ПРИРАЧНИК

ЗА ПРАКТИЧНО СПРОВЕДУВАЊЕ НА ПРАВИЛНИКОТ ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

ДЗЛП
Дирекција за заштита на личните податоци на Република Македонија

П Р И Р А Ч Н И К

за практично спроведување на

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

„Ако мислите дека технологијата ќе ви ги реши проблемите со сигурноста, тогаш не ги разбирате проблемите и не ја разбирате технологијата.”

БРУС ШАЈНЕР,
експерт за сигурност

Скопје, 2010

Прирачник за практично спроведување на Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на личните податоци

Издавач:
Дирекција за заштита на личните податоци

За издавачот:
Маријана Марушиќ, Директор

Уредници:
Маријана Марушиќ
Неда Коруновска
Наде Наумовска

Автор:
Андреј Томшиќ

Лектура на коментарите на Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на личните податоци:
Абакус

Превод од англиски:
Оливер Јордановски

Ликовно-графичко обликување:
Бригада Дизајн

Печат:
Пропоинт

Тираж:
1000

Печатењето на публикацијата финансиски е поддржано од:

FOUNDATION ФОНДАЦИЈА
OPEN ИНСТИТУТ
SOCIETY ОТВОРЕНО
INSTITUTE ОПШТЕСТВО
MACEDONIA МАКЕДОНИЈА

CIP-Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

342.738.03(497.7)(035)

ТОМШИЌ, Андреј
Прирачник за практично спроведување на правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци/ (автор Андреј Томшиќ; превод од англиски јазик Оливер Јордановски). - Скопје: Дирекција за заштита на лични податоци, 2010. – 120 стр.; 21 см.

Превод на делото: Guidance for practical implementation on the rulebook on the tehnical and organization measures for providing secrecy and protection of personal data processing/ Andrej Tomshic.- фусноти кон текстот

ISBN 978-9989-2819-7-6
I.Tomshic, Andrej види Томшиќ, Андреј
а) Заштита на лични податоци- Технички и организациски мерки – Македонија – Прирачници
COBISS.MK-ID 83285002

СОДРЖИНА

ПРЕДГОВОР

Годинава се одбележуваат пет години од воспоставувањето на законската и институционалната рамка за заштита на личните податоци во Република Македонија, како концепт што подразбира вклучување на правото на приватност на граѓаните и заштита на нивните лични податоци во нашиот правен систем, што е исклучително важен момент во историјата на заштитата на основните слободи и права на човекот и граѓанинот.

Искуствата на Дирекцијата покажуваат дека јавноста позитивно ги прифаќа воспоставените начела за заштита на личните податоци, кои треба да бидат лесно применливи во практиката. Во текот на досегашното работење, Дирекцијата оцени дека за целосно почитување на овие начела, од особено значење е и уредувањето на техничките и организациските мерки за тајност и заштита на личните податоци.

Во Законот за заштита на личните податоци и во Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци се утврдени мерките што треба да ги применат контролорите и обработувачите, со цел да се обезбеди тајност и заштита на обработката на личните податоци, а во зависност од природата на податоците што се обработуваат и ризикот при нивната обработка, овие мерки се класифицирани на три нивоа, така што контролорите и обработувачите се должни да водат документација со опис на преземените мерки.

Имајќи ја предвид досегашната практика којашто покажува дека обврските за контролорите и обработувачите што произлегуваат од овој правилник создаваат извесни нејаснотии за нив, искрено веруваме дека со изработката на Прирачникот за негово практично спроведување, во значителна мера ќе се олесни примената на Правилникот.

Затоа, Дирекцијата за заштита на личните податоци ѝ изразува голема благодарност на Фондацијата Институт отворено општество – Македонија за континуираната поддршка, дадена преку потпрограмата „Апроксимација на законодавството", во рамките на која беше изработен и публикуван овој Прирачник, како и за севкупната досега дадена поддршка за афирмација на правото на заштита на личните податоци. Дирекцијата му изразува голема благодарност и на авторот на Прирачникот, г. Андреј Томшич од Република Словенија, експерт во оваа област.

Искрено се надеваме дека Прирачникот за практично спроведување на Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци ќе им овозможи на контролорите и на обработувачите полесно да го разберат Правилникот, а со тоа и побрзо да ја подготват документацијата со која ќе се гарантира тајноста и заштитата на обработката на личните податоци.

Дирекцијата за заштита на личните податоци

ВОВЕД

Целта на овој прирачник за практично спроведување на Правилникот за техничките и организациските мерки **за обезбедување тајност и заштита на обработката на личните податоци** (во натамошниот текст: Прирачник) е да обезбеди насоки за практично спроведување за контролорите кои треба да ги почитуваат одредбите од прописите за заштита на личните податоци (Закон за заштита на личните податоци, „Службен весник на РМ" бр. 38 од 18.3.2009; во натамошниот текст ЗЗЛП), а се фокусира на спроведувањето на Правилникот за техничките и организациските мерки **за обезбедување тајност и заштита на обработката** на личните податоци. Поконкретно, Прирачникот дава јасни анализи и објаснувања на одредбите во Правилникот, нагласувајќи ја важноста на разни одредби и давајќи им препораки на контролорите за тоа како да ги испочитуваат тие одредби, и тоа преку практични примери и насоки за спроведување. Насоките се наменети за да го направат Правилникот почитлив и поразбирлив за контролорите, но тие не можат да бидат решение за сите проблеми во врска со сигурноста на податоците, бидејќи технолошката заднина на контролорите е премногу разновидна за да се даде единствен одговор на нивните сигурносни потреби. Насоките би требало да им помогнат на контролорите да ги разберат условите од Правилникот и да ги водат во изборот и донесувањето информирани одлуки при усвојувањето на потребната документација, технологии и процедури.

I. ОПШТИ ОДРЕДБИ

ПРЕДМЕТ НА УРЕДУВАЊЕ

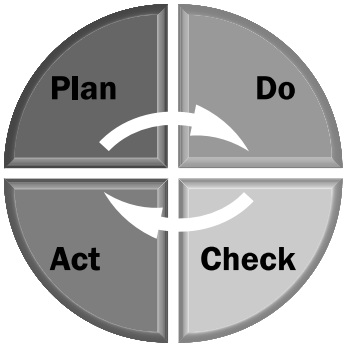
Член 1 **Со овој правилник се пропишуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци што ги применува контролорот на збирка на лични податоци.**

Пред сè, од најголема важност е контролорите јасно да ја разберат разликата меѓу заштитата на податоците и сигурноста на податоците. Иако е само дел од многу поширокиот термин заштита на (лични) податоци, сигурноста на личните податоци е несомнено еден од најважните, ако не и најважен столб на заштитата на податоците. Сигурноста на информациите се заснова на три столба: тајност, потполност и достапност. Како што е наведено во членот 1, сигурноста на личните податоци се состои од технички и организациски мерки и процедури кои обезбедуваат тајност и сигурност на обработката на личните податоци. Со цел да се обезбеди тајноста и сигурноста на обработката на личните податоци, контролорите и обработувачите треба да применуваат соодветни технички и организациски мерки за да ги заштитат личните податоци од секакво случајно или незаконско уништување или случајно губење, менување, неовластено откривање или пристап, особено кога обработката вклучува и пренос на податоци преку мрежа, вклучително и заштитни мерки против кои било други незаконски облици на обработка.

Спроведувањето на техничките и организациските мерки не е еднократна задача. Сигурноста на информациите е процес во кој усвојувањето на неопходната документација е само првата фаза. Правилникот нема да биде од корист ако собира прав на некоја по-

лица. Процедурите пропишани во документацијата треба навистина да се применуваат и да се следат во практиката. Треба да се утврдат недостатоците и да се применат корективни мерки. Тој процес е прикажан во добропознатиот PDCA круг (Plan, Do, Check, Act), (План, Изведба, Проверка, Дејствување) на информацискатa сигурност.

Дијаграм 1: PDCA круг



ПОИМНИК

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

1. **Авторизиран пристап е овластување доделено на корисникот за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории на контролорот;**
2. **Администратор на информацискиот систем е лице овластено за планирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци;**
3. **Документ е секој запис кој содржи лични податоци и истиот може да биде во електронска или хартиена форма, да се чува на медиум и во информатичко комуникациската опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку телекомуникациска мрежа.**
4. **Идентификација е постапка за идентификување на корисникот на информацискиот систем;**
5. **Информатичка инфраструктура е целата информатичко комуникациска опрема на контролорот, во рамките на која се собираат, обработуваат и чуваат личните податоци;**
6. **Информациски систем е систем со кој се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да ги користи;**
7. **Инцидент е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци;**
8. **Контрола на пристап е операција за доделу-**

вање на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на корисникот;

9. **Корисник е лице вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и до информатичко комуникациската опрема;**
10. **Лозинка е доверлива информација составена од збир на карактери кои се користат за проверка на корисникот;**
11. **Медиум е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на кој податоците можат да бидат снимени или од кој истите можат да бидат повторно вратени;**
12. **Одговорно лице за заштита на личните податоци е лице овластено од контролорот за координирање и контрола на техничките и организациските мерки кои се применуваат за тајност и заштита на обработката на личните податоци;**
13. **Проверка е постапка за верификација на идентитетот на корисникот на информацискиот систем;**
14. **Сигурносна копија е копија на личните податоци содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторно враќање.**

Дефинициите дадени во членот 2 треба да ги направат одредбите од Правилникот поразбирливи за контролорите. Изразите што се користат во Правилникот се однесуваат на вообичаените елементи во контекст на информацискатa безбедност, па според тоа не би требало да има поголеми проблеми со дефинициите или да се јават двосмисленост при нивното толкување.

