Политика за заштита на лични податоци

СТАФ 2014 ДОО Скопје

СОДРЖИНА

Врз основа на Законот за заштита на лични податоци (Сл. весник бр. 42/20) и член 6 од Правилникот за безбедност на обработката на личните податоци (Сл.весник бр.122/2020),

СТАФ 2014 ДОО Скопје

донесе,

Политика за заштита на лични податоци на

СТАФ 2014 ДОО Скопје

1. Цел

Политиката за заштита на личните податоци (во понатамошниот текст само**: Политика)** е почетната точка во изградбата на системот за технички и организациски мерки за заштитата на личните податоци во,

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 и соодветните правилници и позитивната законска регулатива.

За остварување на своите цели,

СТАФ 2014 ДОО Скопје

имплементира Правилници во согласност со Политиката и процена на нивото на ризици кон личните податоци.

СТАФ 2014 ДОО Скопје

преку континуиран систем за следење на ризиците во работењето предлага мерки за ажурирање на Политиката и соодветните Правилници со цел на зголемување на нивото на сигурност односно намалување на заканите по интегритетот, доверливоста и достапноста на личните податоци.

2. Подрачје на примена

Секоја информација како личен податои 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

СТАФ 2014 ДОО Скопје

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.

3. 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).
- Сигурноста на Информативниот Систем се дефинира како обезбедување на следниве основни принципи:

● **Доверливост (анг. Confidentiality)**: Информацијата е достапна само на оние коишто имаат овластен пристап до неа;

● **Интегритет (анг. Integrity)**: Заштита на точноста и конзистентноста на информацијата и на методите на обработка;

● **Расположливост (анг. Availability):** Овластените корисници имаат пристап до информацијата и до другите придружни средства потребни за нејзина презентација, кога за тоа има деловна потреба;

● **Неодречливост (ang. Non-Repudiation):** Потврда и непорекливост на активностите поврзани со пристапот и користењето на информациите ;

● **Докажливост (ang. Accountability):** Активностите поврзани со користењето и пристап до информациите може да бидат еднозначно забележани и евидентирани.

- **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.
- **Информативен Систем (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, 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 (ОЗЛП)** 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 недвосмислена изјавена волја на субјектот на личните податоци, преку изјава или јасно потврдено дејствие, а со кои 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 податоци** 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.

4. Политика за заштита на лични податоци

4.1 Организациска поставеност и одговорности

СТАФ 2014 ДОО Скопје
има воспоставено соодветна организациска структура за поддршка на Законот за заштита на личните податоци како и соодвените Правилници, во кој клучна улога има Офицерот за Заштита на Лични Податоци.

СТАФ 2014 ДОО Скопје
има назначено овластено лице за заштита на личните податоци (ОЗЛП - Офицер за заштита на личните податоци).

Контролор

СТАФ 2014 ДОО Скопје
како **контролор на збирка на лични податоци (анг. Controller)** ги утврдува целите и начинот на обработка на личните податоци, и е одговорна 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

Обработувач на збирка на лични податоци (анг. Processor) е физичко или правно лице, законски овластен државен орган што ги обработува личните податоци за сметка на

СТАФ 2014 ДОО Скопје
како Контролор.

Офицер за заштита на личните податоци

Со цел за спроведување и контрола техничките и организациски мерки при прибирањето, обработката и чувањето на личните податоци и заштита на истите, како и усогласеност со законските барања, определува Офицер за заштита на личните податоци.
Офицер за заштита на лични податоци (во понатамошниот текст: ОЗЛП) како овластено лице за заштита на личните податоци е назначено од највисоките органи на управување на

СТАФ 2014 ДОО Скопје

СТАФ 2014 ДОО Скопје
како Контролор е одговорен да обезбеди усогласеност со прописите за заштита на личните податоци и да демонстрира усогласеност со овие прописи, а ОЗЛП е клучната фигура преку која ќе ја исполни оваа обврска. 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.

Поспецифично главните одоговорности и задачи на ОЗЛП се како што следува:

- 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 орханизационите 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 и врши други работи утврдени со закон и со прописи донесени врз основа на законот, како и со внатрешни прописи за заштита на личните податоци и со документацијата за техничките и организациските мерки за обезбедување тајност и заштита 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;
- предлага обука на вработените во врска со заштитата на личните податоци.

