Согласно член 10 од Правилникот за техничките и организациските мерки за обезбедување на тајност и заштита на обработката на личните податоци („Сл. Весник на РМ“ бр. 38/2009, 158/10) и член 55 од Правилникот за внатрешните односи и работењето на Филозофскиот факултет во Скопје во состав на Универзитетот „Св. Кирил и Методиј“- Скопје, Деканатската управа на својата XII редовна седница, одржана на 18. XII 2014 година, донесе

ПРАВИЛНИК
за технички и организациски мерки за обезбедување на тајност и заштита на обработката на личните податоци

Член 1

Со овој правилник се пропишуваат техничките и организациските мерки што ги превзема Филозофскот факултет во Скопје (во натамошкиот текст „Контролорот“) како Конторолор и ги променува за обезбедување на тајност и заштита при обработката на личните податоци.

Вработените кај Контролорот, чии работни обврски налагаат обработка на личните податоци, должни се да постапуваат согласно Законот за заштита на личните податоци („Сл. Весник на РМ“ бр. 07/05 и 103/08).

Член 2

Терминте кои се употребуваат во овој правилник го имаат следново значење:

„Администратор на информацискиот систем“ е лице кое ги планира и применува техничките и организациски мерки за обезбедување тајност и заштита при обработката на личните податоци, како и контрола во текот на овој процес.

„Авторизиран пристап“ е овластување кое му се доделува на лицето кое обработува лични податоци, при користењето на определена информатичка и комуникациска опрема или за пристап до определени работни простории на контролорот.

„Документ“ е секој запис кој содржи лични податоци и истиот може да биде во електронска или хартиена форма, кој се чува на медиум и во информатичко комуникациска опрема која се користи за обработка на податоците, кој се доставува преку пошта или се пренесува преку електронско комуникациска мрежа.

„Корисник“ е физичко лице, вработено или ангажирано кај Контролорот кое има авторизиран пристап до документите и до информатичко комуникациската опрема.

Член 3

Техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци кои Контролорот ги применува се класифицираат во две нивоа:

- основно и
- средно.

На сите документи кои содржат лични податоци задолжително се применуваат технички и организациски мерки класифицирани на основно ниво.

ОСНОВНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 4

Контролорот врши електронска обработка на личните податоци од информацискиот систем со примена на истиот за обработка на личните податоци и тоа на документи во електронска форма (word, excel, PDF или со примена на друга апликативна алатка).

Под информациски систем се подразбира збир од персонални компјутери, сервери, печатари и преносни медиуми како и програмски алатки, како поддршка на информацискиот систем со што се обезбедува тајност и заштита при обработката на личните податоци.

Начинот и постапката на нивното користење е:

1. единствено корисничко име на ниво на оперативен систем;
2. лозинка креирана од секој корисник, која е сочинета со комбинација од најмалку 8 (осум) алфа нумерички карактери (од кои најмалку една голема буква) и специјални знаци;
3. корисничкото име и лозинката му обезбедуваат на корисникот пристап до информацискиот систем во целина, како и до поединечните апликации и/или поединечните збирки на лични податоци потребни за извршување на неговите работни задачи;
4. автоматизирана промена на лозинката по изминат утврден временски период што не е подолг од три месеци;
5. автоматизирано одјавување од информацискиот систем по изминување на определен неактивен период (не подолго од 15 минути), по што за повторно активирање потребно е одново впишување на корисничкото име и лозинката;
6. Инсталирана заштитна мрежна бариера (“firewall”) 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. задолжително користење на ефективна и сигурна анти-вирусна и анти-спајвер заштита на информацискиот систем и постојано ажурирање на истата;
8. ефективна и сигурна анти-спам заштита, која ќе се ажурира;
9. правење на резервна копија на документите со лични податоци во електронска форма;

Во случаите од став 3 точка 5 од овој член, администраторот на информацискиот систем ќе го верификува продолжувањето на пристапот до системот.

Во случај на инцидент, пристап до информацискиот систем има овластениот сервисер задолжен за одржување и сервисирање на информатичкиот систем (во понатамошниот текст „овластениот сервисер“) исклучително во присуство на администраторот на информацискиот систем.