ОБРАБОТУВАЧ НА ЗБИРКА НА ЛИЧНИ ПОДАТОЦИ

Член 3 **Одредбите од овој правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.**

Членот 3 нагласува дека одредбите од Правилникот се однесуваат на обработувачите на збирки на лични податоци. Тоа е важна забелешка којашто е во согласност со одредбите или со примената на самиот Закон за заштита на личните податоци, што не се однесува на некој вид обработка на лични податоци, туку на обработка на лични податоци кои се организирани или се дел од т.н. збирка на лични податоци, дефинирано во членот 2(3) од ЗЗЛП, односно секој структуриран збир од лични податоци до кои може да се пристапи според конкретни критериуми, било да се централизирани, децентрализирани или распространети на функционална или на географска основа. Следствено, овој правилник не се однесува на заштитата на личните податоци кои не се дел од збирка на лични податоци.

Некоја биографија, на пример, или сличен збир неструктурирани податоци (есеј, напис итн.) кои содржат (некои) лични податоци, не се сметаат за збирка на лични податоци доколку нема показатели за структура во рамките на која се организирани податоците.

ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 4 **Одредбите од овој правилник се применуваат за:**

- **целосно и делумно автоматизирана обработка на личните податоци и**
- **друга обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.**

Членот 4 дефинира дека овој правилник важи без оглед на тоа дали личните податоци се обработуваат рачно, делумно автоматски или целосно автоматски. Понатаму, се нагласува дека одредбите од Правилникот се применуваат доколку личните податоци се дел од постојна збирка на лични податоци или ако се наменети да станат дел од таков систем. Овој важен момент нагласува дека контролорите кои само рачно обработуваат лични податоци, исто така треба да се придржуваат до одредбите од Правилникот. Сепак, очигледно е дека далеку поголем обем податоци се обработуваат преку информатичките и комуникациските технологии со помалку или повеќе автоматизирани процедури.

Личните податоци кои се чуваат на хартија и се обработуваат рачно исто така треба да подлежат на сигурносни мерки. Иако некои од одредбите во Правилникот не можат да се применат на рачно обработени лични податоци, извесен број одредби, сепак, се мошне важни, особено организациските мерки. Во поглед на мерките за техничка сигурност, најважни аспекти се прашањата за контрола на пристапот (физичкиот).

Кога личните податоци се обработуваат рачно и се чуваат главно на хартија, треба да се применува строга контрола на пристапот. Корисниците не треба да ги остават документите кои содржат лични податоци на дофат на неовластени лица. По завршувањето на работното време просториите треба да се заклучуваат, а корисниците треба да се придржуваат до т.н. политика на чисто биро (документите се заклучуваат во фиоки, а не се остават на биро).

НИВОА НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 5

(1) Контролорот треба да применува технички и организациски мерки, кои обезбедуваат тајност и заштита на обработката на личните податоци, соодветно на природата на податоците кои се обработуваат и ризикот при нивната обработка.

(2) Техничките и организациските мерки од ставот (1) на овој член се класифицираат во три нивоа:
- основно;
- средно и
- високо.

Членот 5(1) е многу важен затоа што на некој начин им дава малку „слободен" простор и на контролорите и на инспекциските органи. Непрактично е и неизводливо да се бара истото ниво на тајност и сигурност од сите контролори, од контролорите со огромни збирки лични податоци (на пример, голема болница) кои содржат голем обем лични (и чувствителни) податоци, па сè до малите контролори (како, на пример, фризер) кои обработуваат многу малку лични податоци. При одредувањето на соодветното ниво на тајност и сигурност, треба да се земат предвид природата и ризиците за злоупотреба на личните податоци. Затоа, една голема болница треба да применува далеку покомплексни и пошироки мерки за сигурност на податоците бидејќи обработува високочувствителни лични податоци.

Понатаму, Правилникот разликува три нивоа на сигурност и тајност на податоците: основно, средно и високо.

Со цел да се оценат природата и ризиците за личните податоци, би било мудро да се направи проценка на ризикот, што во практична смисла значи дека прво се подготвува преглед на личните податоци што се обработуваат, а во втората фаза се оценуваат природата и ризиците за обработените податоци (на пример, чувствителноста, последиците во случај на злоупотреба или прекршување на законот). Колку е

повисока чувствителноста на податоците и поголеми ризиците што ги носи обработувањето на одредени лични податоци, толку посилни и попробојни треба да бидат мерките за сигурност. Членот 6 од Правилникот обезбедува можно раздвојување според разликите во природата и ризиците на обработувањето на одредени видови лични податоци.

ПРИМЕНА НА НИВОА

Член 6

(1) За сите документи задолжително се применуваат технички и организациски мерки кои се класифицирани на основно ниво.

(2) За документите кои содржат лични податоци што се однесуваат на: кривични дела, изречени казни, алтернативни мерки и мерки на безбедност за извршени кривични дела, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

(3) За документи кои содржат: посебни категории на лични податоци, лични податоци кои се обработуваат за полициски цели и лични податоци кои се обработуваат заради заштита на интересите на државната безбедност и одбраната на Република Македонија, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

(4) За документите кои содржат матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

(5) За документите кои се пренесуваат преку телекомуникациска мрежа, а содржат посебни категории на лични податоци и матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класи-

фицирани на основно, средно и високо ниво.

(6) Со документацијата за технички и организациски мерки, контролорот треба да пропише и обезбеди соодветен степен на заштита на личните податоци, согласно на нивоата кои се определени во овој член.

Основното ниво на сигурност треба да се применува за сите лични податоци. Почувствителните податоци, на пример видовите лични податоци опфатени во членовите 6(2)–6(4), бараат построги сигурносни мерки. Како што е наведено во членот 6(5), за документите што се пренесуваат преку телекомуникациска мрежа, за посебните категории лични податоци (види дефиниција во членот 2(10) од ЗЗЛП) и за матичните броеви на граѓаните е потребно повисоко ниво на сигурност.

ПРАВИЛА ЗА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ НАДВОР ОД РАБОТНИТЕ ПРОСТОРИИ НА КОНТРОЛОРОТ

Член 7

Обработката на личните податоци надвор од работните простории на контролорот се врши врз основа на обезбедено писмено овластување од страна на контролорот и во согласност со соодветното ниво на технички и организациски мерки кои се применувале за обработка на податоците содржани во документите.

Не е невообичаено дел од обработката на личните податоци во име на контролорите да ја вршат изведувачи или обработувачи по договор. Обработувачот по договор може да биде подобро опремен, да има подобро знаење, работна сила и други ресурси, што ќе доведе до тоа дел од обработката на податоците да се врши надвор од просториите на контролорите. На пример, некоја мала фирма може да ги даде по договор дејностите од областа на сметководството или маркетингот или видеонадзорот на фирми кои се специјализираат во таа област. Секако, од витално значење е

давањето под договор на тие лични податоци да се врши единствено со писмено овластување од страна на контролорот и договорниот обработувач на податоци да ги применува истите заштитни мерки за личните податоци.

Се препорачува секоја договорна обработка на личните податоци да се врши врз основа на писмен договор потпишан од обете страни. Составен дел од договорот треба да биде и согласноста меѓу двете страни за организациските и техничките мерки што ги применува договорниот обработувач. Сите вработени кај договорниот обработувач кои ќе работат со податоците треба да се информираат за нивните обврски за заштита на личните податоци. На пример, персоналот за обезбедување кај договорниот обработувач на видеонадзор во име на контролорот (на пример, министерството) мора во секое време да биде свесен што може, а што не може да стори со снимките од видеонадзорот. Ако правилата не се јасни и ако не им се јасно изложени на вработените кај договорниот обработувач, голема е можноста да дојде до прекршување на тајноста на личните податоци.

ЕВИДЕНТИРАЊЕ И ЧУВАЊЕ НА ДОКУМЕНТАЦИЈА ЗА СОФТВЕРСКИ ПРОГРАМИ

Член 8 **Контролорот треба да ја евидентира и да ја чува целокупната документација за софтверските програми за обработка на личните податоци и за сите негови промени.**

Со оглед на тоа дека денес компјутерите обработуваат огромен обем лични податоци, важно е јасно да се следи како функционира софтверот што ги обработува личните податоци. Покрај ова, и измените во софтверот треба добро да се документираат. Нејасната или неажурирана документација за управувањето со софтверот може да доведе до расипување на податоците, излегување, злоупотреба, па дури и до губење на податоците.

