# АНАЛИЗА НА РИЗИК

## Јавно обвинителство на Република Северна Македонија

Во јавните обвинителства се обработуваат следните збирки и категории на лични податоци:

* податоци потребни за кривично-правна обработка,
* податоци потребни за остварување на права од работен однос и за реализација на договорни обврски,
* податоци од видео надзор,
* податоци поврзани со пристап на веб страницата на Јавното обвинителство.

Заради кривично-правна обработка при постапувањето во конкретни предмети, јавните обвинителства ги обработуваат сите податоци неопходни за потребите на кривично-правната постапка.

За остварување на права од работен однос и за реализација на договорни обврски, јавните обвинителства од субјектите може да ги собираат, обработуваат и чуваат следните лични податоци:

* име и презиме на лице или назив на правно лице,
* живеалиште и адреса,
* адреса за електронска пошта и телефон за контакт,
* датум и место на раѓање,
* единствен матичен број/единствен даночен број,
* трансакциска сметка,
* податоци за образование, пол и национална припадност,
* податоци за претходен стаж,
* податоци за здравствена состојба,
* податоци за отсуства од работа,
* податоци за евиденција на работно време,
* податоци за годишни и периодични оценки,
* податоци за поведени дисциплински постапки,
* други податоци неопходни за остварување на права од работен однос и за реализација на договорни обврски согласно соодветните законски прописи.

Со цел да се контролира пристапот и да се обезбеди сигурност на објектот, безбедноста на вработените и странките во јавните обвинителства, како и на имотот и информациите што се лоцирани или се чуваат во просториите на јавните обвинителства, јавните обвинителства вршат видео надзор над службените простории. Податоците од видео надзорот опфаќаат видео снимки од извршениот видео надзор.

За да обезбедат транспарентност на работата, јавните обвинителства ја информираат јавноста за донесените акти и одлуки преку веб страницата на Јавното обвинителство (https://jorm.gov.mk). За секој поединечен пристап на определен дел на страницата, автоматски се врши евидентирање со запис во логови на веб-серверот на податоци за:

* IP адреса и технички детали за точната адреса од интернет страницата на која е пристапено,
* прелистувач од кој е пристапено,
* датум и време на пристапот на интернет страницата.

Обработката на лични податоци се врши во хартиена форма и електронски, а по потреба, согласно закон, се врши и размена на лични податоци со други институции (во функција на кривично-правна обработка и за реализација на договорни обврски).

Податоците во хартиена форма се чуваат во архива и канцеларии кои се заклучуваат и во кои пристапот е уреден електронски (со картичка за евиденција). Дополнително, во ходниците пред канцелариите пристапот е обезбеден со систем на видео надзор. Ништењето на податоците се спроведува согласно законските прописи за архивско работење, со претходна согласност од Државниот архив. Електронските податоци се чуваат на компјутери и сервери до кои пристапот е заштитен со комбинација од корисничко име и лозинка, а за секој влез во ссистемот се води лог-евиденција. Извесен ризик се детектира при преносот на податоци од десктоп на лаптоп компјутери или на други мобилни уреди со цел работата да се заврши надвор од работното место (во суд и сл.). Притоа, се проценува дека ризикот е од ниско или средно ниво и се однесува главно на можноста за кражба на уред или хакирање. Вработените и службените лица задолжени за одржување на системот се свесни за ризикот и ги преземаат сите неопходни мерки за таквиот ризик да се минимизира.

## Прашалник за процена на влијанието на неовластено откривање

|  |  |  |
| --- | --- | --- |
| бр. | Прашање | Проценка |
| 1 | Влијанието што неовластеното откривање може да го има врз личните податоци на поединецот (губење доверливост) – во контекст на деловната активност – и впишете соодветно проценкаПримери на губење доверливост* Досие со документи или лаптоп е изгубен при пренесување
* Опремата е фрлена без да се уништат податоците
* Личните податоци се погрешно испратени до неовластени приматели
* Клиенти можат да пристапат до туѓи податоци
* Личните податоци се објавуваат преку интеренет, или на друг начин се прават достапни
* Усб со личните податоци е украден од просториите
 | * Ниско

X Средно* Високо
* Многу високо
 |

|  |  |  |
| --- | --- | --- |
| бр. | Прашање | Проценка |
| 2 | Влијанието што неовластеното менување на податоците може да го има врз личните податоци на поединецот (губење на интегритет) – во контекст на деловната активност – и впишете соодветна проценкаПримери на губење на интегритет- Податоците кои се битни за точноста на податоците на субјектите на личните податоци се сменети. | X Ниско* Средно
* Високо
* Многу високо
 |
| 3 | Влијанието што неовластеното уништување или губење на личните податоци може да го има врз личните податоци на поединецот (губење на достапноста) - во контекст на деловната активност – и впишете соодветна проценкаПримери - Датабазата со личните податоците екомпромитирана и потребно е преземаање на активности за врќање на податоците* Досието на вработениот е изгубено и поединецот мора да ги достави податоците повторно кај контролорот,
* датабаза е корумпирана и нема копија (back-up) од истите податоци, односно нема начин за враќање на податоците
 | X Ниско* Средно
* Високо
* Многу високо
 |

