**П Л А Н**

**ЗА СОЗДАВАЊE СИСТЕМ НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ**

1. **Цел на планот**

Со овој план се предвидува создавање на соодветен систем за технички и организациски мерки што (назив на здружението) ги применува за обезбедување тајност и заштита на обработката на личните податоци, а кој систем е усогласен со видот, обемот и потребите на дејноста што ја врши (назив на здружението).

1. **Обработка на лични податоци**

Во (назив на здружението) се обработуваат следните категории на лични податоци:

1. Заради спроведување на конкретни права и обврски на трудовото право:

* име и презиме на вработените во (назив на здружението);
* адреса на живеење или престојување;
* единствен матичен број на вработените;
* број на трансакациона сметка на вработените во (назив на здружението);
* извод од матична книга на родени;
* извод од државјанство;
* дипломи, уверенија за стекнато образование.

1. Лични податоци на странките и трети лица при давање правна помош во граѓански, кривични, прекршочни и управни постапки согласно Законот за заштита на личните податоци, Законот за парнична постапка, Законот за кривична постапка, Законот за прекршоците, Законот за општата управна постапка и Законот едношалтерски систем:

* име и презиме
* адреса на живеење или престојување
* единствен матичен број на граѓанинот
* телефонски броеви и е-маил адреса,и

други лични податоци потребни за изведување како докази во постапките согласно законот.

1. **Нивоа на технички и организациски мерки**

На сите документи во (назив на здружението) задолжително се преименуваат техничките и организациските мерки за обезбедување тајност и заштита на личните податоци класифицирани во три нивоа:

* основно ниво;
* средно ниво;
* високо ниво.

1. **Документација за технички и организациски мерки**

Системот за технички организациски мерки за обезбедување тајност и заштита на обработката на личните податоци во (назив на здружението) се состои од следните механизми:

* донесување на Правилник за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци;
* донесување на Правилник за определување на обврските и одговорностите на корисниците при користење на документите и информатичко комуникациската опрема;
* донесување на Правилник за пријавување, реакција и санирање на инциденти;
* донесување на Правилник за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
* донесување на Правилник за начинот на уништување на документите како и за начинот на уништување, бришење и чистење на медиумите;
* донесување на Упатство за начинот на водење, евиденција на лица овластени за вршење на обработка на личните податоци и за пренесување на медиуми надвор од работните простории во (назив на здружението).

Вработените, лицата ангажирани со договор, волонтерите и практикантите во (назив на здружението) се должни секој во рамките на своите работни задачи да ги почитуваат и применуваат овие интерни акти.

Офицерот за заштита на личните податоци е одговорното лице за заштита на личните податоци во (назив на здружението) врши редовна проценка на потребата за изготвување и донесување на нови интерни акти или промена на старите од аспект на нивно усогласување со прописите за заштита на личните податоци.

1. **Периодични контроли**

Офицерот за заштита на личните податоци во (назив на здружението) најмалку еднаш месечно ги врши следните контроли и за тоа изготвува извештај:

* Контрола на технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци,
* Контрола на евиденција за секој авторизиран/невторизиран пристап до информацискиот систем,
* Контрола на доверливоста и сигурноста на лозинките и на останатите форми на идентификација,
* Контрола на начинот за пристап на вработените и ангажираните лица во (назив на здружението) до интернет кој се однесуваат на симнување и снимање на документи преземени од електронска пошта и други извори.
* Контрола на уништување на документи кој содржат лични податоци по истекување на рокот за чување, а како и за начинот на уништување, бришење и чистење на медиумите,
* Контрола на начинот на управување со медиуми кој се носители на лични податоци,
* Контрола на примената на принципот “чисто биро”,
* Контрола на писмените овластувања издадени од страна на Претседателот и/или Управниот одбор на (назив на здружението) за вршење на обработка на личните податоци и за пренесување на медиуми надвор од работните простории на (назив на здружението),
* Контрола на начинот на воспоставување на физичка сигурност на работните простории и опремата каде што се обработуваат и чуваат личните податоци,
* Контрола на начинот на пристап до целиот информациски систем преку персоналните компјутери,
* Контрола на начинот на правење на сигурносна копија, архивирање и чување како и за повторно враќање на зачуваните лични податоци,
* Контрола на евиденцијата за физички пристап до просторијата во која се сместени серверите,
* Контрола на постапката за потпишување на изјави за тајност и заштита на обработката на личните податоци од страна на вработените, лицата ангажирани со договор, волонтерите и практикантите во (назив на здружението).