4.2 Систем на контроли за заштита на личните податоци

Безбедноста е предуслов за постигнување усогласеност со сите други принципи на обработка на личните податоци.

СТАФ 2014 ДОО Скопје
има воспоставено систем со организациски и технички мерки во согласност со Правилникот за безбедност на Агенцијата за заштита на личните податоци.

Овие мерки обезбедуваат соодветно ниво на заштита на податоците и инфраструктурата за обработка на личните податоци.

Безбедноста на личните податоци се обезбедува преку исполнување не следниве атрибути:

- **Доверливост (анг. Confidentiality)**: Податокот е достапен само на оние коишто имаат овластен пристап до неа;
- **Интегритет (анг. Integrity)**: Заштита на точноста и конзистентноста на податоците и на методите на обработка;

- **Расположливост (анг. Availability):** Овластените корисници имаат пристап до податоците и до другите придружни средства потребни за нејзина презентација, кога за тоа има деловна потреба;

- **Неодречливост (ang. Non-Repudiation):** Потврда и непорекливост на активностите поврзани со пристапот и користењето на податоците;

- **Докажливост (ang. Accountability):** Активностите поврзани со користењето и пристап до податоците треба да бидат еднозначно забележани и евидентирани.

Заштита на личните податоци се базира на следниве основни принципи:

- Имплементација на соодветен систем на контроли кои се поделени на
- Физички контроли, служат за обезбедување на адекватна физичка сигурност на информацијата и информативните средства (сервери, мрежни уреди). Како примери на физички контроли се употребата на уреди за непрекинато напојување (анг. UPS), чуварска служба, сензори и аларми и слични мерки за контрола на физичкиот пристап и заштита на ресурсите и средствата кои се користат за оброабитка, пренос и чување на личните податоци..
- Технички контроли, се контроли кои се вградени во информативните средства односно апликативниот софтвер, мрежно - комуникациската опрема и придружните уреди. Техничките контроли уште се наречени и логички контроли.
- Административни контроли, вклучуваат воспоставување процедури и упатства, за овластување на корисниците (вработени, трети лица) кои имаат пристап до информативниот систем и им се овозможува потребната авторизација за извршување на своите деловни процеси.

- Примена на принципот на заштита на личните податоци by design - според овој принцип соодветните технички и организациски во процесот на обработка на личните податоци се применуваат уште во моментот на дефинирање на средствата на обработка. Овој принцип треба да се применува и при тековни активности и средства за обработка, за да се осигура контролорот дека ефективно се справува со целиот животен век на личните податоци коишто ги обработува.
- Примена на принципот на заштита на личните податоци by default - според овој принцип се применуваат соодветни технички и организациски мерки со кои ќе се осигура дека по правило default ги обработува само оние лични податоци коишто се неопходни за постигнување на целта на конкретната обработка. Тоа значи дека со имплементираните мерки, ги обработува само неопходното количество (обем) на лични податоци, во опсег кој е неопходен за исполнување на целта на конкретната обработка, и со време на чување и достапност сè до исполнување на конкретната цел на обработката.

4.3 Општи начела за обработка на личните податоци

Заштитата на личните податоци спаѓа во основните права и слободи на граѓаните загарантирани со Уставот на Република С. Македонија и меѓународни конвенции. Ова особено го подразбира правото на приватност во врска со обработката на личните податоци.
Согласно Законот за заштита на личните податоци (Закон за ЗЛП) и Европската регулатива за заштита на личните податоци (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 сензитивните 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).

- обработуваат согласно со закон, во доволна мера и на транспарентен начин во однос на субјектот на личните податоци („законитост, правичност и транспарентност“),
- собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели,
- соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат („минимален обем на податоци“),
- точни и каде што е потребно 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“),
- чувани 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“),
- обработени на начин кој обезбедува соодветно ниво на безбедност на личните податоци, 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“).
- соодветни технички и организациони мерки треба да се преземат за заштита од неавторизирано или незаконско обработување на личните податоци и спречување на инцидентно губење, уништување или оштетување на личните податоци.
- 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.

