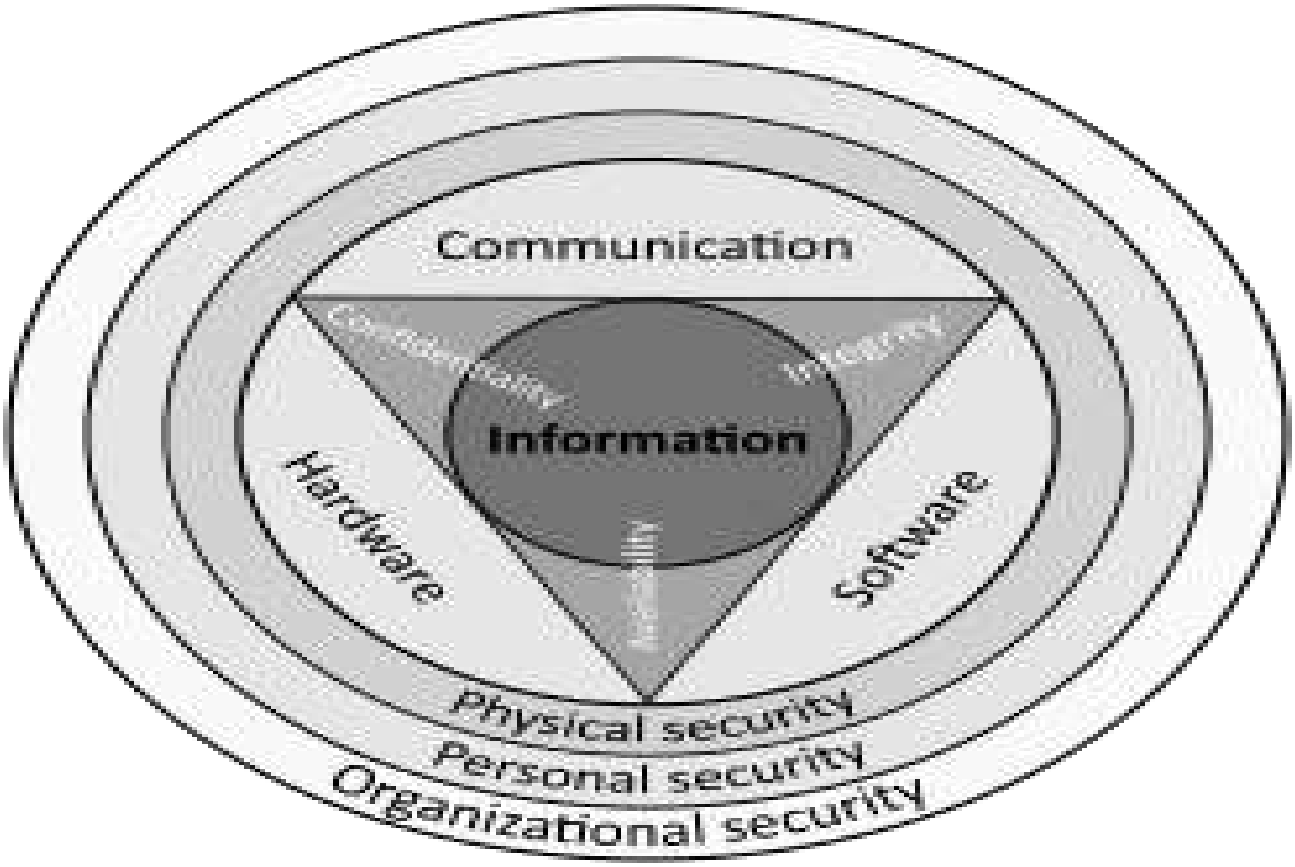
ИНФОРМАЦИОНА БЕЗБЕДНОСТ

- ПРЕЛАЗАК НА ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ
- ИТ И ДРАСТИЧНЕ ПРОМЕНЕ У ДРУШТВУ
- Е-УПРАВА, Е-БАНКИНГ, ДИГИТАЛНЕ БАЗЕ ПОДАТАКА, ДРУШТВЕНЕ МРЕЖЕ, САЈБЕР БЕЗБЕДНОСТ...
- ВЕЛИКИ ПРИСТУП РАЗЛИЧИТИМ ИНФОРМАЦИЈАМА НА ИНТЕРНЕТУ...

БЕЗБЕДНОСТ НА МРЕЖИ, ОДНОСНО ОНЛАЈН БЕЗБЕДНОСТ ЈЕ АКТУЕЛНА ТЕМА КОЈА ИЗАЗИВА ПАЖЊУ МНОГИХ СУБЈЕКАТА, А НАРОЧИТО ЈЕ ЗНАЧАЈНА ЗА КОРИСНИКЕ И ПРОВАЈДЕРЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ (IT)

ПОЈАМ ИНФОРМАЦИОНА БЕЗБЕДНОСТ ПРЕДСТАВЉА СКУП МЕРА КОЈЕ ОМОГУЋАВАЈУ ДА ПОДАЦИ КОЈИМА СЕ РУКУЈЕ ПУТЕМ ИКТ СИСТЕМА БУДУ ЗАШТИЋЕНИ ОД НЕОВЛАШЋЕНОГ ПРИСТУПА, КАО И ДА СЕ ЗАШТИТИ ИНТЕГРИТЕТ, РАСПОЛОЖИВОСТ, АУТЕНТИЧНОСТ И НЕПОРЕЦИВОСТ ТИХ ПОДАТАКА, ДА БИ ТАЈ СИСТЕМ ФУНКЦИОНИСАО КАКО ЈЕ ПРЕДВИЂЕНО, КАДА ЈЕ ПРЕДВИЂЕНО И ПОД КОНТРОЛОМ ОВЛАШЋЕНИХ ЛИЦА.

ПРЕДСТАВЉА ПРАКСУ ЗАШТИТЕ ИНФОРМАЦИЈА УБЛАЖАВАЊЕМ РИЗИКА И ПРЕДСТАВЉА ДЕО УПРАВЉАЊА РИЗИКОМ (INFOSEC)....



ШТА ЧИНИ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ:

1. ЦИЉЕВИ

- очување поверљивости, интегритета и доступности информација
- заштита информација и инф.система од неовлашћеног приступа, коришћења, откривања, ометања, модификације или уништења у циљу обезбеђивања поверљивости, интегритета и доступности
- осигуравају да само овлашћни корисници (поверљивост) имају приступ тачним и потпуним информацијама (интегритет) када је то потребно (доступност)
- заштита интелектуалне својине организације
- управљање ризицима и трошковима информационог ризика за пословање
- обезбеђивање да су инф.ризици и контроле у равнотежи
- заштита информација, инф.система или база података од неовлашћеног приступа, оштећења, крађе или уништења

2. МЕРЕ

- скуп активности и радњи које предузимају државни органи, јавна предузећа, компаније и правна лица ради заштите одређених информација

3. АКТИВНОСТИ

- идентификација информација и сродних средстава, потенцијалних претњи, рањивости и утицаја
- процена ризика
- доношење одлука о третирању ризика (избегавњу, ублажавању, расподели или прихватању)
- избор и дизајн безбедносних контрола и спровођење
- надгледање активности и прилагођавање променама....

САЈБЕР БЕЗБЕДНОСТ

Сајбер безбедност се може представити као примена технологије, процеса и контроле ради одбране рачунара, сервера, мобилних уређаја, електронских система, мрежа и података од сајбер напада.

Циљ сајбер безбедности јесте да се смањи ризик од сајбер напада и заштити од неовлашћеног искоришћавања система, мреже и технологије

ЕЛЕКТРОНСКА УПРАВА

Електронска управа или е-управа (енгл. e-administration) је термин чије дефиниције варирају од употребе информатичке технологије како би се олакшао промет информација и савладале физичке препреке традиционалних система до коришћења технологије како би се повећала доступност и олакшало извршење јавних служби у корист грађана, привредника, као и запослених у тим службама.

Устаљено виђење ствари иза ових дефиниција је да је е-управа заправо аутоматизација, односно компјутеризација постојећег „папир система“, која ће довести до нових стилова управљања, нових начина расправљања и одређивања стратегија, обављања послова, као и организовања и достављања информација.

Развој е-управе у Републици Србији подразумева успостављање ефикасне и кориснички оријентисане управе у дигиталном окружењу, која је интероперабилна како између различитих нивоа јавне управе у Србији, тако и са јавном управом држава чланица ЕУ.

Међутим, пут од стадијума на коме се тренутно налази еУправа у Србији, до наведеног жељеног стања, представља распон жељене промене, који подразумева јасно дефинисање циљева Програма, као и мера за постизање тих циљева, са јасно уочљивим узрочно последичним везама

На основу претходних реченица уочљиво је да сам развој подразумева концепцију и примену електронског пословања које користе сви (запослени у јавној управи, грађани, пословни људи, запослени људи у приватним објектима итд.).

Развојем е-управе омогућава се ефикаснија услуга према становништву, смањење трошкова, једноставније обављање послова уз добру организацију, сузбијање корупције и ефикаснији однос са привредним објектима.

Такође боља функционалност приступа подацима помаже развоју еУправе у Србији јер су грађани у прилици да лако провере тачност својих података и да се по потреби обрате надлежној институцији како би се ти подаци исправили.

ИНФОРМАЦИОНА БЕЗБЕДНОСТ

Закон о информационој безбедности

- Овим законом су уређене мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

ИКТ системи од посебног значаја су системи који се користе:

- у обављању послова у органима јавне власти;
- за обраду података који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности;

ИНФОРМАЦИОНА БЕЗБЕДНОСТ У СРБИЈИ

Информациона безбедност је аспект безбедности који се односи на безбедносне ризике повезане са употребом информационо-комуникационих технологија, укључујући безбедност података, уређаја, информационих система, мрежа, организација и појединаца.

(Стратегија развоја инф.безбедности 2017...)

ИНФОРМАЦИОНА БЕЗБЕДНОСТ

- Безбедност локације (“сајта”)
- Безбедност ресурса
- Безбедност комуникацијске мреже
- Безбедност сервиса
- Безбедност приватности - личних података.

У рачунарским мрежама се у циљу спречавања евентуалних напада и могућих оштећења података примењују одређени сигурносни сервиси, од којих су најзначајнији:

- Аутентификација (authentication);
- Тајност података (data confidiality);
- Непорицање порука (nonrepudation);
- Интегритет података (data integrity);
- Контрола приступа (access control) и
- Расположивост ресурса (resource availability)

Ради повећања IT безбедности органи јавне власти, предузећа, односно компанија обично се примењује шест категорија безбедносних мера.

Избор мера зависиће од потребног нивоа безбедности

- опште безбедносне политике и процедуре,
- софтвер за заштиту од вируса,
- дигитални потписи,
- шифровање,
- заштитни и (противпожарни) зидови и
- прокси сервери

ОПШТЕ БЕЗБЕДНОСНЕ ПОЛИТИКЕ И ПОСТУПЦИ

- Честа промена приступних лозинки
- Ограничавање употребе система
- Ограничавање приступа подацима
- Успостављање контроле физичког приступа
- Подела одговорности
- Шифровање (енкрипција) података
- Успостављање процедуралне контроле
- Провођење едукативних програма
- Инспекција активности унутар система
- Бележење свих трансакција и активности корисника

УРЕДБА О БЛИЖЕМ УРЕЂЕЊУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

- Ближе уређење мера заштите ИКТ система
- Послови и одговорност запослених
- Заштита информационих добара
- Средства и имовина за надзор над пословним процесима
- Управљање ризицима
- Постизање безбедности рада на даљину и мобилних уређаја
- Образовање, обуке и едукације + одговорност
- Заштита после промене радног места (уговор о поверљивости, клаузула забране конкуретности…)
- Класификовање података
- Заштита носача података
- Ограничење приступа и овлашћен приступ
- Мере криптозаштите…

УРЕДБА О БЛИЖЕМ САДРЖАЈУ АКТА О БЕЗБЕДНОСТИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА, НАЧИНУ ПРОВЕРЕ И САДРЖАЈУ ИЗВЕШТАЈА ПРОВЕРЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА

Садржина акта о безбедности ИКТ система:

- мере заштите
- принципи
- начини и процедуре постизања нивоа безбедности
- овлашћења и одговорности
- Ресурси

КОМПАТИБИЛНО СА ISO/SRPS 27001

УРЕДБА О ПОСЕБНИМ МЕРАМА ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ИНФОРМАЦИОНО-ТЕЛЕКОМУНИКАЦИОНИМ СИСТЕМИМА

- Донета на основу Закона о тајности података (обухвата опште мере)
- Уређује посебне мере у раду са тајним подацима у ИКТ системима од посебног значаја
- Посебне мера заштите тајних података у информационо-елекомуникационим системима
- Коришћење система за потребе рада са тајним подацима
- Управљање ризиком безбедности система
- Посебне мере заштите тајних података у ИКТ системима могу бити техничке и организационе, а предузимају се у циљу спречавања случајних грешака, неправилног и недозвољеног прикупљања, чувања, обраде, коришћења, оштећења, уништења, као и фалсификовања и злоупотребе тајних података.

Посебне мере заштите тајних података у систему односе се на:

1. објекат у коме је смештен систем (опрема, документи, програмска подршка и мрежа);
2. простор, просторије, односно безбедносне зоне у којима се обрађују тајни подаци у систему;
3. овлашћена лица за управљање безбедношћу система;
4. све учеснике у раду система;
5. коришћење система за потребе рада са тајним подацима;

6. режим рада система;
7. заштиту тајних података приликом обраде и чувања у систему;
8. заштиту од ризика компромитујућег електромагнетног зрачења, као и инсталирање уређаја за чување тајних података.

НЕКИ ОД ПРОБЛЕМА СА BIG DATA

Big Data је појам који означава велике и комплексне сетове података, код којих традиционалне апликације за обраду података нису применљиве.

Те скупове података карактеришу разноврсност формата, велике брзине обраде и приступа, и велики обим информација.

Big Data не представља јединствену технологију, већ је то комбинација старих и нових технологија које помажу да се стекне делотворан увид у обрађене податке.

Big дата карактеришу три V:

1. Екстремни обим података - volume
2. Широк спектар типова података - variety
3. Брзина којом се подаци морају обрадити - velocity

- Проблеми складиштења, скалабилности и расположивости великих количина података
- Инфраструктура система за обраду података велике количине података
- Складишта великих количина података
- Анализа токова података, анализа веза у подацима.

Вештачка интелигенција и обрада података у Big data

- Интелигенција – способност усвајања, памћења и обраде знања
- Не-биолошки, вештачки систем који имитира људско/интелигентно понашање
- Рачунарски програм/уређај који има способност људске интелигенције
- Паметна аутоматизација процеса обраде података
- Будућност - Вештачка интелигенција и подаци у клауду?

МЕЂУНАРОДНИ СТАНДАРДИ

- Техникама безбедности у овој области бави се ISO/IEC JTC 1/SC 27, Технике безбедности (IT security techniques)
- Овај поткомитет је објавио 185 докумената, а у развоју је још 66 докумената
- Сви ови стандарди имају заједнички први део наслова
  - **Information technology -- Security techniques**
- Међу овим документима је и серија стандарда ISO/IEC 27000 којих укупно има око 40
- Техникама безбедности у овој области бави се и CEN/CLC JTC 13, Сајбер безбедност и заштита података (Cybersecurity and Data Protection) – 8 докумената

СРПСКИ СТАНДАРД

- SRPS ISO/IEC 27001:2014, Информационе технологије – Технике безбедности – Системи менаџмента безбедношћу информација – Захтеви
- Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима (ЗТП)
- Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја (ЗИБ + ЗЗЛП)

SRPS ISO/IEC 27001

- **ISO/IEC 27001** је међународни стандард за управљање безбедношћу информација .
- Детаљно описује захтеве за успостављање, имплементацију, одржавање и континуирано побољшање система управљања безбедношћу информација (ISMS) – чији је циљ да помогне организацијама да учине безбеднијом информациону имовину коју држе.
- Већина организација има бројне контроле безбедности информација.
- Међутим, без система управљања безбедношћу информација (ISMS), контроле имају тенденцију да буду донекле неорганизоване и неповезане, пошто се често примењују као тачна решења за специфичне ситуације или једноставно као ствар конвенције.

- Контроле безбедности које раде обично се баве одређеним аспектима информационе технологије (ИТ) или посебно безбедности података; остављајући не-ИТ информациона средства (као што су папирологија и власничка знања) мање заштићена у целини.
- Штавише, планирањем континуитета пословања и физичком безбедношћу може се управљати сасвим независно од ИТ или информационе безбедности, док се у пракси људских ресурса може мало помињати потреба да се дефинишу и доделе улоге и одговорности у области безбедности информација у целој организацији.

ISO/IEC 27001 захтева да менаџмент:

- Систематски испита ризике по безбедност информација организације, узимајући у обзир претње, рањивости и утицаје;
- Дизајнира и примени кохерентан и свеобухватан скуп контрола безбедности информација и/или других облика третмана ризика (као што је избегавање ризика или пренос ризика) како би се адресирали они ризици који се сматрају неприхватљивим; и
- Усвоји свеобухватни процес управљања како бисте осигурали да контроле безбедности информација настављају да испуњавају потребе организације за безбедност информација на сталној основи.

СТАНДАРДИ ISO/IAC 17799

- политику безбедности;
- организовање информатичке безбедности;
- управљање ресурсима;
- безбедност људских ресурса;
- физичку заштиту;
- управљање радом и комуникацијама;
- контролу приступа;
- набављање, развој и одржавање информатичких система, управљање безбедосним инцидентима;
- управљање континуитетом пословања и усаглашеност за законском регулативом.

ПРИВАТНОСТ

„ПРИВАТНОСТ ЈЕ МРТВА – ПРЕБОЛИТЕ ТО“ (Стив Рамбрам)

ЉУДСКЕ СЛОБОДЕ И ПРАВА

КАРАКТЕРИСТИКЕ

1. Изводе се из природног стања
2. Моралног су порекла
3. Усмерена су против државе – она су политтичка у смислу да се остварују у држави и односе на државу, којима се она ограничавају или се од ње тражи конкретно деловање
4. Изворна и неотуђива
5. Припадају свим људским бићима без икаквог разликовања, па је у њиховој основи начело једнакости и забрана дискриминације.

1. Права три генерације (уједно и подела према критеријумима који се односе на сфере активности појединаца):

- Грађанска и политичка права (крај XVIII i почетак XIX в.)
- Економска, социјална и културна права (XIX и почетак XIX в.)
- Права солидарности (друга половина XX в.)

