20151614615

АГЕНЦИЈА ЗА СУПЕРВИЗИЈА НА КАПИТАЛНО ФИНАНСИРАНО ПЕНЗИСКО ОСИГУРУВАЊЕ

Врз основа на член 23 став (4) и член 52 од Законот за заштита на личните податоци („Службен весник на Република Македонија“ бр.7/05 и 103/08, 124/10 и 135/11), Советот на експерти на Агенцијата за супервизија на капитално финансирано пензиско осигурување на седницата, одржана на 21.4.2015 година, го донесе следниот

ПРАВИЛНИК ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Општи одредби

Член 1

Со овој правилник се пропишуваат техничките и организациските мерки кои ги применува Агенцијата за супервизија на капитално финансирано пензиско осигурување (во понатамошниот текст: Агенцијата) заради обезбедување на тајност и заштита на обработката на личните податоци.

Обработката на личните податоци може да биде:

а) целосно и делумно автоматизирана обработка на личните податоци и

б) друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

„Авторизиран пристап“ е овластување, доделено на овластеното лице за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории на Агенцијата.

„Инцидент“ е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци.

„Лозинка“ е доверлива информација составена од множество на карактери кои се користат за проверка на овластеното лице и операторот.

„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.

„Проверка“ е постапка за верификација на идентитетот на овластеното лице на информацискиот систем.

„Сигурносна копија“ е копија на личните податоци, содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторно враќање.

„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, кои се чувааат во информацискиот систем на Агенцијата.

„Овластено лице” е лице, вработено или ангажирано во Агенцијата, кое има авторизиран пристап до личните податоци кои се чуваат во информацискиот систем на Агенцијата, документите и до информатичко комуникациската опрема.

„Оператор" е овластено физичко лице, вработено или ангажирано кај надворешните субјекти кое има пристап до личните податоци кои се добиваат преку информацискиот систем на Агенцијата,документите и до информатичко комуникациската опрема.

„Офицер за заштита на лични податоци" е овластено лице вработено во Агенцијата кое врши работи поврзани со заштита на личните податоци со кои располага Агенцијата, согласно Законот за заштита на личните податоци.

„Информациски систем на Агенцијата"е целокупниот информациски систем на Агенцијата составен од персонални компјутери, сервер на база на податоци, апликациски сервер,сервер за чување на податоци, интернет портал и останати апликации и опрема кои се користат за обработка на податоци.

„Информатичка инфраструктура" е целата информатичко комуникациска опрема на Агенцијата, во рамките на која се собираат, обработуваат и чуваат личните податоци.

„Интернет портал" е дел од информацискиот систем на Агенцијата кој овозможува ограничен пристап на овластеното лице и оператор преку web форма до податоците за кои е овластен да ги обработува.

„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 електронско комуникациска мрежа.

Член 3

Агенцијата 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.

Техничките и организациските мерки од ставот 1 на овој член се класифицираат во три нивоа:

а) основно;

б) средно и

в) високо.

Член 4

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

За документите кои содржат лични податоци што се однесуваат на: кривични дела, изречени санкции и мерки од контрола, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно и средно ниво.

За документи кои содржат: посебни категории на лични податоци и лични податоци кои се однесуваат на членовите на пензиските фондови, задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

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

За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на лични податоци и/или матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.

Основно ниво на технички и организациски мерки

Член 5

Основното ниво на техничките и организациските мерки ги опфаќа следните видови на заштита: документација за технички и организациски мерки, обезбедување на технички мерки за тајност и заштита на личните податоци, обезбедување на организациски мерки за

тајност и заштита на личните податоци, информирање за заштита на личните податоци, физичка сигурност на информацискиот систем, идентификација и проверка на пристапот на интернет порталот, организациски мерки за заштита на личните податоци при автоматизираната обработка на податоците, контрола на пристап, правило „чисто биро“ и чување и уништување на документи.

Во рамките на основното ниво на техничките и организациските мерки Агенцијата пропишува правила за определување на обврски и одговорности на администраторот на информацискиот систем и на овластените лица и правила за евидентирање на инциденти.

Член 6

Агенцијата задолжително донесува и применува документација за технички и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем.

Член 7

Пристапот до документите треба биде ограничен само за овластени лица на Агенцијата.

