Политика за воспоставување на систем за заштита на личните податоци во Институтот за акредитација на Република Северна Македонија

Основни одредби

Политиката за воспоставување на ситем за заштита на личните податоци (во понатамошниот текст**: Политика)** е почетната точка и рамковен документ во изградбата на системот за технички и организациски мерки за заштитата на личните податоци во Институтот за акредитација на Република Северна Македонија (ИАРСМ), (во понатамошниот текст: **ИАРСМ односно Контролор**).

Политиката е документ кој ги поставува принципите и насоките за остварување на доверливост, интегритет и достапноста на личните податоци во согласност со Законот за заштита на личните податоци, (во натамошниот текст: Законот) како и соодветните подзаконски акти, т.е. Правилници и останата секторска позитивна законска регулатива (Закон за акредитација).

За остварување на своите цели, ИАРСМ имплементира процедури, упатства и стандарди во согласност со проценката на нивото на ризици при обработка на личните податоци.

ИАРСМ како Контролор, а преку континуиран систем за следење на ризиците во работењето предлага мерки за ажурирање на оваа Политика и соодветните процедури и упатства со цел на зголемување на нивото на сигурност односно намалување на заканите по безбедноста на личните податоци и интегритетот, доверливоста и достапноста на личните податоци.

Секоја информација како личен податок која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува (субјект на лични податоци) е потребно соодветно да биде заштитена, независно од формата или средствата преку која се пренесува или чува. Од таму подрачје на примена на оваа Политика е во сите процеси и организациони делови на ИАРСМ.

Примена

Одредбите од оваа Политика се применуваат за:

- целосно и делумно автоматизирана обработка на личните податоци;
- друга обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Дефиниции

- **Личен податок** е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува (субјект на лични податоци), а физичко лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на идентификатор како што се име и презиме, матичен број на граѓанинот, податоци за локација, идентификатор преку интернет, или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, генетски, ментален, економски, културен или социјален идентитет на тоа физичко лице;
- **Информацијата** е основно средство кое треба соодветно да се заштити независно од формата (пишана, говорна, печатена или електронска);
- **Безбедноста на Информацискиот Систем** се дефинира како обезбедување на следниве основни принципи:
  - **Доверливост**: Информацијата е достапна само на оние кои што имаат овластен пристап до неа;
  - **Интегритет**: Заштита на точноста и конзистентноста на информацијата и на методите на обработка;
  - **Расположливост:** Овластените корисници имаат пристап до податоците и соодветните ИТ системи , кога за тоа има деловна потреба;
  - **Веродостојност:** Потврда и веродостојност на активностите поврзани со пристапот и користењето на информациите;
  - **Отчетност:** Одговорноста за активностите поврзани со користењето и пристап до податоците се еднозначно утврдени и јасно одредени.
- **Информатичката технологија - ИТ или Информатичко Комуникациска Технологија – ИКТ**, ги опфаќа информатичко – комуникациските средства (апликации и инфраструктура) која се користи за прибирање, обработка, дистрибуција и/или чување на информацијата во дигитална форма;
- **Информациски Систем**, подразбира систем од информатичко – комуникациски средства, човечки ресурси и процеси кои се користат за прибирање, обработка, дистрибуција и/или чување на информацијата во дигитална форма;
- **Систем-администратор (Администратор на информацискиот систем)** е стручно лице од информатичко-комуникациската област, вработено при ИАРСМ—или надворешно ангажирано правно или физичко лице, кое се грижи за функционалност на информацискиот систем во смисла на обезбедување на интегритетот и сигурноста на податоците, на апликацијата за пристап до податоците и на техничката опрема која е во функција на информацискиот систем, како и за обезбедување тајност и заштита на податоците;
- **Офицер за заштита на личните податоци** е овластено лице од Контролорот кое е одговорно за спроведување и координација на активностите и процесите потребни за усогласување со Законот за ЗЛП**;**