Највисоката вредност се смета за конечна

## Прашалник за проценката на веројатноста за појава на закана

|  |
| --- |
| ***А) средства на контролорот (хардвер и софтвер)*** |
| 1. | Дали некој дел од обработката на личните податоци се врши преку интернет?Да | Кога обработката на личните податоци се изведува целосно или делумно преку интернет, се зголемуваат можните закани од надворешни напаѓачи преку интернет, особено кога услугата е достапна за ситекорсиници на интернет. |
| 2. | Дали е овозможено да се пристапи до внатрешниот систем за обработка на личните податоци преку интернет?Не | Кога се обезедува пристап до внатрешен систем преку интернет, веројатноста за надворешни закани се зголемува. Во исто време се зголемува и веројатноста за случајна или намерна злоупотреба од страна накорисниците. |
| 3. | Дали системот за обработка на личните податоци е поврзан со друг внатрешен или надворешен ИТ систем или услуга?Не | Поврзување со надворешни ИТ системи може да доведе до дополнителни закани поради ризиците и потенцијалните безбедносни пропусти кои се својствени за тие системи. Истото важи и за внатрешните системи,имајќи предвид дека ако не се соодветно |

|  |  |  |
| --- | --- | --- |
|  |  | конфигурирани, таквите врски може да овозможат пристап до личните податоци на повеќе лица кај контролорот. |
| 4. | Дали неовластени лица можат лесно да пристапат до средствата за обработка на личните податоци?Не | Иако фокусот е ставен на електронските системи и услуги, физичката безбедност е важен аспект, кој доколку не е соодветно заштитен, може сериозно да ја загрозибезбедноста. |
| 5. | Дали системот за обработка на личните податоци е дизајниран, имплементиран или одржуван без да се следат најдобрите практики?Да | Лошо дизајнираните, имплементирани и/или одржувани хардверски и софтверски компоненти може да претставуваат сериозни ризици за безбедноста на личните податоци. За таа цел, најдобрите практики го акумулираат искуството од претходните настани и може да се сметаат за практични упатства како да се избегне изложување и дасе постигнат одредени нивоа на издржливост. |
| ***Б) Постапки/процедури поврзани со обработка на личните податоци*** |
| 6. | Дали улогите и одговорностите на вработените за заштита на личните податоци се нејасни или не се јасно дефинирани?Не | Во случај кога улогите и одговорностите не се јасно дефинирани, пристапот па и другиот вид на обработка на личните податоци може да биде неконтролиран, што може да резултира со неовластено пристапување и користење на ресурсите и загрозување нацелокупната безбедност на системот. |
| 7. | Дали е јасно дефинирана употребата на интернет, системот и физичките ресурси кај самиот контролор?Да | Кога употребата на ресусрсите не е јасно дефинирана, може да настанат безбедносни закани поради недоразбирање или намерна злоупотреба. Јасната дефиниција за мрежна инфраструктура, информатичкиот систем и физичките ресурси може да ги намалипотенцијалните ризици. |
| 8. | Дали на вработените им е дозволено да користат свои медиуми (усб, лаптоп...) за да се поврзат со системот за заштита на личните податоци?Да | Вработените што ги користат нивните лични уреди во рамки на контролорот може да го зголемат ризикот од истекување на податоци или неовластен пристап до информатичкиот систем. Покрај тоа, бидејќи уредите не се централно контролорирани, тие може дадоведат вируси и други закани во системот. |
| 9. | Дали на вработените им е дозволено да пренесуваат, складираат или на друг начин да ги обработуваат личните податоци надвор од просториите на контролорот? | Обработката на личните податоци надвор од просториите на контролорот може да понуди поголема флескибилност, но во исто време воведува дополнителни ризици, посебно со пренесување на податоци преку несигурнимрежи (пр. отворени WI-FI мрежи) и со тоа се |

