РЕПУБЛИКА МАКЕДОНИЈА

Дирекција за заштита на личните податоци

ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ
ул. „Самоилова“ бр.10, 1000 Скопје; тел: +389 2 3230 635; факс. +389 2 3230 635;
www.dzlp.mk

У П А Т С Т В О

ЗА НАЧИНОТ НА ВРШЕЊЕ НА НАДВОРЕШНА КОНТРОЛА

Бр. 02 – 904 / 1
18.05. 2012 година

Врз основа на член 41 став 1 алинеја 1 и член 41 – а алинеја 4 од Законот за заштита на личните податоци („Службен весник на Република Македонија" бр. 7/05, 103/08, 124/10 и 135/11), а во врска со членовите 25 и 35-ѓ од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на република Македонија" бр. 38/09 и 158/10), директорот на Дирекцијата за заштита на личните податоци донесе

У П А Т С Т В О
ЗА НАЧИНОТ НА ВРШЕЊЕ НА НАДВОРЕШНА КОНТРОЛА

I. ОПШТИ ОДРЕДБИ

1. Со ова упатство се пропишува начинот на вршење на надворешна контрола на информацискиот систем и информатичката инфраструктура и на рачната обработка на личните податоци кај контролорот (во натамошниот текст: контрола) од страна на независно трето правно лице (во натамошниот текст: тело кое врши контрола).

2. Целта на ова упатство е да се обезбеди:

- проценување на степенот на усогласеност на организациската систем за заштита на личните податоци воспоставен од контролорот со прописите за заштита на личните податоци,
- проценување на степенот на адекватност на контролите на системот за заштита на личните податоци во однос на проценката на ризик кај контролорот,
- идентификување на потенцијалните пропусти и слабости во системот за заштита на личните податоци,
- собирање на информации за контрола на системот за заштита на личните податоци,
- зголемување на нивото на свеста за заштита на личните податоци кај управувачкиот тим и вработените на контролорот и
- подобрување на заштитата на личните податоци на физичките лица, преку намалување на веројатноста од појава на случајно или незаконско уништување на личните податоци, или нивно случајно губење, преправање, неовластено откривање или пристап, а особено кога обработката вклучува пренос на податоци преку електронско комуникациска мрежа.

3.Одделни изрази употребени во ова упатство го имаат следново значење:

1) **План за контрола** (**Audit Plan**) е систематска и структуирана целина на активности кои мора да бидат извршени од страна на лицето кое врши контрола со цел давање на мислење.

2) **Мислење за извршена контрола** (**Audit Opinion**) е целосна оценка за предметот на контрола во однос на применувањето на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци согласно прописите за заштита на личните податоци.

3) **Лице кое врши контрола** (**Auditor**) е надворешно независно и квалификувано лице кое ја врши контролата на системот за заштита на личните податоци.

4) **Тело кое врши контрола** е трговско друштво кое ги исполнува условите дефинирани ова упатство за вршење на контрола на системот за заштита на личните податоци.

5) **Усогласеност** (**Compliance**) е исполнување на барањата за заштита на личните податоци согласно прописите за заштита на личните податоци.

6) **Контрола на системот за заштита на личните податоци** (**Personal Data Protection Audit**) е систематско и независно испитување како би се утврдило дали активностите кои вклучуваат обработка на личните податоци се вршат согласно документацијата за техничките и организациските мерки на контролорот и дали оваа обработка ги исполнува барањата за заштита на личните податоци.

7) **Барања за заштита на личните податоци** (**Data Protection Requirements**) се условите кои ги одразуваат обврските на контролорот за применување на соодветни технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци при воспоставувањето на систем за заштита на личните податоци.

8) **Систем за заштита на личните податоци** (**Data Protection System**) е збир од документирани политики, кодекси на практика, насоки, процедури и работни инструкции донесени од страна на контролорот, а кои се во функција на спроведување на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци согласно прописите за заштита на личните податоци.

Изразите што се употребуваат во ова упатство, а чие значење не е дефинирано во ставот 1 на оваа точка, имаат значење утврдено со прописите за заштита на личните податоци.

II. КРИТЕРИУМИ ЗА ОБЕЗБЕДУВАЊЕ НА НЕЗАВИСНОСТ И НЕПРИСТРАСНОСТ НА ТЕЛОТО КОЕ ВРШИ КОНТРОЛА

4. Телото кое врши контрола, неговите одговорни лица и неговиот стручен персонал (лица кои вршат контрола) одговорен за извршување на контрола на системот за заштита на личните податоци не смеат да бидат обработувачот, третото лице, корисникот, проектантот, производителот, снабдувачот, или одржувачот на софтверските програми за обработка на личните податоци, кои се проверуваат од тоа тело, ниту пак овластениот претставник на која било од страните или пак физичкото или правното лице што ги пушта софтверските програми на пазарот.

Телото кое врши контрола, неговите одговорни лица и неговиот стручен персонал (лица кои вршат контрола) не смеат да бидат вклучени директно, индиректно или како овластени претставници во проектирањето, производството, конструирањето, маркетингот, сервисирањето, одржувањето или во работењето со софтверските програми за обработка на личните податоци, освен кога се работи за размена на технички информации помеѓу производителот и тоа тело.