2. Утужива и неотуђива права (немогућност да се нека права могу остварити путем тужбе).
3. Индивидуална и колективна (право појединца да у заједници с другима ужива неко право).
4. Апсолутна и релативна
5. Општа и посебна

ПРИВАТНОСТ

Универзална декларација о људским правима

Члан 12. прописује да „нико не сме бити изложен произвољном мешању у његову приватност, породицу, дом или преписку, нити нападима на част или углед. Свако има право на заштиту закона против оваквог мешања или напада”.

Међународни пакт о грађанским и политичким правима

Члан 17. прописује да „нико не може бити предмет самовољних или незаконитих мешања у његов приватни живот, његову породицу, у његов стан или његову преписку, нити незаконитих повреда нанесених његовој части или његовом угледу”,

док члан 23. штити породицу и право на склапање брака и оснивање породице, а члан 24. уређује права и заштиту деце и малолетника.

Европска конвенција о људским правима

У ЕКЉП право на приватност представља збирни назив за заштиту неколико на први поглед разнородних права, и то права на поштовање приватног живота, породичног живота, неповредивости дома и преписке, као и части и угледа појединца (члан 8. ЕКЉП).

Конвенција о правима детета Уједињених нација

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

ПРИВАТНОСТ У СРБИЈИ

Појам права на приватност није дефинисан у Уставу Републике Србије, али Устав у неколико чланова гарантује права која проистичу из права на приватност, које обухвата, између осталог, и право на неповредивост стана и право на тајност писама и пошиљки и заштиту података о личности.

Члан 42. Устава који уређује област заштите података о личности, затим, чланом 25. Устава штити физички и психички интегритет, чланом 40. се штити неповредивост стана, а чланом 41. се штити тајност писама и других средстава комуницирања...

Члан 19. Устава наводи да јемства људских права у Уставу служе „очувању људског достојанства...", што значи да штити част и углед као основне вредности заштићене међународним инструментима.

Сва та права заједно, према дефиницијама у међународноправним инструментима, чине право на приватност

Република Србија није донела посебан закон који би се бавио приватношћу – али је ову област уредила кроз више системских прописа

ШТА ЈЕ ПРИВАТНОСТ

Појам приватности можемо посматрати

- у **класичном** (традиционалном) и
- у **савременом** (информатичком смислу).

Савремено доба донело је технологију која иде испред етике

ФИЗИЧКА ПРИВАТНОСТ

- скривање интимних делова тела или одређених интимних радњи од других особа;
- скривање садржаја властитих предмета, стана или возила од других особа.

Информацијска приватност, односно приватност података везаних уз здравствено стање, финансијско стање, политичку активност, боравиште или породично стање неког појединца; уз то је близак појам приватности на Интернету и приватности на друштвеним мрежама...

Паралеле са неовлашћеним фотографисањем (папарацо), ухођењем, прислушкивањем и таблодином штампом.

Приватност на интернету укључује право на личне информације у вези са чувањем, употребом, обезбеђењем од трећих лица и приказивање личних информација преко интернета. Заштита може да подразумева и личне идентификационе информације (ЛИИ) или не-ЛИИ информације које се односе на посетиоца одређене веб странице. ЛИИ се односи на све информације које се могу користити за идентификацију појединца.

Приватност на друштвеним мрежама се односи на степен контроле коју особа има над приступом и употребом личних података. Када је реч о питањима приватности и безбедности на друштвеним мрежама, сајтови за које су најкарактеристичнији ови проблеми уједно су и они који су најпопуларнији. Међутим, питања безбедности коришћења и питања приватности су потпуно две различите ствари. Питање приватности, које укључује неовлашћен приступ приватним информацијама, не мора да укључује безбедносне повреде.

- Приватност је право
- Способност појединца да сачува приватне информације
- Заштита од презира и исмејавања
- Механизам којим контролишемо сопствену репутацију
- Начин регулисања степена наше социјалне интеракције
- Штит од деловања државе (судски и други поступци...)

Посебан облик заштите приватности јесте право на пијетет, односно право на законску заштиту преминулог лица.

Функција: дозвољава појединцима да контролишу токове информација о њима.

Којим вредностима служи спречавање или ограничавање протока истинитих информација?

- Слободи од интервенције државе/закона
- Слободи од социјалних/моралних норми
- Слободи од маркетинга/комерцијалних истраживања

Моћ самодефинисања: од профилисања и „рударења података“ до контрола над уступљеним информацијама: које креирају други...

ПРИВАТНОСТ – класичан концепт

- ПРАВНИ И ДРУШТВЕНИ КОНЦЕПТ
- ПРИВАТНА СФЕРА ИЛИ ПРИВАТНИ ЖИВОТ
- КОНЦЕПТ РАЗВИЈЕН НА ЗАПАДУ
- ТЕШКО ПРЕВОДИВ НА ДРУГЕ ЈЕЗИКЕ (усамљеност, тајновитост, приватни живот)
- Право да се буде остављен на миру (САД XIX в)

Ово право се развило у Сједињеним Америчким Државама под утицајем либералистичке доктрине о положају појединца у друштву. У другој половини 20. века ово право је прерасло у «права на личну аутономију» и састојало се у гарантовању сфере личне аутономије у оквиру које би сваки појединац имао право да самостално, без уплитања државе помоћу правних прописа уређује своје односе са другим људима. У САД се ово право штитило путем тужби за деликте, које признаје common law-a, као што су trespass (сметање поседа) и defamation (лишавање угледа).

Деликтне тужбе којима се данас штити приватност у САД су:

- тужба за intrusion (продирање у физичку приватност лица проваљивањем у стан, телефонским прислушкивањем, тајним снимањем);
- тужба за public disclosure (објављивање приватних података, независно од тога да ли то штети части и угледу),
- тужба за false light (саопштавањем јавности погрешне представе о лицу, било да је дефаматорна или не, попут повреде права на интегритет у нашем праву),

- тужба за appropriation (коришћење туђих личних добара у комерцијалне сврхе, нпр. туђег имена, слике)

Када су у питању личности из јавног живота, у које се убрајају политичари, естрадни и филмски уметници спортисти и слично, судска пракса у САД полази од претпоставке да увек постоји њихова намера да им лик буде комерцијално искоришћен, јер имају својинско право, како на објављивање лика (right of publicity), те уновчавају записе лика (али и гласа, право на коришћење њиховог имена, или сопствених интимних података од стране других).

Права личности у Великој Британији, штите се путем традиционалних тужби за заштиту појединих личних добра, па их примењују и на случајеве повреде приватности. Тиме је утемељена одређена судска пракса, али није прихваћено right of privacy као у САД, пошто нема законског основа за заштиту општег права личности.

У енглеском, али и у америчком праву, користе се тужбе из common law-a, за случај повреде части:

- libel (код увреде писаним путем или за увреду путем штампе или других масмедија, које се сматрају увредама трајног карактера) и
- slander (за увреду која није трајног карактера, а извршена је конклудентно - мимиком, гестом).

Континентални правни круг се разликује од англосаксонског, који предвиђа деликте, као посебне облике повреде права приватности. У Европи, постоји теорија сфера, најразвијенија у Немачкој и Швајцарској, по којој је приватност издељена по сферама које су степеноване као тајна - интимна, лична - приватна, властита, сфера поверљивости и приватно - јавна и заједничка сфера. У Немачкој доктрини право на приватност је било врло ограничено све до доношења пресуде Савезног суда 1954.године којом је признато опште лично право, а изричито и право сваког човека на тајну сферу.

Касније је у правној теорији прихваћена подела на следеће сфере приватности: тајну (интимну), приватну и приватно-јавну.

У последњој сфери појединац у јавности учествује као непозната особа и мора да прихвати околност да свако може да има увид у део његовог живот који се одиграва на јавном месту. Посебан проблем у вези са тим настаје ширењем података приватне природе путем друштвених мрежа, без обзира на то да ли је реч о текстуалним, сликовним, аудио или видео информацијама.

Повреда тајности сматрала се повредом добрих обичаја, према немачкој судској пракси, али се судска заштита праву приватности пружала само у случају настанка имовинске штете коју би титулар права претрпео откривањем тајне и повредом права на лично име и на своју слику.

У параграфу 78. Закона о ауторском праву Аустрије, из 1936. године, поред права приватности, штити се и право на пијетет личности.

Тако се забрањује јавно излагање и искоришћавање нечије слике, ако би се на тај начин вређали интереси портретисаног лица, али и његове ближе родбине, након његове смрти, осим ако постоји наредба да се то учини.

Према параграфу 77. истог закона, ово важи и за писма, дневнике и личне списе.

Швајцарски грађански законик садржи генералну клаузулу о заштити личности, па је тако и право на приватни живот законом заштићено. Међутим и пре доношења овог законика, сматрало се да се право приватности, попут права на част и углед, може штитити као самостално право.

У Француској се оперише јединственим појмом приватног живота, схваћеним уже и са нагласком на тајности. Почев од 1970. године, право приватности у Француској је регулисано законом. Временом се развила судска пракса у погледу заштите личности од објављивања тајних података, па тако и од неовлашћеног објављивања личних списа и записа, због повреде обавезе чувања тајне, као и забране објављивања службене тајне.

Уже одређено право на приватност је апсолутно субјективно право физичког лица да може самостално да одлучи о упознавању трећих лица са било којом манифестацијом своје егзистенције. Из овог права извиру посебно лична права као што су:

- право на приватан живот,
- право на лик,
- право на глас,
- право на списе личног карактера.

У оквиру права на приватни живот треба разликовати:

- **интимну сферу** у коју ималац права никоме не допушта приступ или допушта само најближим лицима; подразумева област скривених интимних података, који ће бити ретко коме откривени, па их особа држи у строгој тајности, јер њихово откривање интимно осећа неповољним по себе.

Неретко су у питању личне тајне, којима се штите и друга лица, за која оне такође представљају интиму. Интимни подаци могу бити одређене девијације у понашању којих је лице свесно, одређене личне и породичне тајне, непријатне успомене и сл.

- **приватну сферу** у коју ималац права допушта приступ одређеном кругу лица (породица, рођаци, пријатељи)

Приватна сфера је нешто познатија сфера живота појединца, у оквиру породичног, фамилијарног, односно круга пријатеља неког лица, где су сви упознати са начином живота титулара права, као и са породичним и здравственим проблемима, пословним, финансијским успесима и неуспесима, политичким и верским опредељењем, животним плановима, хобијима, али и социјалним и интимним релацијама са другим особама

- **приватно-јавну сферу** у коју ималац права допушта већем броју људи да се упознају са одређеним аспектима његовог живота

Приватно-јавна сфера је полуприватна и најпознатија сфера активности и стања, односно живота неког лица, где оно као титулар права на своју приватност, допушта трећим лицима да сазнају оне видове његовог живота који се одвијају на јавном месту, на коме се и она могу наћи, као што је улица, парк, јавна установа, аеродром, биоскоп, хотел и друго.

Приватност (privacy) – дато кроз деликте који угрожавају овај домен – своди се на неколико врста повреда:

- задирање у прилике које чине физичку повученост лица (intrusion),
- објављивање података приватног карактера (public disclosure),
- стварање погрешне представе о лицу у јавности (putting in false light) и
- коришћење туђих личних својстава(имена, слике) у комерцијалне сврхе (appropriation)

Право да се буде остављен на миру

- Међу осталим тумачењима означава право особе да сама изабере «изолацију од присуства других ако то жели и право да буде заштићена од праћења у приватном окружењу као што је властити дом».

ПРАВО НА ПРИВАТНОСТ

- није само «да будемо остављени на миру», већ подразумева и контролу над информацијама о себи, али и о другима, дајемо на увид јавности.

Под **правом на приватни живот** подразумева се право личности да се трећа лица искључе од сазнавања чињеница везаних за титулара овог права. Ради се о чињеницама које човек жели задржати само за себе, није само «да будемо стављени на миру», већ подразумева и контролу над информацијама о себи, али и о другима, које дајемо на увид јавности.

Приватна сфера представља домен породичног и кућног живота који је, теоретски, слободан од утицаја владе и других друштвених институција. У овом домену, одговорност је према себи и осталим члановима домаћинства, а посао и размена могу се одвијати унутар куће на начин који је одвојен од економије већег друштва.

Основна разлика између приватне и јавне сфере се огледа у томе да је јавна сфера политичка област у којој се више лица (која се не морају познавати –странци) састају да се укључе у слободну размену идеја и да су отворени за све, а приватна сфера је мања, обично затворена група (попут породице) и она је отворено само онима који имају дозволу за улазак у њу.

Право на приватни живот из праксе Европског суда за људска права:

1. Име и фотографија одређеног лица
2. Физички и психички интегритет одређеног лица
3. Сексуална оријентација
4. Пословна способност
5. Односи између хранитеља и деце о којима се брину
6. Односи са другим људима који се не заснивају на довољно чврстим везама да би потпали под „породични живот“

ПРАВО НА ПРИВАТНОСТ НИЈЕ АПСОЛУТНО ПРАВО И МОРА БИТИ УСКЛАЂЕНО СА ПОТРЕБАМА ДРУШТВА.

ПРАВО ЈАВНОСТИ ЈЕ ПРЕЧЕ ОД ПРАВА ПОЈЕДИНЦА НА ПРИВАТНОСТ!

Правни, односно друштвени концепт према коме сваки појединац може имати одређене активности и уз њих везане предмете, мишљење или осећања, које може „задржати за себе“…

Заштићено од других појединаца, организација, делова друштва или јавности…

Дефинисање појма се битно разликује међу културама…

Изражавајући жаљење за све већом пролиферацијом података, научни радници тврде да је приватност de facto укинута, мада de iure још постоји.

Пролиферација личних података проблематична је због чињенице да што је већи опсег информација о грађанима доступан одређеним инстанцама, то је већи степен контроле коју оне имају, што може имати директни утицај на грађанске слободе.

И у прошлости је било жучних расправа око тога да ли, на пример, фотографисање других људи без њиховог пристанка представља атак на њихову личну приватност или не (јавне личности, папарацо...).

ИНФОРМАТИЧКА ПРИВАТНОСТ

Информатичка приватност обухвата скуп података (информација) о личности, насталих употребом дигиталне технологије, које дају печат његовој индивидуалности, а које су правно заштићене од неовлашћеног приступа и повреде од стране свих других лица.

Приватност информација је право појединца да одреди када и у којој мери информације о њему могу да се преузму и дистрибуирају другима...

У времену које карактерише обрада огромне количине најразличитијих података, тзв. **„ери великих података”**, лични подаци третирају се као „нова нафта”.

Своје „бесплатне” услуге компаније наплаћују корисницима тако што им заузврат траже све више личних података, јер, како каже стара изрека, „бесплатан ручак не постоји”.

Информатичка приватност није право на тајност, нити на контролу, већ право на одговарајући проток личних података.

Шта то конкретно значи?

То значи да особа има могућност да, у зависности од ситуације и контекста, лично процени шта ће и са ким делити у **дигиталном окружењу**.

Свака особа има право да зна:

- како и у које сврхе се користе њени подаци,
- ко их чува и колико дуго,
- ко све њима располаже,
- као и да може да затражи брисање личних података или исправку нетачних података.

У ужем (техничком) смислу, под појмом приватности (privacy) обично подразумевамо начин прикупљања, употребе и заштите личних информација на мрежи. Проблем приватности није настао тек са појавом компјутера. Огромне могућности IT-а са аспекта складиштења и преузимања података вишеструко су појачале потребу за ефикасном заштитом приватности.

Злоупотребе:

1. Дигитално насиље
2. Нарушавање угледа
3. Ухођење
4. Уцењивање
5. Крађе идентитета
6. Навођење на проституцију/трговину људима
7. Стварање других непријатности...

Има мишљења, чак, да ће, у годинама које су пред нама, заштита приватности представљати главни проблем и баласт у међусобним односима пословних компанија и потрошача.

У неке од најактуелнијх моралних проблема са којима се савремене компаније морају суочити спадају:

- Приватност електронске поште;
- Софтверске лиценце;
- Ауторска права над софтвером;
- Приступ хардверу;
- Власништво над интелектуалном својином;
- Приступ фајловима;
- Власништво над подацима

ЕТИЧКИ МОМЕНАТ И IT ТЕХНОЛОГИЈА

Онлајн морал (ethics)

Скуп неписаних правила понашања корисника које треба поштовати приликом употребе информационе технологије, морално добро и врлина.

ФОКУС ЕТИЧКЕ (НЕ)ДОСЛЕДНОСТИ МОДЕРНОГ СВЕТА

- Питања везана за трансхуманизам и улогу вештачке интелигенције
- Клонирање
- ГМО

ИТ ТЕХНОЛОГИЈЕ - ТРИ МОДЕЛА ПРЕМА КОЈИМА СЕ ДОНОСЕ ОДЛУКЕ (СТРАТЕШКЕ ОДЛУКЕ ДОНЕТЕ ИГНОРИСАЊЕМ РЕАЛНОСТИ):

- Одлуке (из) незнања – игноришу се све чињенице које се односе на политику, право, безбедност, ИТ технологије и економију...
- Предострожан приступ – заснивају се на најгорем сценарију
- Анализа ризика – поступање у сагласности са предвидивим документованим у проценама...

Проблем мешања чињеница са уверењима....

Морално понашање се односи на извршавање очекиваних активности, кроз категорије савести, слободе и самосвести...

Легално понашање обично подразумева извршавање захтеваних активности у складу са прописима, нормативом организације и технолошким упутствима...

УГРОЖАВАЊЕ ПРИВАТНОСТИ НА ИНТЕРНЕТУ

Може се разматрати кроз врсту:

1. Акције – пресретање и ометање пријема података, илегални приступ...
2. Починиоца – хакери, сајбер криминалци...
3. Циља – појединци, компаније, држава...

- Колачићи (cookies)
- Шпијунски програми (Spyware)

- Спам - слање нежељених (unsolicited) имејл порука
- Социјалне мреже (енгл. Social network) – могу бити искоришћене за ширење малвера или крађу поверљивих информација

Друштвене/Социјалне мреже (енгл. Social network) начини манипулације:

- Дезинформације, лажне вести
- Садржај који је усмерен на емоције
- Филтерски мехур

Неетичке појаве:

- **Тролови** – распиривачи бесмислених расправа ради одвлачења пажње
- **Домејнери** – тапкароши интернет домена са туђим брендовима
- **Ботови** – убеђени или плаћени писци оптужби или хвалоспева у коментаримана медијским порталима
- **Хакери** – извршиоци сајбер/интернет кривичних дела
- **Хејтери** – непоштовање антидискриминационих прописа
- **Спамери** – непоштовање трговачких и комуникацијских прописа слањем масовних порука
- **Спин доктори** – објављују ужасавајуће и непроверене информације које нарушавају достојанство, личну безбедност, ради постизања политичког циља, профита или утицаја

ДИГИТАЛНО НАСИЉЕ НА ИНТЕРНЕТУ:

Представља сваки облик насиља које настаје употребом дигиталних технологија.