- **Обработка на личните податоци** е секоја операција или збир на операции кои се извршуваат врз личните податоци или група на лични податоци, автоматски или на друг начин, како што се: собирање, евидентирање, организирање, структурирање, чување, приспособување или промена, повлекување, консултирање, увид, употреба, откривање преку пренесување, објавување или на друг начин правење достапни, усогласување или комбинирање, ограничување, бришење или уништување;
- **Ограничување на обработката на личните податоци** е означување на личните податоци кои се чуваат, а со цел ограничување на нивната обработка во иднина;
- **Профилирање** е секоја форма на автоматска обработка на лични податоци, која се состои од користење на лични податоци за оценување на одредени лични аспекти поврзани со физичкото лице, а особено за анализа или предвидување на аспекти кои се однесуваат на извршување на професионалните обврски на тоа физичко лице, неговата економска состојба, здравје, лични преференции, интереси, доверливост, однесување, локација или движење;
- **Псевдонимизација** е обработка на личните податоци на таков начин што личните податоци не можат повеќе да се поврзат со одреден субјект на лични податоци без да се користат дополнителни информации, под услов таквите дополнителни информации да се чуваат одделно и да подлежат на технички и организациски мерки со кои ќе се обезбеди дека личните податоци не се поврзани со идентификувано физичко лице или физичко лице кое може да се идентификува;
- **Збирка на лични податоци** е структурирана група лични податоци која е достапна согласно со специфични критериуми, без оглед дали е централизирана, децентрализирана или распространета на функционална или географска основа;
- **Контролор** е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело, кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци, а кога целите и начинот на обработка на личните податоци се утврдени со закон, со истиот закон се определуваат контролорот или посебните критериуми за негово определување;
- **Обработувач на збирка на лични податоци** е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело кое ги обработува личните податоци во име на контролорот;
- **Корисник** е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело на кое му се откриваат личните податоци без разлика дали е тоа трето лице или не. Меѓутоа, органите на државната власт и државните органи на кои им се откриваат личните податоци во рамките на посебна истрага во согласност со закон, не се сметаат за корисници, при што обработката на овие податоци од овие органи мора да биде во согласност со важечките правила за заштита на личните податоци според целите на таа обработка;
- **Трето лице** е секое физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело, кое не е субјект на лични податоци, контролор, обработувач или лице, кое

под директно овластување на контролорот или обработувачот е овластено да ги обработува податоците;

- **Согласност** на субјектот на лични податоци е секоја слободно дадена, конкретна, информирана и недвосмислено изјавена волја на субјектот на личните податоци, преку изјава или јасно потврдено дејствие, а со кое се изразува согласност за обработка на неговите лични податоци;
- **Нарушување на безбедност на личните податоци** е секое нарушување на безбедноста, што доведува до случајно или незаконско уништување, губење, менување, неовластено откривање или пристап до личните податоци кои се пренесуваат, чуваат или на друг начин се обработуваат;
- **Посебни категории на лични податоц**и се лични податоци кои откриваат расно или етничко потекло, политички ставови, верски или филозофски убедувања или членство во синдикални организации, како и генетски податоци, биометриски податоци, податоци што се однесуваат на здравјето или податоци за сексуалниот живот или сексуалната ориентација на физичкото лице.

Организациска поставеност и одговорности

Контролорот има воспоставено соодветна организациска структура за поддршка на Законот за заштита на личните податоци (ЗЛП) како и соодветните Правилници, при што одлучувачка улога за нивна примена согласно Законот секако има Офицерот за заштита на лични податоци.

Контролорот има назначено овластено лице за заштита на личните податоци – како надворешен Офицер за заштита на личните податоци.

ИАРСМ како **Контролор на збирки на лични податоци** ги утврдува целите и начинот на обработка на личните податоци и е одговорен за усогласување на своето работење со Законот за личните податоци како и релевантната екстерна и интерната регулатива која произлегува од истиот.

Обработувач на збирка на лични податоци е физичко или правно лице што ги обработува личните податоци за сметка на ИАРСМ како Контролор. ИАРСМ во однос на своите вработени е во својство на обработувач согласно Закон.

Офицерот за заштита на лични податоци (во понатамошниот текст: ОЗЛП) и неговите заменици (доколку бидат назначени) како овластени лица за заштита на личните податоци ке бидат назначени од Директорот како единствен работоводен орган ~~на управување~~ на ИАРСМ.