За пристапувањето до документите задолжително треба да се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

Член 8

Агенцијата треба да обезбеди технички мерки за тајност и заштита на личните податоци, кои се чуваат во информацискиот систем, при пристапот на интернет порталот од страна на овластеното лице и тоа:

а) Креирање на единствено корисничко име за секое овластено лице на интернет порталот на Агенцијата;

б) Лозинка креирана од овластеното лице, составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;

в) Автоматска промена на лозинките на секои три месеци;

г) Ограничен пристап за секое корисничко име и лозинка до одредени делови од информацискиот систем;

д) Воспоставување на автоматизирано одјавување од системот по изминување на одреден период на неактивност (не подолго од 15 минути) и повторно впишување на корисничкото име и лозинката при активирање на системот;

ѓ) Автоматизирано отфрлање од информацискиот систем по три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на овластеното лице дека треба да побара инструкција од администраторот на информацискиот систем (во натамошниот текст: администратор;

е) Воспоставување на ефективна и сигурна антивирусна заштита и анти–спајвер заштита, на информацискиот системот, со постојано набљудување и ажурирање заради превентива од непознати и непланирани закани од нови вируси и спајвери;

ж) 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;

з) Ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и

ѕ) Приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Мерките од став 1 на овој член ги спроведува администраторот и врши нивна периодична проверка.

Вработениот кој е задолжен за управување со човечките ресурси во Агенцијата треба да го известува администраторот за почеток на вработување или ангажирање на овластено лице со право на пристап до информацискиот систем, со цел да биде доделено ново корисничко име и лозинка. При престанок на вработувањето или ангажирањето корисничкото име и лозинката се бришат.

Известувањето од став 3 на овој член се врши и при било кои други промени во работниот или статусниот дел на ангажирањето на овластеното лице што има влијание врз нивото или обемот на дозволениот пристап до збирката на личните податоци.

Член 9

Агенцијата треба да обезбеди технички мерки за тајност и заштита на личните податоци, кои се чуваат во информацискиот систем на Агенцијата, при пристапот на интернет порталот од страна на надворешните субјекти (пензиски друштва, Фондот на пензиското и инвалидското осигурување на Македонија и чуварите на имот на пензиските фондови) и тоа:

а) Креирање на единствено корисничко име;

б) Лозинка креирана од секој оператор на интернет порталот. Лозинката е составена од комбинација на најмалку осум алфанумерички карактери (од кои минимум една голема буква) и специјални знаци;

в) Автоматска промена на лозинките на секои три месеци;

г) Ограничен пристап за секое корисничко име и лозинка до одредени делови од информацискиот систем;

д) Воспоставување на автоматизирано одјавување од системот по изминување на одреден период на неактивност (не подолго од 15 минути) и повторно впишување на корисничкото име и лозинката при активирање на системот;

ѓ) Автоматизирано отфрлање од информацискиот систем по три неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на операторот дека треба да побара инструкција од администраторот;

е) Воспоставување на ефективна и сигурна антивирусна заштита и анти–спајвер заштита на информацискиот систем, со постојано набљудување и ажурирање заради превентива од непознати и непланирани закани од нови вируси и спајвери;

ж) 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;

з) Ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови и

ѕ) Приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

Мерките од став 1 на овој член ги спроведува администраторот и врши нивна периодична проверка во информацискиот систем на Агенцијата.

Надворешниот субјект треба да ја известува Агенцијата за промена на операторот со цел да биде доделено ново корисничко име и лозинка. Претходното корисничко име и лозинка се бришат.

Известувањето од став 3 на овој член се врши и при било кои други промени на операторот што имаат влијание врз нивото или обемот на дозволениот пристап до личните податоци добиени преку информацискиот систем на Агенцијата.

Член 10

Агенцијата треба да обезбеди организациски мерки за заштита на личните податоци во поглед на информирањето на вработените, физичката заштита на работните простории и опремата и заштита на информацискиот систем во целина, вклучувајќи го и преносот на личните податоци.

Член 11

Агенцијата треба да ги запознае надворешните субјекти од член 9 став 1 на овој правилник со значењето и мерките за заштита на личните податоци и да потпише договори со субјектите во кои тие ќе се обврзат на заштита на личните податоци до коишто пристапуваат или ги обработуваат, користејќи го информацискиот систем на Агенцијата.

Член 12

Агенцијата треба да обезбеди физичка сигурност на информацискиот систем. Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, треба да се физички лоцирани, хостирани и администрирани од страна на Агенцијата.

Физички пристап до просторијата во која се сместени серверите може да имаат само лица посебно овластени од Агенцијата.

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 лицето од ставот 3 на овој член.

Просторијата во која се сместени серверите се заштитува од ризиците воопкружувањето 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.

По исклучок од ставот 1 на овој член, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на Агенцијата.

Во случајот од ставот 5 на овој член, меѓусебните права и обврски на Агенцијата и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, треба да бидат уредени со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.

