20201221615

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), а во врска со Насоките за проценка на влијанието врз заштитата на личните податоци (ПВЗЛП) и утврдување дали обработката „веројатно ќе резултира со висок ризик“ за целите на Регулативата 2016/679 (WP 248 rev.01) од Работната група 29 за заштита на личните податоци при Европската унија, директорот на Агенцијата за заштита на личните податоци донесе

ПРАВИЛНИК ЗА ПРОЦЕСОТ НА ПРОЦЕНКА НА ВЛИЈАНИЕТО НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој правилник се пропишуваат упатства за контролорот при процесот на спроведување на проценката на влијанието на заштитата на личните податоци.

Член 2

Проценката на влијанието на заштитата на личните податоци во смисла на овој правилник претставува процес дизајниран да ја опише обработката на личните податоци, да ја процени нејзината неопходност и пропорционалност и да помогне во управувањето со ризиците за правата и слободите на физичките лица кои ќе настанат со обработката преку нивна проценка, како и да се предвидат мерки за справување со тие ризици (во натамошниот текст: ПВЗЛП).

II. СЛУЧАИ ВО КОИ Е ЗАДОЛЖИТЕЛНА ПВЗЛП

Член 3

(1) Во смисла на член 39 став (1) од Законот за заштита на личните податоци, контролорот задолжително спроведува ПВЗЛП кога постои веројатност обработката да предизвика висок ризик за правата и слободите на физичките лица, а особено кога се воведуваат нови технологии за обработка на личните податоци, според природата, обемот, контекстот и целите на обработката, како и кога обработката е вклучена во Листата на видовите операции на обработка за кои се бара ПВЗЛП воспоставена од Агенцијата за заштита на личните податоци (во натамошниот текст: Агенцијата).

(2) Контролорот спроведува ПВЗЛП пред да започне со обработка на личните податоци, притоа обезбедувајќи техничка и интегрирана заштита на личните податоци, односно во фаза на планирање на операциите на обработка, како и кога некои од операциите на обработка се сè уште непознати.

(3) По исклучок од ставот (2) на овој член, контролорот задолжително спроведува ПВЗЛП и пред да се направат значителни промени на некои постојни операции на обработка на лични податоци, а кои претходно биле проверени од страна на Агенцијата.

Член 4

Контролорот за да определи кои операции на обработка веројатно ќе резултираат со висок ризик и за кои ПВЗЛП е задолжителна, мора да ги има во предвид најмалку еден од следните критериуми:

1. Евалуација или бодирање, вклучително и профилирање и предвидување, особено врз основа на аспекти поврзани со работењето на субјектот на лични податоци, економската состојба, здравјето, личните преференции или интереси, сигурност или однесување, локацијата или движења.

2. Автоматско донесување одлуки со правно или слично суштинско дејство, односно обработка насочена кон донесување на одлуки за субјектите на лични податоци што произведуваат правни последици за физичкото лице или на сличен начин значајно влијаат на физичкото лице.

3. Систематско набљудување, односно обработка која се користи за следење, набљудување или контрола на субјектите на лични податоци, вклучително и податоци собрани преку мрежи или „систематско набљудување на јавно достапни простори“.

4. Чувствителни податоци или податоци од изразита лична природа: ова вклучува посебни категории на лични податоци кои се определени во членот 4 став (1) точка 13 од Законот за заштита на личните податоци, како и лични податоци поврзани со казнени осуди и казнени дела.

5. Обемна обработка на податоци. При утврдување дали обработката е обемна според околностите на секој конкретен случај, се земаат предвид следниве фактори:

- број на засегнати субјекти на лични податоци, било да е конкретен број или процент од релевантното население;
- обем на податоци и/или опфат на различни видови податоци што се обработуваат;
- траење или непрекинатост на операциите на обработка на личните податоци; и
- географскиот опсег на активностите за обработка на личните податоци.

6. Сет од лични податоци што се совпаѓаат или комбинираат, на пример оние кои потекнуваат од две или повеќе операции на обработка на лични податоци кои се извршени за различни цели и/или од различни контролори на начин што ги надминува разумните очекувања на субјектот на личните податоци.

7. Податоци кои се однесуваат на ранливи субјекти на лични податоци: обработката на овој вид на податоци е критериум заради зголемената нерамнотежа на моќта помеѓу субјектите на лични податоци и контролорите, при што физичките лица не можат едноставно да се согласат или да се спротивстават на обработката на нивните податоци или да ги остварат своите права. Ранливи субјекти на лични податоци може да вклучуваат деца, вработени, ранливи групи на кои им е потребна посебна заштита (лица со ментална попреченост, барателиа на азил или постари лица, пациенти и др.). како и секој друг случај кога може да се идентификува нерамнотежа во односот помеѓу положбата на субјектот на личните податоци и контролорот.