ОЗЛП е клучната фигура преку која ИАРСМ како Контролор ја обезбедува и ја демонстрира усогласеноста со прописите за заштита на личните податоци. Во таа насока ОЗЛП има стратешка и независна позиција за да се постигне поефикасно извршување на оваа функција и повисок степен на заштита на личните податоци. ОЗЛП ја следи усогласеноста со Законот и со прописите донесени врз основа на Законот што се однесуваат на обработката на личните податоци, како и со внатрешните прописи за заштита на личните податоци и со документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

Главните одговорности и задачи на ОЗЛП во ИАРСМ се :

- учествува во донесувањето на одлуки поврзани со обработката на личните податоци, како и со остварувањето на правата на субјектите на личните податоци,
- ја следи усогласеноста со законот и прописите донесени врз основа на законот, што се однесуваат на обработката на личните податоци, како и со внатрешните прописи за заштита на личните податоци и со документацијата за техничките и организационите мерки за обезбедување на тајност и заштита на обработката на лични податоци,
- ги изработува внатрешните прописи за заштита на личните податоци и потребната документација за организационите и техничките мерки за обезбедување на тајност и заштита на личните податоци,
- ја координира контролата на постапките и упатствата утврдени со внатрешните прописи кои се однесуваат на личните податоци,
- предлага обука на вработените во врска со заштитата на личните податоци
- учествува во донесувањето на одлуки поврзани со обработката на личните податоци, како и со остварувањето на правата на субјектите на личните податоци,
- ја координира контролата на постапките и упатствата утврдени во внатрешните прописи за заштита на личните податоци и во документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци,
- ја координира работата на замениците Офицери(доколку бидат назначени),
- донесува програма за работа на ОЗЛП,
- поднесува до Директорот Годишен извештај за превземените активности ,
- учествува на состаноци, колегиуми,проекти, средби и комуникација каде што предмет на обработка или дискусија се личните податоци,односно обработка на истите
- учествува и членува воработни групи,комисии и други тела во ИАРСМ,како и во домашни и меѓународни здруженија и организации од областа на заштитата на личните податоци ,
- предлага учество на обуки за офицерот и вработените кои обработуваат лични податоци.

- **Менаџментот на ИАРСМ како Контролор** – претставен преку Директорот на ИАРСМ обезбедува адекватна организациска поставеност и алокација на соодветни ресурси за ефикасно управување со процесот на заштита и усогласеност со Законот за заштита на личните податоци.
- **Раководители** - Раководителите на соодветните -организациони единици и членовите на работните тела во ИАРСМ имаат одговорност во процесот на заштита на личните податоци, како што следува:
  - Одговорни се за збирките на личните податоци кои се водат во нивните организациони единици (Сектор/Одделение, или работно тело) доколку се востановени такви збирки;
  - имплементација и одржување на контролите кои се однесуваат на нивниот делокруг на работење, а се поврзани со процесот за заштита на лични податоци;
  - соработуваат со Офицерот за заштита на лични податоци во одредувањето на ризиците и дефинирањето на мерките и контролите за заштита на лични податоци

- ги усогласуваат процесите и интерната документација согласно препораките од Офицерот на лични податоци односно одредбите од Законот за заштита на лични податоци.
- го известуваат Офицерот за заштита на личните податоци за барање и реализација на јавна набавка во која се тангираат личните податоци.
- при подготовка на подзаконска регулатива од областа на електронските комуникации каде што би имало обработка на лични податоци задолжително се консултираат и бараат конфирмација од ОЗЛП

Систем на контроли за заштита на личните податоци

Безбедноста на личните податоци е прашање кое е многу пошироко од едноставна примена на соодветни технички и организациски мерки. Безбедноста е предуслов за постигнување усогласеност со сите други принципи на обработка на личните податоци. Контролорот воспоставува систем на организациски и технички мерки во согласност со Правилникот за безбедност на обработката на личните податоци и со Правилникот за начинот на нарушување на безбедноста на личните податоци и останатата легислатива од областа за заштита на личните податоци и најдобрите практики и воспоставени стандарди. Овие мерки обезебедуваат соодветно високо ниво на заштита на податоците и инфраструктурата за обработка на информациите и податоците, вклучително и личните податоци.

Безбедноста на личните податоци се обезбедува преку исполнување на следниве начела:

- **Доверливост**: Податокот е достапен само на оние кои што имаат овластен пристап до неа;
- **Интегритет** : Заштита на точноста и конзистентноста на податоците и на методите на обработка;
- **Расположливост:** Само овластените корисници имаат пристап до податоците и соодветните ИТ системи , само кога за тоа има деловна потреба;
- **Неодречливост :** Потврда и неодречливост на активностите поврзани со пристапот и користењето на информациите;
- **Отчетност:** Одговорноста за активностите поврзани со користењето и пристап до податоците се еднозначно утврдени и јасно одредени.