1. **Преодни и завршни одредби**

Вработените, лицата ангажирани со договор, волонтерите и практикантите во (назив на здружението) во рок од еден месец од денот на влегувањето во сила на актите за техничките и организационите мерки за обезбедување тајност и заштита на обработката на личните податоци ќе извршат прилагодување на информацискиот систем во согласност со Правила за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци.

Овој Правилник стапува на сила и ќе се применуваат од денот на нивното донесување и одобрување од страна на органот надлежен за заштита на личните податоци.

УПРАВЕН ОДБОР НА (назив на здружението)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Врз основа на Законот за заштита на лични податоци и Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, Управниот одбор на (назив на здружението)), со седиште на (улица) на ден дата година донесе

**УПАТСТВО**

**за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци**

Со ова Упатство (назив на здружението) ги пропишува техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на субјектот на личните податоци што ги применува.

Одделни изрази употребени во ова Упатство го имаат следново значење:

„**Администратор на збирки на лични податоци**“ е физичко лице овластено да се грижи за системот на управување со збирките на лични податоци и за обезбедување тајност и заштита на обработката на личните податоци.

**„Извршител**“ е физичко лице, вработен, лице ангажирано со договор, волонтер, практикант и надворешен соработник во (назив на здружението), а кое извршува работи поврзани со обработка на лични податоци..

„**Авторизиран пристап“** е овластување доделено на администраторот и извршителите за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории во (назив на здружението).

**„Документ“** е секој запис кој содржи лични податоци и истиот може да биде во електронска или хартиена форма, да се чува на медиум и во информатичко комуникациска опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку телекомуникациска мрежа.

**1. Нивоа на технички и организациски мерки**

Техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци во (назив на здружението) се класифицираат во три нивоа и тоа основно, средно и високо ниво.

За сите документи задолжително се применуваат технички и организациски мерки класифицирани на основно ниво.

Технички и организациски мерки класифицирани на основно и средно ниво се применуваат на документи кои содржат матичен број на граѓанинот, адреса на живеење и контакт информации (телефон и е-маил).

Високо ниво се применува на документи кои содржат информации согласно Закон за класифицирани информации.

**2. Правила за обработка на личните податоци надвор од работните простории**

Лични податоци може да се обработуваат само во работните простории на (назив на здружението) и врз основа на писмено овластување дадено од страна на Претседателот на (назив на здружението). Во ваков случај се применува соодветно ниво на технички и организациски мерки.

**3. Одржување на информацискиот систем**

Надворешните лица кои може да ги ангажира (назив на здружението) за одржување на информацискиот систем како и лицата што вршат обработка на личните податоци, треба во целост да ги применуваат и да се придржуваат кон законските и интерните прописи за заштита на личните податоци.

Со надворешните лица ангажирани за одржување на информацискиот систем (назив на здружението) потпишува Договор за доверливост, со кој се уредуваат обврските во доменот на заштитата на личните податоци.

**4. Правила за определување на обврските и одговорностите на корисниците при користење на документите и информатичко комуникациската опрема**

При користењето на документите и информатичко комуникациската опрема на друштвото пропишани се и усвоени Правила за определување на обврските и одговорностите на корисниците при користење на документите и информатичко комуникациската опрема со цел да се обезбеди тајност и заштита при обработката на личните податоци.

**5. Правила за начинот на правење на сигурносна копија, архивирање и чување**

Администраторот ќе врши редовно снимање на сигурносна копија и архивирање на податоците во системот, за да не дојде до нивно губење или уништување. За таа цел контролорот дефинира процедура за back-up на екстерен медиум според која еднаш неделно се меморираат внесените податоци така што во случај на пад на компјутерскиот систем или негово оштетување од каква било причина, сите податоци остануваат сочувани. Детална процедура е пропишана во интерниот акт на (назив на здружението).