Може се одвијати на друштвеним мрежама, апликацијама за размену порука, гејминг платформама и мобилним телефонима. То је понашање које се понавља...

ДИГИТАЛНО НАСИЉЕ НА ИНТЕРНЕТУ ОБУХВАТА:

- Узнемиравање, ухођење и вређање
- Несавестан приступ штетним садржајима
- Ширење насилних и увредљивих коментара
- Снимање насилних сцена и слање претећих порука
- «провaљивање» у адресе електронске поште
- Слање злобних и неугодних садржаја другима
- Креирање интернет странице која садржи приче, слике, снимке...

- лажно представљање, коришћење туђег идентитета, креирање профила на друштвеним мрежама на туђе име;
- недозвољено саопштавање туђих приватних информација, објављивање лажних оптужби или гласина о другој особи на профилима друштвених мрежа, блоговима
- промена или крађа лозинки;
- слање вируса;
- исмевање у онлајн причаоницама и на интернет форумима, непримерено коментарисање туђих слика, порука на профилима, блоговима;
- игнорисање, искључивање (нпр. из група на социјалним мрежама), подстицање мржње (по различитим основама) и др.
- постављање узнемирујућих, увредљивих или претећих порука, слика или видео-снимака на туђе профиле или слање тих материјала СМСом, инстант порукама, имејлом, остављање на чету;
- снимање и дистрибуција слика, порука и материјала сексуалног садржаја;

УКЉУЧУЈЕ БИО КАКАВ ОБЛИК КОЈИ ИМА ЗА ЦИЉ ПОВРЕЂИВАЊЕ, УЗНЕМИРАВАЊЕ, НАНОШЕЊЕ СРАМОТЕ ИЛИ ШТЕТЕ...

CYBERBULLING – злонамерни коментари на статусе и фотографије, постављање туђих слика у групама намењеним исмејавању, прављење лажних профила ради задиркивања, вербални напади на чету... везује се за малолетнике

CYBERSTALKING – организовано насиље преко технологије, са циљем уништавања каријере, угледа, пословног подухвата и одвија се међу запосленима

СЕКСУАЛНО ЗЛОСТАВЉАЊЕ ПРЕКО ИНТЕРНЕТА – слање непримерених порука, фотографија, снимака и осталих медијских садржаја са циљем узнемиравања или настављања са комуникацијом... жртве су најчешће малолетници

ТРГОВИНА ЉУДИМА – углавном се одвија преко друштвених мрежа

Типови насилника на интернету (1):

TROL – напада лица на интернету која износе своја мишљења;

REGRUTER – мами жртве и присиљава их на проституцију или трговину људима

ВРШЊАЧКИ САЈБЕР СИЛЕЦИЈА – шаље злонамерне поруке ради понижавања или наношења срамоте

САЈБЕР ПРОГОНИТЕЉ – прикупља информације о жртвама, ради уцене и застрашивања

ПОРНО ОСВЕТНИК – наставак насиља из партнерских односа, преко постављања приватних фотографија или снимака сексуалне природе

Типови насилника на интернету (2):

ПРОГОНИТЕЉ ИЗА ФОТО АПАРАТА – фотографише жртве без пристанка и поставља њихове фотографије на интернету

ЗЛОНАМЕРНИ ПРОПАГАНДИСТА – користи пропаганду и технологију ради промовисања друштвено спорних вредности и циљева

ИНТЕРНЕТ ПЕДОФИЛ – контактира малолетне жртве преко интернета ради сексуалних односа

ДОКСЕР – прикупља, а потом и објављује приватне податке како би јавно осрамотио жртву

ХАКЕР – неовлашћено/незаконито прикупљање информација и података

МАНИПУЛАТОР СА САЈТОВА ЗА УПОЗНАВАЊЕ – успоставља контролу над жртвом и доводи је у опасне ситуације

Социјални инжењеринг (енгл. Social engineering) – метод психолошке манипулације које нападач користи како би дошао до поверљивих информација или навео жртве да изврше одређење радње. Најчешће су те радње отварање злонамерне веб странице или покретање нежељеног прилога датотеке.

Изводи се обично у четири корака:

- Истраживање
- Стицање поверења
- Искоришћавање односа за добијање информације
- Коришћење прикупљених информација за злоупотребу

ПРИСВАЈАЊЕ ТУЂЕГ ИМЕНА ИЛИ ИДЕНТИТЕТА

НЕОВЛАШЋЕНО КОРИШЋЕЊЕ ИМЕНА ИЛИ ИДЕНТИТЕТА ДРУГОГ ЛИЦА ... (БЕЗ ОДОБРЕЊА ТОГ ЛИЦА!)

Крађа идентитета на Интернету - врста преваре којом се од корисника рачунара путем лажне поруке е-поште или веб-сајта сазнају лични и финансијски подаци.

Криминал којим злочинци имитирају друге људе, обично за финансијску добит. У данашњем друштву, често се од појединаца тражи да открију доста личних информација о себи, као што су бројеви социјалног осигурања, потпис, име, адресу, телефонске бројеве, па чак и информације о банкарским и кредитним картицама.

Може да иде даље од новчаних последица. Лопови могу да користе туђе информације да добију возачку дозволу или неки други документ на коме ће бити њихова фотографија, али туђе име и информације. Са тим документима лопови би могли да добију посао, поднесу захтев за путне исправе, или чак да учине да се и туђе име и поштанска адреса нађу у полицији и другим органима ако је лопов укључен у друге криминалне активности.

Крађа идентитета на Интернету се разликује од обичне крађе идентитета на неколико начина.

Обична крађа идентитета се дешава након што је некоме нешто физички украдено као на пример новчаник са кредитним картицама и возачком дозволом или неисцепан извод кредитне картице из канте за смеће. Лопов би ове украдене ствари користио да направи лажне куповине у нечије име или нешто те природе.

Крађа идентитета на Интернету може бити много гора и може бити много разорнија него конвенционалне крађе идентитета, јер је већина жртава крађе идентитета је потпуно несвесна да је нешто украдено од њих док не буде прекасно.

ШЕРЕНТИНГ (енглеске речи делити и родитељство)

Подразумева различите начине по којима родитељи деле на интернету детаље приватног живота њихове деце (пресвлачење, купање, на базену, на мору...). На тај начин родитељи обликују дигитални идентитет своје малолетне деце пре него што оно постане самостални корисник интернета. Може означити као тенденција родитеља да друштвене мреже и друге интернет платформе „затрпавају" фотографијама, снимцима или личним информацијама о сопственој деци. Скоро 1.500 фотографија свог малишана просечан родитељ објави на мрежи до дететовог петог рођендана, показује истраживање које је спровела „Родитељска зона".

Адекватна едукација родитеља – одговор како успоставити баланс између дечијих права и родбине која живи далеко, односно колико је информација превише информација?

Приватност се просто дефинише као слобода од неовлашћеног упада, узнемиравања и могућност да се посебно личне ствари задрже за себе. У теорији су дефинисане 4 широке категорије обичајног права које су у основи декиката нарушавања приватности.

1. Упад у нечију осаму,
2. Откривање приватних података,
3. Објављивање информација које неоправдано представљају у лажном светлу, и
4. Присвајање туђег идентитета или имена.

УПАД У НЕЧИЈУ ОСАМУ:

Подразумева вредност поседовања сопственог приватног простора и ограду од оних који би желели да га наруше. Прислушкивање и ухођење су два примера који се сматрају упадом у приватност.

ОТКРИВАЊЕ ПРИВАТНИХ ПОДАТАКА

Подразумева да обајвљивање одређених чињеница може нанети штету појединцу (здравствени статус, финансијско стање, личне преписке...)

ОБЈАВЉИВАЊЕ ИНФОРМАЦИЈА КОЈЕ СЕ НЕОПРАВДАНО ПРЕДСТАВЉАЈУ У ЛАЖНОМ СВЕТЛУ

Слично клевети, али може бити знатно суптилније (означава оговарање, омаложавање, вређање части или давање изјаве у којима се тврде неистине ради стварања негативне слике о појединцу, компанији, пословању, производу, групи, народу или држави).

УГРОЖАВАЊЕ ПРИВАТНОСТИ РАДИ КОМЕРЦИЈАЛНОГ ИСТРАЖИВАЊА ТРЖИШТА?

УГРОЖАВАЊЕ ПРИВАТНОСТИ РАДИ ДОБИЈАЊА ЕКСЛУЗИВНИХ ВЕСТИ?

КРЕИРАЊЕ ЈАВНОГ МЊЕЊА?

ДЕЗИНФОРМАЦИЈЕ И ЛАЖНЕ ВЕСТИ?

ДЕЛОВАЊЕ ОРГАНИЗОВАНОГ КРИМИНАЛА – дигитална пиратерија, уцене, навођење на проституцију, трговина људима...

НОВИНАРСКЕ ДИЛЕМЕ:

- Да ли јавне личности имају право на приватност?
- Да ли је неопходно извештавати о заразним болестима и самоубиствима јавних личности?
- Да ли деца јавних личности имају право на приватност?
- Да ли се појам приватности односи и на приватне (интимне) тренутке и на јавним местима?

ОПШТА УРЕДБА О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ – GDPR

Нови Генерални пропис о заштити података Европске уније (EU General Data Protection Regulation - GDPR) назван Општа уредба о заштити података је Уредба (ЕУ)2016/679 Европског парламента и Савета од 27. априла 2016. о заштити појединаца у вези с обрадом личних података и о слободном кретању таквих података, те стављању изван снаге Директиве 95/46/ЕЦ, којом се регулише заштита података и приватност лица унутар Европске уније, а доноси и прописе везане за изношење података у треће земље.

Главни циљеви ГДПР-а су вратити грађанима надзор над њиховим личним подацима и поједноставити регулаторно окружење за међународне компаније уједначавањем прописа у целој Унији.

Ова Уредба много већи акценат ставља на заштиту посебних категорија личних података:

- Расна припадност
- Национална припадност
- Религијска припадност
- Чланство у синдикатима
- Сексуална оријентација

Информације о здрављу (лични подаци који се односе на физичко и ментално здравље појединца, укључујући и пружање здравствених услуга)

Биометријски подаци (лични подаци добијени посебном техничком обрадом, у вези са физичким, физиолошким или карактеристикама понашања особе који омогућују или потврђују јединствену идентификацију те особе, нпр. слике лица или отисци прстију)

Генетски подаци (лични подаци који се односе на наслеђене или стечене генетске карактеристике особе који дају јединствене информације о физиологији или здрављу особе а добијени су анализом њеног биолошког узорка)

ПРИВАТНОСТ У СРБИЈИ

Право на приватност, као самостално и једно од основних људских права, није изричито зајемчено Уставом Републике Србије.

Међутим, имплементацијом поменутих међународних аката, одредбе које се тичу поштовања права на приватност постале су саставни део нашег позитивног права, а свој израз нашле су и у Уставу Републике Србије који, кроз неколико чланова, гарантује право на приватност појединаца тако што јемчи:

- неповредивост стана,
- право на тајност писама и других средстава комуницирања и
- заштиту података о личности.

Венецијанска комисија (Европска комисија за демократију права) под окриљем Савета Европе, разматрајући Устав Републике Србије је истакла како поменуте одредбе Устава које покривају различите аспекте права на приватност, иако посебно и у складу са савременим тенденцијама прокламују и право на заштиту података, ипак немају

изричито и опште јемство за поштовање приватног и породичног живота како је гарантовано чланом 8. Европске конвенције о људским правима.

СТОГА ЈЕ ЗАКЉУЧАК ВЕНЕЦИЈАНСКЕ КОМИСИЈЕ ДА ЧЛАН 8. ЕКЉП НИЈЕ У ПОТПУНОСТИ ИМПЛЕМЕНТИРАН УСТАВОМ

Људска права и слободе зајамчена Уставом Републике Србије:

Члан 23. – Достојанство и слободан развој личности

Члан 40. - Право на неповредивост стана

Чланом 41. - Право на тајност писама и других средстава општења

Члан 42 – Заштита података о личности

Члан 43. - Слобода мисли, савести и вероисповести

Члан 46. – Слобода мишљења и изражавања

Члан 48. – Подстицање уважавања разлика

Правна заштита приватности у Србији:

1. ЗАКОН О ЗАШТИТНИКУ ГРАЂАНА и тужба Уставном суду – уставно правна заштита
2. КРИВИЧНИ ЗАКОНИК – кривично правна заштита
3. Закон о облигационим односима и Закон о заштити података о личности – грађанско правна заштита
4. Закон о заштити података о личности – управно правна заштита

ЗАКОН О ЗАШТИТНИКУ ГРАЂАНА

Заштитник грађана, као независни државни орган, се стара о заштити и унапређењу људских и мањинских права и слобода.

Под појмом грађанин - подразумева се не само физичко лице које је домаћи држављанин, већ и страни држављанин и лице без држављанства, као и свако домаће или страно правно лице о чијим правима и обавезама одлучују органи управе.

Заштитник грађана:

- је овлашћен да контролише законитост и правилност рада органа управе, ради утврђивања да ли је њиховим актима, радњама или нечињењем дошло до кршења права грађана зајемчених Уставом, потврђеним међународним уговорима, општеприхваћеним правилима међународног права, законима, другим прописима и општим актима Републике Србије.
- није овлашћен да контролише рад Народне скупштине, председника Републике, Владе, Уставног суда, судова и јавних тужилаштава.
- може предузимати и процесне и друге радње у поступцима пред државним и другим органима и организацијама, када је за то овлашћен посебним прописима.

ПРИТУЖБУ:

- Заштитнику грађана може да поднесе свако физичко или правно лице, домаће или страно, које сматра да му је актом, радњом или нечињењем органа управе повређено људско или мањинско право и слобода.
- у име физичког лица, уз његову сагласност, може поднети удружење које се бави заштитом људских права.
- због повреде права детета могу поднети његов родитељ или старатељ, као и удружење које се бави заштитом права детета, уз сагласност родитеља или старатеља детета или уз сагласност детета старијег од десет година.

КРИВИЧНО-ПРАВНА ЗАШТИТА ПРИВАТНОСТИ У СРБИЈИ

- ПРОГАЊАЊЕ – чл. 138а КЗ
- НАРУШАВАЊЕ НЕПОВРЕДИВОСТИ СТАНА – чл. 139 КЗ
- НЕОВЛАШЋЕНО ПРИСЛУШКИВАЊЕ И СНИМАЊЕ – чл. 143 КЗ
- НЕОВЛАШЋЕНО ФОТОГРАФИСАЊЕ – чл. 144 КЗ
- Неовлашћено објављивање и приказивање туђег списа, портрета и снимка – чл. 145 КЗ
- Неовлашћено прикупљање личних података – чл. 146 КЗ
- Увреда – чл. 170 КЗ
- Изношење личних и породичних прилика – чл. 172 КЗ
- Повреда угледа – чл. 173 КЗ
- Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију – чл. 185 КЗ
- Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу – чл. 185б КЗ
- Превара – чл. 208 КЗ
- Изнуда – чл. 214 КЗ
- Уцена – чл. 215 КЗ

НЕМАТЕРИЈАЛНА ШТЕТА – Закон о облигационим односима

ОБЈАВЉИВАЊЕ ПРЕСУДЕ ИЛИ ИСПРАВКЕ - У случају повреде права личности суд може наредити, на трошак штетника, објављивање пресуде, односно исправке, или наредити да штетник повуче изјаву којом је повреда учињена, или што друго чиме се може остварити сврха која се постиже накнадом. – ЧЛ. 199 ЗОО

НОВЧАНА НАКНАДА – чл. 200 ЗОО

(1) За претрпљене физичке болове, за претрпљене душевне болове због умањења животне активности, наружености, повреде угледа, части, слободе или права личности, смрти блиског лица као и за страх суд ће, ако нађе да околности случаја, а нарочито јачина болова и страха и њихово трајање то оправдава, досудити правичну новчану накнаду, независно од накнаде материјалне штете као и у њеном одсуству.

(2) Приликом одлучивања о захтеву за накнаду нематеријалне штете, као и о висини њене накнаде, суд ће водити рачуна о значају повређеног добра и циљу коме служи та накнада, али и о томе да се њоме не погодује тежњама које нису спојиве са њеном природом и друштвеном сврхом.

ЗАКОН О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ

Осим пред Повереником, лица могу да остваре своје право на заштиту података о личности подношењем тужбе за заштиту права месно надлежном вишем суду на територији Републике Србије сагласно члану 84. ЗЗПЛ-а, као и подношењем тужбе за накнаду штете сагласно члану 86. истог закона.

Лице на које се односе подаци који се обрађују има право на заштиту пред парничним судом ако сматра да су му радњом обраде повређена права прописана Законом. Поступак заштите покреће се подношењем тужбе против руковаоца, односно обрађивача и то вишем суду на чијој територији тужени има пребивалиште, боравиште или седиште. Тужба се може поднети и суду на чијој територији тужилац има пребивалиште или боравиште, осим ако се тужба подноси против органа власти. Ревизија правноснажне одлуке донете по парничној тужби је увек допуштена.

Закон прописује садржину тужбених захтева који се могу истаћи у поступку пред судом. Ови захтеви се тако односе на давање прописаних информација, исправку, допуну, односно брисање података, ограничавање обраде, давање и преношење података у структурисаном облику и прекид обраде. Ако се ради о одлуци која је донета на основу аутоматизоване обраде података, односно профилисању, тужбом се може захтевати и само утврђивање да је дошло до повреде законских одредаба.

Такође, тужбом се може захтевати и накнада материјалне и нематеријалне штете која је проузрокована повредом Закона.

По правилу, одговорност за штету лежи на руковаоцу. Обрађивач одговара за штету само у случају кад се утврди да није поступао у складу са законским обавезама које се односе само на њега или да није поступао у складу са упутствима руковаоца. Лице на које се односе подаци који се обрађују има право да овласти представника удружења које се бави заштитом права и слобода у области заштите података о личности да га заступа у парничном поступку. Поједина питања заступања и пружања других облика правне помоћи на које се ово правило односи уређују се законом којим се уређује пружање бесплатне правне помоћи.