Тендерските процедури за софтверот треба добро да се документираат, а истото важи и за техничката документација што ја обезбедува (или треба да ја обезбеди) изработувачот на софтверот изнајмен за конкретни софтверски решенија. Сите натамошни измени на софтверот треба да се документираат за да се спречи неочекувано однесување на системот и да се олеснат процедурите за повторно враќање.

Совет за малите контролори

Малите контролори, кои главно се потпираат на широко употребуваните алати за обработка на личните податоци (на пример, Microsoft Office, OpenOffice.org или друг добро познат софтвер за канцелариско работење) треба посебно да внимаваат на примената на сите заштитни поправки и надградби. При купувањето софтвер секогаш се препорачува да се прочитаат критиките од клиентите кои веќе го купиле производот и да се потпирате на софтвер што вообичаено се користи во дејноста на контролорот. Запомнете дека треба да ги користите функциите за следење на промените кај вообичаените софтвери за канцелариско работење, на пример Excel или Access (види и пример под членот 17).

ОДРЖУВАЊЕ НА ИНФОРМАЦИСКИОТ СИСТЕМ

Член 9

(1) Физичките или правните лица кои вршат одржување на информацискиот систем на контролорот треба да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

(2) Одредбите од ставот (1) на овој член се применуваат и ако физичките или правните лица вршат обработка на личните податоци на контролорот.

Одржувањето на информацискитесистемиеуштеедноможност за напад или за губење, во смисла на сигурноста на личните податоци. Затоа, членот 9 уредува дека и правните и физичките лица треба да ги применуваат одредбите за сигурност, без оглед на тоа дали работат за контролорот, директно или не. Тоа е особено важно кога одржувањето на информацискиот систем (базата на податоци, сервисот, апликацијата или други делови од информацискиот систем) го вршат лица кои не се вработени кај контролорот, што е чест случај. Слично на одредбите од претходниот член, тие лица треба да се придржуваат до строгите правила и мерки за тајност на личните податоци.

Ако одржувањето на информацискиот систем (или на дел од него) се дава под договор, добро е да се применат препораките од претходниот член: писмен договор (вообичаено наречен Договор за сервисирање) со конкретни и јасни потребни правила за сигурност на податоците.

Совет за малите контролори

Малите контролори обично се потпираат на договорни информатички услуги бидејќи ним им е скапо да имаат сопствен информатички персонал. При изборот на давателите на информатички услуги (на пример, за информатичко одржување или служба за помош) секогаш проверувајте ја нивната репутација

и, во секој случај, имајте писмен договор со давателот на услугите. Исто така, погрижете се за тоа и давателот на информатички услуги да биде потполно свесен дека и тој треба да ги заштити личните информации до кои може да има пристап и дека треба целосно да ги почитува вашите мерки за заштита на податоците. Вашиот внатрешен акт за заштита на податоците треба да биде суштински дел од договорот со нив.

III. ОСНОВНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

ДОКУМЕНТАЦИЈА ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 10

(1) Контролорот задолжително донесува и применува документација за технички и организациски мерки за корисниците кои имаат пристап до личните податоци и до информацискиот систем.

(2) Документацијата од ставот (1) на овој член особено содржи:

- **План за создавање систем на технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци;**
- **Акт за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;**
- **Правила за определување на обврските и одговорностите на корисниците при користење на документите и информатичко комуникациската опрема;**
- **Правила за пријавување, реакција и санирање на инциденти;**
- **Правила за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;**
- **Правила за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите.**

(3) Документацијата од ставот (2) на овој член, контролорот веднаш ја менува и дополнува кога ќе се направат промени во организационата поставеност на информацискиот систем.

Членот 10 ја опишува потребната документација за технички и организациски мерки, којашто треба да постои и на хартија и во практиката. Накусо, документацијата треба да содржи:

- План за воведување систем за управување со сигурноста;
- Акт со опис на техничките и на организациските мерки за сигурност на податоците (види насоки за членовите 11, 12, 13, 14, 18);
- Обврски и одговорности на корисниците (види насоки за членот 15);
- Процедури за управување со инциденти (види насоки за членот 16);
- Политика на сигурносни копии / ургентен план (види насоки за членовите 21–22), и
- Политика за чистење на медиумите (види насоки за членовите19–20).

Членот 10(3) уредува дека документацијата треба да се ажурира и дека треба да ги одразува измените во информациските системи или во процедурите. Контролорите на податоци треба да решат дали ќе користат хиерархија на документи или ќе ги покријат потребните области со еден документ. При примената на примерите со најдобри практики и прифатените меѓународни стандарди за информатичка сигурност, како ISO/IEC 27001:2005, се препорачува да се оди на хиерархиски пристап и да се покрива секоја тема одделно. Генерално, потребната документација треба да ги покрива барем областите опишани во следниве членови 11–22 од Правилникот и областите кои понатаму ќе се покријат во Прирачникот. Да ги погледнеме првите две точки. Првиот потребен документ е план за воведување систем за управување со сигурноста. Планот треба да содржи дефиниција на опфатот на системот за управување со сигурноста (дефиниција на збирките на лични податоци што треба да се заштитат) и на резултатите од оценката на ризикот. Овие два елемента од планот треба да се одразат во вториот документ – внатрешен акт со кој се дефинира мерката што ќе се воведе за да се намалат или да се сведат на минимум утврдените ризици. На пример, планот треба, да го утврди ризикот од уништување на личните податоци и да дефинира мерки за заштита од овој ризик (на пример, сигурносни копии на друга локација). Содржината на актот се пропишува во членовите 11–22 и вклучува технички мерки, организациски мерки, контрола на пристапот, управување со инциденти итн.

ТЕХНИЧКИ МЕРКИ

Член 11

Контролорот треба да обезбеди соодветни технички мерки за тајност и заштита на обработката на личните податоци и тоа:

1. **единствено корисничко име;**
2. **лозинка креирана од секој корисник, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;**
3. **корисничко име и лозинка која овозможува пристап на корисникот до информацискиот систем во целина, на поединечни апликации и/или поединечни збирки на лични податоци потребни за извршување на неговата работа;**
4. **автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути) и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;**
5. **автоматизирано отфрлање од информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на корисникот дека треба да се побара инструкција од администраторот на иниформацискиот систем;**
6. **инсталирана хардверска/софтверска заштитна мрежна бариера („фајервол") или рутер помеѓу информацискиот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот;**
7. **ефективна и сигурна анти-вирусна и анти–спај-**

вер заштита на информацискиот систем, која постојано ќе се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвер;

8. **ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и**
9. **приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.**

Членот 11 уредува низа неопходни технички мерки. Единствени кориснички имиња значи дека секој корисник треба да има свое корисничко име, што е особено важно од аспект на одговорноста и отчетноста. Со групни кориснички имиња не може да се обезбеди отчетност, зашто е многу потешко злоупотребата на лични податоци да му се припише на едно лице. Контролорите кои применуваат некаков систем за управување со идентитет (како Active Directory) треба да ги користат функциите на групна политика за да ги постават условите дадени во овој член (на пример, должина и состав на лозинката).

Контролорот може да користи добри практики при генерирањето лозинки, на пример да ги има предвид следниве препораки[1]:

1. Избегнувајте да користите зборови од речник! Хакерите лесно ги пробиваат тие лозинки со електронски речник.
2. Не користете лични информации! Кој било дел од името, роденденот, матичниот број или слични информации за блиските се лош избор за лозинка.
3. Избегнувајте вообичаени секвенци, како последователни броеви или букви („123”, „абв” или повторување на броеви или букви („аааа”)!
4. Повеќето лозинки разликуваат големи и мали букви, па користете комбинација од големи и мали букви, бројки и специјални знаци, како $, # и &.
5. Лозинките потешко се пробиваат доколку имаат повеќе знаци, па затоа подолгите лозинки се подобри од пократките. Силен напад лесно може да пробие лозинка со седум или со помалку знаци. Силата на лозинката може да се провери

[1] Прилагодено од: http://www.privacyrights.org/ar/alertstrongpasswords.htm

на некои интернет страници, како на пример:

www.microsoft.com/protect/yourself/password/checker.mspx

6. За полесно да ја запомните лозинката, направете ја да биде од првите букви на зборовите во некоја реченица, фраза или име на песна! Внимавајте да додадете бројки и/или посебни знаци.
7. Направете посебни лозинки за различни профили и апликации! Ако ви пробијат една лозинка, другите профили нема да ви бидат изложени на ризик. Не користете иста или варијации од иста лозинка за различни апликации.
8. Размислете за сигурен систем за помнење на лозинките! Критики за нив може да најдете на: http://lifehacker.com/5042616/five-best-password-managers.
9. Ако веќе имате слаба лозинка, променете ја!

Членот 11(3) ја нагласува важноста на различните кориснички имиња за пристап до информацискиот систем и разни апликации – воопшто не е безбедно да се има исто корисничко име за различни намени. Членот 11(4) бара автоматска одјава по извесен неактивен период, не подолг од 15 минути. Автоматското одјавување (политика на чист монитор) може да се воведе со чувар на екранот (screensaver) или преку самата апликација, преку систем за управување со идентитетот или преку самиот информациски систем. Треба да се напомене дека во некои случаи автоматското одјавување по 15 минути може да предизвика оперативни проблеми (помислете на работно место во службата за итни случаи), но секое отстапување од овој принцип треба да биде можно единствено ако тоа е навистина неопходно за вршење на работните задачи.

