ПРАВИЛНИК ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Службен В. на Р.М. бр: 266/2024 од 25.12.2024

Влегува во сила на: 25.12.2024

Се применува инфо: ќе започне да се применува од 1 јули 2025 година.

Извор: АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Врз основа на член 66 став (6) од Законот за заштита на личните податоци ("Службен весник на Република Северна Македонија" бр.42/20 и 294/21), директорот на Агенцијата за заштита на личните податоци донесе.

ПРАВИЛНИК ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Предмет

Член 1

Со овој правилник се пропишуваат насоки за активностите кои контролорите треба да ги преземаат при планирање, воспоставување, применување, преиспитување и ажурирање на техничките и на организациските мерки за да се обезбеди безбедност на обработката на личните податоци.

Поимник

Член 2

Одделните изрази употребени во овој правилник и во неговите прилози го имаат следново значење:

1. Цел на заштита е обезбедување на правно усогласена обработка на личните податоци преку соодветни технички и организациски мерки, со цел да се ублажат ризиците и да се избегнат негативните влијанија врз правата и слободите на физичките лица;
2. Минимизирање на личните податоци е цел на заштита преку ограничување на обработката на личните податоци на она што е соодветно, релевантно и неопходно за конкретната цел. Минимизирањето се однесува на дизајнот на системите за обработка на личните податоци, количината на обработени лични податоци, обемот на обработка, достапноста и периодот на чување;
3. Доверливост е цел на заштита преку која треба да се обезбеди дека ниту едно неовластено лице не може да пристапи до личните податоци или да користи лични податоци;
4. Интегритет е цел на заштита преку која се гарантира дека личните податоци што се обработуваат се целосни, точни и ажурирани. Интегритетот се однесува на барањето дека процесите и системите за информатичка технологија континуирано се усогласуваат со спецификациите што биле дефинирани за да ги извршуваат нивните предвидени функции;
5. Достапност е цел на заштита преку која треба да се обезбеди непречен пристап и контитуирана расположливост на личните податоци, односно пристапот до личните податоци и нивната обработка се можни без одложување, како и дека личните податоци може да се користат правилно во предвидениот процес;
6. Неповрзливост е цел на заштита преку која треба да се обезбеди дека личните податоци се обработуваат строго ограничувајќи се на целта за која првично биле собрани, како и дека нема да се спојуваат или да се поврзуваат со други лични податоци што се собрани за други цели.
7. Транспарентност е цел на заштита преку која треба да се обезбедат информации за обработката на личните податоци, односно можност да се идентификува на различно ниво кои податоци се собираат и се обработуваат, кога и за кои цели на обработка, кои системи и процеси се користат за да се утврди дали личните податоци се обработуваат според определената цел, како и кој има одговорност во различните процеси на нивната обработка;
8. Интервенирање е цел на заштита преку која треба да се обезбеди ефективно остварување на правата на субјектите на лични податоци, како и применување на мерки за идентификување и автентикација на субјектите на лични податоци кои сакаат да ги остварат своите права;

9. Ризик е постоење можност за појава на настан што сам по себе претставува штета (вклучително и неоправдано вмешување во правата и слободите на физичките лица) или може да доведе до дополнителна штета за едно или за повеќе физички лица. Сериозноста на ризикот е комбинација од влијанието на штетата и веројатноста дека настанот и последователната штета ќе се случат. Ризикот во контекст на заштита на личните податоци секогаш се оценува во однос на негативните влијанија врз правата и слободите на физичките лица;
10. Процес на управување со ризик е систематска примена на политики, процедури и практики за управување со активностите кои се однесуваат на: комуницирање, консултирање, утврдување на контекстот, идентификување, анализирање, евалуирање, третирање, следење и проверување на ризикот;
11. Систем за заштита на лични податоци е збир од документирани политики, кодекси на однесување, насоки, процедури и работни инструкции донесени од страна на контролорот, а кои се во функција на спроведување на технички и организациски мерки за постигнување на целта на заштита согласно прописите за заштита на личните податоци;
12. Информациски систем е целина од компоненти преку кои се обработуваат личните податоци при активностите за нивна обработка. Ова ги опфаќа вклучените системи (на пример, работни станици, сервери, мрежни или безбедносни уреди), услуги (на пример, процедура, единствена функција или збир од функции што служат за одредена цел) и податоци (на пример, специфични полиња од лични податоци што се користат за обработка);
13. Инцидент или таканаречен настан е појава или промена на одредени околности кои што влијаат врз правата и слободите на физичките лица.

