16. Мерење на произведената електрична енергија и моќност

Мерење на произведената, односно испорачаната електрична енергија во дистрибутивниот систем се врши во пресметковното мерно место во постапка и начин утврден согласно Мрежните правила за дистрибуција на електрична енергија.

17. Обврска за овозможување на пристап до производните единици и непосреден увид во документацијата

Носителот на лиценцата е должен по барање на Регулаторната комисија за енергетика, да и овозможи непосреден увид во целокупната документација, како и пристап во објектите, деловните простории, простори, инсталации, како и на средствата и опремата потребни за вршење на енергетската дејност, во согласност со Правилникот за лиценци за вршење на енергетски дејности.

18. Квалитет на услугата

Носителот на лиценцата е должен да обезбеди технички средства и други услови кои ќе овозможат постојан квалитет на произведената електрична енергија, согласно Мрежните правила за дистрибуција на електрична енергија.

Носителот на лиценцата е должен да врши постојан мониторинг на параметрите кои го определуваат квалитетот на произведената електрична енергија и по барање на Регулаторната комисија за енергетика, да доставува писмен извештај за движењето на сите параметри кои што го определуваат квалитетот на произведената електрична енергија во определен временски период.

19. Изменување и продолжување како и пренесување, престанување, суспендирање и одземање на лиценцата

Изменување и продолжување, како и пренесување, престанување, суспендирање и одземање на оваа лиценца ќе се врши во согласност со одредбите од Законот за енергетика и од Правилникот за лиценци за вршење на енергетски дејности.

20. Мерки во случај на неисполнување на обврските од страна на носителот на лиценцата

Доколку носителот на лиценцата не ги исполнува обврските содржани во оваа лиценца, Регулаторната комисија за енергетика ќе превземе мерки согласно Правилникот за лиценци за вршење на енергетски дејности.

Прилог 2

Податоци за фотоволтаичен систем приклучен на дистрибутивна мрежа согласно Табела VI:

1. **Име на фотоволтаичен систем:**
- Фотоволтаична централа „ФЕЦ Дуброво 950 kW“;

2. **Локација на фотоволтаичниот систем на дистрибутивната мрежа:**
- Приклучок од среднонапонска 10(20) kV ќелија во ТС 35/10/6/ kV ТЕЦ Неготино;

3. **Општи податоци:**
- година на почеток на градба: 2012 год.;
- година на завршеток на градба: 2012 год.;
- година на почеток на работа: 2012 год;
- проценет животен век на фотоволтаичниот систем: 35 години;
- зголемување на капацитетот, број на фотоволтаични модули и номинална моќност по години не е предвидена;

4. **Податоци за опрема:**
- број на фотоволтаични модули 3958 модули;
- тип, производител и номинални податоци на фотоволтаичниот модул тип: Canadian Solar CS6P-240Wp;
- производител: Канада;

Номинални податоци за фотоволтаичен систем:
- моќност на модул 240 W; напон 29,9 V; струја 6,96 A;
- вкупна моќност на ФВ генератор: 3958 x 240 = 949,92 kW;
- тип, производител и номинални податоци на батерија: нема батерија;
- тип, производител и номинални податоци на инвертор:
- тип: инвертор Sunways Solar Inverters PT 33k, AC output 33,3 kW;

производител: Austria;
- номинални податоци: моќност од 28x33,3 kW, AC напон 400 V;

5. **Годишно сончево зрачење на таа локација:** 4.291 kWh/m2 на хоризонтална површина;

6. **Очекувано производство на електрична енергија:** 1.136.101 MWh.

ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ

2079.

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 организацискиот 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 временетраење 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“.

Бр. 02-904/1
18 мај 2012 година
Скопје

Директор,
Димитар Ѓеорѓиевски, с.р.

Прилог бр.1

_____, со адреса на седиштето _____ и ЕМБС _____застапувана од _____ (во натамошниот текст: **Нарачател**) и

_____, со адреса на седиштето на _____ и ЕМБС_____ застапуван од _____ (во натамошниот текст: **Тело кое врши контрола**)

На ден_____ склучија

Писмо за ангажирање

1.Предмет

1.1. Со ова писмо се регулираат меѓусебните права и обврски на договорните страни при извршувањето на надворешната контрола на информацискиот систем и информатичката инфраструктура и на рачната обработка на личните податоци кај Нарачателот (во натамошниот текст: контрола на системот за заштита на личните податоци).