УПРАВНО-ПРАВНА ЗАШТИТА У СРБИЈИ

ЗАКОН О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ – тужба управном суду

Транспарентност и начин остваривања права – чл. 21, Ограничење права на приступ – чл. 28, Остваривање права лица на које се односе подаци када обраду врши надлежни органу посебне сврхе и провера Повереника – чл. 35,

Предвиђају право на тужбу суду, односно покретање управног спора против одлуке Повереника.

НОРМАТИВНО УРЕЂЕЊЕ ПОДАТАКА

ПРАВНИ АСПЕКТИ ИЛИ НОРМАТИВНА ПИРАМИДА

Политички систем (модел)

дефинише се као целина оних државних и недржавних институција и актера, правила и процедура који су укључени у текуће процесе формулисања и решавања политичких проблема и у производњу и спровођење општеобавезујућих политичких одлука у дефинисаним оквирима политичке структуре.

Систем власти (уређење власти, government)

- институције, њихова овлашћења и правила рада

Политички процес (учесници-актери, politics)

- грађани, политичке странке, интересне групе, канали и токови утицаја

Доношење политичких одлука и њихово спровођење

- области јавне политике (policy-making)

ПРАВНИ СИСТЕМ

- скуп међусобно усклађених правила која важе у једној држави.

ПРАВНИ ПОРЕДАК

- представља понашање које је у складу са сти правилима (прописима).

Правни систем у Републици Србији

Представља систем кодификованих, одн. писаних норми које уређују сферу јавног и приватног живота у Републици Србији. Њега чине Устав Републике Србије донет 2006. године, као највиши и најважнији правни акт, као и читав систем закона који регулишу све области друштвеног живота у Републици Србији.

1. МЕЂУНАРОДНИ И УСТАВНИ ОКВИРИ
2. ПОЛИТИКЕ, СТРАТЕГИЈЕ, ДОКТРИНЕ
3. СИСТЕМСКИ ЗАКОНИ, МЕЂУНАРОДНИ СПОРАЗУМИ (СТАНДАРДИ – НОРМАТИВНИ, ТЕХНИЧКИ, ИНФОРМАТИЧКИ, ОРГАНИЗАЦИОНИ...)
4. ПОДЗАКОНСКИ АКТИ – УРЕДБЕ, ПРАВИЛНИЦИ, УПУТСТВА, ИНСТРУКЦИЈЕ, ОДЛУКЕ, ЗАКЉУЧЦИ ....
5. ИНТЕРНИ АКТИ ИЛИ НОРМАТИВА – ДИРЕКТИВЕ, ПЛАНОВИ, ОДЛУКЕ, СМЕРНИЦЕ...

ОБЛИГАТОРНИ (Обавезујући) – на основу: ресорних/секторских прописа, прописа о државној управи, прописа о јавним набавкама, прописа о ППЗ, прописа о подацима (тајним и личним), план интегритета (корупција), информатор о раду (слободан

приступ информацијама), акт о безбедности ИКТ система (информациона безбедност)…

АЛТЕРНАТИВНИ (необавезујући) – на основу: стандарда ISO 27001, режим уласка и изласка, етичких кодекса (професионална тајна), прописа о пословној тајни…

Непостојање интерних аката прекршај или кумулативно кривично дело…

ПРОБЛЕМ: Третман од стране управних и парничних судова?

УСТАВ РЕПУБЛИКЕ СРБИЈЕ

- Правни поредак Републике Србије је јединствен.
- Устав је највиши правни акт Републике Србије.
- Сви закони и други општи акти донети у Републици Србији морају бити сагласни са Уставом.
- Потврђени међународни уговори и општеприхваћена правила међународног права део су правног поретка Републике Србије. Потврђени међународни уговори не смеју бити у супротности са Уставом.
- Закони и други општи акти донети у Републици Србији не смеју бити у супротности са потврђеним међународним уговорима и општеприхваћеним правилима међународног права.
- Сви подзаконски општи акти Републике Србије, општи акти организација којима су поверена јавна овлашћења, политичких странака, синдиката и удружења грађана и колективни уговори морају бити сагласни закону.
- Статути, одлуке и сви други општи акти аутономних покрајина и јединица локалне самоуправе морају бити сагласни са законом.
- Сви општи акти аутономних покрајина и јединица локалне самоуправе морају бити сагласни њиховим статутима.

УСТАВ И ЗАКОН О НАРОДНОЈ СКУПШТИНИ – доноси законе и друге опште акте, Стратегију одбране;

УСТАВ И ЗАКОН О ВЛАДИ – доноси опште и појединачне правне акте;

Закон о планском систему Републике Србије

1) **Јавне политике** - правци деловања Републике Србије и правци деловања аутономне покрајине и јединице локалне самоуправе (локална власт), у одређеним областима, ради постизања жељених циљева на нивоу друштва;
2) Плански систем - скуп елемената планирања, који чине:

- планска документа;
- учесници у планском систему;
- процес управљања системом јавних политика;
- процес усаглашавања садржаја планских докумената са садржајем других планских докумената и прописа;
- повезивање процеса усвајања и спровођења јавних политика са процесом средњорочног планирања;

Плански документ јесте акт којим учесник у планском систему поставља циљеве, утврђује приоритете јавних политика, односно планира мере и активности за њихово достизање, у оквирима својих надлежности и у вези са својим функционисањем.

Врсте планских докумената су:

1) документи развојног планирања;
2) документи јавних политика, и
3) остали плански документи.

Документ јавних политика јесте плански документ којим учесници у планском систему, у складу са својим надлежностима, утврђују или разрађују већ утврђене јавне политике.

Врсте докумената јавних политика јесу:

1) стратегија;
2) програм;
3) концепт политике, и
4) акциони план.

Стратегијски оквир представљају:

- Стратегија националне безбедности
- Стратегија одбране
- Национална стратегија заштите и спасавања
- Стратегија развоја електронских комуникација
- Стратегија развоја информационог друштва
- Стратегија развоја електронске управе
- Стратегија информационе безбедности
- СТРАТЕГИЈА ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ

Законска регулатива која се бави овом материјом заокружена је усвајањем:

- Закона о слободном приступу информацијама од јавног значаја
- Закона о заштити података о личности
- Закона о тајности података
- Закон о информационој безбедности
- Закон о заштити пословне тајне/Закон о привредним друштвима
- одређеног броја уредби
- АУТОНОМНО ИЛИ УНУТРАШЊЕ ПРАВО?

Закон о тајности података

Овим законом уређује се јединствен систем одређивања и заштите тајних података који су од интереса за националну и јавну безбедност, одбрану, унутрашње и спољне послове Републике Србије, заштите страних тајних података, приступ тајним подацима и престанак њихове тајности, надлежност органа и надзор над спровођењем овог закона, као и одговорност за неизвршавање обавеза из овог закона и друга питања од значаја за заштиту тајности података.

Закон о слободном приступу информацијама од јавног значаја

Овим законом уређују се права на приступ информацијама од јавног значаја којима располажу органи јавне власти, ради остварења и заштите интереса јавности да зна и остварења слободног демократског поретка и отвореног друштва.

Закона о заштити података о личности

Овим законом уређује се 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.

Овим законом уређује се и право на заштиту физичких лица у вези са обрадом података о личности коју врше надлежни органи у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности, као и слободни проток таквих података.

Закон о заштити пословне тајне

Овим законом уређује се правна заштита пословне тајне од незаконитог прибављања, коришћења и откривања.

ПОСЛОВНА ТАЈНА ЈЕ КАТЕГОРИЈА ИНТЕЛЕКТУАЛНЕ СВОЈИНЕ

Закон о заштити пословне тајне

- Правна заштита пословне тајне од радњи нелојалне конкуренције
- “LEX SPECIALIS” у односу на Закон о парничном поступку и Закон о облигационим односима
- Грађанско-правна заштита пословне тајне (тужба, привремена мера, обезбеђење доказа...)
- **Категорија пословне тајне која у себи садржи податак од интереса за Републику Србију (тајни податак)**

Чл. 72 Закона о привредним друштвима из 2011. (примењује се од 01.02.2012.):
МАТЕРИЈАЛНА ДЕФИНИЦИЈА - пословна тајна је податак чије би саопштавање трећем лицу могло нанети штету друштву, као и податак који има или може имати економску вредност зато што није опште познат, нити је лако доступан трећим лицима која би његовим коришћењем или саопштавањем могла остварити економску корист и који је од стране друштва заштићен одговарајућим мерама у циљу чувања његове тајности.
ФОРМАЛНА ДЕФИНИЦИЈА - Пословна тајна је и податак који је законом, другим прописом или актом друштва одређен као пословна тајна.

Матичне књиге и регистри - У зависности од надлежности одређених органа јавне власти (јурисдикције), примери јавних евиденција укључују информације које се односе на:

- Матичне књиге рођења, смрти, бракове, држављанства...
- Катастар непокретности
- Регистар политичких странка

- Регистар управних округа и локалне самоуправе
- Јединствени бирачки списак
- Централни регистар становништва
- Судски регистри – вођење истрага...
- Пореске евиденције
- Питање приступа – административни поступак за који се плаћа такса

Питање јавних регистара – ЈАВНО ДОСТУПНИ ЛИЧНИ ПОДАЦИ?

- Регистри имовине и прихода јавних функционера – Агенција за борбу против корупције
- Е-Катастар непокретности – Републички геодетски завод
- Регистри Агенције за привредне регистре (привредна друштва, предузетници, заложно право, медији, удружење, стечајне масе, факторинг, спортска удружења…)
- Регистри Министарства финансија (корисника буџетских средстава, евидентирани ПДВ обвезници, пореске пријаве…)
- Регистри адвоката, судских вештака, лекара, стечајних управника…

РЕГИСТРИ СА ПРИСТУПОМ И СА ОГРАНИЧЕНИМ ПРИСТУПОМ (плаћање таксе?)

РАД СА ТАЈНИМ ПОДАЦИМА

ЗАКОН О ТАЈНОСТИ ПОДАТАКА – подзаконски акти

- УРЕДБА о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА” и „СТРОГО ПОВЕРЉИВО” - "Службени гласник РС", број 46 од 24. маја 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у органима јавне власти - "Службени гласник РС", број 79 од 29. јула 2014.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Министарству одбране - "Службени гласник РС", број 66 од 29. јуна 2014.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Министарству унутрашњих послова "Службени гласник РС", број 105 од 29. новембра 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Безбедносно-информативној агенцији "Службени гласник РС", број 70 од 7. августа 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Канцеларији Савета за националну безбедност и заштиту тајних података "Службени гласник РС", број 86 од 30. септембра 2013.
- УРЕДБА о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа "Службени гласник РС", број 63 од 19. јула 2013.
- УРЕДБА о посебним мерама физичко-техничке заштите тајних података "Службени гласник РС", број 97 од 21. децембра 2011.
- УРЕДБА о посебним мерама надзора над поступањем са тајним подацима „Службени гласник РС“, број 90 од 30. новембра 2011.
- УРЕДБА о посебним мерама заштите тајних података у информационо-телекомуникационим системима "Службени гласник РС", број 53 од 20. јула 2011.
- УРЕДБА о начину и поступку означавања тајности података, односно докумената "Службени гласник РС", број 8 од 11. фебруара 2011.
- УРЕДБА о садржини, облику и начину вођења евиденција за приступ тајним подацима "Службени гласник РС", број 89 од 29. новембра 2010.

- УРЕДБА о садржини, облику и начину достављања сертификата за приступ тајним подацима „Службени гласник РС“, број 54 од 4. августа 2010.
- УРЕДБА о увећању плате државних службеника и намештеника који обављају послове у вези са заштитом тајних података у Канцеларији Савета за националну безбедност и заштиту тајних података и Министарству правде "Службени гласник РС", број 79 од 29. октобра 2010.
- УРЕДБА о обрасцима безбедносних упитника "Службени гласник РС", број 30 од 07. маја 2010.
- ПРАВИЛНИК о службеној легитимацији и начину рада лица овлашћених за вршење надзора "Службени гласник РС", бр. 85 од 27. септембра 2013, 71 од 11. јула 2014.

Стратегија националне безбедности

Стратегија одбране

- Закон о основама уређења служби безбедности
- Закон о одбрани и Закон о Војсци
- Закон о полицији
- Закон о спољним пословима
- Закон о Безбедносно-информативној агенцији
- Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији
- Законик о кривичном поступку и Кривични законик
- Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције
- Закон о државним службеницима
- Закон о информационој безбедности
- Закон о јавним набавкама и Уредба о јавним набавкама у области одбране и безбедности "Службени гласник РС", број 93 од 1. јула 2020.
- Закон о електронским комуникацијама
- Закон о пореском поступку и пореској администрацији
- Закон о заштити узбуњивача
- Закон о приватном обезбеђењу

НА ОСНОВУ ЧЛ. 102. ЗАКОНА О ОДБРАНИ

- **УРЕДБА о подацима и пословима значајним за систем одбране који се морају чувати и штитити у складу са законом којим се уређује заштита тајности података и о критеријумима за попуну радних места на којима се ти задаци и послови обављају** "Службени гласник РС", број 8 од 31. јануара 2020.

РАД СА ЛИЧНИМ ПОДАЦИМА

Општа уредба о заштити података о личности ЕУ 2016/679 од 27. априла 2016. године

Стратегија заштите података о личности за период од 2023. до 2030. године "Службени гласник РС", број 72 од 31. августа 2023.

Закон о заштити личних података – подзаконски акти

- УРЕДБА о обрасцу за вођење евиденције и начину вођења евиденције о обради података о личности “Службени гласник РС” број 50 од 10. јула 2009.
- ПРАВИЛНИК о начину претходне провере радњи обраде података о личности "Службени гласник РС", број 35 од 12. маја 2009.
- ПРАВИЛНИК о обрасцу и начину вођења интерне евиденције о повредама Закона о заштити података о личности и мерама које се у вршењу инспекцијског надзора предузимају "Службени гласник РС", број 40 од 7. јуна 2019.
- ПРАВИЛНИК о обрасцу и начину вођења евиденције лица за заштиту података о личности "Службени гласник РС", број 40 од 7. јуна 2019.
- ПРАВИЛНИК о обрасцу притужбе "Службени гласник РС", број 40 од 7. јуна 2019.
- ПРАВИЛНИК о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности "Службени гласник РС", број 40 од 7. јуна 2019.
- ПРАВИЛНИК о обрасцу и начину вођења евиденције лица за заштиту података о личности "Службени гласник РС", број 40 од 7. јуна 2019.
- Закон о држављанству Републике Србије
- Закон о матичним књигама
- Закон о електронској управи
- Закон о пореском поступку и пореској администрацији
- Закон о поступку уписа у катастар непокретности и катастар инфраструктуре

- Закон о војној, радној и материјалној обавези
- Закон о банкама
- Закон о осигурању
- Закон о полицији
- Закон о евиденцијама и обради података у области унутрашњих послова
- Закон о спречавању корупције
- Закон о здравственој заштити
- Закон о здравственој документацији и евиденцијама у области здравства
- Закон о пензијском и инвалидском осигурању
- Закон о детективској делатности
- Закон о приватном обезбеђењу
- Закон о заштити потрошача
- Закон о заштити узбуњивача
- Закон о државним службеницима
- Закон о раду
- Закон о евиденцијама у области рада
- Закон о електронским комуникацијама

ОБРАДА ЛИЧНИХ ПОДАТАКА, ПОРЕД НАВЕДЕНИХ НАЛАЗИ СЕ ЈОШ У ЧИТАВОМ НИЗУ ПРОПИСА....

РАД СА ПРОФЕСИОНАЛНОМ ТАЈНОМ

- Закон о црквама и верским заједницама – члан 8. «Свештеник не може бити позван да сведочи о чињеницама и околностима које је сазнао приликом исповести.»
- Кодекс професионалне етике адвоката
- Кодекс медицинске етике Лекарске коморе Србије
- Кодекс новинара Србије

КАТЕГОРИЈЕ И КЛАСИФИКАЦИЈА ПОДАТАКА

КЛАСИФИКАЦИЈА ПОДАТАКА

Заштићени подаци су општи термин за податке који се не сматрају за јавне, односно који треба да буду заштићени из било ког разлога, на основу закона или уговора, као и ради заштите људских слобода и права (право на приватност).

- Представља поступак разврставања и категоризације података у различите врсте, облике или било коју засебну класу.
- Омогућава одвајање и разврставање података према захтевима скупова података за различите државне, пословне или личне циљеве.
- То је углавном поступак управљања подацима.

Класификација – Одвајање података у различите категорије:

- Подаци од интереса за Р. Србију (тајни подаци)
- Лични подаци
- Пословне тајне
- Професионалне тајне
- Јавни подаци
- Архивска грађа

РАЗЛИКОВАЊЕ ТАЈНОГ ПОДАТКА ОД ДРУГИХ ВРСТА ПОДАТАКА

(личног податка, пословне тајне, професионалне тајне...)

Основна разлика је у:

- **законским основима** за одређивање режима заштите ових података и области у којој настаје штета (имовинска – стварна штете и изгубљена добити и неимовинска – нематеријална и морална)...
- **критеријуми** за одређивање заштите тајности су различити.... (ШТЕТА? – по интересе Р. Србије, уставна права грађанина – приватност, имовину – интелектуалну и материјалну…)
- **одговорност** за непоштовање обавезе чувања тајности је различита... (кривично дело, прекршај, повреда радне дисциплине...)

КРИТЕРИЈУМИ И ШТЕТА КОД ТАЈНИХ ПОДАТАКА

- **ДРЖАВНА ТАЈНА** – неотклоњива тешка штета
- **СТРОГО ПОВЕРЉИВО** – тешка штета
- **ПОВЕРЉИВО** – штета
- **ИНТЕРНО** – штета за рад, обављање задатака и послова органа јавне власти

ПРОЦЕНА ШТЕТЕ

- КО ЈЕ ВРШИ?
- НА КАКАВ НАЧИН?
- ПОСТОЈИ ЛИ МЕТОДОЛОГИЈА?
- ПИТАЊЕ ПОСЛЕДИЦА?

ПИТАЊЕ: ПРАВНА ИЛИ БЕЗБЕДНОСНА ПРОЦЕНА?