Примена

Член 3

Одредбите од овој правилник кои се однесуваат на воспоставување на информациски систем се применуваат за:
- целосно и делумно автоматизирана обработка на личните податоци и
- друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Одредбите од овој правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Воспоставување на информациски систем

Член 4

(1) Контролорот е одговорен за воспоставување на функционален и одржлив информациски систем според прописите за заштита на личните податоци.
(2) За воспоставување на информациски систем, контролорот треба да подготви соодветна документација за системот, која особено опфаќа:
- прикажување на определената цел за обработка на личните податоци;
- прикажување на редоследот на активности за обработка на личните податоци;
- прикажување на сите употребени и генерирани лични податоци;
- опишување на техничките компоненти што се користат (хардвер, софтвер и инфраструктура);
- евиденција на активностите за обработка;
- разграничување со други активности кои што не се однесуваат на обработка на лични податоци;
- прикажување на релации со други системи за контрола и верификација на движењето на личните податоци.

(3) Пред воспоставување на информациски систем, контролорот треба да ја процени подготвената документација од ставот (2) на овој член според:
- начелата поврзани со обработката на личните податоци;
- законитост на обработката на личните податоци;
- правата на субјектите на личните податоци;
- неопходноста од вршење на проценка на влијанието на заштитата на личните податоци;
- примената на соодветни технички и организациски мерки од страна на обработувачите;
- условите за пренос на лични податоци.

(4) Доколку се исполнети околностите од ставот (3) на овој член, контролорот треба да изврши процена на ризикот според Методологијата за процена на ризик (Прилог бр.1), која е составен дел на овој правилник, а за да се избегнат негативните влијанија врз правата и слободите на физичките лица.
(5) Според проценатa на ризикот од ставот (4) на овој член, контролорот треба идентификуваните ризици да ги ублажи до соодветно ниво на прифатливост на ризикот преку избор и примена на соодветни технички и организациски мерки за да се обезбеди ниво на безбедност соодветно на ризикот, а според Прилог бр. 2 - Цели на заштита, закани и мерки,

кој е составен дел на овој правилник.
(6) За воспоставување на информациски систем, контролорот треба да преземе активности за усогласување на околностите од ставот (3) на овој член со соодветното ниво на прифатливост на ризикот од проценатa на ризикот од ставот (4) на овој член.
(7) Документираниот процес од овој член во однос на воспоставување на информациски систем ќе се смета за систем за заштита на личните податоци според прописите за заштита на личните податоци.

Одржување на информацискиот систем

Член 5

(1) Контролорот е одговорен за преиспитување и ажурирање на информацискиот систем, а особено во однос на техничките и организациските мерки кои ги применува за да обезбеди безбедност на обработката на личните податоци согласно прописите за заштита на личните податоци.
(2) Физичките или правните лица кои вршат одржување на информацискиот систем во име на контролорот треба да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

Пренос на лични податоци во трети земји

Член 6

Во случај на хардверско и/или софтверско одржување или на други активности на информацискиот систем може да се врши пренос на лични податоци во трети земји само согласно условите утврдени во прописите за заштита на лични податоци.

Систем за заштита на лични податоци

Член 7

(1) Според најновите технолошки достигнувања, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризиците со различно ниво на сериозност во однос на нивното влијание врз правата и слободите на физичките лица, контролорот воспоставува систем за заштита на личните податоци преку примена на технички и организациски мерки за да обезбеди ниво на безбедност соодветно на ризикот.
(2) Техничките и организациските мерки од ставот (1) на овој член треба да ги вклучуваат сите неопходни мерки за гарантирање на целите на заштитата и тоа: минимизирање на личните податоци, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање (Прилози бр.1 и бр.2).
(3) Контролорот задолжително ги преиспитува и ги ажурира техничките и организациските мерки, при што секогаш ги применува оние мерки кои се соодветни за гарантирање на целите на заштита пропишани со одредбите на овој правилник.
(4) Процесот за управување со системот за заштита на личните податоци од ставот (1) на овој член се дефинира како дел од политиката на контролорот за системот за заштита на личните податоци кој треба да е соодветен на природата, обемот и сложеноста на активностите коишто контролорот ги врши при обработката на личните податоци и ризиците на коишто е изложен системот.
(5) Контролорот задолжително ја ревидира и ажурира документацијата во врска со системот за заштита на личните податоци според направените промени во неговите операции на обработка на личните податоци.