2. Цел

2.1 Примарна цел на контролата на системот за заштита на личните податоци е обезбедување на независно мислење за степенот до кој Нарачателот при обработката на личните податоци е во согласност со прописите за заштита на личните податоци.

2.2 Со контролата на системот за заштита на личните податоци ќе се утврди и до кој степен Нарачателот (во рамки на делокругот на контролата) покажува добри практики во неговото раководење со заштитата на личните податоци и управувањето со личните податоци.

3. Временски рок

3.1. Телото кое врши контрола се обврзува да ја изврши контролата на системот за заштита на личните податоци во рок од _____ работни дена, сметано најдоцна _____ дена од денот на влегувањето во сила на ова писмо, а според Планот за контрола и методологијата наведени во Понудата за _____, која е составен дел на ова писмо.

4. Опсег

4.1 Обемот на контролата на системот за заштита на личните податоци ќе ја оцени усогласеноста со соодветните начела за заштита на личните податоци, примената на прописите за заштита на личните податоци и добрите практики, како и ефективноста на активностите за заштита на личните податоци со особено повикување на:

а. XXXX

б. XXXX

в. XXXX

г. XXXX

д. XXXX

5.Надвор од опсегот

5.1 Телото кое врши контрола ќе ја ограничи активноста на контролата на системот за заштита на личните податоци на одделенијата и локациите согласно опсегот дефиниран во ова писмо.

5.2 Со контролата на системот за заштита на личните податоци нема да се разгледуваат и да се обезбедуваат коментари за индивидуалните случаи, освен до таа мера кога таквата работа може да го демонстрира степенот до кој Нарачателот ги исполнува своите обврски и покажува добри практики во заштитата на личните податоци.

5.3 Телото кое врши контрола го задржува правото да коментира за било кои слабости забележани во текот на контролата на системот за заштита на личните податоци со кои би можеле да се загрозат добрите практики на заштита на личните податоци.

6. Вршење на контрола на системот за заштита на личните податоци

6.1 Тимот одговорен за контролата пред самата контрола на системот за заштита на личните податоци ќе се сретне со претставници од Нарачателот:

- За да добие стратешки преглед на раководењето со процесот на обработка на личните податоци во рамки на организационата поставеност на Нарачателот и било какви други релевантни информации,
- За соодветно да го насочат и договорат опсегот на вршењето на контролата и
- Да ги дискутираат локациите идентификувани од страна на Телото кое врши контрола за посета и времетраењето на посетата.

6.2 Телото кое врши контрола може да побара посета на клучните одделенија и места во рамки на опсегот на контролата на системот за заштита на личните податоци и организационата поставеност како што е договорено со Нарачателот.

6.3 Идентификувањето на соодветните локации за посета Телото кое врши контрола ќе ги врши врз основа на:

- воспоставените внатрешни политики, процедури и акти за заштита на личните податоци,
- пројавените слабости и пропусти констатирани со внатрешните контроли и проверки на воспоставениот систем за заштита на личните податоци.

6.4 Распоредот на средбите и активности за контрола ќе се договорат со номинираните лица за контакт кај Нарачателот и идентификуваните бизнис области.

6.5 Тимот одговорен за контролата ќе се сретне со релевантните овластени лица за управување со процесот на контрола на усогласеноста со обврските за заштита на личните податоци. Ова ќе се постигне преку дискусија со вработените, преглед на релевантната евиденција и преглед на процедурите во практиката.

6.6 Тимот одговорен за контролата ќе бара пристап до релевантните клучни места каде е возможно да се разбере начинот на кој вработените ги обработуваат личните податоци (обезбедено е ограничување на опсегот).

6.7 Тимот одговорен за контролата ќе го разгледа степенот до кој офицерот за заштита на личните податоци ја вклучува контролата на заштита на личните податоци во својата програма за контрола и ја усогласува работата за избегнување на дуплирање на работата.