КАТЕГОРИЈЕ ПОДАТАКА

- Подаци од интереса за Р. Србију
- Подаци значајни за безбедност и одбрану...
- Задаци и послови од посебног значаја за одбрану
- Подаци о судским и другим поступцима
- Подаци о личности
- Подаци о производима (патенти, технологије, материјали...)
- Подаци о правним лицима...
- Пословне тајне + банкарске тајне
- Професионалне тајне...
- Подаци о критичној инфраструктури – енергетици, саобраћају, производњи хране…
- Јавни подаци доступни преко интернета…

Отворени подаци представљају концепт у коме одређени подаци треба да буду слободно доступни свима, на коришћење и поновну употребу, без ауторских или било каквих других ограничења.

Информација од јавног значаја је информација којом располаже орган јавне власти, настала у раду или у вези са радом органа јавне власти, садржана у одређеном документу, а односи се на све оно о чему јавност има оправдан интерес да зна.

Пословна тајна је податак који може имати економску вредност зато што није опште познат, нити је лако доступан трећим лицима која би његовим коришћењем или саопштавањем могла остварити економску вредност.

Информације које се штите као пословна тајна - финансијски, економски, пословни, научни, технички, технолошки, производни подаци, студије, тестови, резултати истраживања, укључујући и формулу, цртеж, план, пројекат, прототип, код, модел, компилацију, програм, метод, технику, поступак, обавештење или упутство интерног карактера и слично, без обзира на који начин су сачувани или компилирани

Пословна тајна – КРИТЕРИЈУМИ:

- Врста и структура основних и обртних средстава
- Производни капацитети и број запослених
- Производни и перспективни планови
- Стање залиха сировина и готових производа
- Стање кредита
- Калкулација цена
- Утврђивање услова у понудама пре конкурса
- Купопродајни уговори са домаћим и страним партнерима
- Технолошки процеси производње
- Финансијски резултати пословања
- Усвајање нове производње по лиценци
- Планови осигурања и обезбеђења правног лица, компаније, установе
- Нова техничка решења
- Нацрти, модели и остала документација која није заштићена патентом
- Сви други подаци који су означени као тајни на основу одлуке државног органа или правног лица (У ПРАКСИ ТАЈНИ И ЛИЧНИ ПОДАЦИ – ПОСЛОВНА ТАЈНА?)

Банкарска тајна је врста пословне тајне, која у себи садржи и професионалну тајну и лични податак:

- општи акти банке, уговори које она закључује са својим пословним партнерима, уговори о раду са запосленима у банци па у неким случајевима и уговори које банка закључује са својим клијентима.
- предмет заштите банкарском тајном су подаци до којих банка долази у пословању са клијентима док предмет заштите пословном тајном (банке) могу бити и неки други подаци везани за пословање као што су рецимо пословни планови и стратегије, висина зарада запослених и слично.

Професионална тајна односи се на све што професионалац у контакту са клијентом сазна, о личном или породичном животу, а што не сме бити доступно другим особама, посебно оним од којих клијенти могу имати штете или трпети последице.

Посебно је неопходна у професијама које раде са особама изражених психолошких, психопатолошких или социјалних проблема. Професионална тајна у себи садржи личне податке повезане са правилима струке, односно представља тумачење одређених личних и других података правилима струке. Регулише се посебним кодексима уз стриктну обавезу чувања професионалне тајне са евентуалним изузецима за које морају постојати веома важни разлози или судски налог.

Лекарска тајна, је обавеза сваког лекара да по сазнању неких чињеница кроз анамнезу, објективни преглед и остала испитивања и лечење о болеснику, чува непрекидно као тајну. Сматра се да је лекарска тајна пре свега име и презиме болесника и болест од које он болује.

Адвокат има обавезу и право да све што чује од свог клијента третира као тајну (ТАЈНИ ПОДАТАК, ПОСЛОВНУ ТАЈНУ, ПРОФЕСИОНАЛНУ ТАЈНУ ИЛИ ПОДАТАК О ЛИЧНОСТИ) и није обавезан да је икоме саопшти. Из тог разлога се адвокат не може увек позивати као сведок, а адвокатске канцеларије имају посебан статус.

АРХИВСКА ГРАЂА

Представља изворни, репродуковани, писани, цртани, дигитализовани, штампани, фотографисани, филмовани, микрофилмовани, фонографисани или на други начин забележени документарни материјал. Архивска грађа је културно наслеђе од општег интереса за Републику Србију и као таква ужива посебну заштиту утврђену законом којим се уређује заштита културних добара.

ЈАВНА АРХИВСКА ГРАЂА из периода:

- српске државе у XIX веку (кнежевина Србија, Краљевина Србија...)
- Краљевине СХС, Краљевине Југославије

- Другог светског рата
- ДФЈ, ФНРЈ и СФРЈ – Социјалистичке Републике Србије...
- СРЈ и ДЗ СЦГ
- Републике Србије
- Посебна проблематика коју покрива Војни архив

ПРИВАТНА АРХИВСКА ГРАЂА

Је градиво настало радом и деловањем физичких и правних лица, које није настало у обављању јавних овлашћења и јавне службе и није у власништву републике србије и јединица локалне и подручне самоуправе, односно правних лица чији је оснивач држава.

ОЗНАКЕ ПОДАТАКА КОЈЕ НЕДОСТАЈУ У РЕПУБЛИЦИ СРБИЈИ

Ознака **Unclassified** не представља, у техничком смислу, степен тајности, већ карактеристику неких режима за одређивање тајности; користи се за означавање државних докумената који не испуњавају критеријуме за доделу одређеног степена тајности, односно докумената са којих је скинут степен тајности. Ови документи се штите процедурама „ограничене дистрибуције“.

OFFICIAL – Ова ознака се користи за све редовне послове, активности и услуге које се врше у јавном сектору. Много државних ресора и органа функционише користећи искључиво овај степен.

PROTECT – Неовлашћено објављивање тих података узроковало би неприлике лицима, финансијски губитак или неоправдану материјалну корист, довело у питање истрагу или олакшало извршење кривичног дела, ставило владу у неповољан положај приликом вођења преговора трговинске или политичке природе. Ознаку PROTECT треба увек користити са дескрипторима, као што су: “Commercial”/Трговински, “Management”/Управљање, “Personal”/ Лични или слични термин.

Термин **For Official Use Only (FOUO)**, у преводу „Само за службену употребу“ је безбедносна назнака (десигнација) коју примењују неке државне администрације.

Службена употреба подразумева **употребу од стране запосленог, заступника или овлашћеног представника владе или једног од њених уговарача током трајања радног односа, заступања или представљања**.

Осетљиви подаци (**Sensitive information**) су подаци или сазнања који би могли резултирати губитком одређене предности или степена безбедности, уколико би били откривени другим лицима која могу бити непријатељски настројена или чија је поузданост мала или непозната. Губитак, злоупотреба, измена или неовлашћени приступ осетљивим подацима може се негативно одразити на приватност неког лица, пословних тајни одређеног пословног субјекта или чак на безбедност,

унутрашње и спољне послове одређене државе у зависности од степена осетљивосати и природе тих података.

Дефиниција Law Enforcement Sensitive (LES)/Осетљиво – само за полицијске службе – ова назнака није намењена за податке који су чисто административне природе или потичу из јавног извора. Користи се у случају када „би се могло очекивати да би неовлашћено откривање, измена или уништавање таквих података могло нанети штету активностима полицијских служби тако што би угрозило истраге, компромитовало операције, или изазвало ситуације које доводе у опасност животе поверљивих доушника, сведока или агената“.

Сматрају се осетљивим подацима без ознаке тајности чије би откривање нанело штету активностима полицијских органа или угрозило њихове истраге или операције.

ТАЈНИ И ЛИЧНИ ПОДАЦИ

Политика националне безбедности јесте део укупне државне политике и представља скуп ставова, начела и опредељења којима се усмерава одлучивање и деловање Републике Србије ради заштите и остварења националних интереса.

Политика националне безбедности спроводи се предузимањем свеобухватних и усклађених мера у различитим областима друштвеног живота.

(Стратегија националне безбедности)

Основни категоријални концепти безбедности

- Индивидуална
- Национална
- Регионална
- Глобална

Сектори безбедности

- Економска безбедност
- Социјетална безбедност
- Енергетска безбедност
- Политичка безбедност
- Еколошка безбедност
- Војна безбедност

Систем националне безбедности и заштита тајних података представљају два концепта који се узајамно преплићу. Систем националне безбедности представља материјални (суштински) део.

ПОДАТАК ОД ИНТЕРЕСА ЗА РЕПУБЛИКУ СРБИЈУ ИЛИ ТАЈНИ ПОДАТАК

1) **податак од интереса за Републику Србију** је сваки податак или документ којим располаже орган јавне власти, који се односи на територијални интегритет и суверености, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње послове и спољне послове;

2) **тајни податак** је податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређен и означен одређеним степеном тајности;

Као тајни податак може се одредити податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета, ако је потреба заштите интереса Републике Србије претежнија од интереса за слободан приступ информацијама од јавног значаја, односе се нарочито на:

1) националну безбедност Републике Србије, јавну безбедност, односно на одбрамбене, спољнополитичке, безбедносне и обавештајне послове органа јавне власти;

2) односе Републике Србије са другим државама, међународним организацијама и другим међународним субјектима;

3) системе, уређаје, пројекте, планове и структуре који су у вези са подацима из тач. 1) и 2) овог става;

4) научне, истраживачке, технолошке, економске и финансијске послове који су у вези са подацима из тач. 1) и 2) овог става.

Закон о одбрани чл. 102 – мере заштите тајних података

Тајни подаци који се односе на систем одбране означени као подаци од интереса за националну безбедност Републике Србије, као и тајни подаци настали у раду команди, јединица и установа Војске Србије, чијим би откривањем неовлашћеним лицима настала штета, штите се у складу са законом којим се уређује заштита тајности података и не могу се учинити доступним јавности.

Тајним подацима значајним за систем одбране сматрају се:

1) подаци и документа од значаја за систем националне безбедности, чијим би откривањем неовлашћеним лицима могла настати штета по интересе и циљеве у области одбране;

2) подаци о плановима употребе Војске Србије, ратној организацији и формацији команди, јединица и установа Војске Србије, подаци о борбеним и другим материјалним средствима, односно врстама покретних ствари намењених потребама одбране, чијим би откривањем неовлашћеним лицима могла настати штета по оперативну и функционалну способност Војске Србије;

3) подаци о патентима значајним за одбрану земље и средствима и уређајима намењеним одбрани који су у процесу усвајања и испитивања;

4) подаци о војним објектима и другим непокретностима значајним за одбрану земље, изузев података који су према прописима о заштити животне средине неопходни за процену утицаја на животну средину;

5) подаци о предузетим мерама, радњама и поступцима садржани у одлукама, наређењима, саопштењима и другим актима у области одбране земље, чије би откривање нанело штету интересима снага одбране.

МАТЕРИЈАЛНИ ЕЛЕМЕНТИ – садржина, основи критеријума чл. 2, 8 и 14. ЗТП

ФОРМАЛНИ ЕЛЕМЕНТИ – облик испољавања, ознака тајности чл. 13 ЗТП + Уредба о начину и поступку означавања тајности података, односно докумената; Уредба о ближим критеријумима за одређивање степена тајности ДРЖАВНА ТАЈНА и СТРОГО ПОВЕРЉИВО...

КРИТЕРИЈУМИ ЗА ОДРЕЂИВАЊЕ ТАЈНИХ ПОДАТАКА „ДРЖАВНА ТАЈНА“

Тајни податак из Уредбе о ближим критеријумима за одређивање степена тајности Државна тајна и Строго поверљиво, може се одредити и означити степеном тајности „ДРЖАВНА ТАЈНА” ако би његовим откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала неотклоњива тешка штета по интересе Републике Србије, која за последицу може имати:

1) непосредно и изузетно озбиљно угрожавање територијалног интегритета и суверености Републике Србије;

2) непосредно и изузетно озбиљно угрожавање уставног поретка и демократских принципа Републике Србије;

3) масован губитак људских живота или изузетно озбиљну претњу по живот или здравље људи или имовину великог обима;

4) изузетно озбиљну и дугорочну штету по економске интересе Републике Србије;

5) изузетно озбиљно угрожавање националне и јавне безбедности, одбране или активности безбедносних и обавештајних служби;

6) изузетно озбиљно угрожавање интереса кривичног гоњења, сузбијања кривичних дела и функционисања правосуђа;

7) изузетно озбиљно угрожавање оперативних и функционалних способности Војске Србије и других снага одбране Републике Србије;

8) изузетно озбиљно угрожавање међународног положаја Републике Србије и сарадње са другим државама, међународним организацијама и другим међународним субјектима.

КРИТЕРИЈУМИ ЗА ОДРЕЂИВАЊЕ ТАЈНИХ ПОДАТАКА НА ОСНОВУ ПРОПИСА О ОДБРАНИ

Подаци значајни за систем одбране који се морају чувати и штитити у складу са законом којим се уређује заштита тајности података су:

1) подаци садржани у војним, економским и другим проценама, на којима се заснива политика Републике Србије;
2) подаци садржани у Плану одбране Републике Србије;
3) подаци садржани у плановима употребе Војске Србије;
4) подаци о оперативним и функционалним способностима Министарства одбране и Војске Србије, као и других органа, предузећа и правних лица када су у функцији одбране;
5) подаци садржани у актима о организацији и формацији Војске Србије;
6) подаци садржани у плановима и програмима развоја за јавна предузећа, привредна друштва и друга правна лица која су од посебног значаја за одбрану земље;
7) подаци о врсти, укупној количини и размештају робних резерви Републике Србије и капацитетима и могућностима ратне производње;
8) подаци садржани у анализама и оценама стања припрема за одбрану Републике Србије;
9) подаци садржани у плановима припрема и уређења државне територије за потребе одбране земље;
10) подаци о војним објектима и објектима који су одлуком надлежног органа одређени као објекти од посебног значаја за одбрану земље (локација, назив, структура, опремљеност и други подаци који би у ратном и ванредном стању били од посебног значаја за одбрану земље);
11) подаци о научним, техничким и технолошким проналасцима који су од посебног значаја за одбрану земље;
12) подаци о средствима и уређајима намењеним одбрани земље, који су у процесу усвајања и испитивања;
13) подаци садржани у проценама, анализама и појединим мерама државних органа, који су од посебног значаја за одбрану земље;

14) подаци који се односе на организацију телекомуникационо-информационих система у миру и рату, планове и средства за криптозаштиту, као и подаци који се односе на прописане норме и поступке спровођења криптозаштите;

15) подаци који се односе на ратну организацију државних органа;

16) подаци садржани у мобилизацијским плановима јавних предузећа, привредних друштава и других правних лица која су од посебног значаја за одбрану земље;

17) подаци садржани у плановима организације безбедносно-обавештајних служби, оперативни подаци служби безбедности у вези са контраобавештајном и безбедносном заштитом и обавештајни подаци и подаци у вези са њима;

18) подаци Војне полиције о обављању послова сузбијања криминалитета, обезбеђења одређених личности, најзначајнијих војних објеката, докумената и наоружања и подаци у вези са њима;

19) подаци садржани у безбедносним проценама и подаци садржани у документима донетим у складу са безбедносним проценама;

20) подаци о материјалним средствима намењеним потребама одбране;

21) подаци који проистекну из истраживања геолошког састава земљишта, геомагнетизма, хидролошких карактеристика терена, који су од посебног значаја за одбрану земље;

22) подаци садржани у анализама и оценама стања припрема за одбрану јединица локалне самоуправе, појединих државних органа и других правних лица;

23) подаци садржани у инспекцијским извештајима са обилазака о стању одбрамбених припрема;

24) прописи о раду државних органа, привредних друштава и других правних лица за време ратног и ванредног стања;

25) подаци о дужностима и радним и формацијским местима значајним за одбрану земље;

26) подаци о организацији, формацији и структури војнотериторијалних органа и јединица;

27) подаци садржани у картографским публикацијама који су од интереса за одбрану земље;

28) аерофото снимци подручја значајних за одбрану;

29) подаци о укупној структури кадра и њиховом распореду на ратне дужности;

30) подаци о врстама и капацитетима природних и вештачких склоништа за заштиту становништва и материјалних добара у рату;

31) подаци о предузетим мерама и спроведеним радњама и поступцима, на основу одлука, наређења, саопштења и других аката којима се регулише област одбране земље, а чијим откривањем би се могла нанети штета по интересе Републике Србије и снагама одбране земље;

32) други подаци који су од стране надлежног органа утврђени као подаци од значаја за систем одбране.

Послови од посебног значаја за систем одбране које у државним органима, предузећима и другим правним лицима треба штитити применом посебних мера безбедности - чл. 3 Уредбе је предвиђено 10 категорија...

ТАЈНОСТ ПОДАТАКА ЈЕ УВЕК УСЛОВЉЕНА

- Која врста података је у питању?
- Под каквим околностима?
- Колико дуго се морају чувати (максимално)?

ОПОЗИВ ТАЈНОСТИ

- Окончањем правног посла или реализацијом неког догађаја...
- У периодичној процени....
- На предлог...
- У поступку вршења контроле...
- На основу одлуке надлежног органа...
- У јавном интересу (питање посебно интересантно у пракси...)
-

ПРОБЛЕМ У ПРАКСИ - ТАЈНИ ПОДАТАК (ОРГАН ЈАВНЕ ВЛАСТИ)

Орган јавне власти је државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, као и правно лице које оснива државни орган или се финансира у целини, односно у претежном делу из буџета, а који поступа са тајним подацима, односно који их ствара, прибавља, чува, користи, размењује или на други начин обрађује;

ТУМАЧЕЊЕ чл. 2. т. 7 ЗТП – даје Министарство правде

Људске слободе и права и заштита личних података представљају два концепта који се узајамно преплићу.

Људске слободе и права (приватност) представљају материјални (суштински) део.

ПОДАЦИ О ЛИЧНОСТИ

- **„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;

- **Теоријски** – представљају карактеристичну особину одређеног људског бића, односно сваку информацију која се односи на физичко лице, које се у неком тренутку може идентификовати.