Управување со ризик

Член 8

(1) При идентификување и процена на ризиците (управување со ризик), контролорот задолжително ги зема предвид ризиците кои се поврзани со обработката на личните податоци за да ги обезбеди целите на заштитата и тоа: минимизирање на личните податоци, доверливост, интегритет, достапност, неповрзливост, транспарентност и интервенирање (Прилози бр.1 и бр.2).
(2) Управувањето со ризикот од ставот (1) на овој член опфаќа неколку фази и тоа:
а) список (преглед) на информацискиот систем во целина со сите системи, услуги и податоци што се користат за обработка на личните податоци;
б) процена на ризиците за секој процес на обработка на личните податоци;
в) спроведување и проверка на планираните мерки и
г) спроведување на периодични безбедносни проверки.

(3) Списокот на системи, услуги и податоци што се користат за обработка на личните податоци од ставот (2) точка а) на овој член треба да биде опфатен со описот на техничките и организациските мерки кои се применуваат за обезбедување безбедност на обработката на личните податоци.
(4) Проценатa на ризиците од ставот (2) точка б) на овој член, за секој ризик, го вклучува најмалку следното: (а) идентификување на потенцијалните влијанија и ефекти врз правата и слободите на засегнатите физички лица во однос на можните закани за целите на заштитата како што следува:
- минимизирање на личните податоците (на пример, имплементација на периоди за чување, криптирање или анонимизација),
- достапност (на пример, привремена или целосна недостапност на личните податоци),
- интегритет (на пример, несакани промени на личните податоци),
- доверливост (на пример, неовластен пристап до личните податоци),
- неповрзливост (на пример, ограничување на овластувањата за обработка, користење и пренос),
- транспарентност (на пример, записи за пристап до личните податоци) и
- интервенирање (на пример, имплементација на стандардизирани процедури за обезбедување на правото на пристап на субјектите на личните податоци); (б) идентификување на изворите на ризик кои што би можеле да бидат причина за секој непосакуван настан, со соодветно разгледување на внатрешните и на надворешните човечки ресурси (на пример, администратор на информациски систем, овластено лице, надворешен напаѓач, конкурент), како и други внатрешни и надворешни извори (на пример, вода, опасни материјали, пожар, вирус); (в) идентификување на лице или субјект со одговорност и овластување да управува со конкретниот ризик (сопственик на ризик); (г) идентификување на можните закани кои би можеле да се случат преку медиуми на кои се обработуваат личните податоци (на пример, хардвер, софтвер, комуникациски канали, документи во хартиена форма, итн.), кои би можеле да се:
- користат на несоодветен начин (на пример, злоупотреба на овластувањата, грешка при ракување);
- изменат (на пример, "заразен" софтвер или хардвер со снимач на записите на тастатурата, инсталирање на злонамерен односно малициозен софтвер итн.);
- изгубат (на пример, кражба на лаптоп или губење мемориски уреди);
- надгледуваат (на пример, геолокација на опремата);
- оштетат (на пример, вандализам, деградација поради природно абење);
- преоптоварат (на пример, медиумот за чување на лични податоци е целосно пополнет, напад на одбивање услуга итн.); (д) процена на веројатноста за појава (веројатност) во однос на претходните елементи предвидени во овој став на скала за процена: ретко, повремено и често; (ѓ) процена на нивото на влијание во однос на претходните елементи предвидени во овој став на скала за процена: ниско, средно и високо; (е) процена на сериозноста на ризикот во однос на претходните елементи предвидени во овој став на скала за процена: незначителен ризик, ризик и висок ризик.
(5) Контролорот задолжително врши спроведување и проверка на планираните мерки од ставот (2) точка в) на овој член за да обезбеди дека тие се применуваат и тековно се тестираат.
(6) Контролорот задолжително спроведува периодични безбедносни проверки од ставот (2) точка г) на овој член, за што се изготвува акционен план чија имплементација се следи од страна на раководството на контролорот.

Период на прилагодување

Член 9

Во смисла на член 28 став (1) од Законот за заштита на личните податоци ("Службен весник на Република Северна Македонија" бр.42/20 и 294/21), контролорот задолжително го прилагодува своето работење со одредбите на овој правилник во рамките на предвидениот период на преиспитување и ажурирање на техничките и организациските мерки кои се применуваат за обезбедување безбедност на обработката на личните податоци.