Заштитата на личните податоци кај Контролорот се базира на следниве основни принципи:

- Проценка на нивото на ризик, за што постои соодветната Методологија за проценка на влијанието на заштита на личните податоци во ИАРСМ,
- ИАРСМ како Контролор при утврдувањето и проценатa на ризикот (управување со ризик) ги зема во предвид ризиците кои се поврзани со обработката, особено од случајно или незаконско уништување, губење, менување или неовластено откривање на личните податоци,
- Соодветна структура на документација составена од Политики, процедури, упатства и други интерни акти – со кои се дефинирани процесите и одговорностите во процесот

на спроведување и контрола на техничките и организациски мерки за заштита на личните податоци.

- Имплементација на систем на контроли кои се поделени на:
  - Физички контроли, кои служат за обезбедување на адекватна физичка сигурност на личните податоци и информативните средства (сервери, мрежни уреди). Како примери на физички контроли се употребата на уреди за непрекинато напојување (на пр: UPS), служба за обезбедување, видеонадзор во објектите на Контролорот, сензори и аларми и слични мерки за контрола на физичкиот пристап и заштита на ресурсите и средствата кои се користат за обработка, пренос и чување на личните податоци.
  - Технички контроли, се контроли кои се вградени во информатичките средства односно апликативниот софтвер, мрежно - комуникациската опрема и придружните уреди кои се користат за прибирање, обработка, пренос и/или чување на личните податоци.
  - Административни контроли, вклучуваат воспоставување процедури и упатства, за овластување на корисниците (вработени, трети лица) кои имаат пристап до личните податоци и потребната авторизација за извршување на своите деловни процеси.
- Примена на принципот на заштита на личните податоци по принципот by default и by design - според овој принцип Контролорот ИАРСМ имплементира соодветни технички и организациски мерки со кои ќе се осигура дека по правило (default) ги обработува само оние лични податоци кои што се неопходни за постигнување на целта на конкретната обработка. Тоа значи дека со имплементираните мерки Контролорот го обработува само минималното количество на лични податоци, во опсег кој е неопходен за исполнување на целта на конкретната обработка.

Општи начела за обработка на личните податоци

Заштитата на личните податоци спаѓа во основните права и слободи на граѓаните загарантирани со Уставот на РепубликаСеверна Македонија и Европските, односно меѓународните Конвенции. Ова особено го подразбира правото на приватност во врска со обработката на лични податоци.

Согласно Законот за заштита на личните податоци (Закон за ЗЛП) и Европската регулатива за заштита на личните податоци (EU General Data Protection Regulation-GDPR) воспоставени се осум принципи на заштита на податоците како темелни вредности:

- личните податоци се прибираат и обработуваат со законски основ, на транспарентен начин (претходно информирање) и со почитување на правилата за обработка на посебните категории лични податоци (лични податоци што го откриваат расното или етничко потекло, политичката определба, религиозни или филозофски определби, членување во синдикати и обработка на податоци за здравствената состојба или сексуалниот живот).
- личните податоци се обработуваат согласно со закон, во доволна мера и на транспарентен начин во однос на субјектот на личните податоци („законитост, правичност и транспарентност“),

- личните податоци се собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели пропишани со Законот за електронски комуникации ?
- личните податоци се соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат („минимален обем на податоци“),
- личните податоци се точни и ажурирани, при што ќе се преземат сите соодветни мерки за навремено бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени („точност“),
- личните податоци се чуваат во форма која овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за целите поради кои се обработуваат личните податоци. Личните податоци може да се чуваат подолго од нивниот рок на чување ако се обработуваат за статиститички цели, подготовка на извештаи, остварување на законските обврски на Контролорот, а со применување на соодветни технички и организациски мерки согласно со овој закон, заради заштита на правата и слободите на субјектот на личните податоци („ограничување на рокот на чување“),
- личните податоци се обработени на начин кој обезбедува соодветно ниво на безбедност, вклучувајќи заштита од неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување, со примена на соодветни технички или организациски мерки („интегритет и доверливост“).
- личните податоци нема да се пренесуваат во земја или територија надвор од Европската Унија или Европската Економска Заедница доколку таа земја или територија не обезбеди соодветно ниво на заштита на правата и слободите на субјектите во врска со обработката на личните податоци.

За остварување на овие основни цели Контролорот, развива и одржува систем на интерни контроли, во согласност за Законот за заштита на лични податоци, како и релевантните најдобри практики и стандарди, како што е опишано во Правилникот за безбедност на обработката на личните податоци во ИАРСМ.