- **EU GDPR (Закон о заштити података о личности)** – сви подаци који се односе на физичко лице чији је идентитет одређен или се може одредити.
- **лични живот** – старост, висина, тежина, тен, облик тела...
- **јавни живот** – породични живот, социјално окружење (пријатељи, везе, чланство у организацијама)
- **професионална сфера** – образовање, радна историја, пословни и финансијски подаци
- **«обичне» и «посебне» категорије података** – обичне носе уобичајне информације, док се посебне односе на лични идентитет лица (политичко и верско опредељење, раса, сексуални живот...)
- **малолетна и пунолетна лица** – различити механизми правне заштите података
- **заштићени подаци** – који уживају правну заштиту
- **јавни подаци о личности** – јавно објављени документи, фотографије, ауди записи

Посебна категорија података о личности, чија обрада није дозвољена (осим под одређеним условима – постојање јавног или претежнијег приватног интереса):

1) Расно и етничко порекло; **2)** политичко мишљење; **3)** верско опредељење; **4)** синдикална припадност; **5)** генетски подаци; **6)** биометријски подаци; **7)** здравстено стање; **8)** сексуални живот и оријентација лица.

„генетски податак” је податак о личности који се односи на наслеђена или стечена генетска обележја физичког лица која пружају јединствену информацију о физиологији или здрављу тог лица, а нарочито они који су добијени анализом из узорка биолошког порекла;

„биометријски податак” је податак о личности добијен посебном техничком обрадом у вези са физичким обележјима, физиолошким обележјима или обележјима понашања физичког лица, која омогућава или потврђује јединствену идентификацију тог лица, као што је слика његовог лица или његови дактилоскопски подаци;

„подаци о здрављу” су подаци о физичком или менталном здрављу физичког лица, укључујући и оне о пружању здравствених услуга, којима се откривају информације о његовом здравственом стању;

КОНФЛИКТНЕ СИТУАЦИЈЕ:

- Финансијска приватност – пореско законодавство

- Национална безбедност и кривичне истраге – посебна категорија података о личности
- Слобода изражавања (јавног говора) – приватност

Заштићени лични подаци обично укључују, али се не ограничавају на:

- податке чије објављивање захтева доставу обавештења (Notice Triggering Data);
- податке о платним картицама (PCI Data),
- Податке о становању и породици лица (Home and Family Data);
- подаци који могу послужити за идентификацију лица (PII Data);
- подаци који се штите на основу прописа о заштити евиденција о ученицима и студентима (FERPA-Protected Data) и
- Заштићени подаци на основу уговорног односа (Contractual Protected Data)

ЛИЧНИ ПОДАЦИ	• Адреса са именом и презименом • E-mail адреса, ЈМБГ, број телефона • Идентификација за исплату преко кредитне картице: име и задња 4 броја кредитне картице • Датум рођења • Вероисповест • Здравствено стање
ОПШТИ ПОДАЦИ	• Адреса без имена • Име без адресе • Генеричка e-mail adresa npr. info@mip.sr • Сви подаци из којих се не може открити идентитет појединца

УСПОСТАВЉАЊЕ ЗБИРКИ ПОДАТАКА О ЛИЧНОСТИ

ЛИЧНИ ПОДАЦИ НА ИНТЕРНЕТУ МОГУ СЕ ГРУПИСАТИ У КАТЕГОРИЈЕ:

1) **АКТИВНИ ДИГИТАЛНИ ТРАГОВИ** – подаци о себи (или о другима) које сами корисници остављају приликомкоришћења интернета, обично свесно, мада не нужно и намерно (на пример – приликом куповине неких производа, преузимањем нечега са интернета, постављања фотографија, отварања профила на некој друштвеној мрежи...)

2) **ПАСИВНИ ДИГИТАЛНИ ТРАГОВИ** – подаци које корисници остављају на интернету приликом коришћења, углавном несвесно (путем колачића, отисака прстију, података о локацији, коришћења паметних ствари и паметних играчака)

3) Подаци добијени **анализом прве две категорије података**, помоћу алгоритама (кроз профилисање) и у комбинацији са другим изворима података.

Директно увођење - Нови систем замењује стари у одређено време.

Паралелна имплементација - и стари и нови систем се користе истовремено све док програмери не буду сигурни да нови систем функционише исправно.

Пилот пројекат – Увођење новог система на неки део активности или организациону јединицу, како би се видело како ће се исти показати. Ако су резултати добри онда се нови систем уводи у целости у систем.

ЗАКОН О ТАЈНОСТИ ПОДАТАКА **Тајни податак**
МЕРЕ ЗАШТИТЕ **Опште мере заштите; посебне мере заштите; чување, преношење и достављање ТП; дужност обавештавања**
РУКОВАЛАЦ ТАЈНИХ ПОДАТАКА Процена могуће штете по интересе Р. Србије
Процедуре одређивања тајних података - Формални део - Материјални део
Приступ тајним подацима – без сертификата, са сертификатом и безбедносном провером….
Поступак издавања сертификата – безбедносни упитник, провера, решење, жалба и управни спор
Контрола и надзор – унутрашња контрола, Канцеларија СНБиЗТП, Министарство правде
Кривично дело (чл. 98) Прекршајна одговорност (чл. 99 и 100)

ЗАКОН О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ **Податак о личности**
МЕРЕ ЗАШТИТЕ **Техничке, организационе и кадровске мере** **Обавештавање Повереника о повреди ЛП**
РУКОВАЛАЦ ЛИЧНИХ ПОДАТАКА и ОБРАЂИВАЧ Процена утицаја на обраду ЛП и мишљење Повереника
Податак о личности дефинисан законом - Начела - Права лица
Приступ личним подацима – на основу закона (ОСЛ), на пристанак, налог тужилаштва и суда…
Кодекс поступања и издавање сертификата (не примењује се на МУП…)
Повереник Правна средства, одговорност и казне
Прекршајна одговорност (чл. 95) Неовлашћено прикупљање личних података (чл. 146 КЗ)

АРХИВСКА ГРАЂА

- **Закон о архивској грађи и архивској делатности** ("Службени гласник РС", број 6 од 24. јануара 2020),
- **Закон о културном наслеђу** ("Службени гласник РС", број 129/2021) и
- **Закон о културним добрима** („Службени гласник РС”, бр. 71 од 22. децембра 1994, 52 од 15. јула 2011 - др. закони, 99 од 27. децембра 2011 - др. закон, 6 од 24. јануара 2020 - др. закон, 35 од 8. априла 2021 - др. закон, 129 од 28. децембра 2021 - др. закон).
- Законом о архивској грађи уређује се: систем заштите архивске грађе као културног наслеђа и документарног материјала, њихово чување сређивање и обрада, услови и начин коришћења, као и заштита Архивског фонда Републике Србије као културног наслеђа.
- Република Србија, аутономне покрајине и јединице локалне самоуправе су дужне да штите и чувају архивску грађу од општег интереса, да обезбеде за њу адекватне објекте, стручно руковођење и задовољавања потреба грађана.

Питање у пракси – када и на који начин штићени подаци постају архивска грађа?

Државни архив Србије је институција која чува и штити архивску грађу насталу радом државних органа и институција Србије до краја 1918. године, архивску грађу из времена Другог светског рата и послератног периода, као и личне и породичне фондове и збирке.

Постоји и архивска мрежа Републике Србије...

Јавна архивска грађа која садржи податке о личности (матичне књиге, лична и персонална досијеа, судски предмети, пореска и финансијска документа, историје болести и медицинска документација, пописи становништва и др.) доступна је за коришћење након истека рока од 70 година од дана настанка, односно 100 година од рођења лица на које се односи. Јавна архивска грађа која је настала у раду служби безбедности користи се у складу са одредбама из члана 54. и 56. Закона о архивској грађи и архивској служби (ограничења права на приступ!) као и посебног Закона о отварању досијеа лица насталих у раду служби безбедности (није донет!).

По прописима о канцеларијском пословању, регистратурски материјали препознају 1202 категорије материјала које се чувају углавном трајно …

ВОЈНИ АРХИВ

Главни задатак Војног архива је да прикупља, обрађује, чува, ставља на увид и публикује документа настала у српској и југословенској војсци у периоду од 1847. године до данас, а и надаље.

Војни архив је установа заштите архивске грађе и документарног материјала који настају у раду Министарства одбране и Војске Србије, или се код њих налази, обавља архивску делатност за потребе органа управе надлежног за одбрану, у складу са одредбама Закона о архивској грађи и архивској делатности ("Службени гласник Републике Србије" број 6/2020) које регулишу делатност и надлежности јавних архива, прописима о одбрани и прописима којима се уређује вршење архивске делатности за потребе одбране и Војске Србије.

Војни архив прикупља, чува, сређује и обрађује архивску грађу војне провенијенције настале у раду:

- Војске Краљевине Србије,
- Војске Краљевине Срба, Хрвата и Словенаца, односно Краљевине Југославије,
- свих војски и војних формација из Другог светског рата са територије коју је обухватала бивша Социјалистичка Федеративна Република Југославија,
- послератна архивска грађа Југословенске армије / Југословенске народне армије, као и надлежних савезних органа за народну одбрану,
- Војске Југославије / Војске Србије и Црне Горе проистекле из ЈНА и
- Министарства Одбране Републике Србије и Војске Србије.

Данас Војни архив чува око четрдесет милиона листова архивске грађе у укупној количини од око 7300 дужних метара. Већи део архивске грађе је у добром стању и расположив је за коришћење у читаоници Војног архива. Најстарија архивска грађа, као и грађа која је оштећена и у лошем стању, дигитализована је или је у процесу дигитализације те се иста не издаје на коришћење, већ само она у дигиталном облику.

КОМПРОМИТАЦИЈА ПОДАТАКА

КОМПРОМИТАЦИЈА ЗНАЧЕЊЕ

Компромитовати:

- Споразумети се да спор реши изборни судија;
- Довести нешто у питање;
- Стварати лоше мишљење о некоме; покварити нечији углед, добар глас; (о)брукати; (о)срамотити; унизити; понизити; озлогласити; опљунути;
- (компромитовати се) доћи, долазити на лош глас; (из)губити углед;
- Открити штићене податаке/информације лицима којима није дозвољен приступ, односно која немају право на овлашћен приступ.
-

КОМПРОМИТАЦИЈА

1) Остављање металне касе/сефа који садржи штићене податке незакључаног, отвореног и без надзора
2) Омогућавање особама које не поседују проверу и сертификат да имају приступ тајним подацима, било увидом у те податке или вођењем дискусија о тајним подацима у необезбеђеном подручју или преко небезбедне телефонске линије.
3) Омогућавање приступа појединцима који не поседују посебно одборење комбинацијама за металне касе/сефове у којима се штићени подаци чувају.
4) Слање штићених података путем факс машина.
5) Уклањање штићеног податка из зграде у којој се иначе чува без одговарајуће дозволе.
6) Копирање или уништавање штићеног податка без одговарајуће процедуре и одбрења.
7) генерисање штићеног податка на неодобреном рачунару.
8) Чување писане комбинације за отварање металне касе/сефа у неодобреном контејнеру.

КОМПРОМИТАЦИЈА ПОДАТАКА

Security breaches/кршење безбедности је неовлаштени приступ информацијама на мрежама, серверима или уређајима, заобилажење сигурности на тим системима, што на крају резултира отицањем или компромитацијом података. Нарушавање безбедности, такође познато као повреда података, је неовлашћени приступ или откривање поверљивих информација. Украдени акредитиви за пријаву, украдена средства или цурење интелектуалне својине су све врсте кршења података. Кршење безбедности може утицати на било коју организацију, без обзира на величину.

КЉУЧНИ РАЗЛОЗИ ЗА КРШЕЊЕ БЕЗБЕДНОСТИ ПОДАТАКА:

- ЉУДСКИ ФАКТОР
- МАЛВЕР
- НЕДОСТАТАК ФИЗИЧКЕ ЗАШТИТЕ ОПРЕМЕ У САЈБЕР БЕЗБЕДНОСТИ

Безбедносни инцидент се дешава када постоји стварни или потенцијални ризик за штићене податке и даље категорисан као кривично дело или прекршај. Безбедносни инциденти обично укључују безбедносну процедуру која није била спроведена на месту или није било правилно надзирана или праћена, као што су необезбеђени штићени подаци, неприкладни пријем ових информација од стране органа јавне власти, или отицања података које укључује штићене податке на некласификованој и неакредитованој ИКТ мрежи.

Прекршај је безбедносни инцидент који не доводи до губитка, компромитовања или сумње на безбедносни инцидент. Прекршаји захтевају спровођење поступка унутрашње контроле да би се проценили и предузеле радње за исправљање потенцијалних недостатака и слабости у безбедносном програму. Иако не представљају кршење безбедности, ако се не исправи, прекршај може довести до губитка или компромитовања тајних података/штићених података. Прекршаји могу бити ненамерни или ненамерни и могу открити недавне или понављајуће обрасце сумњивог расуђивања, неодговорности или немара.

Кривично дело је безбедносни инцидент који би разумно могао да доведе или јесте довео до губитка или компромитовање штићених података и захтева истрагу ради даље анализе и покретања кривичног поступка.

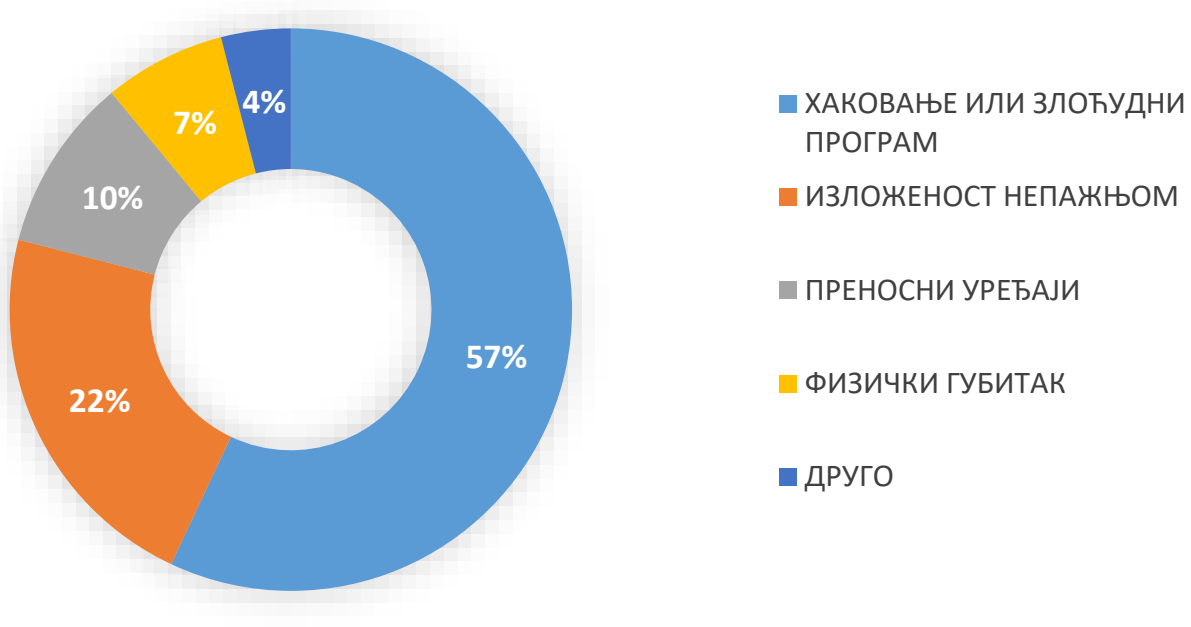
Кршења безбедности се обично користе у оквиру компанија, организација или владиних институција у којима је систем заштите података успостављен за приступ поверљивим информацијама као што су идентитети, адресе е-поште, лозинке, осетљиве финансијске информације итд.

Дефиниција:

Data Breach/Компромитација података је безбедносни инцидент у коме се осетљиви, заштићени или поверљиви подаци копирају, преносе, гледају, краду или користе од стране појединца који је неовлашћен за приступ тим подацима.

Повреде личних података могу да укључују финансијске податке као што су кредитна картица или банковни подаци, подаци о здравственом стању (личном здрављу), личне идентификационе информације, пословне тајне корпорација или интелектуалне својине. Већина компромитација података укључује прекомерно изложене и рањиве неструктуриране податке - датотеке, документе и осетљиве информације.

ГЛАВНИ УЗРОЦИ КОМПРОМИТАЦИЈЕ ПОДАТАКА



КОМПРОМИТАЦИЈА ТАЈНИХ ПОДАТАКА

- Ненамеран неовлашћени приступ и коришћење
- Неовлашћена употреба базе тајних података
- Проблем идентификације и чувања података
- Нестручно и немарно руковање техником и подацима
- Губитак носача података
- Шпијунажа, диверзија, хактивизам…
- Сајбер криминал, организовани криминал…
- Крађе идентитета
- Неовлашћена употреба базе личних података
- Проблем идентификације и чувања података
- Нестручно и немарно руковање техником и подацима
- Губитак носача података
- Сајбер криминал, организовани криминал…

САЈБЕР ПРЕТЊЕ

ДЕЛОВАЊЕ У САЈБЕР ПРОСТОРУ РАДИ НАНОШЕЊА ШТЕТЕ ИКТ СИСТЕМИМА

- **Државе** – „сајбер ратовање“
- **Корпорације** – сајбер напади на системе за обраду података
- **Компаније за MALVERe** – наношење штете и крађа информација
- **Инсајдер** – проблематичан појединац унутар брањеног простора
- **Сајбер терористи**
- **Ботнет оператери** – врше нападе преко заражених компјутера
- **Злоупотребе интернета и друштвених мрежа** – крађе идентитета, крађе интелектуалне својине, преваре, злоупотреба деце преко интернета, недозвољена трговина…

Могу се поделити на две категорије када је реч о лицима која се тиме баве:

1. Аматери – имају основно знање или уопште немају техничко знање;
2. Хакери – имају напредно техничко знање и деле се у три групе:
    a. са белим шеширом (енгл. White hat) – „добри ликови“ који раде за организације како би ојачали безбедносни систем;
    b. са сивим шеширом (енгл. Gray hat) – хакују рачунарске системе, али не чине то злонамерно, некада могу тражити неку врсту накнаде за свој рад;
    c. са црним шеширом (енгл. Black hat) – неовлашћено хакују рачунарске системе из злонамерних разлога, како би нанели штету или остварили неку добит

Организовани хакери

баве се шпијунажом, организованим криминалом, тероризмом, хактивизмом, спонзорисани су од стране неке државе.