8. Иновативна употреба или примена на нови технолошки или организациски решенија, како што се комбинирање на употреба на отпечаток од прст и препознавање на лице за подобрување на контролата на физичкиот пристап, итн.

9. Ситуации кога самата обработка ги спречува субјектите на лични податоци да остварат одредени права или да користат услуга или договор. Ова вклучува процедури за обработка кои се насочени кон овозможување, модифицирање или одбивање на пристапот на субјектите на личните податоци до одредена услуга или склучување на договор.

III. СЛУЧАИ КОГА ПВЗЛП НЕ Е ЗАДОЛЖИТЕЛНА

Член 5

(1) ПВЗЛП е незадолжителна во следните случаи кога:

- операциите на обработка може да одговараат на случаите наведени во членот 4 на овој правилник, но контролорот оценил дека истите нема веројатност да резултираат со висок ризик за правата и слободите на физичките лица;
- природата, обемот, контекстот и целите на обработката се слични на обработката за која била спроведена ПВЗЛП; и
- обработката е вклучена во Листата на видовите операции на обработка за кои не се бара ПВЗЛП воспоставена од Агенцијата.

(2) Контролорот задолжително ги оправдува и документира причините за неизвршување на ПВЗЛП при што го наведува и мислењето на офицерот за заштита на личните податоци (во натамошниот текст: офицерот).

IV. УЛОГИ И ОДГОВОРНОСТИ

Член 6

(1) Во смисла на член 39 од Законот за заштита на личните податоци, контролорот е исклучиво одговорен да го спроведува ПВЗЛП при што ги определува лицата задолжени за извршување на ПВЗЛП и ги документира советите и одлуките на офицерот во рамките на ПВЗЛП.

(2) Во согласност со ставот (1) на овој член, контролорот при спроведување на ПВЗЛП може да ангажира надворешни лица или да побара совет или мислење од независни експерти, а според природата на технолошките и организациските решенија кои ќе се применуваат при операциите на обработка на личните податоци.

(3) Кога обработката целосно или делумно ќе биде извршувана од страна на обработувачот, тогаш обработувачот е должен да му помогне на контролорот во спроведувањето на ПВЗЛП при што улогите, обврските и одговорностите на контролорот и обработувачот задолжително се дефинираат со договор согласно прописите за заштита на личните податоци.

V. БАРАЊЕ НА МИСЛЕЊЕ ОД СУБЈЕКТОТ НА ЛИЧНИТЕ ПОДАТОЦИ

Член 7

(1) Според околностите на секој конкретен случај за кој се изработува ПВЗЛП, контролорот може да побара мислење од субјектите на личните податоци или нивните претставници, преку различни средства, во зависност од контекстот (на пример, општа студија поврзана со целта и средствата на процесот на обработка, со поставување на прашања до претставниците на субјектите на лични податоци, или преку анкети кои се испраќаат до идните клиенти на контролорот).

(2) Кога конечната одлука на контролорот се разликува од мислењето на субјектите на лични податоци, причините за продолжување или прекин на обработката на личните податоци задолжително треба да се документираат при процесот на ПВЗЛП.

(3) Кога контролорот ќе одлучи да не бара мислење од субјектите на лични податоци (на пример: доколку со тоа би се загрозила доверливоста на работните планови во организацијата или истото е несразмерно или неизводливо), образложението за ваквата одлука треба да се документира при процесот на ПВЗЛП.

VI. ПРЕИСПИТУВАЊЕ НА ПВЗЛП

Член 8

(1) Контролорот го преиспитува ПВЗЛП по промена на ризиците што произлегуваат од операциите на обработка (на пример, употреба на нова технологија, кога личните податоци се користат за друга цел итн.).

(2) Доколку одредени промени го намалат ризикот, во вакви ситуации, преиспитувањето на направената анализа на ризик може да покаже дека не е потребно контролорот да спроведе ПВЗЛП.

VII. ОСНОВНИ КАРАКТЕРИСТИКИ НА ПВЗЛП

Член 9

(1) ПВЗЛП задолжително содржи:

- опис на предвидените операции на обработка и целите на обработката;
- проценка на потребата и пропорционалноста на обработката;
- проценка на ризиците за правата и слободите на субјектите на личните податоци; и
- мерки предвидени за:
  - управување со ризиците; и
  - демонстрирање на усогласеност со прописите за заштита на личните податоци.

(2) Процесот на спроведување на ПВЗЛП графички е прикажан во Прилогот бр.1 кој е составен дел на овој правилник.