Престанување на важење

Член 10

Со денот на применувањето на овој правилник престанува да важи Правилникот за безбедност на обработката на личните податоци ("Службен весник на Република Северна Македонија" бр.122/20).

Влегување во сила и примена

Член 11

Овој правилник влегува во сила осмиот ден од денот на објавувањето во "Службен весник на Република Северна Македонија", а ќе започне да се применува од 1 јули 2025 година.
Бр. 01-1320/1 23 декември 2024 година Скопје Директор, Имер Алиу, с.р.

Прилог бр.1

Методологија за процена на ризик

1. Подготовка на анализа на ризик

Идентификување на процесот што треба да се евалуира и предвидената цел

Процес на обработка на лични податоци	
Цел	

Пример:

Процес на обработка на лични податоци	*Педагошка документација и педагошка евиденција вклучително и досие на детето*
Цел	*Детската градинка/центарот за ран детски развој води педагошка документација и педагошка евиденција за воспитно-образовните активности согласно Законот за заштита на децата*

Информациите за процесот којшто треба да се евалуира и предвидената цел може да се преземат од евиденцијата на активности за обработка која контролорот ја води според одредбите на членот 34 од Законот за заштита на личните податоци.

Анализата на ризик ги опфаќа постапките (специфичен начин за извршување на активноста) кои што треба да се проценат, вклучувајќи ги сите технички и организациски мерки кои се користат од страна на контролорот.

Доколку се планирани други технички и организациски мерки, но истите сè уште не се интегрирани во постапките, тогаш контролорот тие мерки не ги зема предвид при оваа анализа на ризик.

Првиот чекор е да се идентификуваат субјектите на лични податоци односно категориите на субјекти на лични податоци (физички лица) за кои се обработуваат лични податоци во текот на процесот (збир на активности кои меѓусебно се поврзани или се во меѓусебна зависност).

Субјекти на лични податоци (категории на субјекти на лични податоци)	

Пример:

Субјекти на лични податоци (категории на субјекти на лични податоци)	*Деца, воспитувачи*

Потоа се идентификуваат личните податоци односно категориите на лични податоци што се обработуваат во текот на процесот.

Категории на лични податоци	

Пример:

Категории на лични податоци	*Деца: име и презиме на детето, датум и место на раѓање, државјанство, адреса на живеење* *Воспитувачи: име, презиме, степен на образование, лиценца*

Понатаму, следува идентификување на другите компоненти што се вклучени во процесот на обработка (системи, услуги и процеси).

Системи	
Услуги	
Процеси	

Пример:

Системи	*Лаптоп, софтвер за обработка на документи или друг специјализиран софтвер, локална мрежа, сервери*
Услуги	*Регистрирање*
Процеси	*Методи на внесување, ажурирање и бришење*

2. Скала на влијание

Контролорот потребата за заштита ја идентификува преку личните податоци коишто се обработуваат, нивната природа, обем, контекст и цел на обработка и истата треба да одговара на максималното ниво на влијание на кои можат да бидат изложени правата и слободите на засегнатите физички лица во однос на можните закани на целите на заштитата.

Целите на заштита се следните:

- Минимизирање на личните податоци
- Доверливост
- Интегритет
- Достапност
- Неповрзливост
- Транспарентност
- Интервенирање

На потребата за заштита не влијаат техничките и организациските мерки кои ги користи контролорот и истата е предвидена на скала од три нивоа како што следува:

Влијание	**Дефиниција**	**Примери**
Ниско [Вредност = 1]	Тоа се лични податоци чија обработка *не предизвикува сериозни влијанија* за засегнатите субјекти на лични податоци.	Име и презиме без известување за ограничување, назив/звање на работно место
Средно [Вредност = 2]	Тоа се лични податоци чија обработка *може негативно да влијае* врз засегнатите субјекти на лични податоци во однос на нивната социјална или економска положба.	Година на раѓање, датум на раѓање, податоци за висина на плата, податоци за други лични приходи
Високо [Вредност = 3]	Тоа се лични податоци чија обработка *може значително да влијае* врз засегнатите субјекти на лични податоци во однос на нивната социјална или економска положба, како и за нивната лична слобода.	Генетски податоци, биометриски податоци, здравствени податоци или податоци што се однесуваат на сексуалниот живот или на сексуалната ориентација, податоци поврзани со казнени осуди и казнени дела, единствен број на граѓанинот.