ОБЛИЦИ ОДГОВОРНОСТИ

- Кривично правна
- Прекршајна
- Радно правна и дисциплинска
- Облигационо правна (за накнаду штете)
- Морална

НАПОМЕНА

НИЈЕ СВАКА КОМПРОМИТАЦИЈА ПОДАТАКА КРИВИЧНО ДЕЛО, ПРЕКРШАЈ ИЛИ ПОВРЕДА РАДНЕ ДИСЦИПЛИНЕ…

ОБРАДА ПОДАТАКА

О ОБРАДИ ПОДАТАКА

Обрада података је, генерално, "прикупљање и употреба података ради стварања смислене информације."

У том смислу могло се сматрати подскупом обраде информација, "што је промена (обрада) информација на било који начин који детектује посматрач."

Обрада података је свака радња предузета у вези са подацима као што су:

прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин .

ПОДЕЛА ВРСТА ОБРАДЕ ПОДАТАКА

- Ручна
- Полуаутоматизована
- Аутоматизована

Учешће вештачке интелигенције у обради података?

РУЧНА ОБРАДА ПОДАТАКА

Иако је употреба појма обрада података широко распрострањена од педесетих година 20. века, функције обраде података ручно су извршаване миленијумима. На пример, књиговодство укључује функције као што су обављање трансакција и израду извештаја као што су биланс стања и извештај о токовима готовине. Потпуно ручне методе унапређене су применом механичких или електронских калкулатора. Особа чији је посао био да израчунава прорачуне ручно или користећи калкулатор звао се „рачунар.“

Аутоматска обрада података

Појам аутоматска обрада података примењена је на операције извршене помоћу опреме за снимање, као што је примена система бушених картица Хермана Холерита за попис Сједињених Америчких Држава 1890. године. „Коришћењем Холеритовог система бушених картица, канцеларија за попис је успела да заврши табулацију већине пописаних података из 1890. године за две до три године, у поређењу са пописом из 1880. године за коју било потребно седам до осам година....

Такође се процењује да је коришћење система који је осмислио Херман Холерит уштедело око 5 милиона долара у трошковима обраде“ (1890. године) чак и са двоструко већим бројем питања у односу на 1880. годину.

ЕЛЕКТРОНСКА ОБРАДА ПОДАТАКА

Односи се на употребу аутоматских метода за обраду комерцијалних информација. Компјутеризована обрада података, или електронска обрада података настала је касније, где се користи рачунар уместо неколико појединачних уређаја. Биро за попис у почетку је ограничено користио електронске рачунаре за попис становништва 1950. године Сједињених Америчких Држава, користећи систем УНИВАЦ I, испоручен 1952. године.

Извори података се деле у две категорије – структуирани и неструктуирани.

Структуирани подаци:

- Рачунарски или машински генерисани: појам машински генерисани подаци се односи на податке које производи машина без људског утицаја (сензорски, Weblog, у тренутку продаје и финансијски подаци) .
- Људски генерисани: ово су подаци које обезбеђују људи у интеракцији са компјутерима (улазни, клик и везани за игре).

Неструктуирани подаци:

- Сателитске слике – временске прилике или подаци прикупљени сателитским надгледањем.
- Научни подаци – сеизмичке слике, атмосферски подаци, физика високих енергија и слично.

Може обухватити различите процесе, укључујући:

- **Валидација** – Обезбедити да су испоручени подаци тачни и релевантни.
- **Сортирање** – „Уређивање ставки у неком редоследу и/или у различитим скуповима.“
- **Сумирање** – Смањивање детаља података на главну поенту.
- **Агрегација** – Комбиновање више делова података.
- **Анализа** – „Прикупљање, организација, анализа, интерпретација и представљање података.“
- **Извештавање** – Листа детаља или резиме података или израчунате информације.
- **Класификација** – Одвајање података у различите категорије (ТАЈНИ ПОДАЦИ, ЛИЧНИ ПОДАЦИ, ПОСЛОВНЕ ТАЈНЕ, ПРОФЕСИОНАЛНЕ ТАЈНЕ…).

ПОДЕЛА ВРСТА ОБРАДЕ ПОДАТАКА

- Са пристанком лица
- Без пристанка лица
- На основу закона
- На основу уговора
- За личне потребе
- За потребе научног рада, статистика…
- збирке података
- физичка и правна лица
- размена података са другим полицијама, службама безбедности…
- примена посебних доказних радњи или специјалних истражних техника
- примена посебних поступака и мера за тајно прикупљање података (ВБА и ВОА)
- Примена оперативних метода, мера и радњи и одговарајућих оперативно-техничких средстава, као и посебних мера којима се одступа од неповредивости тајности писама и других средстава општења (БИА)

ОБРАДА ПОДАТАКА О ЛИЧНОСТИ У СЕКТОРУ БЕЗБЕДНОСТИ И ОДБРАНЕ

- Обрада података о личности за потребе кривичног поступка (КЗ, ЗКП…)
- Обрада података о личности у оквиру Министарства финансија (пореска полиција, царина, Закон о спречавању прања новца и финансирања тероризма…)
- Обрада података о личности у приватном сектору (ЗП, ЗПО, ЗД…)
- Обрада података о личности за потребе безбедности и одбране (ЗО, ЗБИА, ЗВБАиВОА, ЗТП…)
- Демократски надзор над обрадом података о личности без пристанка

Стандарди формулисани кроз начела :

- легалитета
- супсидијарности
- сразмерности

У СКЛАДУ СА ДОКУМЕНТИМА УН, ЕУ и УСТАВОМ РЕПУБЛИКЕ СРБИЈЕ – ЉУДСКЕ СЛОБОДЕ И ПРАВА

ОБРАДА ПОДАТАКА О ЛИЧНОСТИ У:

- Јавној управи
- Јавним предузећима (ЕПС, водоводи, канализације…)
- Здравству
- Просвети
- Банкарству
- Осигуравајућим заводима…
- Трговини на велико и мало
- Маркетингу и истраживањима тржишта

Регистре различитих облика делатности води АПР…

НАДЗОР НАД БЕЗБЕДНОСНОМ ПОЛИТИКОМ (ОБРАДОМ ПОДАТАКА?)

ПОСЕБНА КОНТРОЛА И НАДЗОР САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ

- НАРОДНА СКУПШТИНА (одбори, комисије...)
- ВЛАДА (креирање буџета, одбори, министарства...)
- ПРАВОСУЂЕ (посебне мере, поступци...)
- ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА
- ЈАВНОСТ И НЕВЛАДИН СЕКТОР
- УН, САВЕТ ЕВРОПЕ, ЕУ...
- ЗАШТИТНИК ГРАЂАНА И ПОВЕРЕНИЦИ

АСПЕКТИ ЗАШТИТЕ ПОДАТАКА

Заштита података је скуп различитих технолошких метода којима се дигитални подаци штите током процеса дигиталног преноса података или дигиталне комуникације. Њиховом применом се осигурава приватност како личних, тако и јавних података.

Заштита података је неопходна током дигиталног преноса података осетљивог садржаја, као што су владина документа, банковни подаци, документа државних служби, подаци великих предузећа, и сл. Да би дигитални подаци стигли нетакнути на своје одредиште, током преноса они морају бити константно заштићени од неовлашћеног откривања и приступа, преусмеравања и прекида, инспекције и модификације, снимања и уништења.

Заштита података о личности је скуп међусобно повезаних активности, метода, техника и норми којима се обезбеђује приватност, сигурност, поверљивост, расположивост и интегритет података од свих опасности које им прете.

Систем заштите података о личности садржи скуп правила које се односе на:

- Податке који се прикупљају
- Услове за дозвољеност прикупљања
- Случајеве где постоји забрана и изузетке
- Права лица
- Орган надлежан за надзор

Опште мере заштите се односе на:

- процену значаја података;
- избор просторије за рад и лица;
- начин чувања и коришћења;
- забрану приступа и уласка;
- забрану снимања и уношења техничких средстава;
- забрану излагања и приказивања;
- физичко-техничко обезбеђење;
- забрану разговора и контролу мера.

Посебне мере се односе на:

- вођење евиденције о подацима;
- тајни назив активности;
- касе и посебне просторе;
- посебно обезбеђивање просторија;

- утврђивање броја примерака;
- писмено упутство за рад са податком;
- комисијско уништавање радних материјала;
- преношење куриром;
- писмена изјава о чувању тајности;
- писмена примопредаја и крипто-заштита.

Мере у односу са странцима се односе на:

- претходно проучавање и процену;
- одређивање података;
- одређивање и припремање лица;
- одређивање програма кретања странаца по предузећу;
- забрану ангажовања странаца;
- забрану непосредног увида.

Организационе мере заштите односе се на организацију заштите процеса рада и функционисања информационо-комуникационог система у редовним околностима и ванредним ситуацијама.

Организационе мере заштите нарочито обухватају:

- Доношење општег акта о мерама заштите и техничких упутстава за рад;
- Одређивање одговорног лица задуженог за спровођење мера заштите информационо-комуникационог система;
- Утврђивање обавезних елемената заштите при пројектовању информационо-комуникационог система (подсистема) и при оперативном раду;
- Заштиту приступа подацима и заштиту од неовлашћеног коришћења података и информација;
- Утврђивање поступака у случају ванредних ситуација (мере заштите у ванредним ситуацијама односе се на наставак рада у измењеним условима или наставак рада на резервним локацијама и опреми);
- Остале мере неопходне за ефикасно функционисање информационо-комуникационог система (контрола кадрова при пријему, дефинисање послова и задатака учесника у раду информационог система, стручно усавршавање кадрова, дефинисање обавеза правних и физичких лица ангажованих на одржавању појединих делова информационо-комуникационог система).

- Организационе мере заштите спроводе се у складу са прописом којим се уређује заштита података о личности и обезбеђивање и заштита информационо-комуникационих система државних органа.

Техничке мере заштите односе се на обезбеђење и заштиту података и информација и других елемената информационо-комуникационог система, који се остварују применом посебних техничко-технолошких процеса рада и/или спровођењем физичко-манипулативних мера заштите у било којој процедури у оквиру рада ИКТ система.

Техничке мере заштите нарочито обухватају:

- Физичку заштиту објекта у коме је смештена рачунарска опрема и противпожарну заштиту;
- Обезбеђивање и заштиту рачунарске опреме и рачунарских носиоца података;
- Заштиту програмске подршке;
- Заштиту рачунарских мрежа.

Техничке мере заштите обухватају и вођење евиденције и вршење контроле:

- Аутентичности података и информација, њихових извора и корисника;
- Селективног приступа подацима и информацијама и осталим елементима ИКТ система;
- Интегритета података израдом заштитне копије на почетку и крају сваког процеса рада и заштите архивских копија и просторија у којима се оне чувају;
- Интегритета података и информација у ИКТ систему у односу на појаву вируса;
- Интегритета и заштита поверљивости података;
- Коришћења постојећих и одређивања резервних локација, уређаја и опреме на којима ће се чувати копије база података и пројектно-програмска подршка за несметан рад у случају отказивања и нарушавања редовног рада ИКТ система;
- Примене стандардних и посебних хигијенско-техничких мера за све елементе ИКТ система приликом њихове изградње и коришћења.

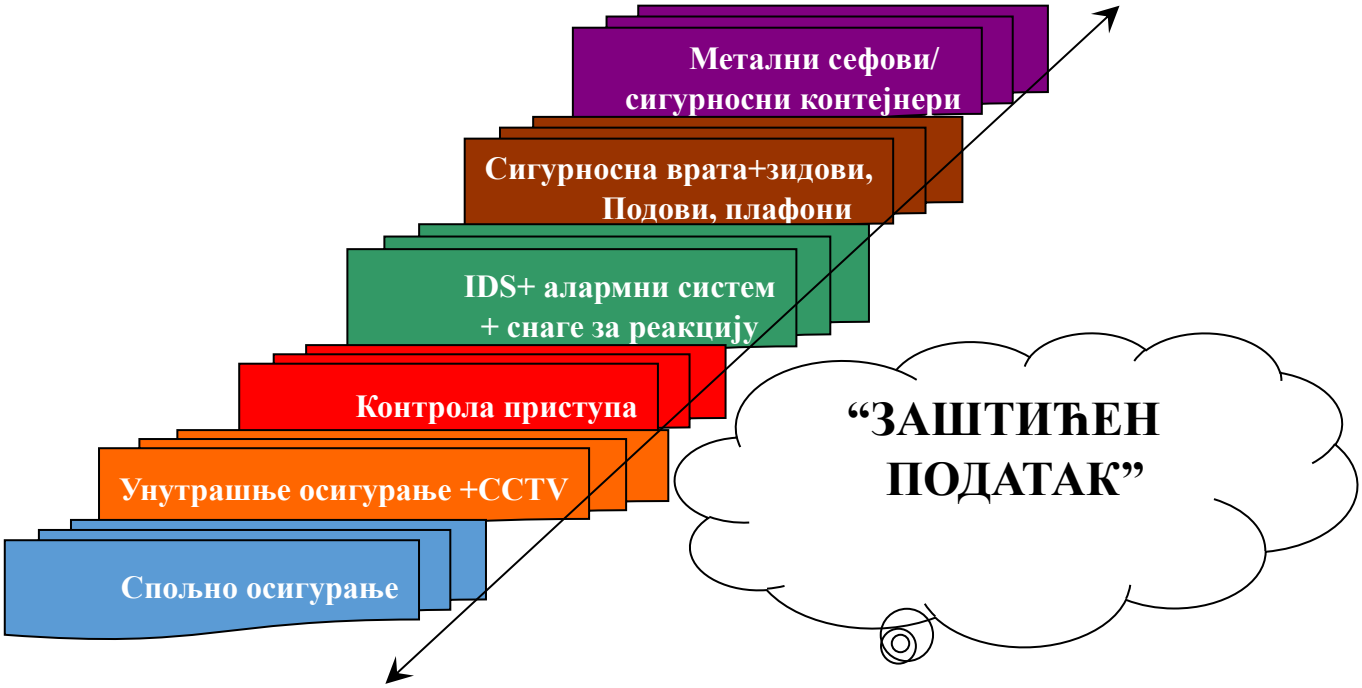
Техничке мере заштите примењују се на све процесе прикупљања, обраде, архивирања, преноса и дистрибуције података и информација и све делове ИКТ система и спроводе се у складу са прописом којим се уређује заштита података о личности и обезбеђивање и заштита ИКТ система државних органа.

ДЕФИНИЦИЈА

Физичка безбедност или сигурност подразумева примену мера физичке и техничке заштите на појединачним локацијама, зградама или отвореним просторима на којима

се налазе или чувају штићени подаци (информације) које захтевају заштиту од губљења, неовлашћеног приступа, компромитовања или отуђења.

ВИШЕСЛОЈНИ СИСТЕМ ЗАШТИТЕ-ОДБРАНА ПО ДУБИНИ



- Јасно дефинисане и видљиво означене просторије безбедносног подручја/зона (периметри) или “рестриктивни простори”
- Физичко осигурање/чувар, стража + тим за хитне интервенције (ПОДЗАКОНСКА АКТА, ИНТЕРНИ ПРОПИСИ или СРПС А:Л2.002)
- Просторије (зидови, подови, плафони) – грађевинске мере заштите
- Металне касе – сефови (EN 1134-1)
- Кључеви и комбинације (EN 1300)
- Резач папира – Шредер
- Посебна улазна врата... (EN 1627)
- Прозори заштићени решеткама, непровидним завесама или сигурносним фолијама
- Обележени телефони, рачунари, принтери и сл.
- Резервно напајање електричном енергијом, клима уређај
- Вентилацијски, канализациони или други отвори заштићени металним решеткама
- Видео надзор – CCTV (ISO 9001 или ISO 14001)

- Контрола приступа (EN 50133-1 и EN 50133-1/A1)
- Противпровални систем осигурања /IDS (EN 50131-1)
- Противпожарни систем, детектори дима (EN 54-1, EN 54-2, EN 54-3, EN 54-4, EN 54-5, EN 54-11)
- Алармни систем (EN 50134-1)

Плафони, зидови и подови

Плафони, зидови и подови морају бити израђени од армираног бетона или чврстог незапаљивог материјала. У случају да су просторије међусобно повезане размаком између плафона и крова, морају бити одвојени чврстим незапаљивим материјалом.

Заштита од директног увида у просторију

Ако се просторија/соба у којој се налазе штићени подаци може видети споља када су врата отворена, преграде или завесе морају бити инсталиране, како би се онемогућио директан увид споља у просторију у којој се налазе штићени подаци.

Улаз

У принципу мора постојати само један улаз.

Расвета (ноћна светла) на улазу/излазу врата мора да функционише чак и у случају нестанка струје.

У случају да није могуће унети/изнети опрему и инструменте на тај улаз, може се направити улаз за отпрему/пријем.

По потреби могу постојати и врата за случај опасности која се могу отворити само изнутра.

Врата и браве

Врата за улаз, улаз за отпрему/пријем или излаз у случају опасности морају бити челичнау принципу. Код двокрилних врата на спојним деловима морају бити астрагали (конвексна лајсна или дрвена трака преко површине или преградне плоче, обично полукружног попречног пресека). Уколико је потребно поставити прозоре – морају бити затворени са спољним или унутрашњим металним решеткама.

Просторија се не сме видети кроз прозоре.

Улазна врата и врата за отпрему/пријем морају бити двоструко закључана са 3 механичке комбиноване браве (више од 1000 комбинација) и бравом на кључ.

Као алтернативна мера, међутим, може се користити и дигитални уређај за закључавање као нпр уређај за биометријску аутентификацију уместо механичке комбиноване браве.

Механизам за евакуацију у случају ванредних ситација мора бити инсталиран, тако да се може отварати само изнутра.

Прозори

Прозор се у принципу не сме инсталирати.

Када је неизбежна уградња прозора, они морају бити ограничени на минимум и опремљени гвозденим шипкама пречника 13мм или више и интервалима од 10 цм или више, у складу са СРПС ЕН Стандардима.

Прозорско стакло мора бити непрозирно са слојем жичане мреже или једноставно непрозирно, са заштитом од провале.

Отвори/вентилација/канал

Да бисте спречили улазак, осматрање или прислушкивање, канале, плафонске прозоре, одводе, тунели и остали отвори морају бити затворени жичаном мрежом или гвозденим шипкама пречника од 13 mm или више, са интервалима мањим од 10 cm, у складу са SRPS EN стандардима.

Алармни систем

Мора постојати аутоматски алармни систем који детектује отварање/затварање врата и неовлашћене упаде.

Алармни систем мора бити директно повезан са сигурносним контролним центром и тако подешен, да функционише и у случају нестанка електричне енергије.

Повезивање алармног система (ожичење) се не сме лако прекинути, тако да се систем мора алармира ти када се искључи електрична енергија или прекине ожичење.