Документите во хартиена форма се чуваат во ормани, физички заштитени и до нив пристап имаат само лица со одобрение од Контролорот.

Корисникот кој ги врши работите за човечки ресурси кај Контролорот ќе го известува администраторот на информацискиот систем, за вработувањето или ангажирањето по друга основа на секој Корисник со право на пристап до информацискиот систем, заради доделување на корисничко име и лозинка, како и во случај на престанок на вработувањето, заради бришење на корисничкото име и лозинка, односно исклучување за натамошен пристап. Соодветно известување ќе се врши и при било кои други промени во работниот или во статусот на ангажирањето на Корисникот, доколку таквите промени имаат влијание врз нивото или обемот на дозволениот пристап до збирките на лични податоци преку информацискиот систем.

Член 5

Контролорот обезбедува организациски мерки за тајност и заштита при обработката на личните податоци, во поглед на информирањето на вработените, физичката заштита на работните простории и опремата и заштита на информацискиот систем како целина, вклучувајќи го и преносот на податоците,

За Администратор на информацискиот систем, се определува еден од вработените од страна на деканот на Факултетот.

Член 6

Контролорот при автоматизираната обработка на личните податоци ги обезбедува пропишаните организациски мерки за заштита на обработката на личните податоци, кои се состојат во:

1. ограничен прстап, односно идентификација на пристап до личните податоци, преку целосна доверливост и сигурност на лозинките и на останатите форми на идентификација;
2. воспоставување и примена на организациски правила за пристап на Корисниците до интернет, кои се однесуваат на симнување и снимање на документи превземени од електронската пошта и други извори;
3. уништување на документи кои содржат лични податоци по истекување на рокот на нивно чување, со примена на правила утврдени со документација за технички и организациски мерки;
4. издавање на посебно овласување и контрола од страна на Администраторот на информацискиот систем при секое изнесување на било кој медиум кој е носител на лични податоци (компакт диск, преносliв хард диск и други медиуми за пренос на податоци) надвор од работните простории, со цел да не дојде до нивно губење или незаконско користење;
5. воспоставување и примена на мерки за физичка сигурност на работните простории и информатичко-комуникациската опрема каде што се собираат, чуваат и обработуваат личните податоци;
6. почитување на техничките упатства при инсталирање и користење на информатичко-комуникациската опрема на која се обработуваат лични податоци.

Член 7

Лицата кои ќе се вработат кај Контролорот, пред нивното отпочнување со работа ќе се запознаат со прописите за заштита на личните податоци, како и со сите акти, односно документација донесена од страна на Контролорот заради примена на технички и оганизациони мерки.

Вработените кај Контролорот и лицата кои се ангажираат кај Контролорот за извршување на работа кај Контролорот, склучуваат договор за вработување, односно ангажирање, кој договор задолжително содржи одредби за обврските и одговорностите на овие лица во насока на заштита на личните податоци.

Контролорот, непосредно пред започнувањето со работа на корисниците поврзана со обработка на лични податоци, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.

Лицата кои се вработуваат или се ангажираат кај Контролорот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита при обработката на личните податоци. Оваа изјава особено содржи клаузула 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. Овие изјави задолжително се чуваат во досијеата на лицата кои се вработуваат или ангажираат кај контролорот.

Изјавата за тајност предвидена во предходниот став од овој член се потпишува според образец пропишан од страна на Контролорот, кој образец претставува составен дел на овој Правилник.

Доколку се појави потреба било кое трето физичко или правно лице, неспоменато во овој правилник да дојде во контакт со лични податоци, предмет на обработка од страна на Контролорот, третото лице предходно задолжително ќе потпишува изјава во форма и на начин како е предвидено во предходниот став на овој член.

Во насока на обезбедување тајност и заштита на обработката на личните податоци овластениот сервисер, склучува договор со Контролорот, во кој договор се регулираат обврските и одговорностите на овластениот сервисер како правно лице и вработените кај овластениот сервисер како физички лица, а во поглед на примената на правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Сл. Весник на РМ“ бр. 38/09, 158/10), и документацијата за технички и организациски мерки за обезбедување тајност и заштита при обработката на личните податоци усвоена од Контролорот.