Методологија за спроведување на ПВЗЛП

Член 10

Контролорот задолжително донесува соодветна Методологија за спроведување на ПВЗЛП според критериумите дадени во Прилогот бр. 2 кој е составен дел на овој правилник.

Фази на спроведување на ПВЗЛП

Член 11

ПВЗЛП се спроведува во четири фази и тоа:

1. Дефинирање на контекстот – во првата фаза се дефинира контекстот на обработка и се наведуваат, односно опишуваат најмалку следниве информации:

- збирка на лични податоци;
- цел на обработката;
- движење на податоци;
- метод(и) на добивање на податоците;
- начин и средства за обработка на податоците (користена опрема, мрежи, човечки ресурси итн.);
- субјекти кои се вклучени во обработката (контролори, обработувачи, корисници итн.); и
- рок на чување.

2. Анализа на ризик – во втората фаза се идентификуваат заканите (несакани исходи), како и се одредува веројатноста и влијанието (последицата) од остварување на секој ризик.

Ризикот се изразува како функција од веројатноста да се случи несаканиот исход (заканата) и влијанието (последицата) од несаканиот исход доколку се случи.

Ризикот = (веројатност да се случи заканата) x (степен на влијанието)

Влијанието може да биде:

- ниско, кога физичките лица можат да се соочат со неколку помали непријатности, кои ќе ги надминат без проблем;
- средно, кога физичките лица можат да се соочат со значителни непријатности, кои ќе можат да ги надминат и покрај одредени тешкотии;
- високо, кога физичките лица можат да се соочат со значителни последици, кои би требало да можат да ги надминат, но со сериозни тешкотии; и
- многу високо, кога физичките лица можат да се соочат со значителни, па дури и неповратни последици, кои најверојатно нема да можат да ги надминат.

Проценката на ризикот се спроведува според начелата за заштита на личните податоци.

3. Управување со ризик – во третата фаза треба да се опфатат заштитните мерки, односно мерките на безбедност и механизмите дизајнирани да го намалат ризикот на прифатливо ниво, како и да се обезбеди заштита на личните податоци и да се прикаже усогласеност со прописите за заштита на личните податоци.

Мерките, исто како и кај проценката на ризикот треба да се поделат според начелата за заштита на личните податоци.

4. Составување извештај од спроведена ПВЗЛП – Контролорот ги документира сите фази на спроведување на ПВЗЛП, по што изработува извештај.

Извештајот од спроведената ПВЗЛП особено содржи: опис на процесот на обработка, внатрешни и надворешни лица вклучени во процесот на спроведување на ПВЗЛП, анализа на ризик, дефинирани мерки за управување со ризикот, резиме/заклучок, акциски план, мислење на офицерот и на другите лица вклучени во процесот, одобрување на ПВЗЛП од страна на функционерот или одговорното лице кај контролорот.

Објавување на ПВЗЛП

Член 12

(1) Контролорот самостојно одлучува дали јавно ќе го објави извештајот од ПВЗЛП.

(2) Контролорот демонстрира почитување на начелото на отчетност и транспарентност преку објавување на делови од извештајот, на пример преку објавување на краток преглед или заклучок од спроведената ПВЗЛП.

(3) Контролорот е должен да го достави извештајот од спроведената ПВЗЛП на барање на Агенцијата.

VIII. КОНСУЛТАЦИЈА СО АГЕНЦИЈАТА

Член 13

Кога контролорот не може да најде соодветни мерки за да го намали ризикот на прифатливо ниво (т.е. ако преостанатите ризици останат високи), задолжително се консултира со Агенцијата во смисла на член 40 од Законот за заштита на личните податоци.