7. Тимот одговорен за контролата

7.1 Следниве лица ќе бидат дел од Тимот одговорен за контролата

XXXX	Тим менаџер
XXXX	XXXX
XXXX	XXXX

8. Извештај

8.1. Контролата на системот за заштита на личните податоци се смета за завршена:

- по потпишување на записникот за прифаќање на завршниот Извештај од двете одговорни лица на договорните страни.

8.2. Во рок од 10 (десет) работни дена од денот на прифаќањето на Извештајот од ставот 1 на оваа точка, Нарачателот може да достави забелешки во писмена форма на завршниот Извештај и да побара дополнителни објаснувања од Телото кое врши контрола.

8.3. Доколку во рокот наведен во ставот 2 на оваа точка, Нарачателот не испрати забелешки во писмена форма, се смета дека Извештајот конечно е прифатен.

9. Контакти

9.1.Лица за контакт

XXXX

XXXX

9.2 Посебен распоред на овластените лица на Нарачателот кои ќе бидат активно вклучени во посетите ќе биде документиран и однапред договорен меѓу страните на ова писмо.

10. Администрација

10.1 Индивидуалните аранжмани за пристап и контрола ќе бидат организирани преку лицата за контакт утврдени во ова писмо.

10.2 Кога е тоа возможно, интервјуата ќе се извршат кај Нарачателот. Со исклучок на прегледите и интервјуата преземени на специјализирани технички места кои можат да се извршат само со претходна согласност од Нарачателот.

11.Влегување во сила

11.1.Ова писмо влегува во сила на денот на потпишувањето од овластените претставници на двете договорни страни.

11.2. Ова писмо е составено во 4 (четири) еднакви примероци и секое има важност на оригинал, а по 2 (две) за секоја договорна страна.

НАРАЧАТЕЛ ТЕЛО КОЕ ВРШИ КОНТРОЛА

_____ _____

М.П М.П

Прилог бр. 2

	План за контрола	Број на предмет	
Контролор		Страна	
Оддел		Датум на контрола	

Датум	Време	Област/Функции	Лице кое врши контрола	Активност/ЛП Оценувани прашања

ПЛАНОТ ЗА КОНТРОЛА Е СОСТАВЕН ОД:	ПОТПИС:	ДАТУМ:

Прилог бр.3

НАСОКИ ЗА ВРШЕЊЕ НА КОНТРОЛА НА СИСТЕМОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

1. Доверливост и безбедност

Опис на начелото:

Контролорот мора да примени соодветни технички и организациски мерки за заштита од случајно или незаконско уништување на личните податоци, или нивно случајно губење, преправање, неовластено откривање или пристап, особено кога обработката вклучува пренос на податоци преку електронско комуникациска мрежа и заштита од какви било незаконски облици на обработка. Мерките обезбедуваат, имајќи ги во предвид достапната технологија и трошоците за имплементација, соодветно ниво на безбедност. Адекватноста на нивото на безбедност зависи од ризикот вклучен во обработката и од природата на личните податоци. Мерките исто така, имаат за цел спречување на непотребно собирање и понатамошна обработка на личните податоци, односно обезбедување на соодветен квалитет на личните податоци.

Контролорот може да пренесе работи од неговиот делокруг на работа поврзани со обработка на лични податоци на обработувач кој обезбедува доволно гаранции за применување на технички и организациски мерки за тајност и заштита на обработката на личните податоци. Меѓусебните права и обврски на контролорот и обработувачот мора да бидат уредени со договор во писмена форма согласно одредбите од член 26 од Законот за заштита на личните податоци.

Релевантни прописи:

- Законот за ратификација на Конвенцијата за заштита на физичките лица која се однесува на автоматската обработка на личните податоци на Совет на Европа бр.108 од 1981 година („Службен весник на Република Македонија бр. 7/05),
- Законот за ратификација на Дополнителниот протокол кон Конвенцијата во врска со надзорните тела и прекуграничниот пренос на податоци („Службен весник на Република Македонија бр. 103/08),
- Директивата 95/46/ЕК за заштита на личните податоци и слободниот проток на таквите податоци на Европскиот парламент и Советот на Европската унија од 24 октомври 1995 година,
- Законот за заштита на личните податоци („Службен весник на Република Македонија“ бр. 7/05, 103/08, 124/10 и 135/11) (член 23),
- 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).