Во случај на ниско или средно ниво на влијание, има потреба за заштита на најмалку на „основно ниво“ од страна на контролорот, а при високо ниво на влијание се јавува потреба за заштита од „високо ниво“.

Притоа, важен индикатор за активностите за обработка се категориите на лични податоци, особено кога станува збор за посебни категории на лични податоци (генетски податоци, биометриски податоци, податоци што се однесуваат на здравјето и други податоци), па врз основа на овие категории на лични податоци, би можело да се предвиди соодветна потреба за заштита („високо ниво“) без дополнителна анализа, а според претходно наведената скала на влијание.

Пример: за обработка на лични податоци на деца секогаш постои најмалку „високо ниво“ на потреба од заштита, а за обработка на податоци на воспитувачите вообичаено постои потреба за заштита на „основно ниво“.

Потребите за заштита што се предвидени во овој дел, имаат влијание и врз системите, услугите и процесите што се вклучени во обработката на личните податоци. По правило, потребата за заштита се однесува и на компонентите со кои се врши обработка на личните податоци. Во одредени случаи, како на пример во однос на централните компоненти како што се серверите, истите може да се класифицираат и поинаку доколку компонентата се користи и за други постапки или доколку е редундантна.

☐ Ниско	☐ Средно	☐ Високо

3. Идентификување (релевантни) закани за компонентите на постапката

Секоја обработка на лични податоци сама по себе претставува настан што може негативно да влијае врз правата и слободите на физичките лица. Затоа, од една страна, заканите на тие права и слободи може да произлегуваат од дизајнот на самата активност за обработка, односно од дизајнот на поврзаните системи и услуги и пот процеси.

Примери за ова би биле: правата за пристап според правилото „потребно е да знае“ или ограничување на правата на субјектите на лични податоци.

Од друга страна, заканите на правата и слободите на физичките лица може да произлегуваат од безбедноста на информатичката технологија која се користи за обработка на личните податоци, како и од организациското опкружување на обработката, а тоа може да има индиректно влијание врз активноста на обработка и на личните податоци што се обработуваат, особено поради недоволните заштитни мерки кои се користат од страна на контролорот.

Пример за ова би било: напад со злонамерен софтвер што може да ја загрози доверливоста на личните податоци.

Закани	

Пример:

Закани	*Ненамерно менување на податоците поради неправилна работа на софтверската апликација* *Неовластен пристап до (и откривање на) податоците на децата поради кражба на лаптоп*

4. Скала на веројатност за појава

За секоја идентификувана закана, веројатноста за појава се одредува на скала од три нивоа како што следува:

Веројатност за појава	**Дефиниција**
Ретко ***[Вредност = 1]***	▫ Може да настане штета, но конкретните околности спречуваат таков настан и не треба да се очекува дека тој ќе се појави. ▫ Можно е да настане штета, но зависи од однесувањето на трети лица, а конкретните околности укажуваат на тоа дека третите лица преземаат активности против настанување на штета и не се очекува тоа да се промени.
Повремено ***[Вредност = 2]***	▫ Може да настане штета, која зависи од несигурностите што не можат да се предвидат. ▫ Може да настане штета, која зависи од однесувањето на трети лица кое не може да се предвиди.
Често ***[Вредност = 3]***	▫ Може да се очекува да настане штета. ▫ Може да настане штета и треба да се очекува дека ќе настанат околности што ќе ја предизвикаат истата. ▫ Може да настане штета, која зависи од однесувањето на трети лица, кое веќе произлегува/се појавува за што постои ефективна ситуација за предизвикување

Пример:

Веројатност за појава	*Ненамерно менување на податоците поради неправилна работа на софтверската апликација* ***Ретко*** *Неовластен пристап до (и откривање на) податоците на децата поради кражба на лаптоп* ***Често***

При процена на веројатноста за појава во однос за настан што произлегува од самиот дизајн на активноста на обработката, начелно мора да се претпостави најголемата веројатност за појава („често“), а во однос на закани што потекнуваат надвор од планирањето на активноста за обработка може да биде на пониско ниво.