Обработката на личните податоци во ИАРСМ е законита, бидејќи се врши врз основа на Законот за ЗЛП, подзаконските акти донесени од Агенцијата за заштита на лични податоци во кои се имплементирани и одредбите од соодветна ресорна легислатива релевантна за работењето на Контролорот од национален и меѓународен карактер, правична и се одвива на транспарентен начин во однос на субјектот на личните податоци.

Проценка на влијанието на заштитата на личните податоци (ПВЗЛП)

Кога при користење на нови технологии за некој вид на обработка, според природата, обемот, контекстот и целите на обработката, постои веројатност истата да предизвика висок ризик за правата и слободите на физичките лица пред да биде извршена обработката, ИАРСМ како Контролор извршува проценка на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци. Една проценка може да се однесува на серија слични операции на обработка, кои претставуваат слични високи ризици. Проценката на влијанието на заштитата на личните податоци како алатка

дефинирана во Методологијата за проценка на влијанието за заштитата на личните податоци се користи од страна на ИАРСМ како Контролор со цел да ги идентификуваат и адресираат сите проблеми со обработката на личните податоци кои што може да настанат при развој на нови продукти или услуги, или при преземање нови активности кои вклучуваат обработка на лични податоци. Мерките за заштита на личните податоци во ИАРСМ се имплементирани врз основа на претходно спроведена процена на ризиците.

Проценката на влијанието на заштитата на личните податоци задолжително се изведува пред започнување на обработка на лични податоци со користење на нови технологии, и обработка која може да има висок ризик за правата и слободите на физичките лица.

Пренос на лични податоци во трети земји

ИАРСМ во својство на Контролор има обврска за известување до Агенцијата за заштита на личните податоци за преносот на лични податоци на субјекти кои ги обработува во случај да истите се пренесуваат кон земјите на Европската Унија или Европската Економска Заедница.

Во случај преносот на личните податоци да е потребно да се изврши кон земја која не е членка на Европската Унија или Европската Економска Заедница, односно преносот се врши во трети земји или меѓународни институции или организации, неопходна е претходна согласност од страна на Агенцијата за заштита на личните податоци пред да се оствари самиот пренос . Барањето за за добивање одобрение за пренос се доставува 15 дена пред денот на започнување на преносот на личните податоци, а Агенцијата за заштита на личните податоци доставува одговор во рок од 90 дена од денот на поднесувањето на податоците.

Во случај кога третата земја или меѓународна организација во која треба да се пренесат личните податоци обезбедува соодветен степен на заштита на личните податоци, ИАРСМ во својство на Контролор може да изврши пренос на личните податоци врз основа на одлука за соодветност донесена од страна на Агенцијата за заштита на личните податоци.

Во основа, преносот на лични податоци во други земји ИАРСМ може да го врши кога:

- преносот е неопходен за спроведување на деловна или друга активност за која субјектот на лични податоци дал изречна согласност,
- заштита на животот или суштинските интереси на субјектот на лични податоци,
- други со закон определени причини, во обем предвиден со законот.

ИАРСМ како Контролор на личните податоци, има воспоставено правила и принципи за пренос на личните податоци, во согласност со релевантната законска регулатива кои се содржани во Правилникот за пренос на личните податоци на ИАРСМ.

Видео надзор

Видео надзорот во ИАРСМ може да се врши:

- заради обезбедување контрола над влегувањето и излегувањето од службените простории само за безбедносни цели и
- заради заштита на сопственоста.

Процесот на воспоставување на систем за видео надзор и превземените мерки и одговорностите се дефинираат во соодветен Правилник за видео надзор на ИАРСМ. ИАРСМ ќе истакне соодветно известување за видео надзор со кое ќе им овозможи на субјектите на лични податоци да се запознаат со поставеноста, обврските и правата поврзани со инсталираниот систем за видео надзор. Пристап до соодветната регулатива со неопходните податоци може да биде остварен преку веб страната и преку скенирање на код кој е поставен на известувањето.

Записите кои се прават во процесот на снимање од видео надзорот ќе бидат сочувани додека се исполнат причините за нивната цел определена во подзаконската регулатива, но, во принцип не подолго од 30 дена, освен ако со друг закон не е предвиден подолг рок во кој се содржани заштитни мерки и други мерки за заштита на правата и слободите на субјектите на личните податоци во согласност со одредбите од овој закон.