Совет за малите контролори

Корисниците треба да знаат дека обичното одјавување е добра практика кога се напушта работното место или канцеларијата и дека тоа се прави лесно со CTRL+ALT+DEL и ENTER (или WIN key+L).

И ограничувањето на бројот на неуспешни обиди за најава во системот е добра сигурносна практика (како PIN броеви за банкомати). Контролорите би требало да воведат процедура која уредува кому треба да му се обрати корисникот ако има премногу неуспешни обиди за најава.

Мерките против спајвер и вируси се клучни во современата информатичка заштита, но тие треба постојано да се ажурираат

за да понудат ефективна заштита од сигурносните закани, како што се бара во членот 11(7). Истото важи и за заштитата од спамови.

Членот 11(9) уредува дека контролорот треба да воведе непрекинато снабдување со струја (UPS), кое ќе биде секундарен механизам во случај на прекин на снабдувањето со струја (на пример, поради невреме). Тоа е честа сигурносна мерка и е основна кај поголемите контролори, особено кај контролорите со многу трансакции и барања за достапност на податоци (на пример, банките). Помалите контролори (малите и средните претпријатија) веројатно ќе треба да инвестираат во поекономични решенија за UPS. Иако тоа не се спомнува во членот 11, процедурите за спасување и планирањето за непрекинато работење исто така се препорачуваат за поголемите контролори и за контролорите кои обработуваат многу чувствителни лични податоци.

ОРГАНИЗАЦИСКИ МЕРКИ

Член 12

(1) Контролорот треба да обезбеди соодветни организациски мерки за тајност и заштита на обработката на личните податоци и тоа:

1. **ограничен пристап или идентификација за пристап до личните податоци;**
2. **организациски правила за пристап на корисниците до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори;**
3. **уништување на документи по истекот на рокот за нивно чување;**
4. **мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци и**
5. **почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци.**

(2) Вработеното лице кое ги врши работите за човечки ресурси кај контролорот, го известува администраторот на информацискиот систем за вработувањето или ангажирањето на секој корисник со право на пристап до информацискиот систем, за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето за да му бидат избришани корисничкото име и лозинката, односно заклучени за натамошен пристап.

(3) Известувањето од ставот (2) на овој член се врши и при било кои други промени во работниот статус или статусот на ангажирањето на корисникот што има влијание врз нивото на дозволениот пристап до информацискиот систем.

Членот 12 се фокусира на организациските мерки што треба да ги придружуваат техничките мерки за сигурност на личните податоци.

Пред сè, пристапот до личните податоци треба да биде ограничен и да се следи. Кога добиваат пристап до личните податоци во просториите на контролорите, лицата кои не се вработени кај контролорите секогаш треба да бидат придружени од вработен. Контролорот треба да постави јасни правила за соодветна употреба на интернетот и да ја забрани употребата на штетни или нелегални интернет страници или друга несоодветна активност на интернет. Со оглед на сè поголемата важност да се задржи извесно ниво на приватност на работното место, се препорачува да се постават јасни правила за тоа во која мера канцелариската опрема (компјутер, мобилни телефони, пристап до интернет итн.) може да се користи за приватни цели. Работодавачите би требало да се воздржат од политиките на опширна контрола на вработените со обработка на нивните лични податоци (на пример, следење на нивните активности на интернет). Организациските мерки треба да ја дефинираат процедурата за уништување на документите по истекот на периодот за чување (на пример, задолжителна употреба на машини за сечење хартија за хартиени документи кои содржат лични податоци). Посебно внимание треба да се посвети на контролата на физичкиот пристап, која може да вклучува чувари, магнетни картички, видеонадзор или други методи на контрола на физичкиот пристап кои, секако, треба да се воведат во согласност со соодветните правни одредби и оценката на ризикот. Корисниците треба да се предупредат да ги следат техничките насоки за инсталација и користење на информатичката опрема за обработка на личните податоци.

Контролорот треба да ја пропише процедурата со која се даваат/укинуваат корисничките права. Правилникот уредува дека процедурата би требало да ги вклучува шефот на Одделението за човечки ресурси и администраторот за информатика.

Совеѿ за малиѿе конѿролори

Малите контролори кои немаат такви (посебни) одделенија за човечки ресурси или информатика треба, во најмала рака, да го поделат *давањеѿо* кориснички привилегии од *извршувањеѿо* кај различни лица. Давањето/укинувањето на корисничките права треба да се ажурира и да ги следи промените во работниот статус (на пример, ако некој вработен

го смени работното место во фирмата, неговите кориснички права треба соодветно да се променат). Не треба да се нагласува дека доделувањето кориснички права треба да одговара на задачите што ги вршат вработените (на претставникот за продажба, на пример, не му треба пристап до личните досиеја што ги води Одделението за човечки ресурси).

ФИЗИЧКА СИГУРНОСТ НА ИНФОРМАЦИСКИОТ СИСТЕМ

Член 13

(1) Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, треба да се физички лоцирани, хостирани и администрирани од страна на контролорот.

(2) Физички пристап до просторијата во која се сместени серверите може да имаат само овластени лица од контролорот.

(3) Доколку е потребен пристап на друго лице до просторијата и личните податоци зачувани на серверите, тогаш тоа лице треба да биде придружувано и надгледувано од овластено лице од ставот (2) на овој член.

(4) Просторијата во која се сместени серверите се заштитува од ризиците во опкружувањето преку примени на мерки и контроли со кои се намалува ризикот од потенцијални закани вклучувајќи кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

Членот 13 може да се покаже како тежок за спроведување за некои контролори кои не одат на хостирање на интернет и сервер, што е доста честа појава. Членот 13(1) треба да се толкува на тој начин што во секој случај просториите со сервери треба добро да се заштитат, без оглед на тоа дали се наоѓаат во просториите на контролорот или не. Ако контролорот реши да ја даде оваа функција под договор, тогаш тој е одговорен неговиот договорен партнер исто така да ги применува мерките за физичка безбедност на своите простории со сервери. Пристапот до просториите со сервери треба строго да се ограничи и да се следи (секое влегување во просториите со сервери треба да се запишува, и тоа со име и презиме на лицата кои влегуваат, датумот, времето и причината за влегувањето). Слично како и во членот 12, на лицата кои не се вработени кај контролорот (на пример, лицата кои се задолжени за одржување на клима-уредите или друг персонал за одржување) треба да им се дозволи влез во просториите со сервери единствено во придружба на вработен и треба да бидат под надзор во секој момент додека се во просториите со сервери. Просториите со сервери треба добро да се заштитат и од природни ризици, на пример од топлина, поплава, пожар и др., наведени во членот 13(4). Секогаш е важно сигурносните мерки да се приспособат на новите хардверски инсталации (сервери итн.) кои можеби бараат поинтензивен систем за ладење.

ИНФОРМИРАЊЕ ЗА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 14

(1) Лицата кои се вработуваат или се ангажираат кај контролорот, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

(2) За лицата кои се ангажираат за извршување на работа кај контролорот во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(3) Контролорот пред непосредното започнување со работа на корисниците, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.

(4) Лицата кои се вработуваат или се ангажираат кај контролорот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

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

(6) Изјавата од ставот (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кај контролорот.

Членот 14 е еден од најважните зашто техничките и организациските сигурносни мерки можат да бидат ефективни единствено ако корисниците се свесни за своите обврски и одговорности за заштитата на личните податоци. Не е толку незамислива ситуацијата, корисниците кај контролорот да мислат дека доколку имаат (официјален) пристап до личните податоци, имаат дозвола за сè. Корисниците треба да знаат дека дури и пристапот или увидот во податоци бара правна основа –љубопитност или правење услуги за други не се дозволени.

Затоа, сите вработени треба да се запознаат со одредбите од ЗЗЛП и тие треба да бидат дел од нивните договори со работодавачот. Во зависност од неговите задачи и одговорности, контролорот треба дополнително да ги информира за воведените сигурносни мерки за податоците и за сите други важни одговорности. Администраторите за информатика, на пример, кои обично имаат многу широк пристап до огромен обем лични податоци, треба да добијат мошне јасни упатства и обука за рамките на нивните права и случаите кога може да ги прекршат одредбите од ЗЗЛП. Вработените кои обработуваат лични податоци треба да потпишат изјава дека ќе ги почитуваат прописите за заштита на личните податоци, дека ќе ги следат упатствата на контролорот за обработка на личните податоци и дека ќе ја чуваат тајноста на личните податоци, освен ако не е поинаку уредено со закон. Таа изјава се чува во личното досие на вработениот.

Проактивниот пристап за информирање на корисниците за одговорностите подразбира и обука за социјално инженерско планирање (препознавање и одбрана од такви напади).

ОБВРСКИ И ОДГОВОРНОСТИ НА КОРИСНИЦИТЕ

Член 15

(1) Обврските и одговорностите на секој корисник кој има пристап до личните податоци и до информацискиот систем, контролорот ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на корисниците при користење на документите и информатичко комуникациската опрема.