Член 8

Со посебна документација за технички и организациски мерки, што ја донесува Контролорот, се уредуваат:

- правила за определување на обврските и одговорностите на администраторот на информацискиот систем и овластените лица 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.

Оваа документација заедно со овој Правилник соодветно се применуваат од страна на Контролорот, неговите вработени и лицата кои Контролорот повремено или постојано ги ангажира за вршење на работи кај Контролорот.

Документацијата од став 1 на овој член Контролорот ја менува и дополнува веднаш штом ќе настанат промени во организациската поставеност на информацискиот систем.

МЕРКИ ЗА ФИЗИЧКА СИГУРНОСТ

Член 9

Контролорот воспоставува и применува мерки за физичка сигурност на информацискиот систем преку физичко обезбедување на работните простории и информатичко-комуникациската опрема каде што се собираат, чуваат и обработуваат личните податоци.

Заради обезбедување на физичка сигурност, серверите на кои се инсталирани софтверските програми за обработка на личните податоци, задолжително физички се лоцирани, хостирани и администрирани од страна на Контролорот.

Заради обезбедување физичка сигурност, физички пристап до просторијата во која се сместени серверите може да имаат само лица кои од страна на Контролорот имаат добиено посмено овласување кое гласи на нивно лично име и во кое од страна на Контролорот е прецизирано својството на лицето на кое му се издава овласување за пристап и во кое се образложени причините, односно потребата за издавање на овластувањето за пристап на конкретното лице. Пристап до просториите каде е сместен информацискиот систем може да се допушти само на корисник кој ги задоволува следните критериуми:

- да е вработен кај Контролорот, со работни задачи на администратор на збирки на лични податоци или на асистент на администратор на збирки на лични податоци;
- да има потпишано изјава за тајност и заштита на обработка на лични податоци.

Заради обезбедување на физичка сигурност, доколку е потребен пристап на друго лице до просторијата каде личните податоци се чуваат на серверите, тогаш тоа лице задолжително ќе биде приддружувано и надгледувано од овластено лице кое е предвидено во предходниот став на овој член.

Заради обезбедување на физичка сигурност, Контролорот применува мерки за заштита на просторијата каде се сместени серверите и тоа заради заштита од ризиците од окружувањето и намалување на ризикот од потенцијални закани, односно намалување на ризикот од кражба, додека со инсталирање на соодветни апарати и аларми се врши заштита, односно намалување на ризикот од потенцијалните закани како што се: пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетско зрачење.

КОНТРОЛА НА АВТОРИЗИРАН ПРИСТАП

Член 10

Заради идентификација и проверка на авторизираниот пристап, 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.

Контролорот врши проверка на авторизираниот пристап преку кој се овозможува:

1. евидентирање на работната станица и корисничкото име на сите корисници кај Контролорот кога пристапуваат до базите на податоци, заедно со нивото на авторизиран пристап, времето и датумот на пристап, како и снимање на овие податоци;
2. идентификување на компјутерскиот систем од кој се врши надворешен обид за пристап во оперативните функции или податоци без потребно ниво на авторизација и генерирање извештај за секој чекор од неавторизираните пристапи и
3. изготвување на тековни извештаи за сите регистрирани промени (дополнувања, измени и бришења) направени во базите на лични податоци, заедно со корисничкото име, идентификацијата на работната станица од која е извршена промената како и времето и датумот на промената на лични податоци кон кои е пристапено, запис за авторизација за секое пристапување, запис за секој неавтризиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

Врз основа на механизмите наведени во предходните ставови на овој член, Контролорите во можност да врши идентификација и проверка на авторизираниот пристап, односно контрола на пристапот до личните податоци и информатичко-комуникациската опрема од страна на корисниците, со обезбеден постојан увид во моменталниот и минатиот пристап и превземени операции во базите на податоци од страна на сите овластени лица.