**6. Технички мерки**

Заради автоматизираната обработка на личните податоци администраторот има воведено технички мерки за обезбедување заштита на обработката на личните податоци кој предвидува:

**- единствено корисничко име** за пристапдо главните бази на податоци

**- корисничко име и лозинка која дозволува пристап** на извршителите до деловите од системот потребни за извршување на нивната работа. Лозинка креирана од секое овластено лице, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;

***-* автоматизирано отфрлање од системот после три неуспешни обиди за најавување** (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на извршителот дека треба да се побара инструкција од администраторот на збирки на лични податоци;

***-* ефективна и сигурна анти-вирусна и анти-спајверзаштита** на системот заради превенција од непознати и непланирани закани од нови вируси

***-* ефективна и сигурна анти-спам заштита**, која постојано се ажурира заради заштита од спамови

- приклучување на серверот на енергетска мрежа преку уред кој обезбедува непрекинато напојување и при пад на електричната енергија до негово безбедно исклучување

- администраторот ќе обезбеди соодветна **заштита – мрежна бариера (“firewall“)** помеѓу интерниот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или побивање на системот.

- доделување/одземање на корисничко име и лозинка при нови вработувања/престан ќе извршува само одговорното лице во (назив на здружението).

**7. Организациски мерки**

Контролорот обезбедува организациски мерки за заштита на обработката на личните податоци, и тоа:

* целосна доверливост и сигурност на лозинките и на останатите форми на идентификација за пристап до личните податоци;
* организациски правила за пристап на извршителите до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори;
* уништување на документи кои содржат лични податоци по истекување на рокот на чување;
* секое изнесување на било кој медиум кој е носител на лични податоци (компакт диск, пренослив компјутер и други медиуми за пренос на податоци), надвор од работните простории да биде со посебна дозвола и контрола за да не дојде до нивно губење или незаконско користење;
* мерки за физичка сигурност на работните простории и опремата каде што се чуваат и обработуваат личните податоци и тоа преку Агенција за обезбедување на работните простории со:
* физичка заштита на серверот
* почитување на техничките упатства при инсталирање и користење на опремата на која се обработуваат лични податоци.

**8.Физичка сигурност на информацискиот систем**

Просторијата во која е сместен серверот на кои се инсталирани програмите за обработка на личните податоци се заштитени од сите ризици и потенцијални закани како кражба, пожар, експлозија, вода, пречки во снабдување со електрична енергија и електромагнетно зрачење.

Физичкиот пристап до серверот е дозволен само на овластени лица во (назив на здружението).

**9. Информирање за заштитата на личните податоци**

(1) Лицата кои ќе се вработат или ќе бидат ангажирани во (назив на здружението), пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

(2) За лицата кои се ангажирани за изршување на работа во (назив на здружението), во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(3) (назив на здружението) пред непосредното започнување со работа на овластените лица, дополнително ги информира за непосредните обврски за заштита на личните податоци.

(4) Лицата кои се вработени, лица ангажирани со договор, волонтери и практиканти во (назив на здружението), пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

(5) Изјавата од став (4) на оваа точка особено содржи: дека лицата ќе ги почитуваат начелата за заштита на личните податоци пред нивниот пристап до личните податоци, ќе вршат обработка на личните податоци согласно упатствата добиени од Претседателот на (назив на здружението), освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита.

(6) Изјавата од став (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат во (назив на здружението).

(7) (назив на здружението) задолжително врши континуирано информирање на овластените лица за непосредните обврски и одговорности за заштита на личните податоци.

**10. Идентификација и проверка**

Во информацискиот систем во (назив на здружението) е овозможен пристап само од лица кои се авторизирани преку воспоставени механизми за проверка и идентификација на корисникот.

Кога проверката се врши врз основа на корисничко име и лозинка се применуваат правила кои ја гарантираат доверливоста при пријавувањето, доделувањето и чувањето на истите. Секое право на надворешен пристап од вработен или корисник од надвор во компјутерскиот систем или локална мрежа ќе биде посебно контролирано и евидентирано.

Лозинките треба автоматски да се менуваат по изминат временски период што не може да биде подолг од пет месеци утврден во Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, како и да се чуваат заштитени со соодветни методи, така што нема да бидат разбирливи додека се валидни.

**11. Контрола на пристап и евидентирање на авторизираниот пристап**

Пристап до личните податоци, предмет на обработка, имаат само вработени лица чии работни задачи опфаќаат учество во обработката на податоците, распоредени во две нивоа на пристап, и тоа:

Прво ниво на пристап - овозможува пристап заради внесување, прегледување и обработување на личните податоци и ги опфаќа извршителите во соодветните сектори односно дирекции.

Второ ниво на пристап - овозможува пристап заради внесување, прегледување, обработување и бришење на личните податоци и го дава администраторот.