☐ Ретко	☐ Повремено	☐ Често

Оттука, описот на поединечните ризици е целосен кога се состои од: прецизирање на ризична ситуација во компонентата што е вклучена во процесот на обработка (настан на штета), потребата за заштита на соодветните лични податоци, како и веројатноста за појава на штетниот настан.

5. Матрица за процена

Ризиците што се идентификувани и рангирани во однос на влијанието и веројатноста за појава, може да се прикажат на дводимензионален дијаграм за илустрирање и одредување на сериозноста на конкретниот ризик.

Добиената вредност на ризик може да се пресмета како: Ризик = Влијание x Веројатност за појава.

Обработката со проценето *средно влијание* (вредност 2) и процена *често* (вредност 3) за веројатноста за појава ќе доведе до резултат од *висок ризик* (2 x 3 = 6).

Резултат на матрицата на ризик :

Влијание			
Високо	**3**	**6**	**9**
Средно	**2**	**4**	**6**
Ниско	1	**2**	**3**
Веројатност за појава (Веројатност)	Ретко	Повремено	Често

☐ **Зелена: Незначителен 1-2**
☐ **Жолта: Ризик 3-4**
☐ **Црвена: Висок ризик >= 6**

6. Евалуација/толкување

За секој идентификуван ризик, се врши процена земајќи ги предвид нивото на влијание и веројатноста за појава.

Во случај на резултат во **зелените** полиња (*незначителен ризик*), обработката може да се реализира.

Во случај на резултат во **жолтите** полиња (*ризик*), контролорот треба да има предвид дали обработката може да се реализира во предвидената форма.

Во случај на резултат во **црвените** полиња (*висок ризик*), обработката на личните податоци не е дозволена без примена на дополнителни мерки за заштита.

7. Постапување со ризик

Контролорот за да може да управува со идентификуваните ризици, мора за секој ризик да добие резултат во жолта или зелено поле со примена на соодветни мерки за заштита за да може обработката да се реализира во предвидената форма. Доколку со предвидените мерки, контролорот не може да го ублажи ризикот со резултат во жолто или зелено поле, во тој случај контролорот треба да се консултира со Агенцијата за да се оцени дали и под кои услови предвидената обработка би можела да се реализира според одредбите од членот 40 од Законот за заштита на личните податоци.

Предвидените мерки за заштита може да влијаат како на нивото на влијание, така и на нивото на веројатноста за појава или на двете нивоа заедно.

Доколку се предвидат мерки за заштита, како, на пример, исклучување на одредени категории на лични податоци од процесот на обработка или спроведување други форми на минимизирање на личните податоци, тогаш тоа претставува значајна промена во активностите за обработка на личните податоци и во тој случај, контролорот мора да ја повтори анализата на ризик и постапувањето со активностите за обработка. При настанатите промени во активностите за обработка на овој начин, контролорот може да идентификува потреба од промена на мерките за заштита. Ако контролорот не идентификува потреба од промена на мерките за заштита, тогаш треба да ја повтори само

проценатa на веројатноста за појава.

За проверка на предвидените мерки за заштита, контролорот може проверката да ја изврши преку прашалникот во кој се структурирани мерките во однос на целите за заштита, даден во оваа методологија.

Прашалник за проверка

Минимизирање на личните податоци	
Заштитната цел на минимизирање на личните податоци се однесува на основното барање од Законот за заштита на личните податоци за ограничување на обработката на лични податоци само на тоа што е соодветно, релевантно и неопходно за целите на обработката. Барањето за минимизирање не се применува само на количината на лични податоци што се обработуваат, туку и на опфатот на самата обработка, периодот на чување и достапноста на податоците. Поконкретно, треба да се обезбеди дека личните податоци се чуваат во форма која дозволува само идентификација на субјектите на лични податоци сè додека тоа е неопходно за целите на обработката.	
☐	Намалување на евидентираните категории на лични податоци;
☐	Намалување на операциите за обработка во секој процес;
☐	Намалување на можностите за давање на информации за личните податоци;
☐	Воспоставување на стандардни поставки за субјектите на лични податоци што ја ограничуваат обработката на нивните лични податоци на она што е неопходно за целта на обработката
☐	Воведување на мерки за автоматско блокирање и бришење;
☐	Маскирање на податоците за прикривање на полињата со личните податоци и воведување на процедури за автоматско блокирање и бришење и мерки за псевдонимизација и анонимизација;
☐	Редовно ажурирање на воспоставените процедури врз основа на спроведени контроли.