Врз основа на механизмите предвидени во овој член се овозможува секој од корисниците да има авторизиран пристап само до личните податоци и информатичко-комуникациската опрема кои се неопходни за извршување на нивните задачи, како и се овозможува пристап на корисниците до лични податоци и информатичко-комуникациска опрема со права различни од тие за кои се овластени корисниците.

При вршење на проверката, Контролорот се грижи за примена на воспоставените правила за заштита на доверливоста и интегритетот на лозинките при нивно пријавување, доделување и чување.

Администраторот на информатичкиот систем е овластен да го доделува, менува или да го одзема авторизираниот пристап до лични податоци и информациско-комуникациска опрема. При тоа како критериум за авторизиран пристап до лични податоци и информациско-комуникациска опрема, администраторот се раководи од работното место на секој од корисниците, од што зависи опсегот на пристап на секој од корисниците до личните податоци што е задолжен да ги обработува.

Член 11

Контролорот задолжително врши тестирање на информатичкиот систем пред неговото имплементирање или по извршените промени, со цел да се провери дали системот обезбедува тајност и заштита при обработката на лични податоци, согласно со документацијата за технички и организациски мерки и прописите за заштита на лични податоци. Ваквото тестирање се врши преку обработка на документи кои содржат имагинарни лични податоци од страна на независно трето лице.

СРЕДНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 12

Контролорот во секое време има овластено едно лице за заштита на лични податоци, кое е одговорно за координација и контрола на постапките и упатствата во документацијата за техничките и организациските мерки кои се применуваат за тајност и заштита при обработката на личните податоци (во понатамошниот текст „Офицер за заштита на личните податоци“).

Член 13

Информатичкиот систем и структура на Контролорот задолжително подлежат на внатрешна и надворешна контрола, со цел да се провери дали постапките и упатствата содржани во документацијата за техничките и организациските мерки се применуваат и се во согласност со прописите за заштита на личните податоци.

Контролорот врши надворешна контрола на информатичкиот систем и инфраструктура на секои три години, а внатрешна контрола секоја година.

Надворешна контрола се врши преку обработка на документи од страна на независно правно лице.

Во извештајот од извршената контрола задолжително треба да има мислење за тоа во колкава мера постапките и упатствата содржани во документацијата за техничките 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 и дополнителни мерки за нивно отстранување.

Во извештајот треба да се содржани и податоците и фактите врз основа на кои е изготвено мислењето и се предложени мерките за отстранување на констатираните недостатоци.

Извештајот се анализира од страна на Офицерот за заштита на личните податоци, кој доставува предлози на Контролорот за превземање на потребните корективни или дополнителни мерки за отстранување на констатираните недостатоци.

Извештајот треба да биде достапен за увид на Дирекцијата за заштита на лични податоци.

Член 14

Заради евидентирање на медиуми кои се примаат кај Контролорот од надвор, а со цел да се овозможи директна или индиректна идентификација на видот на медиумот, Контролорот води евиденција во електронски систем во кој се внесуваат следните податоци за секој медиум примен од надвор:

- датум и време на примање;
- испраќач;
- тип на медиум и број на примени медиуми;
- вид на документот кој е снимен на медиумот;
- начин на испраќање на медиумот; и
- име и презиме на лицето овластено за прием на медиумот.

Информатичкиот систем кај Контролорот располага со можност за дескремблирање/декриптирање на податоци содржани во медиуми кои кај Контролорот се примаат од надвор.

Системот опишан во предходниот став од овој член се воспоставува и подеднакво се применува и за евидентирање на медиуми кои се испраќаат од страна на Контролорот. Ваквите медиуми, пред изнесување односно пред испраќање од страна на Контролорот се предмет на посебни информатички мерки-скремблирање/криптирање, со што се обезбедува заштита од неовластено обработување на личните податоци што се снимени на ваквите медиуми.

Член 15

Овој Правилник влегува во сила со денот на донесувањето.

Д Е К А Н
на Филозофски факултет

Проф. Д-р Горан Ајдински

Изработил:м-р Катерина Пејкова