IX. ЗАВРШНА ОДРЕДБА

Член 14

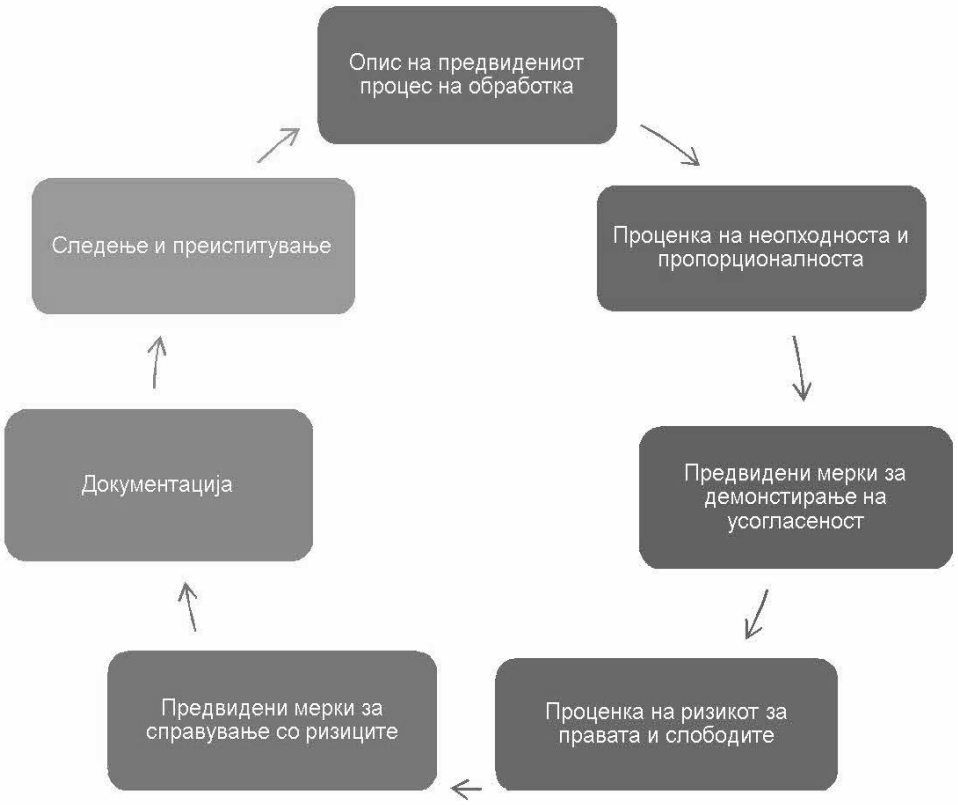
Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-606/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Прилог бр. 1

Графички приказ на процесот за спроведување на ПВЗЛП



Напомена: Секоја од фазите ќе треба да се спроведе неколку пати пред да заврши ПВЗЛП.

Прилог бр. 2

Критериуми за прифатлива ПВЗЛП

Критериумите што контролорот може да ги користи за да оцени дали ПВЗЛП или методологијата за спроведување на ПВЗЛП е доволно сеопфатна за да се усогласи со прописите за заштита на личните податоци, се следни:

- ☐ проценката содржи систематски опис на обработката:
  - ☐ земени се предвид природата, обемот, контекстот и целите на обработката;
  - ☐ евидентирани се личните податоци, примателите и периодот на чување на личните податоци;
  - ☐ даден е функционален опис на операцијата на обработка;
  - ☐ идентификувани се средства од кои зависат личните податоци (опрема, софтверски програми, мрежи, лица, документи во хартиена форма или канали за испраќање документи во хартиена форма);
  - ☐ исто така, земена е предвид усогласеноста со одобрените кодекси на однесување;
- ☐ проценета е неопходноста и пропорционалноста:
  - ☐ одредени се мерките предвидени за усогласување со прописите за заштита на личните податоци, земајќи ги предвид:
    - ☐ мерки што придонесуваат за пропорционалност и неопходност од обработка врз основа на:
      - ☐ конкретни, јасни и легитимни цели;
      - ☐ законитост на обработката;
      - ☐ соодветни и релевантни лични податоци и ограничени на она што е потребно;
      - ☐ ограничен рок на чување;
    - ☐ мерки кои придонесуваат за правата на субјектите на личните податоци:
      - ☐ информации доставени на субјектот на личните податоци;
      - ☐ право на пристап и преносливост на податоците;
      - ☐ право на исправка и бришење;
      - ☐ право на приговор и ограничување на обработката;
      - ☐ односи со обработувачите;
      - ☐ заштитни мерки кои се однесуваат на преносот;
      - ☐ претходна консултација.
- ☐ контролирани се ризиците за правата и слободите на испитаниците:
  - ☐ се проценува изворот, природата, особеноста и сериозноста на ризикот или подетално, за секој ризик (неовластен пристап, несакани промени и исчезнати податоци) од гледна точка на субјектите на личните податоци:
    - ☐ земени се предвид изворите на ризик;
    - ☐ утврдени се можните ефекти врз правата и слободите на субјектите на личните податоците, меѓу другото, во случај на неовластен пристап, несакани промени и исчезнати податоци;
    - ☐ идентификувани се закани што може да доведат до неовластен пристап, несакана промена и исчезнати податоци;
    - ☐ проценета е веројатноста и сериозноста;
  - ☐ предвидени се одредени мерки за да се отстранат овие ризици;
- ☐ вклучени се засегнатите страни:
  - ☐ побаран е совет од офицерот;
  - ☐ каде што е соодветно, побарани се мислења на субјектите на личните податоци или нивните претставници.