(2) Контролорот задолжително ги информира корисниците од ставот (1) на овој член со документацијата за технички и организациски мерки кои се однесуваат на извршувањето на нивните обврски и одговорности.

Како што е уредено во членот 10, контролорот треба да ги дефинира обврските и одговорностите на корисниците кои имаат пристап до личните податоци. Корисниците треба добро да се информираат за техничките и организациските мерки релевантни за нивната позиција кај контролорот.

Иако членот 15(1) се однесува на „секој" корисник, одговорностите и обврските можат да се утврдат и за групи корисници, под услов тие да имаат исти или многу слични задачи и одговорности (на пример, група вработени во Одделението за човечки ресурси, додека нивниот шеф може да има построги одговорности, во согласност со неговите задачи). Корисниците во Одделението за човечки ресурси, на пример, треба да бидат свесни за воведените технички и организациски мерки кои ги штитат тајноста и сигурноста на личните податоци содржани во досиејата на вработените, како и другите лични податоци што се обработуваат во нивното одделение.

ЕВИДЕНТИРАЊЕ НА ИНЦИДЕНТИ

Член 16 **Во Правилата за пријавување, реакција и санирање на инциденти, контролорот го определува начинот на евидентирање на секој инцидент, времето кога се појавил, корисникот кој го пријавил, на кого е пријавен и мерките кои се преземени за негово санирање.**

Членот 16 бара подготовка на т.н. процедури за управување со инциденти. Контролорот треба да пропише процедура како да се реагира при појава на инцидент со кој се загрозени личните податоци. Тоа може да се направи, на пример, преку електронска пошта до посебни електронски адреси за таа цел. Треба да се назначи лице кое ќе биде одговорно за известување, кое ќе ги документира инцидентите и ќе решава за мерките што треба да се преземат за да се ограничат ефектите или да се спречи друга таква појава или инцидент. Прецизната евиденција на утврдените инциденти е од особено значење за успешно справување со инцидентите во иднина.

Совет за малите контролори

Еден од вработените треба да биде специјално обучен за заштита на лични податоци и треба да биде одговорен за управување со инциденти. Одберете вработен со доволно знаење, мотивација и, пред сè, со чувство за одговорност и посветеност.

ИДЕНТИФИКАЦИЈА И ПРОВЕРКА

Член 17

(1) Контролорот задолжително води евиденција за корисниците кои имаат авторизиран пристап до документите и информацискиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

(2) Кога проверката се врши врз основа на корисничко име и лозинка, контролорот секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите.

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

За контролорот е од исклучителна важност да овозможи подоцнежно утврдување кога се внесени индивидуалните лични податоци во збирката, кога се користеле или поинаку се обработиле и кој го сторил тоа. Контролорот треба да ги чува т.н. траги за следење, кои овозможуваат со личните податоци да се утврдат корисникот и неговите активности. Со цел да се спречи злоупотребата на личните податоци, од суштинско значење е контролорот:

1. да знае кој има пристап до личните податоци (права на пристап), и
2. да знае точно кој пристапил до кои податоци и кога (траги за следење или записи).

Ако контролорот има воведено само права на пристапување, но не и траги за следење, нема да може да се утврди дали личните податоци се користеле со несоодветна причина и кој е одговорен за тоа.

Совет за малите контролори

Најголем дел од збирките на податоци кај малите контролори се во обични формати, како Excel, Word, Access или други слични слободни формати (како Open Office.org). Повеќето од овие канцелариски апликации нудат пристојни траги за следење, што им овозможуваат на контролорите да видат кога е внесен некој личен податок во збирката, кога е изменет или избришан. Тие записи можеби не го регистрираат секој пристап до податоците (на пример, пристап без измени), но се регистрира секоја измена, ажурирање или бришење на податоците. Регистрирањето може да се вклучи со опциите за следење на промените и заштита на документите во вообичаените софтвери за канцелариско работење (види пример подолу). Примерот покажува кој ја извел која операција на личните податоци, а следењето на промените може да се заштити со лозинки, за да се спречат подоцнежни промени.

Дијаграм 2: Траги за следење во обичен софтвер за табели

File Edit View Insert Format Tools Data Window IDC Help

Calibri 10

K32

	A	B	C	D	E	F	G	H	I
1	Action Number	Date	Time	Who	Change	Sheet	Range	New Value	Old Value
2	1	23.9.2009	11:50	secretary	Cell Change	customer database	B2	<blank>	9121929
3	2	23.9.2009	11:50	secretary	Cell Change	customer database	A4	<blank>	3345938
4	3	23.9.2009	11:50	secretary	Cell Change	customer database	A7	<blank>	2354132
5	4	23.9.2009	14:50	John	Cell Change	customer database	B8	<blank>	3454317
6	5	23.9.2009	15:50	John	Row Auto-Insert	customer database	21:21		
7	6	23.9.2009	16:50	John	Cell Change	customer database	B21	naslov20	<blank>
8	7	23.9.2009	17:50	John	Cell Change	customer database	A21	2000	<blank>
9	8	23.9.2009	18:50	Mark	Cell Change	mailing database	C11	mail1@con.org	<blank>
10	9	23.9.2009	19:03	Mark	Cell Change	mailing database	C8	mail_382@igoo.com	<blank>
11	10	23.9.2009	19:03	Mark	Cell Change	mailing database	C4	ana.hus@gmail.com	<blank>
12	11	23.9.2009	19:03	Mark	Cell Change	mailing database	B4	tsan@hotmail.com	<blank>
13	12	23.9.2009	19:03	Mark	Cell Change	mailing database	B8	ivo@fmail.com	<blank>
14	13	23.9.2009	19:03	Mark	Cell Change	mailing database	B11	natasa.76@mscom	<blank>
15	14	23.9.2009	19:03	Mark	Cell Change	mailing database	B14	no e-mail	joe@company.net
16	15	23.9.2009	19:47	Enes	Cell Change	mailing database	B16	no e-mail	ftc@gov.uk
17	16	23.9.2009	19:47	Enes	Row Auto-Insert	mailing database	B19		
18	17	23.9.2009	19:47	Enes	Cell Change	mailing database	B21	no e-mail	maria@olin.net
19	18	23.9.2009	19:47	Enes	Cell Change	mailing database	C21	no e-mail	ester.noe@coop.org
20									
21	The history ends with the changes saved on 23.9.2009 at 19:47.								

КОНТРОЛА НА ПРИСТАПОТ

Член 18

(1) Корисниците задолжително имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи.

(2) Контролорот воспоставува механизми за да се оневозможи пристап на корисниците до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.

(3) Во евиденцијата на корисниците утврдена во член 17 став (1) на овој правилник се внесуваат и нивоата на авторизиран пристап за секој корисник.

(4) Администраторот на информацискиот систем кој е овластен со Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци може да доделува, менува или да го одзема авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна на контролорот.

Корисниците кои обработуваат лични податоци треба да имаат пристап единствено до оние лични податоци што им се неопходни за вршење на работните задачи. Во информатичкиот систем треба да има механизми кои управуваат со корисничките права и на тој начин спречуваат да дојде до злоупотреба на корисничките права. Доделувањето на корисничките права би требало да се врши според природата на работата на корисникот. На пример, сметководителот во болница не треба да има пристап до медицинските досиеја на пациентите. Секако, многу е важно да имате информатички администратори кои уживаат потполна доверба од контролорот и се сосема свесни дека вообичаено имаат многу широки права на пристап поради природата на нивната работа. Контролорот, сепак, треба да ги ограничи произволните активности на информатичките администратори, во поглед на управувањето со корисничките права – информатичките администратори треба да ги следат упатствата на контролорот, а не да дејствуваат на своја рака.

УПРАВУВАЊЕ СО МЕДИУМИ

Член 19

(1) Со медиумите треба да се овозможи идентификација и евидентирање на категориите на лични податоци и истите треба да се чуваат на локација до која пристап имаат само овластените корисници утврдени во Актот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

(2) Пренесувањето на медиумите надвор од работните простории се врши само со претходно писмено овластување од страна на контролорот.

Контролорот треба да има попис на статичните и мобилните медиуми што содржат идентификација на категориите податоци зачувани на нив. И самите медиуми и информациите за категориите на податоците зачувани на нив треба да се заштитат од неовластен пристап, намерно или ненамерно губење или оштетување. Кога медиумите се пренесуваат надвор од просториите на контролорот, за тоа е потребно претходно писмено овластување од контролорот. Контролорот треба да внимава на сигурноста на медиумите во текот на преносот. На пример, доколку се пренесуваат на преносливи медиуми (USB, CD/DVD, итн.), личните податоци треба да се заштитат со лозинка или да се криптираат за да се спречи неовластен пристап до нив. Малите преносливи медиуми лесно се губат, а во денешно време може да содржат огромни количества лични податоци, па затоа заштитата со лозинка или криптирање (во зависност од чувствителноста на податоците) е многу важна сигурносна мерка.

Совет за малите контролори

На интернет има некои бесплатни алатки за заштита со лозинка и криптирање. Видете ги, на пример следниве:

- http://passwordsafe.sourceforge.net/
- http://www.truecrypt.org/.