Периметар

Периметар се мора поставити на око објектата у којима се налазе штићени подаци, како би се спречило неовлашћен приступ.

Према околностима, потребна је ограда висине од 2 метра или више, прекривена бодљикавом жицом или сензорима који регују на контакт. Ова ограда би требала бити или на бетонским армираним или на челичним стубовима.

Периметарска ограда мора бити постављена око сигурносних објеката или читавог простора укључујући објекте.

Периферне контролне области

Да би се спречио неовлашћени приступ безбедносним објектима, изван периметра, периферне контролне области морају бити одређене и приступ тим подручјима је потребно контролисан.

Сигурносни контејнери/КАСЕ

Тајни подаци морају се складиштити у следећим сигурносним касама/контејнерима у зависности од степена тајности:

- за ДРЖАВНУ ТАЈНУ (ДТ), каса/сеф који се закључава са три положаја точкића, комбинована брава,
- за СТРОГО ПОВЕРЉИВО (СП), челична каса/сеф која се закључава са комбинованом бравом,
- за поверљиво (П), челична кутија која се може закључати са комбинованом бравом за бирање; и
- за интерно (И), челичну кутију која се може закључати.

Уредба о одређивању послова безбедносне заштите одређених лица и објеката

УРЕДБА о посебним мерама физичко-техничке заштите тајних података

Правилник о пословном простору за обављање детективске делатности и физичко-техничким мерама за чување збирки података и других евиденција

Правилник о начину вршења послова техничке заштите и коришћења техничких средстава

Стандард SRPS A.L2.002:2015 – Друштвена безбедност – услуге приватног обезбеђења

РЕЛЕВАНТНИ ФАКТОРИ

Релевантни фактори за одређивање степена потребних мера физичко-техничке заштите су:

- Процена претње за безбедност података
- Врста података
- Природа/облик документа у коме је садржан податак (штампани/електронски)

ПРОСТОРИ СА РЕСТРИКТИВНИМ ПРИСТУПОМ

- Административна подручја/зоне
- Безбедносна подручја / зоне:
    - подручје I степена заштите
    - подручје II степена заштите

УОПШТЕ БЕЗБЕДНОСНА ПОДРУЧЈА/ЗОНЕ

Безбедносна подручја/зоне захтевају:

- систем улазног надзирања;
- посебна организација рада;
- забрана уноса (механичких,електронских,магнетно - оптичких делова и сл.);
- физичко и противпровално осигурање после радног времена - алармни систем повезан са снагама за реакцију и надзорним центром

БЕЗБЕДНОСНА ПОДРУЧЈА/ЗОНЕ КОД ТАЈНИХ ПОДАТАКА

- Руковање подацима степена тајности ПОВЕРЉИВО или вишег степена могуће искључиво у безбедносном или сигурносном подручју I или II степена заштите.
- подручје I степена заштите:
    - улазак у ово подручје подразумева истовремено и приступ тајним подацима.
- подручје II степена заштите:
    - улазак у ово подручје не подразумева истовремено и приступ тајним подацима.

Поред Закона о информационој безбедности, то је и материја Закона о тајности података, Закона о заштити личних података, али и прописа у сектору безбедности и одбране, као и спољних послова

КРИПТОБЕЗБЕДНОСНА ЗАШТИТА ЗАКОН О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

Компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

Криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

- криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;
- криптографски производ је софтвер или уређај путем кога се врши криптозаштита;
- криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

КОМПАРАТИВНИ ПРИКАЗ ЗАШТИТЕ ПОДАТАКА У ПРИВАТНИМ КОМПАНИЈАМА И ДРЖАВНИМ ОРГАНИМА

БЕЗБЕДНОСТ У ДРЖАВНИМ ОРГАНИМА	**БЕЗБЕДНОСТ У ПРИВАТНИМ КОМПАНИЈАМА**
Заштита података од интереса за државу **Тајни подаци, лични подаци, професионалне тајне (изузетно и пословне тајне)**	**Заштита података од интереса за компанију** **Пословне тајне, лични подаци, професионалне тајне (изузетно и тајни подаци)**
Процена ризика – законска обавеза Означавање степена тајности (ДТ, СП,П,И)	Процена ризика – уговорна обавеза Означавање степена поузданости - *confidence* (С1, С2, С3)
Контролисан приступ, руковање и достављање података (системски закони, канцеларијско пословање…) Руковалац тајним подацима + руковалац личним подацима + уговорне обавезе за пословне тајне	Интерне процедуре за руковање подацима (Статут, уговорне обавезе…) Руковалац личних података + уговорне обавезе за тајне податке и пословне тајне
Безбедносно сертификовање физичких лица – КОЗ, заштитни режим радних места + уговарачи (?)	Вршење провера преко приватних компанија – корпоративна безбедност, интелектуална својина…
Безбедносно сертификовање правних лица (поверљиве набавке И и П + пројекти СП и ДТ)	Вршење провера преко Судова, АПР-а
Акредитација ИКТ система + Закон о тајности података – примена мера криптозаштите ИКТ системи од посебног значаја	Комерцијални INFOSEC стандарди (27001, 17799) ИКТ системи од посебног значаја – акт о безбедности ИКТ
Физичко-техничка безбедност (МУП + приватно обезбеђење)	Физичко-техничка безбедност (приватно обезбеђење)

ПРОБЛЕМИ У ПРАКСИ

Кашњење у законодавним активностима – измена прописа из различитих области и њихово усаглашавање са Законом о информационој безбедности, Законом о тајности података, Законом о заштити података о личности.

Избегавање законом предвиђених обавеза, недостатак процедура и нормативе на нижим нивоима, проблеми са канцеларијским пословањем, заштитом тајних података и личних података, отицањем истих у медије – одређивање руковаоца тајних и личних података у органу, израда одговарајућих упутстава за рад са тајним и личним подацима, планови одбране, планови за ванредне и хитне ситуације, преношење тајних и личних података и слично.

Интенција да се сва питања решавају законом – проблематика ИКТ система и штићених података - помоћу система „хоризонталне“ координације, али и односа између сектора у органу јавне власти. На тај начин стиче се утисак да је намера појединих структура да се успостављање ИКТ система и заштите података (хоризонталне комуникације) уреди законом је у пракси тешко изводљиво и неприхватљиво, односно могуће је само подзаконским актима, уредбама и правилницима.

Рад са тајним и личним подацима у ИКТ системима, електронски потпис, електронска администрација и њихово преношење кроз сајбер простор – модели који се развијају у оквиру стратегије развоја информационог друштва и за сада представљају теоријски модел, без националног акредитационог тела и промовисање система кроз разне прописе тзв. „саморегулације“ и „самоакредитације“.

Лажно, нетачно, малициозно и злонамерно извештавање доносилаца одлука (ради избегавања примене прописа) о системским проблемима и потребама реформе рада са ИКТ системима и штићеним подацима.

Разврставање и класификација података са којима располаже организација?

Активирање механизама правне и безбедносне заштите података и пренаглашавање ИТ структура?

Последице?

Рад са тајним подацима без имплементације Закона о тајности података – директно угрожавање националне безбедности?

Рад са личним подацима без имплеметнације Закона о заштити података о личности – директно угрожавање људских слобода и права (приватности)? Овакве ситуације су и кривично дело и прекршај.

Непоштовање процедура у раду са тајним и личним подацима

Неовлашћено коришћење ИКТ система за рад са тајним/личним подацима без одговарајуће тахнолошке и безбедносне акредитације система.

Неадекватна и недовољна заштита података

1. Могућност злоупотребе процедура и података
2. Неуједначен степен заштите
3. Правна несигурност
4. Проблем организационих и технолошких недостатака
5. Недовољно јасан и неусклађен правни оквир са ЗТП и ЗЗЛ
6. Недостатак безбедносне културе о заштити података
7. Различито тумачење прописа

Збирке тајних података – ПЛАН ОДБРАНЕ, ПОВЕРЉИВЕ НАБАВКЕ, СПЕЦИЈАЛНЕ ИСТРАЖНЕ ТЕХНИКЕ:

- Режим рада са тајним подацима
- Процедуре обраде и чувања тајних података
- Објављивање података са степеном тајности у медијима?
- Процедуре у случају отицања или губитка тајног податка?

Збирке личних података:

- Режим рада са тајним подацима (преклапања?)
- Процедуре обраде личних података (или их нема или су предетаљне?)
- Јавне збирке доступне јавности (уз сагласност или не - питање доступности личних података?)

РАД СА ТАЈНИМ ПОДАЦИМА ИЛИ ПИТАЊЕ „ПРИМАТА (ЈАЧЕГ) „ ПРОПИСА:

- Када збирке података које су означене степеном тајности прелазе у режим рада личних података?
- Разграничење различитих области рада, оперативног рада, националне безбедности, повреда радне дисциплине, процесуирања прекршаја и кривичних дела…

Усклађивање постојећег нормативног оквира са Законом о тајности података и ГДПР-ом и Законом о заштити података о личности:

- Модел нормативе МУП-а
- Сврха, који лични подаци, збирке…
- „lex specialis derogat lege generali“, са доношењем ГДПР-а више није применљива?

Проблем рада са личним подацима у јавним регистрима који садрже личне податке:

- Регистар правних лица
- Регистар непокретности
- Регистар залога и других терета…

Питање коришћења оперативних збирки података у поступцима безбедносних провера (ЗТП – не наводе се извори у извештају)?

Питање последица давања нетачних података у упитнику за безбедносне провере – кривична или радно-правна одговорност?

Спровођење (злоупотребе) процедура заштите тајних података – безбедносно кадрирање, злостављање на раду, дискриминација?

Каква је санкција за злоупотребу права на заштиту личних података у парничном, кривичном и прекршајном поступку?

Колико ће то коштати пореске обвезнике или буџет Републике Србије?

Проблеми у судским и другим поступцима са спровођењем вештачења или недостатак вештака?

Судска пракса поражавајућа када је у питању заштита података, било тајних, било личних....

ПИТАЊЕ ТЕСТА

САДРЖИНА РЕШЕЊА ЗА СЛОБОДАН ПРИСТУП ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА

- одавање државне тајне из члана 316. став 6.; одавања службене тајне из члана 369. став 5.; одавања војне тајне из члана 416. став 5. КЗ
- члана 3. Закона о тајности података
- Члан 4, 8, 9, 13 и 14. Закон о слободном приступу информацијама од јавног значаја
- Члан 3. Закон о заштити пословне тајне

- Да ли је реч о тајном податку или информацији којом располаже орган јавне власти?
- Да ли се утврђивањем тајности података прикрива постојање тешких повреда основних права човека?
- Да ли се утврђивањем тајности података прикрива постојање угрожавања уставног уређења и безбедности Србије?
- Да ли се утврђивањем тајности података прикрива учињено кривично дело за које се може изрећи 5 година затвора?
- Да ли се утврђивањем тајности података прикрива постојање кривичног дела?
- Да ли се утврђивањем тајности података прикрива прекорачење овлашћења?
- Да ли се утврђивањем тајности података прикрива злоупотреба службеног положаја?
- Да ли се утврђивањем тајности података прикрива други незаконит акт?

- Да ли је потреба заштите интереса Р. Србије претежнија од интереса за слободан приступ информацијама од јавног значаја?
- Да ли је интерес набројан у закону (9,13 и 14. Закона о слободном приступу информацијама од јавног значаја) супротстављен интересу тражиоца да зна?
- Да ли би приступом овој информацији супротан интерес био озбиљно повређен (питање процене последица или баланса права)?
- Да ли потреба заштите супротног интереса претеже над потребом заштите интереса тражиоца да зна, просуђујући неопходност ускраћивања приступа по мерилима демократског друштва?

ТЕСТ ЈАВНОГ ИНТЕРЕСА

Члан 8. ЗСПИЈЗ

- **да постоје супротстављени интереси праву јавности да зна**,
- одавањем информације тај интерес **био би озбиљно повређен (тест штете)**,
- потреба заштите другог интереса **претеже над интересом јавности да зна**,
- **ако је то неопходно у демократском друштву** (ако се ускраћивањем ионако не могу заштитити ти интереси, ако се заштита тих интереса може подједнако остварити на други начин, ако се приступ тиме ускраћује у већој мери него што је дозвољено)

Сврха :

успостављање правичне равнотеже између супротстављених интереса

Код примене теста јавног интереса између:

Права јавности да зна – права на приступ информацијама и права на приватност је:

Случај Фон Хановер против Немачке-објављивање информација у вези болести и неге принца Ранијеа од Монака и фотографија

ЕСЉП-повреда права на поштовање приватног и породичног живота

Кључни фактор :

Степен у коме објављивање информација доприноси дискусији о питањима од општег интереса- постоји ли јавни интерес за откривање информација или се ради о задовољењу радозналости

Остали фактори:

Каква је садржина тражених информација, форма и околности у којима су фотографије снимљене (да ли се односе на приватне или јавне ствари)

Који би ефекат на лице на које се односи имало откривање информације и каква су његова очекивања

Какве су могуће реакције лица која су укључена и последице мера славе особе (политичар или само јавна личност која не обавља никакве званичне функције)

Који фактори не треба да буду релевантни у примени теста интереса?

- Стварање непријатности било ком јавном функционеру или службенику,
- Могућност губитка поверења у јавну управу-службу
- Могућност да би информација могла бити превише стручна или техничке природе и да је тражилац не би могао лако разумети
- Могућност да је информација непотпуна и да би могла да дезинформише јавност

Јавни интерес за обелодањивање информација треба да буде јак :

- Када се питање тиче јавне безбедности или јавног здравља
- Ако ће објављивање информација унапредити поузданост и транспарентност у процесу одлучивања
- Када се питање тиче стицања и трошења јавног новца
- Ако ће обелодањивање информација помоћи да јавност разуме питање о коме се води јавна или парламентарна дебата, односно расправа
- Када се неко питање тиче широког круга појединаца или кампање

СТАНДАРДИ В. Британија-Повереник

ПИТАЊЕ ТЕСТА

- ПРЕПОРУКА ЈЕ ДА ОДГОВОРИ НА СВА ОВА ПИТАЊА БУДУ САДРЖАНИ У ОБРАЗЛОЖЕЊУ РЕШЕЊА КОЈИМ СЕ ОДБИЈА ПРИСТУП ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА…
- ПРОЦЕНЕ ИЗ ТЕСТА БИ ТРЕБАЛЕ БИТИ ТРАНСПАРЕТНЕ И ДОСТУПНЕ ЈАВНОСТИ, АЛИ ЗАШТИЋЕНИ ПОДАЦИ НИКАКО!!!

НА КРАЈУ

ПРЕПОРУКЕ

Потребно је преко успостављања система едукација, на више нивоа, константно подизати ниво безбедносне културе и свести када су у питању штићени подаци.

Питање подизања капацитета организационе културе и сајбер хигијене...

Потребно је нормативом и посебним одлукама руководства или менаџмента јасно одредити одговорну организациону структуру за одређене категорије података, посебно за тајне податке, личне податке, пословне тајне и професионалне тајне које представљају најосетљивије категорије штићених података, као и устројити одговарајуће интерне процедуре за обраду и заштиту тих података.

Потребно је успоставити технолошке капацитете за обраду и заштиту података, набављањем одређене опреме и имплементацијом одговарајућих стандарда, SRPS/СРПС ISO/IAC 27001, ISO 14001 и слично, односно успостављање ISMS.

Појам ISMS представља Систем менаџмента безбедности информација и његов задатак је успостављање организационо-систематског приступа за успостављање, примену, спровођење, праћење, преиспитивање, одржавање и побољшавање безбедности процедура обраде и заштите података ради постизања законом или уговором предвиђених циљева рада органа јавне власти или циљева пословања компаније.

Потребно је успоставити систем надлежности да је сасвим јасно ко шта ради и ко за шта одговара.

Нпр. **Синергија** - Правници би требали бити носиоци правне проблематике и тумачења прописа, безбедњаци би требали бити носиоци активности документовања одређених догађаја, ИТ служба би требала бити носилац одређених процедура, али све три структуре би требале радити као тим, вођен менаџментом (руководством) организације...

ПИТАЊА

- ТРАНСПАРЕТНОСТ ПРОТИВ ТАЈНОСТИ?
- ЉУДСКЕ СЛОБОДЕ И ПРАВА ПРОТИВ БЕЗБЕДНОСТИ?
- КАКО ДЕФИНИСАТИ ГРАНИЦЕ?
- БЕЗБЕДНОСТ ИЛИ СИГУРНОСТ....
- ПИТАЊЕ УНОСА ПОДАТАКА У ЗБИРКЕ (ПРАВНИ ОСНОВ, СА И БЕЗ ЗНАЊА ЛИЦА, АУТЕНТИЧНОСТ И ИСТИНИТОСТ….)
- ПИТАЊЕ ЗЛОУПОТРЕБЕ ПРАВА

ФИЗИЧКЕ И ТЕХНИЧКЕ МЕРЕ ЗАШТИТЕ ПОДАТАКА У СУШТИНИ ПРЕДСТАВЉАЈУ КОМБИНАЦИЈУ БЕЗБЕДНОСНИХ ПРОЦЕДУРА И ТЕХНИЧКИХ СТАНДАРДА, КОЈА СЕ ЗАСНИВАЈУ НА ПРОЦЕНИ И ПРАКСИ...

ЧАРОБНИ ШТАПИЋ ИЛИ ПРИГОДНИ МАГИЈСКИ РИТУАЛ НЕ ПОСТОЈИ...

ИСКУСТВА СА ПРЕТХОДНИХ РАДНИХ МЕСТА СУ ДОБРА, АЛИ НИСУ ДОВОЉНА...

КОНСТАТАЦИЈА:

ПРИВАТНОСТ СЕ МАНИФЕСТУЈЕ КАО ПИТАЊЕ ОБРАДЕ И ЗАШТИТЕ ПОДАТАКА У ИКТ СИСТЕМИМА.

НЕ ПОСТОЈИ САВРШЕНА ЗАШТИТА ПОДАТАКА И ИНФОРМАЦИЈА У САЈБЕР ПРОСТОРУ!

УМЕСТО ЗАКЉУЧКА

ЗА САДА ЧОВЕК СЕ НАЛАЗИ ЈОШ УВЕК У ЦЕНТРУ САЈБЕР ПРОСТОРА!

ЧОВЕК ЈЕ УВЕК НАЈСЛАБИЈА КАРИКА СВАКОГ СИСТЕМА