Член 13

Претседателот на Советот на експерти на Агенцијата определува офицер за заштита на личните податоци кој ги врши следниве работи:

а) учествува во донесувањето на одлуки поврзани со обработката на личните податоци, како и со остварувањето на правата на субјектите на личните податоци;

б) ја следи усогласеноста на работењето на Агенцијата со прописите кои се однесуваат на обработката на личните податоци, со овој правилник и со документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;

в) ги изработува внатрешните прописи за заштита на личните податоци и документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;

г) ја координира контролата на постапките и упатствата утврдени во овој правилник и во документацијата за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;

д) предлага обука на вработените во врска со заштитата на личните податоци и

ѓ) врши други работи утврдени со закон и со овој правилник.

Член 14

Агенцијата треба да обезбеди организациски мерки за заштита на личните податоци при автоматизираната обработка на податоците, која вклучува читање или обработка на лични податоци, и тоа:

а) Почитување на целосна доверливост и сигурност на лозинките и на останатите форми на идентификација за пристап до информацискиот систем кој содржи лични податоци;

б) Електронско уништување на документи кои содржат лични податоци по истекување на рокот за чување;

в) Изнесувањето на медиум кој е носител на лични податоци (компакт диск, дискета, преносliв компјутер и други медиуми за пренос на податоци), надвор од работните простории да биде со посебна дозвола и контрола за да не дојде до нивно губење или незаконско користење;

г) Воспоставување физичка сигурност на работните простории и опремата каде што се чуваат и обработуваат личните податоци;

д) Почитување на процедурите за пристап до целокупниот информациски систем преку персоналните компјутери;

ѓ) Почитување на процедурите од корисничката документација за пристап до софтверската апликација; и

е) Почитување на процедурите од техничката документација за користење на софтверската апликација и информацискиот систем на Агенцијата кој содржи лични податоции.

Член 15

Агенцијата треба да обезбеди мерки за заштита на личните податоци при автоматизираната обработка, која вклучува читање или обработка на лични податоци, до кои пристапуваат надворешните субјекти (пензиските друштва, Фондот на пензиското и инвалидското осигурување на Македонија и чуварите на имот на пензиските фондови) и тоа:

а) Почитување на целосна доверливост и сигурност на лозинките и на останатите форми на идентификација, официјално издадени од Агенцијата за пристап до информацискиот систем кој содржи лични податоци;

б) Електронско уништување на документи кои содржат лични податоци по истекување на рокот за чување;

в) Изнесувањето на медиум кој е носител на лични податоци (компакт диск, дискета, преносliв компјутер и други медиуми за пренос на податоци), надвор од работните простории да биде со посебна дозвола и контрола за да не дојде до нивно губење или незаконско користење;

г) Обезбедување физичка сигурност на работните простории и опремата каде што се чуваат и обработуваат личните податоци; и

д) Почитување на кориснички упатства за користење на софтверска апликација преку која се пристапува до информацискиот систем на Агенцијата кој што во себе содржи лични податоци и начинот на преземање на личните податоци од истиот.

Член 16

Лицата кои се вработуваат во Агенцијата, пред нивното започнување со користење на информатичкиот систем на Агенцијата треба да се запознаат со процедурите за заштита на личните податоци.

Во договорите со лицата коишто се ангажираат за извршување на работа во Агенцијата треба да се наведат обврските и одговорностите за заштита на личните податоци.

Пред непосредното започнување со работа, на овластеното лице, поврзана со пристап или обработка на личните податоци, Агенцијата дополнително го информира за непосредните обврски за заштита на личните податоци.

Секој вработен или ангажиран во Агенцијата потпишува изјава во која е наведено дека е запознат со процедурите за заштита на личните податоци.

Член 17

Пристапот до документите треба биде ограничен само за овластени лица на Агенцијата.

За пристапувањето до документите задолжително треба да се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

Доколку е потребен пристап на друго лице до документите тогаш треба да бидат воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Член 18

Агенцијата задолжително го применува правилото „чисто биро“ при обработката на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Член 19

Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.

Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот 1 на овој член, Агенцијата треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.

Ако документите не се чуваат заштитени на начин определен во ставовите 1 и 2 на овој член, тогаш Агенцијата треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Член 20

Уништувањето на документите се врши со ситнење или на друг начин, при што истите повторно да не можат да бидат употребливи.

Во случајот од ставот 1 на овој член комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на личните податоци содржани во истиот.