|  |  |  |
| --- | --- | --- |
|  | Да | зголемува ризикот од неовластен пристап иупотреба на овие податоци. |
| 10. | Дали е возможно да се обработат личните податоци без притоа за истото да се зачува лог (запис)?Не | Недостаток на соодветни механизми за мониторирање и запишување на логови може да ја зголеми злоупотребата на процесите/процедурите и ресурсите, што резултира со злупотреба на личнитеподатоци. |
| ***В) Различни страни и поединци вклучени во обработката на личните податоци*** |
| 11. | Дали обработката на личните податоци се врши од недефиниран број на вработени?Не | Кога пристапот (и понатамошната обработка) на личните податоци е отворен за голем број на вработени, се зголемуваат можностите за злоупотреба од човечки фактор. Јасно дефинирање на пристап до личните податоци и ограничување на пристапот само на тие лица може да придонесе за безбедноста наличните податоци. |
| 12. | Дали некој дел од активностите на обработка на личните податоци се врши од трета страна (обработувач)?Да | Кога обработката се врши од страна на обработувачи, контролорот може делумно да ја загуби контролата врз овие податоци. Контролорот мора да подготви соодветна процедура за избор на обработувачи, кои можат да понудат високо ниво на безбедност и јасно да се дефинира кој дел од обработката им е доделен, одржувајќи колкушто е можно повисоко ниво на контрола. |
| 13. | Дали страните/поединците кои се вклучени во обработката на личните податоци се јасно информирани за нивните обврски?Да | Кога вработените не се јасно информирани за нивните обврски, заканите од случајна злоупотреба, како што се откривање или уништување на податоците значително се зголемуваат. |
| 14. | Дали вработените кои се вклучени во обработката на личните податоци се обучени, односно имаат знаење од областа на осигурување на безбедност на активностите на обработка?Да | Кога вработените не се свесни за потребата од примената на безбедносни мерки, тие случајно можат да претставуваат дополнителни закани за системот. Обуката во голема мера ќе придонесе за освестување на вработените, како за нивнтие обврски за заштита на личните пдоатоци, така и запримена на специфични мерки. |
| 15. | Дали страните/поединците кои се вклучени во обработката на личните податоци го занемаруваат безбедното складирање/чување на податоците, како и уништувањето на личнитеподатоци? | Многу нарушувања на личните податоци се случуваат поради недостаток на мерки за физичка заштита, како што се брави и безбедносни системи за уништување. Датотеките базирани на хартија обично седел од влезот или излезот на |

|  |  |  |
| --- | --- | --- |
|  | Не | информативниот систем, може да содржат лични податоци и исто така треба да бидатзаштитени од неволастено откривање и повторна употреба. |
| ***Г) Деловниот процес и обемот на обработка*** |
| 16. | Дали сметате дека вашиот бизнис е склон кон сајбер напади?Да | Доколку до сега се случил вакво напад во овој деловен сектор, постои индикација дека организацијата треба да преземе соодветнимерки за да се избегне сличен настан. |
| 17. | Дали сте претрпеле некој сајбер напад или друг начин на нарушување на безбедноста во последните две години?Не | Ако конторолорот веќе бил цел на напад треба да се преземат мерки за да се спречат слични настани во иднина. |
| 18. | Дали сте добиле некое известување и/или поплака во однос на безбедноста на ИТ системот користен за обработка на личните податоци во последните две години?Не | Безбедносни грешки, односно слабости може да се искористат за извршување на сајбер или физички напади на системот или услугите. |
| 19. | Дали активностите на обработка опфаќаат голем обем на лични податоци за субјектите?Да | Видот и обемот на личните податоци може да ги направат активностите на обработка привлечни за напаѓачи. |
| 20. | Дали постојат посебни најдобри практики за вашиот деловен сектор кои не биле соодветно следени?Не | Специфични безбедносни мерки за секторот обично се прилагодуваат на потребите и ризиците на конкретниот сектор. Напочитување на соодветните најдобри практики може да биде показател за лошоуправување со безбедноста. |

Следејќи го овој пристап, нивото на веројатност за појава на закана може да се дефинира за секоја од областите на проценка, и тоа:

* Ниско: мала е веројатноста дека заканата ќе се оствари,
* Средно: постои разумна шанса заканата да се оствари,
* Високо: заканата најверојатно ќе се оствари.

## Ниско : \_\_\_\_\_\_\_\_\_\_\_\_\_

Средно: постои мала шанса заканата да се оствари, но нивото на влијание на заканата би било ограничено

Високо:

Конечна евалуација – процена на ризик

## Влијание Х веројатност за појава на заканата = ниво на ризик

|  |
| --- |
| Нивото на влијание |
|  | Ниско | Средно | Високо/многувисоко |
| Можната појава на заканата | Ниско | X |  |  |
| Средно |
| Високо |  |  |

 низок ризик среден ризик висок ризик

Изготвила:

Билјана Арсовска

Офицер за заштита на личните податоци

Јавно обвинителство на Република Северна Македонија