2. Активности кои ќе бидат извршени од страна на лицето кое врши контрола

Определување дали контролорот ги има преземено соодветните технички и организациски мерки, имајќи го во предвид идентификуваниот ризик на обработка на личните податоци и нивната природа.

Техничките и организациските мерки генерално може да бидат групирани во следниве 14 категории:

1. Безбедносна политика, безбедносен план и имплементација на системот за процедури и мерки(документација за техничките и организациските мерки)
2. Административна организација
3. Свест за безбедноста
4. Персонални услови
5. Дизајн на работното место
6. Администрирање и класификација на информатичката инфраструктурата
7. Менаџмент за пристап
8. Мрежа и надворешна поврзаност
9. Употреба на софтвер
10. Масовна обработка на податоците
11. Чување на податоците
12. Уништување на податоците
13. Непредвидено планирање
14. Склучување на договори за обработка на личните податоци

Определување дали личните податоци се обработени од страна на обработувачот. Доколку е тоа случај:

- Определување кои активности се извршени од страна на обработувачот во име и за сметка на контролорот
- Определување дали постои адекватен договор поврзан со обработката на личните податоци

Определување како контролорот се обезбедува дека обработувачот има соодветни технички и организациски мерки и/или како контролорот го проверува постапувањето на обработувачот при обработката на личните податоци согласно договорот и прописите за заштита на личните податоци.

3. Собирање на докази

Прашања:

- Дали постои политика за безбедност на личните податоци, односно документација за техничките и организациските мерки? Доколку тоа е случај, кој/кои оддел(и) е (се)

одговорни за изготвување и спроведување на Политиката за безбедност на личните податоци, односно на документацијата за техничките и организациските мерки кај контролорот?

- Како потенцијалната штета врз субјектот на личните податоци и природата на податоците е проценета за да се одлучи дали политиката, односно документацијата е соодветна?

- Дали нивото на безбедност е поставено на соодветно ниво, земајќи ја во предвид состојбата на технолошкиот развој во технолошките производи и трошоците за нивно распоредување?

- Колку често е разгледувана политиката за заштита на личните податоци, односно документација за техничките и организациските мерки ?

- Дали политиката за заштита на личните податоци, односно документацијата за техничките и организациските мерки конкретно одговара на проблемите за заштита на податоците?

- Дали контролорот го применува меѓународниот стандард ISO/IEC27001:2005 или друг безбедносен стандард / кодекс на практика (на пример COSO, ITIL и COBIT)?

- Кои се процедурите за следење на усогласеноста со Политиката за безбедност на личните податоци, односно со документацијата за техничките и организациските мерки во рамки на организационата поставеност на контролорот? Колку често се оценува усогласеноста со Политиката за безбедност на личните податоци, односно со документацијата за техничките и организациските мерки и во кој оддел? Дали постојат процедури за управување со не – усогласеноста?

- Дали Политиката за безбедност на личните податоци, односно документацијата за техничките и организациските мерки јасно идентификува што претставува незаконска и неовластена обработка?

- Кои безбедносни мерки се однесуваат за спречување на какво било неовластена и незаконска обработка на:

    - Податоци што се чуваат во автоматизиран формат (на пример: лозинка за контролирање на пристапот до компјутерите)

    - Податоци кои се чуваат во рачна евиденција (на пример: заклучени простории)

- Дали постои повисок степен на безбедност за спречување од неовластена и незаконска обработка на посебни категории на лични податоци?

- Кои процедури се однесуваат на откривање на нарушување на безбедноста (оддалеченост (remote), физички или логички)?

- Дали вработените се обврзани и се овластени за обработка на личните податоци и се свесни за Политиката за безбедност на личните податоци, односно за документацијата за техничките и организациските мерки?

- Дали на вработените им е овозможена некоја обука за безбедност и управување со ризикот, како и за заштита на личните податоци?

