Врз основа на член 94 од Законот за високото образование (Сл. весник на РМ бр. 82/2018, Сл. весник на РСМ бр. 178/21 и Сл. весник на РСМ бр. 58/24), Законот за заштита на личните податоци (Сл. весник на РСМ 42/20 и Сл. весник на РСМ бр. 294/21) и член 23 од Статутот на Универзитет Американ Колеџ Скопје, Универзитетскиот сенат на Универзитет Американ Колеџ Скопје на својата 2-ра седница одржана на 5.2.2025 година го донесе следниот:

П Р А В И Л Н И К

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

со

ПРАВИЛА ЗА ОПРЕДЕЛУВАЊЕ НА ОБВРСКИТЕ И ОДГОВОРНОСТИТЕ НА АДМИНИСТРАТОРОТ НА ИНФОРМАЦИСКИОТ СИСТЕМ И НА ОВЛАСТЕНИТЕ ЛИЦА ПРИ КОРИСТЕЊЕ НА ДОКУМЕНТИТЕ И ИНФОРМАТИЧКО-КОМУНИКАЦИСКАТА ОПРЕМА

Член 1

Со овој Правилник се пропишуваат техничките и организациските мерки што Универзитет Американ Колеџ Скопје во својство на Контролор ги применува за обезбедување тајност и заштита на обработката на личните податоци.

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

„**Личен податок**" е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува, а лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на матичен број на граѓанинот или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, ментален, економски, културен или социјален идентитет;

„**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 комуникациска опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку телекомуникациска мрежа;

„**Обработка на личните податоци**" е секоја операција или збир на операции што се изведуваат врз лични податоци на автоматски или друг начин, како што е: собирање, евидентирање, организирање, чување, приспособување или промена, повлекување, консултирање, употреба, откривање преку пренесување, објавување или на друг начин правење достапни, изедначување, комбинирање, блокирање, бришење или уништување;

„Збирка на лични податоци" е структурирана група лични податоци која е достапна согласно со специфични критериуми, без оглед дали е централизирана, децентрализиран или распространета на функционална или географска основа.

„Субјект на лични податоци" е секое физичко лице на кое се однесуваат обработените податоци;

„Согласност на субјектот на лични податоци" е слободно и изречно дадена изјава на волја на субјектот на лични податоци со која се согласува со обработката на неговите лични податоци за однапред определени цели;

„Писмена согласност на субјектот на лични податоци" е потпишана согласност од страна на субјектот на личните податоци во форма на документ или одредба во договор;

„Контролор на збирка на лични податоци" е Универзитет Американ Колеџ Скопје како правно лице, кое самостојно ги утврдува целите и начинот на обработка на личните податоци (во натамошниот текст: Контролор). Кога целите и начинот на обработка на личните податоци се утврдени со закон или друг пропис, со истиот закон, односно пропис се определуваат контролорот или посебните критериуми за негово определување;

„Трето лице" е секое физичко или правно лице, орган на државната власт или друго тело, кое не е субјект на лични податоци, контролор, обработувач на збирка на лични податоци или лице кое под директно овластување на контролорот или обработувачот на збирка на лични податоци е овластено да ги обработува податоците;

„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 во информацискиот систем;

„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.

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

„Лозинка" е доверлива информација составена од множество на карактери кои се користат за проверка на овластеното лице;

„Проверка" е постапка за верификација на идентитетот на овластеното лице на информацискиот систем;

„Идентификација" е постапка за идентификување на овластеното лице на информацискиот систем;

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

„Информациски систем" е систем со кој може да се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да ги користи;

„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;

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

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

„Контрола на пристап" е операција за доделување на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на овластеното лице;

Член 3

Одредбите од овој правилник се применуваат за:

1. целосно и делумно автоматизирана обработка на личните податоци и

2. 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.

ОСНОВНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 4

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

Начинот и постапките на нивно користење се:

1. единствено корисничко име;
2. лозинка креирана од секој Корисник, која е сочинета 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 овластеното лице 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 спречување во рок од 30 минути за повторно најавување во системот;
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. инсталирана антивирусна програма, како ефективна и сигурна анти-вирусна и анти-спајвер заштита на информацискиот систем, која постојано се ажурира заради превентива од непознати и непланирани закани од нови вируси и спајвери;
8. ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови; и
9. правење на резервна копија на документите со лични податоци во електронска форма;
10. забрана за пренос на документи со лични податоци во електронска форма преку електронска пошта;
11. одобрување од Контролорот за користење на преносен медиум за пренос на документи со лични податоци надвор од работните простории.

Во случаите од став 1 точка 5 од овој член, Администраторот на информацискиот систем ќе го верификува продолжувањето на пристапот до системот.

Во случај на инцидент, пристап на информацискиот систем има овластениот сервисер задолжен за одржување и сервисирање на информатичкиот системот (во понатамошниот текст "Овластениот сервисер") исклучиво во присуство на Администраторот на информацискиот систем.

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

Член 5

Контролорот обезбедува организациски мерки за тајност и заштита на 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 Контролорот.

Обврските и одговорностите на администраторот на информацискиот систем, контролорот ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема.

Контролорот задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.