Средно ниво на технички и организациски мерки

Член 21

Средното ниво на техничките и организациските мерки ги опфаќа следните видови на заштита: дополнителни правила за контрола во документацијата за технички и организациски мерки, обезбедување контрола на информацискиот систем и

информатичката инфраструктура на Агенцијата, обезбедување на идентификација и проверка на пристап до и информацискиот систем, евидентирање на авторизиран пристап, физичка сигурност на простории, начин на чување на документи сигурносни копии и тестирање на информацискиот систем.

Член 22

Во документацијата од член 6 на овој правилник Агенцијата пропишува постапки за вршење периодични контроли заради следење на усогласеноста на работењето на Аганцијата 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.

Член 23

Информацискиот систем и информатичката инфраструктура на Агенцијата 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.

Надворешната контрола од став 1 на овој член се врши од страна на независно правно лице на секои три години.

Внатрешната контрола од став 1 на овој член се врши еднаш годишно.

Овластените лица за извршените контроли од ставовите 2 и 3 на овој член изготвуваат извештај во кој 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 констатираат недостатоците и да се предложат неопходни мерки за нивно отстранување.

Извештајот заедно со предлог мерките се доставува до претседателот на Советот на експерти на Агенцијата.

Одредбите за контрола од овој член соодветно се применуваат и на применуваат и при друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

Член 24

Информацискиот систем на Агенцијата е затворен според дефиницијата во Законот за податоците во електронски облик и електронски потпис. Дозволен е пристап само од локација на Агенцијата и од локациите (интернет адреси) на ограничен број надворешни субјекти.

Член 25

Агенцијата води електронска евиденција на овластени лица и оператори кои имаат авторизиран пристап на интернет порталот на информацискиот систем на Агенцијата и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

Агенцијата води електронска евиденција за авторизираниот пристап со следните податоци: име и презиме на овластеното лице или операторот, 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.

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 потребно ниво на авторизација.

Операциите кои овозможуваат евидентирање на податоците од ставовите 1 и 2 на овој член треба да бидат контролирани од страна на офицерот за заштита на лични податоци и администраторот и истите не може да се деактивираат.

Евиденцијата од ставот 1 на овој член се чува најмалку пет години.

Офицерот за заштита на лични податоци и администраторот на информацискиот систем вршат проверка на податоците од ставовите 1 и 2 на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Член 26

Плакарите (орманите), картотеките или другата опрема за чување на документи задолжително треба да бидат сместени во простории заклучени со соодветни заштитни механизми. Просториите треба да бидат заклучени и за периодот кога документите не се обработуваат од овластените лица.

Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот 1 на овој член, Агенцијата треба да примени други мерки за да се спречи секој неовластен пристап до документите.

Член 27

Агенцијата треба да врши редовно снимање на сигурносна копија и архивирање на податоците во системот, за да не дојде до нивно губење или уништување.

Сигурносни копии задолжително се прават секој работен ден и на крајот од работната седмица, а по потреба и секој последен работен ден во месецот.

Сигурносните копии задолжително се прават на начин со кој ќе се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

Сигурносните копии кои се чуваат на друга оддалечена локација од местото каде е сместен информатичкиот систем треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

Офицерот за заштита на лични податоци и администраторот вршат проверка на спроведување на мерките од овој член.

Член 28

Агенцијата 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.

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

Високо ниво на технички и организациски мерки

Член 29

Високо ниво на техничките и организациските мерки ги опфаќа следните видови на мерки на заштита: криптирано пренесување на документи, копирање или умножувањето на документи по претходно овластување и заштита при физички пренос на документите.

Член 30

Агенцијата треба да обезбеди заштита на личните податоци при нивната размена со надворешните субјекти преку медиуми и електронска комуникациска мрежа, овозможувајќи криптирана врска за размена, строги правила за идентификација при размената (лозинки тешки за пробивање) и електронско потпишување на документите за размена. Криптираните документи може да ги декриптира само администраторот или лице овластено од него.

Мерките за заштита од став 1 на овој член Агенцијата може да ги пренесе и на надворешните субјекти со потпишување на договор.

Член 31

Копирањето или умножувањето на документи кои содржат лични податоци може да се врши единствено со претходно писмено овластување од страна на претседателот на Советот на експерти на Агенцијата.

Уништувањето на копиите или умножените документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

Член 32

Во случај на физички пренос на документите Агенцијата задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои се пренесуваат.

Преодни и завршни одредби

Член 33

Со овој правилник престанува до важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ бр. 74/2010).

Член 34

Овој правилник влегува во сила наредниот ден од денот на објавување во „Службен весник на Република Македонија“.

Бр. 01-528/9
27 април 2015 година
Скопје

Претседател
на Советот на експерти,
д-р **Булент Дервиши**, с.р.