Нивоа на мерки за безбедност на обработката на личните податоци

Земајќи ги предвид природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица, контролорот е должен да примени соодветно ниво на технички и организациски мерки кое ќе биде пропорционално и на активностите за обработка на личните податоци.

Техничките и организациските мерки кои ги применува ИАРСМ може да се класифицираат во две нивоа:

- стандардно и

- високо.

Стандардно ниво

Во ИАРСМ се применуваат следните нивоа на технички и организациски мерки од стандардно ниво:

- Физичка безбедност на серверите и другата опрема која се користи за обработка на личните податоци;
- Соодветни методи за автентикација и регистрација на корисниците;
- Соодветни политики и правила за управување со лозинките;
- Обезбедување на серверите и другата опрема која се користи за обработка на личните податоци;
- Автоматизирано одјавување на информацискиот систем после изминување на определен период од 15 минути на неактивност и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;

- Инсталирана хардверска/софтверска заштитна мрежна бариера („анг. Firewall“) и рутер помеѓу информацискиот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот;
- Ефективна и сигурна анти-вирусна и анти-спајвер заштита на информацискиот систем, која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвери;
- Ефективна и сигурна анти-спам заштита, која постојано се ажурира заради превентивна заштита од спамови;
- Приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување;
- Обезбедување на соодветна издвоена локација за чување на сигурносни копии (backup) од личните податоци во заштитена форма;
- Обезбедување на локација за опоравување од катастрофа (disaster recovery location) каде се прави репликација на податоците од серверите на примарната локација – ИАРСМ во Скопје, а во кој се вклучени file server, e-mail server, web server, итн.;
- Процес за ефикасна детекција и справување со сигурносни инциденти;
- Управување со преносливи медиуми

Високо ниво

Во ИАРСМ се применуваат следните нивоа на технички и организациски мерки од високо ниво:

- Управување со лозинки – кои се однесуваат на заштита и злоупотреба на системот за чување и користење на лозинките (password hashing);
- Управување со преносливи медиуми - преку користење на соодветни методи за заштита (енкрипција) кои гарантираат дека податоците нема да бидат читливи од неавторизирани лица, како на пример користење на алатка за енкрипција на дисковите на преносните компјутери;
- Тестирање на информацискиот систем - воведување на практика за редовно независно и професионално тестирање на механизмите и контролите за заштита на податоците и сајбер закани, како на пример етичко хакирање;
- Пренесување на личните податоци преку мрежа за електронски комуникации со користење на соодветни методи за енкрипција и заштита.

Ниво на примена

За сите збирки ИАРСМ задолжително применува технички и организациски мерки кои се класифицирани на стандардно ниво.

За збирките кои содржат: посебни категории на лични податоци, лични податоци кои се обработуваат заради заштита на безбедноста и интересите на државата, задолжително се применуваат технички и организациски мерки кои се класифицирани на стандардно и високо ниво

За документите кои содржат матичен број на граѓанинот, задолжително се применуваат технички и организациски мерки кои се класифицирани на стандардно и високо ниво.

Законитост на обработката

Во рамките на управувањето со системот за заштита на личните податоци во ИАРСМ како Контролор, а согласно неговите надлежности и функции утврдени со Законот за акредитација како и другите позитивни прописи, се востановуваат следните збирки на лични податоци:

-Збирка на лични податоци на вработени и договорно ангажирани лица

-Збирка на лични податоци на оценувачи и експерти.

Составен дел на оваа Политика е и Прилог 1: Евиденција на активности на обработка во која се дадени условите кои ја одредуваат законитоста на обработката, целите на обработката, категориите на лични податоци кои се предмет на обработка, категориите на субјекти на личните податоци како и роковите на чување на личните податоци.

Завршни одредби

Политиката за заштита на личните податоци е предмет на редовни прегледи и ажурирања согласно промени во организациската поставеност, техничката инфраструктура или нови законски и /или регулаторни барања.

Офицерот за заштита на личните податоци најмалку еднаш годишно подготвува Извештај до Директорот на ИАРСМ за усогласеноста и адекватноста на оваа Политика кој е составен дел на Годишниот Извештај на ОЗЛП.

Оваа Политика стапува на сила и почнува да се применува на денот на донесувањето.

Институт за Акредитација на
Република Северна Македонија

Директор,
М-р Слободен Чокревски

Скопје, _____