Достапност
Заштитната цел на достапноста се однесува на непречен пристап и континуирана расположливост на обработката на личните податоци. За таа цел, овластените лица треба да имаат пристап до личните податоци и при нивната обработка да ги применуваат предвидените процедури/политики. Достапноста вклучува конкретна можност за враќање на личните податоци, на пример преку системи за управување со податоци, структурирани бази на податоци и функции за пребарување, како и способност на техничките системи да ги презентираат податоците.

☐	Правење на сигурносни копии, соодветно планирање на состојбите на (во) процесот, конфигурирање, структурирање на податоците, историја на трансакции, според тестиран концепт;
☐	Заштита од надворешни влијанија (злонамерен софтвер, саботажа, виша сила);
☐	Документирање на синтаксата на податоците;
☐	Редундантност на хардвер, софтвер и инфраструктура;
☐	Спроведување на мерки за навремено повторно воспоставување на достапноста до личните податоци и пристапот во случај на инцидент, како и за правење на сигурносна копија;
☐	Подготвување на План за итни состојби кој ги предвидува мерките за обновување на активностите за обработка на личните податоци;
☐	Воведување на мерки за обезбедување на замена на овластените лица кои имаат пристап до личните податоци.

Интегритет	
Заштитната цел на интегритет од една страна се однесува на барањето дека процесите и системите за информатичка технологија континуирано се усогласуваат со спецификациите што биле дефинирани за да ги извршуваат нивните предвидени функции, а од друга страна интегритетот гарантира дека личните податоци кои се обработуваат континуирано се точни, целосни и ажурирани.	
☐	Ограничување на привилегиите за внес и промени;
☐	Користење на алгоритми за криптирање при обработката на личните податоци (контролни суми, електронски печат и потпис);
☐	Документирање на постапките за идентификација и проверка на пристапот на овластените лица и доделените улоги;
☐	Бришење и ажурирање на неточни лични податоци;
☐	Зајакнување на информациските системи преку склучување и минимизирање на секундарни функционалности;
☐	Идентификација и автентикација на овластените лица и опремата која се користи;
☐	Континуирано оценување, евалуација и ажурирање на документацијата за технички и организациски мерки;
☐	Дефинирање на процесите и редовно тестирање на функционалноста, ризиците, безбедносните празнини и несаканите ефекти на процесите;

☐	Определување на процесите и нивно редовно тестирање;
☐	Заштита од надворешни влијанија (шпионажа, хакирање).

Доверливост	
Заштитната цел на доверливоста треба да обезбеди дека ниту едно неовластено лице не може да пристапи до личните податоци или да користи лични податоци. Неовластени лица не се само трети лица надвор од контролорот, туку и вработени кај обработувачи за кои не е потребен пристап до личните податоци за да ја извршат услугата или лица во организациски единици кај контролорот што немаат никаква поврзаност со обработката на личните податоци.	
☐	Сегрегација на должности и одговорности на овластените лица според правилото ,,потребно е да знае", при што да се има предвид судирот на интереси при извршувањето на нивните работни задачи;
☐	Воведување мерки за автентикација на овластените лица;
☐	Спецификација и мониторинг на користењето на авторизираните ресурси, а особено комуникациските канали;
☐	Определување на опкружувањето (згради, простории) кои се опремени за обработка на лични податоци;
☐	Воведување мерки за вршење контрола на примената на организациските мерки, интерните процедури и договорните аранжмани со обработувачите;
☐	Користење на алгоритми за криптирање на личните податоци кои што се чуваат или се пренесуваат, како и воспоставување процеси за управување и заштита на криптираните информации;
☐	Заштита од надворешни влијанија (шпионажа, хакирање).

Неповрзливост	
Заштитната цел на неповрзувањето е да се обезбеди дека личните податоци нема да се обработуваат за друга цел различна од целта за која првично биле собрани при што натамошната нивна обработка би можела да биде дозволена само во строго дефинирани околности. Неповрзливоста треба да се обезбеди со технички и организациски мерки.	
☐	Воведување на мерки за ограничување на пристапот за обработка, користење и пренос на податоци од страна на овластените лица;
☐	Програмски пропуст или деактивирање на интерфејси во методите и компонентите при обработка на личните податоци;

Комплетниот прилог во (pdf формат) може да ги превземете на следниот
линк