Телото кое врши контрола не смее да врши контрола на системот за заштита на личните податоци кај контролор во времетраење од три години од датумот на престанување на неговите деловни односи со контролорот наведени во ставовите 1 и 2 од оваа точка.

5. Телото кое врши контрола и неговиот стручен персонал (лица кои вршат контрола) се должни да ја извршуваат контролата на системот за заштита на личните податоци со највисок степен на професионален интегритет и техничка компетентност и да бидат ослободени од сите притисоци и влијанија, посебно финансиски, кои би можеле да влијаат врз нивната оцена или врз резултатите од контролата, особено од лица или од групи на лица кои имаат интерес за резултатите од контролата.

6. Телото кое врши контрола е должно да го има на располагање потребниот стручен персонал (лица кои вршат контрола) за да може правилно да ги врши

административните и техничките задачи поврзани со активностите за контрола на системот за заштита на личните податоци.

Телото кое врши контрола е должно да има вработено на неопределено работно време, најмалку три стручни лица (лица кои вршат контрола) кои можат да бидат вклучени во процесот на контрола на системот за заштита на личните податоци и да поседуваат важечки еден или повеќе од следните сертификати:

1. CISM (Certified Information Security Manager),
2. CRISC (Certified in Risk and Information Systems Control),
3. IS0 27001 Lead Auditor,
4. CISA (Certified Information Systems Auditor),
5. CISSP (Certified Information Systems Security Professional).

7. Стручниот персонал (лица кои вршат контрола) одговорен за контрола на системот за заштита на личните податоци треба да има:

- квалитетна техничка и професионална обука,
- соодветно познавање на барањата за заштита на личните податоци кои што се утврдени во прописите за заштита на личните податоци, а се докажува со сертификат за посетена обука од Дирекцијата за заштита на личните податоци и
- способност потребна за составување на записници и извештаи со кои се докажува дека контролата била извршена.

8. Телото кое врши контрола задолжително треба да врши дејност која што се однесува на информациска сигурност или на ИТ ревизијата и да поседува сертификат согласно со меѓународниот стандард ISO/IEC 27001, како и да има добиено мислење од Дирекцијата за заштита на личните податоци за усогласеност со прописите за заштита на личните податоци.

Телото кое врши контрола е должно да ја гарантира непристрасноста на неговиот стручен персонал (лица кои вршат контрола) за вршење на контрола на системот за заштита на личните податоци и нивните плати не треба да зависат од бројот на извршени контроли или од резултатите на тие контроли.

III. НАЧИН НА ВРШЕЊЕ НА КОНТРОЛА НА СИСТЕМОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

9. Обемот на контролата на системот за заштита на личните податоци задолжително треба да биде дефиниран во Писмото за ангажирање (**Engagement Letter**) кое согласно договорот се склучува меѓу контролорот и телото кое врши контрола. Во Писмото за ангажирање особено се наведени делокругот на контролата на системот за заштита на личните податоци, целите кои треба да се постигнат, кои ресурси се потребни, временскиот рок на контролата и извештајот кој ќе биде подготвен (Прилог бр.1).

Контролорот и телото кое врши контрола задолжително склучуваат и договор за доверливост со кој се уредува заштитата на тајноста на податоците до кои дошле при вршењето на контролата на системот за заштита на личните податоци.

10. Контролата на системот за заштита на личните податоци ги вклучува следните фази:

- Дефинирање на задачата за извршување на контрола,
- Подготвување на контролата,
- Извршување на контролата и
- Формирање на мислење за извршената контрола – составување на Извештај.

1. Фаза 1- Дефинирање на задачата за извршување на контрола

11. Лицето кое врши контрола секогаш ја врши контролата на системот за заштита на личните податоци за потребите на контролорот, поради тоа двете страни треба да се согласат за задачата која е почетна точка на контролата и основа за Планот за контрола.

Задачата за извршување на контрола треба да биде документирана и како минимум да определува:

- Нарачател и корисник,
- Целта и природата на задачата,
- Објаснување на задачата,
- Контролорот,
- Опсегот на контролата, и тоа:

а) објектот (ите) (опис на операциите за обработка на личните податоци),

б) аспектот(ите) (доверливост, интегритет, континуитет и способност за контрола),

в) условите (кои прописи, стандарди и најдобри практики за заштита на личните податоци ќе бидат земени во предвид),

- Периодот,
- Способноста за заштита на личните податоци (дизајн, постоење, ефективност),
- Целна група / корисници на мислењето за извршената контрола,
- Форма и зачестеност на известување,
- Потребно време и буџет,
- Ограничувања во однос на извршување на контролата,
- Пристап до информации,
- Упатувања на важечкото законодавство и
- Ограничувања поврзани со одговорноста.

12. Во оваа фаза лицето кое врши контрола мора да биде сигурен дека ја разбира комплексноста и/или специфичните карактеристики на операциите за обработка на личните податоци кои ќе бидат опфатени со контролата на системот за заштита на личните податоци кај контролорот.