Нивоата на пристап се воспоставени и вградени во компјутерскиот систем по пат на корисничко име и лозинка како за влез во секој персонален компјутер од системот така и за влез во посебниот софтвер, во зависност од нивото на пристап што го има вработениот.

Информатичкиот систем воведен во (назив на здружението) обезбедува можност за:

1. утврдување на работната станица и корисничкото име за сите извршители кога пристапуваат до податоците, време и датум на пристапување, видот на пристапот со операциите кои се превземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање на информацискиот систем и снимање на овие податоци;
2. идентификување на компјутерскиот систем од кој се врши надворешен обид за пристап во оперативните функции или податоци;
3. регистрирање на сите промени (дополнувања, измени и бришења) направени во податоците, заедно со корисничкото име, идентификацијата на работната станица и времето и датумот на промената;

како резултат на што во секое време е обезбеден увид во моменталниот и минатиот пристап и преземени операции во базите на податоци од страна на сите овластени лица.

**12. Управување со медиумите**

Овластен корисник на медиумот е вработен, лице ангажирано со договор, волонтер или практикант кој го користи медиумот во процесот на работа.

Пренесувањето на медиумите надвор од работните простории се врши само со претходна согласност дадена од Претседателот на (назив на здружението).

По пренесување на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот се уништува, се брише или пак се чисти од личните податоци кои се снимени на него.

Уништувањето на медиумот се врши согласно пропишаните Правила за начинот на уништување на документите како и за начинот на уништување, бришење и чување на медиуми.

**13. Дополнителни правила за технички и организациски мерки**

Администраторот презема дополнителни технички и организациски мерки при обработката на личните податоци кои вклучуваат:

* обработка на посебни категории на лични податоци;
* обработка на единствениот матичен број на граѓанинот.

Преку дополнителните технички и организациски мерки предвидени во претходниот став од овој член се обезбедува:

* можност за препознавање на секој поединечен овластен пристап до информатичкиот систем;
* работа со податоците во редовното работно време во (назив на здружението).

**14. Контрола на информацискиот систем и информатичката инфраструктура**

Информацискиот систем и информатичката инфраструктура подлежат на внатрешна и надворешна контрола со цел да се провери дали постапките и упатствата содржани во интерните акти се применуваат и се во согласност со законската регулатива.

Надворешната контрола се врши на секои три години преку обработка на документи од страна на независно трето лице со цел да се провери дали постапките и упатствата се применуваат и се во согласност со прописите за заштита на лични податоци.

Внатрешната контрола се врши од страна на овластеното лице за заштита на лични податоци назначено во (назив на здружението) преку проверка на утврдените периодични контроли на начинот и степенот на заштита на личните податоци.

Извештајот од извршената контрола содржи мислење за тоа колку и како се применуваат техничките и организациски мерки за заштита на личните податоци дали се констатирани недостатоци како и дадените препораки за нивно надминување. Во извештајот треба да се содржани и податоци и факти врз основа на кои е изготвено мислењето и се предложени мерки за отстранување на констатираните недостатоци.

Извештајот се анализира од страна на одговорното лице за заштита на личните податоци. Извештајот треба да биде достaпен за увид на Дирекцијата за заштита на личните податоци.

**15.Тестирање на информацискиот систем**

Тестирањето на системот се спроведува преку професионално, објективно и независно оценување на ефикасноста и адекватноста на имплементираните сигурносни контроли.

Комплетно тестирање на системот е извршено пред негово имплементирање, а дополнително се врши на годишна основа од страна на надворешниот стручен соработник, доколку таков има, со кој (назив на здружението) има склучено договор за одржување на информацискиот систем, во облик на проверка на безбедносните привилегии на вработените во информативниот систем. Овие проверки се со цел да се провери дали системот обезбедува тајност и заштита на обработката на личните податоци.

**16. Дополнителни мерки за пренесување на посебна категорија на лични податоци или ЕМБГ на граѓанинот преку телекомуникациска мрежа**

Документите кои содржат посебна категорија на лични податоци или ЕМБГ на граѓанинот можат да се пренесуваат преку телекомуникациска мрежа само ако се криптирани и посебно заштитени со соодветни методи кои гарантираат дека нема да бидат читливи при преносот.

Администраторот при обработка на “посебните категории на лични податоци“ во секоја фаза од обработката (собирање, пренос, внес на податоци, складирање, уништување итн.) ќе обележува дека се работи за обработка на наведените категории на податоци.

УПРАВЕН ОДБОР НА (назив на здружението)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_