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 пристап, односно идентификација за 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 преземени од електронската пошта и други извори;
3. издавање на посебно овластување и контрола од страна на Администраторот на информацискиот систем при секое изнесување на било кој медиум кој е носител на лични податоци (компакт диск, дискета, преносliв компјутер и други медиуми за пренос на податоци) надвор од работните простории, со цел да не дојде до нивно губење или незаконско користење;
4. уништување на документи кои содржат лични податоци по истекување на рокот на нивно чување, со примена на правила утврдени со документацијата за технички и организациски мерки;
5. воспоставување и примена на мерки за физичка сигурност на работните простории и инфоматичко – 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 запознаваат со прописите за заштита на личните податоци, како и со сите акти, односно документација донесена од страна на Контролорот заради примена на технички и органзациски 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 пред непосредното започнување со работа на Корисниците поврзана со обработка на личните 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 на 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 претходниот 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, неспомнато во овој правилник, да дојде во контакт со лични податоци, предмет на обработка од страна на Контролорот, таквото лице претходно задолжително ќе потпишува изјава во форма и на начин како е предвидено во претходниот 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 Законот за заштита на личните податоци (Сл. весник на РСМ 42/20 и Сл. весник на РСМ бр. 294/21) и документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци усвоена од Контролорот.

МЕРКИ ЗА ФИЗИЧКА СИГУРНОСТ

Член 8

Контролорот воспоставува и применува мерки за физичка сигурност на информацискиот систем преку физичко обезбедување на работните простории и инфоматичко – 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 се физички лоцирани, хостирани и администрирани од страна на Контролорот.

Заради обезбедување на физичка сигурност, физички пристап до просторијата во која се сместени серверите може да имаат само лица кои од страна на Контролорот имаат издадено писмено овластување кое гласи на нивно лично име и во кое од страна на Контролорот е прецизирано својството на лицето на кое му се издава овластување за пристап и во кое се

образложени причините, односно потребата за издавањето на овластување 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 обработката на личните поадтоци;

Заради обезбедување на физичка сигурност, доколку е потребен пристап на друго лице до просторијата и личните податоци зачувани на серверите, тогаш тоа лице задолжително ќе биде придружувано и надгледувано од овластено лице како е предвидено во претходниот став од овој член.

Заради обезбедување на физичка сигурност, Контролорот применува мерки и контроли за заштита на просторијата во која се сместени серверите, и тоа заради заштита од ризиците од опкружувањето и намалување на ризикот од потенцијални закани, односно намалување на ризикот од кражба.

КОНТРОЛА НА АВТОРИЗИРАН ПРИСТАП

Член 9

Заради идентификација и проверка на авторизираниот пристап, Контролорот задолжително води евиденција за корисниците кои имаат авторизиран пристап до документите и информатичкиот 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 за 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 потребното 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 неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.
4. Криптирање на податоците при трансфер преку телекомуникациските врски (интернет врски, бежични врски или друг вид на врски) со соодветни софтверски и технички мерки.

Врз основа на механизмите наведени во претходните ставови од овој член, Контролорот е 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 преземени операции во базите на податоци од страна на сите овластени лица и се чува најмалку пет години.

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 оневозможува пристап на Корисниците до лични податоци и информатичко – комуникациската 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 личните податоци и информатичко – комуникациската опрема. Притоа, како критериум за авторизиран пристап до личните податоци и информатичко - комуникациската опрема, Администраторот се раководи од работното место на секој од Корисниците, од што зависи и опсег на пристап на секој од Корисниците до личните податоци што е задолжен да ги обработува.

Член 10

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 на обработката на личните податоци согласно со докуметнацијата за технички и организациски мерки и прописите за заштита на личните податоци. Ваквото тестирање се врши преку обработката на документи кои содржат имагинарни лични податоци од страна на независно трето лице.

Член 11

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.

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. И континуирано ја проверува функционалноста на сигурносните копии.

Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат и се физички и криптографски заштитени, заради оневозможување на каква било модификација.

СРЕДНО НИВО НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Член 12

Контролорот во секое време има овластено едно лице за заштита на личните 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 на обработката на личните податоци (во понатамошниот текст само "Одговорно лице за заштита на личните податоци„)

Член 13

Информатичкиот систем и информатичката 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 информатичката инфраструктура на секои три години, а внатрешна контрола секоја година.

Надворешната контрола се врши преку обработка на документи од страна независно трето 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 одговорното/офицерот лице за заштита на личните податоци, кој доставува предлози на Контролорот за преземање на потребните корективни или дополнителни мерки за отстранување на констатираните недостатоци.

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

Документите во хартиена форма, картотеки се чуваат во ормани физички заштитени и пристап до нив имаат само лица со овластување од Контролорот, и просториите се заклучени и за периодот кога документите не се обработуваат од овластени лица.

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 однадвор:

- 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 однадвор.

Системот опишан во претходниот 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.

Сигурносните копии се чуваат надвор од објектот во која се наоѓаат серверите или персоналните компјутери во кои се сместени збирките на лични податоци за кои се прави сигурносна копија.

Во случајот на меѓусебните права и обврски на контролорот и правното, односно физичкото лице каде се чуваат сигурносните копии, 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 15

Овој правилник влегува во сила со денот на донесувањето.

Универзитетски сенат
доц. д-р Ивона Милева, претседател

Ивона Милева

Digitally signed by Ивона Милева
Date: 2025.02.05 14:01:44 GMT