- Како е ограничен пристапот до личните податоци на овластените лица? На пример: потребно е да знае.

- Дали организацијата користи криптирање за заштита на (посебните категории) личните податоци? Доколку е тоа случај, како се управуваат и користат клучевите за криптирање?

- Како е ограничен пристапот до системите и локациите за овластените лица?
- Како се спречува неовластено копирање, принтање и правење сигурносна копија на (посебните категории) лични податоци?
- Дали вработените се овластени да преземаат опрема/софтвер за надворешна употреба/за работа од дома (на пример:преносен компјутер (lap top)?
    - Доколку е тоа случај, дали тие добиваат посебни инструкции во однос на тоа како да бидат заштитени личните податоци кои се зачувани во таа опрема/софтвер?
- Како се врши уништувањето на личните податоци кои повеќе не се потребни со цел да се заштитат од неовластен пристап?
- Дали постојат различни процедури за уништување на посебни категории на лични податоци?
- Дали постои резервен план за управување со ефектите од непредвидливите настани?
    - Доколку е тоа случај, дали се врши тестирање на тој план? Колку често?
- Дали вработените се известени за резервните процедури?

Кои се процедурите за управување со ризик, доколку ги има за враќање на личните податоци (и автоматизирано и рачно) кои би можеле да бидат уништени или изгубени при:

- Човечка грешка
- Компјутерски вирус
- Пад на мрежата
- Кражба
- Пожар
- Поплава
- Друга виша сила?

Во случај на обработка од трети лица:

- Дали се врши обработка од трети лица?
    - Доколку не, ова начело не е применливо
    - Доколку да, кои процеси на обработка на личните податоци се доверени на обработувачот?
- Дали контролорот и обработувачот имаат договор за регулирање на обработката?

4. Собирање на материјали

- Информациска безбедносна политика
- Информациски безбедносен план
- Документација за технички и организациски мерки
- Процедури, работни инструкции и насоки во однос на административната организација
- Процедури, работни инструкции и насоки во однос на заштитата на медиумите
- Процедури, работни инструкции и насоки во однос на пренесување на медиуми

- Процедури во однос на правење на сигурносни копии, реконструкција и вонредно планирање
- Процедури, работни инструкции и насоки во однос на чување/снимање (архивирање) и уништување на податоци (бришење)
- Процедури, работни инструкции и насоки во однос на праќање на личните податоци по пошта или преку електронска пошта и кодекс на однесување или упатство или прописи за електронска комуникација
- Постапка за овластување
- Процени за определување на овластувањата
- Инструкции за тајност
- Процедури, инструкции и насоки во однос на справување со безбедносни инциденти
- Насоки во однос на грешки во системот (како контролорот се справува со грешките во системот, односно врши проверување на инцидентите)

Во случај на обработка од трети лица, исто така:

- Договори со обработувачот, вклучувајчи ги сите документи кои ги опишуваат релевантните аспекти на обработката на личните податоци и обврските на обработувачот за заштита на личните податоци
- Процедури, инструкции и насоки во однос на аспектите кои треба да се земат во предвид при обработката на личните податоци од трети лица
- Извештаи од контролорот во однос на периодичните проверки на постапувањето на обработувачот при обработката на личните податоци или извештај од страна на (надворешен) независен ревизор кој спровел проверка на обработката.

5. Набљудување

Релевантно набљудување во овој случај може да биде дека лицето кое врши контрола ги потврдува записите од авторизираниот пристап во однос дали само овластените лица имаат пристап до личните податоци. Друг пример за можно набљудување ќе биде следењето на процедурите за "чисто биро". Бироата на вработените не треба да содржат лични податоци (посебни категории) кои мораат да бидат заштитени од неовластен пристап.

Ќе се преземат активности онаму каде што постои несигурност во однос на вклученоста на трети лица/ во случај на обработка од трети лица:

- Проверка дали трети лица се вклучени во обработката на податоците. Дали некои од вработените им дале на трети лица пристап до системот кој се користи за обработка на личните податоци?
- Проверка дали контролорот е зависен од трети лица, каде е во интерес интегритетот, исклучивоста и/или достапноста на личните податоци.