Овие алатки можат да се користат за да се заштитат преносливите медиуми, како, на пример, криптирање на целото USB.

УНИШТУВАЊЕ, БРИШЕЊЕ ИЛИ ЧИСТЕЊЕ НА МЕДИУМОТ

Член 20

(1) По пренесувањето на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот треба да се уништи, избрише или да се исчисти од личните податоци снимени на него.

(2) Уништувањето на медиумот се врши со механичко разделување на неговите составни делови, при што истиот повторно да не може да биде употреблив.

(3) Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените лични податоци.

(4) За случаите од ставовите (2) и (3) на овој член се составува записник, кој ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци снимени на истиот.

Медиумите кои содржат лични податоци треба соодветно да се бришат или да се уништат со цел да се спречи подоцнежно извлекување на личните податоци од медиумите. Чест проблем е и несигурната заштита, затоа што хард-дисковите не се уништуваат или бришат соодветно, па неовластени лица можат да ги извлечат податоците што биле зачувани на тие дискови. Честа е заблудата кај корисниците дека бришењето на документите или форматирањето на хард-дискот засекогаш ги брише податоците од дисковите. Бришењето податоци зачувани на хард-дисковите треба да се изведе на тој начин што врз дисковите неколкупати се испишуваат неодредени низи нули и единици. Стандардот на Министерството за одбрана на САД (DoD, 522.22M), на пример, пропишува седумкратно испишување врз податоците.

Доколку податоците не можат да се избришат (на пример, од непроменливи медиуми), за да се спречи да дојде до реконструк-

ција на податоците медиумите треба физички да се уништат. Има повеќе фирми кои нудат сигурно уништување на медиумите со документирана постапка и записник од уништувањето, кои се обврзни според членот 20(4) од Правилникот. Записникот треба да содржи информации за медиумот (на пример, сериски број, тип, големина) и информации за категориите лични податоци што се уништиле.

СИГУРНОСНИ КОПИИ И ПОВТОРНО ВРАЌАЊЕ НА ЗАЧУВАНИТЕ ЛИЧНИ ПОДАТОЦИ

Член 21

(1) Контролорот е одговорен за проверка на примената на Правилата за начинот на правење на сигурносна копија, архивирање и чување, како и за повторното враќање на зачуваните лични податоци.

(2) Во Правилата од ставот (1) на овој член, задолжително треба да се содржани постапките за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

(3) Сигурносни копии задолжително се прават секој работен ден, на крајот од работната седмица и секој последен работен ден во месецот.

Поединците чиишто лични податоци – намерно или ненамерно – се уништени или загубени, можат да претрпат сериозни последици, додека контролорот, од друга страна, може да се соочи со сериозни штети во облик на губење на довербата или пропаѓање на бизнисот, како и казни за непридржување до ЗЗЛП. Замислете си што би се случило, на пример, кога една болница би ги изгубила податоците за пациентите, кога една банка би ги изгубила регистрите со податоци или кога тоа би ѝ се случило на некоја мала фирма, која во целост зависи од лични податоци (на пример, маркетиншки центар за повици). Затоа, сигурносните копии на личните податоци или медиумите кои содржат лични податоци се многу важни и процедурите треба беспрекорно да се опишат во споменатиот план за непрекинато работење (види во членот 10). Политиката, меѓу другото, треба да содржи и опис на:

- зачестеноста на изработката на сигурносните копии (според членот 21(4));
- местото каде што се чуваат сигурносните копии;
- процедурата како се изработуваат сигурносните копии и

како се пренесуваат до местото на чување, и

- мерките и процедурите што се преземаат во случај на губење на оригиналните податоци (процедура за враќање на податоците).

Совет за малите контролори

Користете преносливи медиуми за еднократно снимање (на пример CD-R и DVD-R медиуми) и криптирајте ја содржината со бесплатен софтвер. Не заборавајте да ги чувате сигурносните копии на друга локација и обезбедени од можни манипулации или други опасности, како пожари или поплави. Се препорачува да инвестирате во огноотпорен шкаф. И не заборавајте редовно да правите сигурносни копии!

НАЧИН НА ЧУВАЊЕ НА СИГУРНОСНИТЕ КОПИИ

Член 22

(1) Сигурносните копии се чуваат во просторија која се наоѓа надвор од објектот во кој е сместен информацискиот систем.

(2) Сигурносните копии треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

Секогаш чувајте ги сигурносните копии на локација што се разликува од локацијата на оригиналните податоци. Несреќен случај, како пожар или поплава, може да ги уништи и оригиналните и сигурносните податоци, доколку се сместени на истото место. Сигурносните копии треба да се чуваат на сигурна локација (на пример, во заклучен огноотпорен шкаф). Податоците со основно ниво на заштита не мора да се чуваат на друга локација (надвор од објектот на контролорот), нешто што се бара за техничките и организациските мерки од средно и од високо ниво.

Покрај физичката заштита, во членот 22(2) се бара криптографски да се заштитат и сигурносните копии. Поголемите контролори веројатно веќе имаат воведено сигурносен софтвер со криптографска заштита.

Совет за малите контролори

Малите контролори ќе треба да се потпрат на други решенија. Truecrypt[2] е пример на бесплатен софтвер за криптографска заштита, кој може ефикасно да се користи на сигурносните копии, како и другите медиуми што содржат лични податоци.

[2] www.truecrypt.org

СРЕДНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

ДОПОЛНИТЕЛНИ ПРАВИЛА ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 23

Во документацијата за технички и организациски мерки утврдена во член 10 од овој правилник, задолжително треба да се содржани постапките за овластување на одговорно лице за заштита на личните податоци, за вршење периодични контроли, заради следење на усогласеноста на работењето на контролорот со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки, како и за мерките кои треба да се преземат при користење на медиумите.

Средното ниво на технички и организациски мерки бара повисок степен на заштита на податоците, што може да се постигне со назначување одговорно лице за заштита и тајност на личните податоци. Институтот Одговорно лице за заштита на личните податоци/ Одговорно лице за усогласеност (Chief Data Protection Officer/Chief Compliance Officer) се покажал како функционален во некои други земји (на пример, во Германија[3], Обединетото Кралство[4] и во Белгија[5]). Затоа, членот 23 го предвидува условот процедурата за назначување на такво одговорно лице да ја пропишува контролорот во документацијата уредена со членот 10 од Правилникот. Одговорното

[3] Bundesdatenschutzgesetz (BDSG), 15.11. 2006, see Article 4(f) (Сојузен закон за заштита на податоци од 15.11.2006 година, види член 4 (f))

[4] Data Protection Act 1998 (Закон за заштита на податоци од 1998 г.)

[5] Belgian Law on the protection of privacy in relation to the processing of personal data (Belgian Official Journal, 18.03.1993) (Белгиски закон за заштита на приватноста при обработката на лични податоци (белгиски Службен весник од 18.3.1993 година)

лице за заштита на податоците/ Одговорното лице за усогласеност треба да биде лице од доверба, по можност со комбинација од правни и технички знаења, а се препорачува и ревизорско искуство. Одредбите треба да ја покријат и периодичната проверка на обработката на личните податоци од страна на контролорот, во однос на тоа дали се придржува до условите од ЗЗЛП и Правилникот.

ОДГОВОРНО ЛИЦЕ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 24 **Контролорот задолжително овластува едно или повеќе лица за заштита на личните податоци кои ќе бидат одговорни за координација и контрола на постапките и упатствата утврдени во документацијата за техничките и организациските мерки.**

Контролорот има обврска да назначи и да овласти едно или повеќе лица кои ќе бидат одговорни за координација и контрола на процедурите и одредбите утврдени во документацијата за техничките и организациските мерки. За да ги постигне очекуваните резултати, институтот Одговорно лице за заштита на личните податоци/ Одговорно лице за усогласеност треба да ја ужива довербата на контролорот, но и да има можност да се заштити во однос на другите вработени и самиот контролор. Не е невообичаено одговорните лица за заштита на податоците да рапортираат со наодите за утврдените инциденти и прекршоци, а токму тоа е причината зошто им е потребна целосна поддршка од страна на управата.

КОНТРОЛА НА ИНФОРМАЦИСКИОТ СИСТЕМ И НА ИНФОРМАТИЧКАТА ИНФРАСТРУКТУРА

Член 25

(1) Информацискиот систем и информатичката инфраструктура на контролорот задолжително подлежат на внатрешна и надворешна контрола со цел да се провери дали постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци.

(2) Контролорот врши надворешна контрола на информацискиот систем и информатичката инфраструктура на секои три години, а внатрешна контрола секоја година.

(3) Надворешната контрола од став (1) на овој член се врши преку обработка на документи од страна на независно трето лице.

(4) Во извештајот од извршената контрола од ставот (1) на овој член задолжително треба да има мислење за тоа во колкава мера постапките и упатствата содржани во документацијата за технички и организациски мерки се применуваат и се во согласност со прописите за заштита на личните податоци, да се наведени констатираните недостатоци, како и предложените неопходни корективни или дополнителни мерки за нивно отстранување.