2. Фаза 2- Подготовување на контролата

13. За да се обезбеди ефикасен и ефективен пристап, лицето кое врши контрола мора да одлучи кои видови на активности ќе треба да ги изврши со цел да ги обезбеди потребните докази за неговото мислење за извршената контрола во однос на воспоставениот систем за заштита на личните податоци кај контролорот. Поради тоа, пред започнување на било кои активности, лицето кое врши контрола задолжително треба да изработи План за контрола (Прилог бр.2).

14. Планот за контрола претставува систематска и структуирана целина на активности кои треба да бидат извршени од страна на лицето кое врши контрола, за да може да го оцени дизајнот, спроведувањето/постоењето и/или ефективноста/континуираното работење на системот на мерки и процедури кои ги презема контролорот со цел правилно да ги заштити личните податоци кои ги обработува.

15.При изработувањето на Планот за контрола, лицето кое врши контрола за да може правилно да ги дефинира активностите мора да направи анализа на ризикот во однос на барањата за заштита на личните податоци кои произлегуваат од:

- Прописите за заштита на личните податоци,

- Општо прифатените практики и стандарди за заштита на личните податоци,
- Природата на личните податоци кои се обработуваат и
- Ризикот при нивната обработка.

При вршењето на анализа на ризикот, телото кое врши контрола задолжително го определува нивото на ризик (висок, среден и низок) на кое припаѓа контролорот според следните критериуми:

- Бројот на збирки на лични податоци,
- Бројот на овластени лица кои вршат обработка на лични податоци,
- Бројот на вработени лица кај контролорот.

3. Фаза 3- Извршување на контролата

16. При вршењето на контролата на системот за заштита на личните податоци, лицето кое врши контрола може да се користи со едно или со повеќе од следниве средства:

- Истражување,
- Собирање на докази и друг начин на документирање,
- Набљудување, или
- Користење на специјализирани ревизорски софтвери (т.н. Computer assisted audit techniques-CAAT's).

Во случај на користење на специјализирани ревизорски софтвери, во Писмото за ангажирање мора прецизно да се утврдат ревизорските софтвери кои ќе бидат употребувани во вршењето на контролата.

Насоките за вршење на контролата на системот за заштита на личните податоци се наведени во Прилогот бр.3.

17. За време на контролата на системот за заштита на личните податоци, лицето кое врши контрола е должно да направи доказно досие како дел од комплетното досие за извршената контрола. Доказното досие може да содржи:

- Извештаи од интервјуа и белешки од различни активности,
- Собрани информации/документации,
- Наоди, согледувања и одлуки кои се однесуваат на мислењето за извршената контрола.

18. За време на контролата на системот за заштита на личните податоци, лицето кое врши контрола мора да ги потврди своите наоди со одговорните лица кај контролорот.

4. Фаза 4- Формирање на мислење за извршената контрола – составување на Извештај

19. Врз основа на собраните информации, лицето кое врши контрола е должно да оцени дали се случиле повеќе или помалку материјални грешки кои можат да имаат влијание врз сигурноста на воспоставениот систем за заштита на личните податоци кај контролорот.

Лицето кое врши контрола е должно изграденото мислење за извршената контрола документирано да го образложи во Извештајот од извршената контрола кој што е утврден во одредбите од член 25 на Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на република Македонија“ бр. 38/09 и 158/10).

Во Извештајот од извршената контрола, лицето кое врши контрола е должно да ги наведе сите податоци и факти врз основа на кои го има изградено своето мислење за извршената контрола и ги има предложено мерките за остранување на констатираните недостаци на системот за заштита на личните податоци кај контролорот. Со ваквиот

пристап му се овозможува на корисникот на Извештајот од извршената контрола да добие сознание за начинот како лицето кое вршело контрола дошло до своето мислење за извршената контрола.

20. Контролорот има обврска да ги реализира препорачаните решенија за остранување на констатираните недостатоци на системот за заштита на личните податоци и да го следи нивното спроведување преку неговиот офицер за заштита на личните податоци.

21. Телото кое врши контрола има обврска Извештајот од извршената контрола да го доставува и до Дирекцијата за заштита на личните податоци.

IV. ПОСЕБНИ ОДРЕДБИ

22. Одредбите од ова упатство соодветно се применуваат и при вршењето на внатрешна контрола од страна на контролорот согласно одредбите од членовите 25 и 35-ѓ од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци, како и при проверката на постапувањето на обработувачот при обработката на личните податоци во смисла на член 26 став 3 од Законот за заштита на личните податоци.

23. Прилозите од број 1 до број 3 се составен дел на ова упатство. Содржината во Прилозите од број 1 до број 3 претставува само основа за понатамошно разработување на материјата која што се однесува на контрола на системот за заштита на личните податоци од страна на лицата кои вршат контрола.

V. ЗАВРШНА ОДРЕДБА

24. Ова упатство влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Македонија“.

Директор,
Димитар Ѓеорѓиевски