4.4 Законитост, правичност и транспарентност

Обработката на личните податоци, во,

СТАФ 2014 ДОО Скопје

како Контролор се базира на следниве основни принципи:

- **Законитост** - Обработката на личните податоци ќе се смета дека е законита само доколку се врши врз некој од основите наведени во Законот за ЗЛП
- **Правичност** - Следниот принцип што треба да се воспостави, откако ќе се утврди постоењето на законски основ за обработката на личните податоци, е правичноста. Правичната (фер) обработка е поврзана со идејата дека субјектот на личните податоци мора да биде свесен дека неговите лични податоци ќе се обработуваат. Тоа ќе му овозможи да донесе информирана одлука за тоа дали се согласува со таквата обработка и ќе му овозможи исполнување на своите права во однос на заштитата на своите лични податоци
- **Транспарентност** - Директно поврзан со принципот на правична обработка е принципот на транспарентност кој значи дека контролорот мора да биде отворен и јасен кон субјектот на личните податоци при обработка на неговите лични податоци. Контролорот има обврска за известување на Агенцијата за заштита на личните податоци за збирките на лични

податоци коишто се обработуваат, но и за тоа да ги известува субјектите на личните податоци. Известувањето мора да биде навремено, со користење на јасен и едноставен јазик.

- **Отчетност (Accountability**) - Успешноста на Контролорот да го примени принципот на отчетност се гледа низ призмата на усогласување со принципите на обработка на личните податоци и способноста таа усогласеност да ја докаже. Воедно, Контролорот мора да примени и соодветни технички и организациски мерки имплементирани врз основа на претходно спроведена процена на ризиците. Колку е поголем ризикот, толку построги треба да бидат мерките.

4.5 Проценка на влијанието на заштитата на личните податоци (DPIA)

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, контролорот е должен да изврши проценка на влијанието на предвидените операции на обработкатаво однос на заштитата на личните податоци. Една проценка може да се однесува на серија слични операции на обработка, кои претставуваат слични високи ризици.

СТАФ 2014 ДОО Скопје

во согласност со Законот за ЗЛП као и насоките на Агенцијата за заштита на личните податоци објавени во вид листа на видови на операции на обработка, развива и имплементира соодветен Правилник за проценка на влијанието врз заштитата на личните податоци.
Проценката на влијанието на заштитата на личните податоци како алатка се користи од со цел да се идентификуваат и адресираат сите проблеми со обработката на личните податоци коишто може да настанат при развој на нови продукти или услуги, или при преземање нови активности кои вклучуваат обработка на лични податоци. 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.

4.6 Пренос на лични податоци во трети земји

Преносот на лични податоци во трети земји соодветно се контролира со цел да се осигура дека во државата во која се примаат личните податоци ќе биде обезбеден соодветен степен на заштита на личните податоци.

СТАФ 2014 ДОО Скопје

како контролор има обврска за известување на Агенцијата за заштита на личните податоци за преносот на лични податоци ако истиот се остварува кон земјите на Европската Унија или Европската Економска Заедница.
Доколку преносот е кон земја која не е во Европската Унија или Европската Економска Заедница потребна е претходна согласност од страна на Агенцијата за заштита на личните податоци пред да се оствари самиот пренос.
Во основа преносот на лични податоци во други земји се 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

СТАФ 2014 ДОО Скопје

како Контролор на личните податоци, воспоставува правила и принципи за пренос на личните податоци, во согласност со релевантната законска регулатива соодветно опишани во Правилникот за пренос лични податоци.

4.7 Видео надзор

СТАФ 2014 ДОО Скопје
за остварување на заштитата на имотот, животот и здравјето на комитентите и вработените и обезбедување на контрола над влегувањето и излегувањето од службените и /или деловните простории може да врши видео надзор со примена на соодветни организациони мерки и технички средства.
Процесот на воспоставување на систем за видео надзор и презмените мерки и одговорностите се дефинирани во соодветниот Правилник за видео надзор.
Банката ќе истакне соодветно известување, видливо и разбирливо, со што ќе им овозможи на субјектите на лични податоци да се запознаат со перформансите на инсталираниот видео надзор. Неопходните податоци кои ќе бидат објавени на известувањето се регулирани со подзаконските акти издадени од страна на Агенцијата за заштита на лични податоци.
Записите кои се направени со помош на видео надзорот ќе бидат запамтени додека се исполнети причините за негово воспоставување, но, не подолго од 30 дена, доколку со друг закон не е побаран различен период на чување на видео записите.

5. Завршни одредби

Оваа Политика стапува на сила на денот на усвојувањето.

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 за усогласеноста и адекватноста на Политиката.

Датум на усвојување

Одобрил – Одоговорно лице
/ Директор

Потпис