(5) Во извештајот од ставот (4) на овој член треба да се содржани и податоците и фактите врз основа на кои е изготвено мислењето и се предложени мерките за отстранување на констатираните недостатоци.

(6) Извештајот од ставот (4) на овој член се анализира од страна на одговорното лице за заштита на личните податоци, кој доставува предлози

на контролорот за преземање на потребните корективни или дополнителни мерки, за отстранување на констатираните недостатоци.

(7) Извештајот од ставот (4) на овој член треба да биде достапен за увид на Дирекцијата за заштита на личните податоци.

Членот 25(1) пропишува дека контролорот подлежи на внатрешна и надворешна контрола, за да се утврди дали се придржува до техничките и организациските мерки. Контролата се врши на информацискиот систем и на информатичката инфраструктура на контролорот. Внатрешна контрола се врши еднаш годишно, додека надворешна контрола се врши еднаш на три години. Внатрешната контрола може да ја врши соодветниот кадар на контролорот, додека надворешната контрола треба да им се довери на независни организации кои се специјализирани за контрола. Резултат од надворешната контрола е извештај со наодите од ревизорите, како и препораки за потребните корективни мерки за воочените недостатоци или за воведување на мерките кои недостигале. Податоците и фактите од контролата кои ја сочинуваат основата за мислењето на ревизорот и за препораките треба да се прикажат во извештајот од контролата. Одговорното лице (Одговорно лице за заштита на личните податоци/ Одговорно лице за усогласеност) е задолжено да ги анализира наодите од извештајот и да му предложи на контролорот дополнителни или корективни мерки за да се отстранат утврдените грешки и недостатоци. Последниот став од членот 25 уредува дека ревизорскиот извештај треба да ѝ биде достапен на Дирекцијата за заштита на личните податоци. На тој начин инспекциските постапки на Дирекцијата за заштита на личните податоци ќе бидат поефикасни и побрзи.

Многу е важно контролорите обврските од овој член да не ги гледаат како пречка, туку како можност да си ги проверат процедурите и системите и да ги прифатат внатрешната и, што е уште поважно, надворешната контрола како корисно средство и помош. Затоа, контролорот треба да им помогне на внатрешните и на надворешните ревизори и да им ги даде сите неопходни информации. Не се препорачува ревизорите да прикриваат податоци и факти зашто тоа ќе доведе до понеквалитетни извештаи, кои на крај ќе резултираат со кршење на актот за заштита на податоците.

ИДЕНТИФИКАЦИЈА И ПРОВЕРКА

Член 26 **Контролорот треба да воспостави механизми кои ќе овозможуваат јасна идентификација на секој корисник кој пристапил до информацискиот систем и можност за проверка на авторизацијата за секој корисник.**

Со цел да се обезбеди заштита и тајност на личните податоци, треба да се воведат соодветни процедури за да се овозможи следење на обработката на личните податоци. Контролорот треба да ги чува т.н. траги за следење, кои овозможуваат идентификација на корисникот и на неговите активности со личните податоци. Со цел да се лоцира злоупотребата на личните податоци, од суштинско значење е контролорот да знае:

1. кој има пристап до личните податоци (право на пристап), и
2. кој точно пристапил, до кои податоци и кога (траги за следење или записи).

Ако контролорот има воведено само права на пристапување, но не и траги за следење, нема да може да се утврди дали личните податоци се користеле со несоодветна причина и кој е одговорен за тоа.

Пример

За да се утврди дали некој полицаец ги злоупотребил правата и дали ги проверил името и адресата на некоја жена што ја запрел или само му правел услуга на некој пријател, полицијата треба да води евиденција за пристапот до личните податоци содржани во регистарот на возила. Ако полицаецот немал легитимна причина да ги провери тие лични податоци (на пример, формална процедура), трагата за следење ќе овозможи подоцнежна истрага и откривање дали личните податоци се користеле за некоја друга намена. Друг пример е медиумите да дојдат до многу чувствителни податоци за некоја медицинска институција. Ако нема права на пристап и процедури за записи, нема да биде можно да се најде лицето кое им ги открило информациите на медиумите.

Контролорите кои обработуваат големи количества лични податоци или обработуваат чувствителни лични податоци треба да воведат многу строги записнички политики. Записите треба да ги содржат барем следниве податоци: до кои лични податоци или до која група лични податоци е пристапено, кој го сторил тоа и кога. Контролорите треба да се погрижат за следново:

- да не може да се исклучи регистрирањето;
- записите да не може да се менуваат или да се бришат.

Тоа може да се обезбеди преку т.н. принцип на четири очи (пристапот е дозволен единствено за две или повеќе лица истовремено), преку поделба на задачите и правата на пристап (за да се спречи системските администратори да ги менуваат записите) или со технички мерки (на пример, зачувување на записите на непроменливи медиуми, на пример на CD/DVD дискови за еднократно впишување).

ЕВИДЕНТИРАЊЕ НА АВТОРИЗИРАНИОТ ПРИСТАП

Член 27

(1) Контролорот води евиденција за секој авторизиран пристап која треба да ги содржи особено следните податоци: име и презиме на корисникот, работна станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

(2) Во евиденцијата од ставот (1) на овој член се внесуваат и податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.

(3) Операциите кои овозможуваат евидентирање на податоците од ставовите (1) и (2) на овој член треба да бидат контролирани од страна на одговорното лице за заштита на личните податоци и истите не може да се деактивираат.

(4) Евиденцијата од ставот (1) на овој член се чува најмалку десет години.

(5) Одговорното лице за заштита на личните податоци врши периодична проверка на податоците од ставовите (1) и (2) на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Трагите за следење што се водат во информацискиот систем треба да ги содржат следниве податоци:

- име и презиме на корисникот;
- работно место од кое лицето влегло во информацискиот систем;
- датум и време на пристапот;
- лични податоци до кои се пристапило;
- вид пристап и обработка на лични податоци;
- евиденција на авторизацијата на секој пристап, и
- евиденција на секој неавторизиран пристап и евиденција на автоматското одбивање од информацискиот систем.

Во однос на видот на пристапот, треба да биде јасно дека тоа се однесува на преземените дејства од страна на корисниците (на пример, додавање, бришење, ажурирање, внесување или други активности со податоци). Ставот 1, исто така, бара да се евидентира секој пристап, што е многу важна мерка при утврдувањето дали дошло до злоупотреба на личните податоци. Информацискиот систем на контролорот треба да ги евидентира и обидите за неавторизиран пристап во информацискиот систем и автоматските одбивања од него. Контролорот треба да води и евиденција за обидите за неавторизиран пристап.

Трагите за следење треба да ги контролира одговорното лице за заштита на податоците (Одговорно лице за заштита на личните податоци/Одговорно лице за усогласеност) и тие не треба да се исклучуваат. Трагите за следење од ставот 1 треба да се чуваат десет години.

Одговорното лице за заштита на личните податоци/Одговорното лице за усогласеност треба да ги контролира трагите за следење најмалку еднаш месечно и да изготвува извештај за своите активности и наоди.

КОНТРОЛА НА ФИЗИЧКИ ПРИСТАП

Член 28 **Во документацијата за технички и организациски мерки, контролорот треба да определи критериуми за корисниците кои можат да имаат пристап до просториите каде е сместен информацискиот систем.**

Контролорите треба да ги утврдат критериумите за пристап до информацискиот систем (просториите со сервери). Најчесто тоа им се дозволува на лица од Секторот/Одделението за информатика, иако често нема потреба сите од Секторот/Одделението за информатика да имаат пристап до просториите со сервери (пристапот треба да се ограничи и во рамките на самиот Сектор/Одделение за информатика). Сите вработени во Одделението за информатика не вршат задачи за кои е потребен физички пристап до просториите со сервери. Процедурата за влез во просториите со сервери треба да вклучува и регистар каде што се запишува секој пристап. Информациите во регистарот треба да ги содржат името на лицето/лицата, датумот и времето на влезот, причината за влез и потпис од лицето. На лицата кои не се вработени кај контролорот треба да им се дозволи пристап до просториите со сервери единствено ако ги придружува вработен кај контролорот и ако нивните задачи бараат пристап до просториите со сервери (на пример, инсталација на нов хардвер, клима-уреди и слично).

УПРАВУВАЊЕ СО МЕДИУМИ

Член 29

(1) Контролорот треба да воспостави систем за евидентирање на медиумите кои се примаат со цел да овозможи директна или индиректна идентификација на видот на медиумот кој е примен, датум и време на примање, испраќач, број на медиуми кои се примени, вид на документ кој е снимен на медиумот, начин на испраќање на медиумот, име и презиме на лицето овластено за прием на медиумот.

(2) Одредбите од ставот (1) на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на контролорот.

(3) За пренесените медиуми надвор од работните простории на контролорот, треба да бидат преземени неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Членот 29 уредува дека контролорот треба да води евиденција за работењето со медиумите, вклучително и податоци за директна или индиректна идентификација на типот на применените медиуми, датумот и времето на прием, испраќачот, серискиот број на медиумите, видот на документите запишани на медиумите и името и презимето на овластеното лице за прием на медиуми. Истото би требало да важи и за медиумите што ги праќаат контролорите. Како што е дадено погоре (види насоки за членот 19), медиумите што содржат лични податоци и се пренесуваат надвор од просториите на контролорот треба да се заштитат. Контролорот треба да внимава на сигурноста на медиумите во текот на преносот доколку, на пример, личните податоци се пренесуваат на преносливи медиуми (USB, CD/DVD итн.). Личните податоци треба да се заштитат со лозинка или да се криптираат за да се спречи неовластен пристап до нив.

ЕВИДЕНТИРАЊЕ НА ИНЦИДЕНТИ

Член 30

(1) Во Правилата за пријавување, реакција и санирање на инциденти, контролорот ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на корисниците кои ги извршиле операциите за повторно враќање на личните податоци, категориите на личните податоци кои се вратени и кои биле рачно внесени при враќањето.

(2) За повторно враќање на личните податоци, контролорот издава писмено овластување на корисниците за да ги извршат операциите за враќање на податоците.

Членот 16 бара подготовка на т.н. процедури за управување со инциденти. Контролорот треба да пропише процедура како да се реагира при појава на инцидент со кој се загрозени личните податоци. Прецизната евиденција на утврдените инциденти е од особено значење за успешно справување со инцидентите во иднина. Покрај обврските уредени во член 16, член 30 уредува дека процедурите за враќање податоци ги пропишува контролорот. Тие треба да вклучуваат евиденција за тоа кој ги вратил податоците и кои категории лични податоци се вратени. Враќањето на личните податоци треба да се врши единствено со писмено овластување за корисниците кои имаат средства да ги вратат податоците.

СИГУРНОСНИ КОПИИ

Член 31 **Сигурносните копии задолжително треба да бидат чувани на друга оддалечена локација од местото каде е сместен информацискиот систем и истата треба да биде обезбедена со соодветни технички и организациски мерки согласно документацијата за технички и организациски мерки.**

Основното ниво на технички и организациски мерки бара сигурносните копии да се чуваат на безбедно место (на пример, во заклучен огноотпорен шкаф). Сепак, за средното ниво на технички и организациски мерки треба да се чуваат сигурносни копии на друга (втора) локација, различна од првата локација на контролорот. Втората сигурносна локација треба да ги има поставено истите технички и организациски мерки како и првата. Тие мерки се вообичаени за средините каде што се обработуваат големи количества важни податоци и вообичаено влегуваат во доменот на Центрите за спасување од катастрофи или Планирањето за непрекинато работење. Сигурносните податоци или се праќаат до Центрите за спасување од катастрофи по електронски пат, преку посебни линии, за да се спречи неовластен пристап, или, пак, се пренесуваат по сигурен пат (на пример, периодично се пренесуваат преку официјални курирски служби). Секундарни сигурносни центри најчесто имаат банките или другите фирми специјализирани за сефови итн.

ТЕСТИРАЊЕ НА ИНФОРМАЦИСКИОТ СИСТЕМ

Член 32

(1) Контролорот задолжително врши тестирање на информацискиот систем пред неговото имплементирање или по извршените промени со цел да се провери дали системот обезбедува тајност и заштита на обработката на личните податоци согласно со документацијата за технички и организациски мерки и прописите за заштита на личните податоци.

(2) Тестирањето од став (1) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци од страна на независно трето лице.

Членот 32 бара контролорот да го тестира информацискиот систем пред да го пушти во употреба или пред да воведе значителни промени во работењето со системот (т.н. управување со промени). Во вториот случај може да се работи за нова апликација или за нов хардвер (на пример, нов сервер), со кои значително се менува опфатот на работењето на информацискиот систем. Таквите тестови се важни зашто новиот софтвер и хардвер носат промени во системот кои можат да донесат и нови начини за напад или експлоатација на системот што би довеле до злоупотреба или губење на личните податоци.

Членот 32(2) уредува дека фазите на тестирање треба да се извршат со пробни податоци, а не со вистински лични податоци, и дека тестирањето треба да го изврши независно трето лице. Тоа би можело да претставува сериозна обврска за повеќето контролори зашто може да вклучува надворешни информатички ревизори способни за такви задачи.

IV. ВИСОКО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

СЕРТИФИКАЦИОНИ ПОСТАПКИ

Член 33 **Контролорот може да применува и други технички мерки за тајноста и заштита на обработката на личните податоци, преку примена на сертификациони постапки согласно прописите за податоците во електронски облик и електронски потпис.**

Членот 33 уредува дека контролорот може да користи други технички и организациски мерки за тајност и заштита на личните податоци, но тие процедури треба да ги следат прописите за електронски податоци и електронски потпис.

Сигурноста и доверливоста на електронските податоци може да се обезбеди преку употребата на дигитални сертификати и т.н. инфраструктура на јавен клуч (Public Key Infrastructure - PKI) за управување со дигитални сертификати. Дигиталните сертификати се засноваат на криптографија на јавен клуч, шема којашто користи парови од јавен и приватен клуч. Приватниот клуч го знае само сопственикот и тој се користи за да се создаде дигитален потпис. Корисникот треба во секое време да го чува тој клуч во тајност. Јавниот клуч е нашироко познат и се користи за проверка на дигиталниот потпис. PKI е шема што ги поврзува јавните клучеви со соодветниот кориснички идентитет преку тело за сертификација. Дигиталниот сертификат издаден од телото за сертификација може да се употреби за да се идентификува јавно или приватно лице на интернет страници и може да понуди авторизиран пристап до приватни и заштитени информации. Електронската комуникација може да се потпише и заштити со читач на електронска пошта компатибилен со S/MIME (Secure/Multipurpose

Internet Mail Extensions). Контролорите можат да користат електронски потпишани документи со дигитални сертификати издадени од овластените тела за сертификација во Македонија (на пример, „Македонски телекомуникации" и „КИБС"). Повеќе информации за PKI и за дигиталните сертификати може да најдете на интернет страниците на горенаведените тела за сертификација:

- „Македонски телекомуникации" - http://www.telekom.mk/mk/
- КИБС - http://ca.kibs.com.mk/defaulten.aspx

Таму ќе најдете информации за тоа како да добиете дигитален сертификат, каде и како да го користите, кои се техничките услови за неговата употреба, како и други корисни информации.

ПРЕНЕСУВАЊЕ НА МЕДИУМИ

Член 34 **Медиумите можат да се пренесуваат надвор од работните простории само ако личните податоци се криптирани или ако се заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи, при што само администраторот на информацискиот систем може да ги декриптира или лице овластено од него.**

Пренесувањето медиуми надвор од просториите на контролорот е дозволено само ако податоците се пренесуваат на начин на кој не можат да се читаат. Тоа се постигнува со соодветни методи за криптирање што дозволуваат единствено овластен персонал, како информатичкиот администратор, да ги декриптираат податоците до читлив облик. Криптирањето податоци може да се врши на преносliв медиум, како USB или хард-дискови, каде што се криптира целиот медиум, но и на начин каде што податоците се криптираат пред да се снимат на преносliв медиум (види насоки за членот 19 со примери за корисен софтвер).

ПРЕНЕСУВАЊЕ НА ЛИЧНИТЕ ПОДАТОЦИ ПРЕКУ ТЕЛЕКОМУНИКАЦИСКА МРЕЖА

Член 35

Личните податоци можат да се пренесуваат преку телекомуникациска мрежа само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

Ако податоците се пренесуваат преку интернет, треба да се користат сигурни протоколи. Еден од тие протоколи е HTTPS, кој е комбинација од HTTP и криптографски протокол. HTTPS врските често се користат за платежни трансакции на интернет и за чувствителни трансакции во корпоративните информациски системи. Сигурни протоколи треба да се користат и ако податоците се разменуваат преку електронска пошта. На пример, протоколот SMTPS за сигурна размена на електронска пошта, но и други решенија како PGP (Pretty Good Privacy). Други методи за заштита на преносот на лични податоци преку телекомуникациски мрежи се дигиталните сертификати засновани на PKI – за повеќе информации видете ги насоките за членот 33.

Совет за малите контролори

Ако во вашата дејност треба да пренесувате лични податоци преку телекомуникациски мрежи, се препорачува да побарате соодветни решенија кои ќе ги задоволат условите од Правилникот со разумна инвестиција. Сигурниот пренос на податоци преку електронска пошта се постигнува, на пример, со решенија што функционираат со OpenPGP. Голем број даватели на услуги за електронска пошта обезбедуваат заштита усогласена со OpenPGP. Повеќе информации може да најдете на следнава адреса:

http://en.wikipedia.org/wiki/Pretty_Good_Privacy#OpenPGP.

Ако имате намера да пренесувате лични податоци преку интернет со HTTP, погрижете се да користите протокол TLS (SSL) или решенија за виртуелна приватна мрежа (VPN).

V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

ПРЕСТАНУВАЊЕ НА ВАЖЕЊЕ

Член 36 **Со денот на отпочнувањето на примената на овој правилник престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија" бр. 111/05).**

ВЛЕГУВАЊЕ ВО СИЛА

Член 37 **Овој правилник влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Македонија", а ќе се применува од 1 јуни 2009 година.**