

Машински факултет
Број 01-162/2
24.01.2017 год.
Скопје

Врз основа на член 23 од Законот за заштита на личните податоци („Службен весник на Република Македонија“ број 7/2005, 103/2008, 124/2010, 135/2011, 43/2014, 153/2015 и 99/2016), член 10, став 2, алинеа 2 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“, број 38/2009 и 158/10), како и член 59 од Правилникот за внатрешните односи и работењето на Машинскиот факултет во Скопје во состав на Универзитетот „Св. Кирил и Методиј“ во Скопје, Деканатската управа на Факултетот, на 13-та редовна седница одржана на 24 јануари 2017 година, донесе

ПРАВИЛНИК
за техничките и организациските мерки за обезбедување тајност и
заштита на обработката на личните податоци на
на Машинскиот факултет во Скопје

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 Машинскиот факултет во Скопје во состав на Универзитетот „Св. Кирил и Методиј“ во Скопје (во натамошниот текст – Факултетот).

Обработка на личните податоци

Член 2

Одредбите од овој правилник се применуваат за:

- целосно или делумно автоматско обработување на личните податоци и
- 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.

Нивоа на технички и организациски мерки

Член 3

Факултетот обезбедува 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 и тие се класифицираат во три нивоа:

- основно;
- средно и
- високо.

Примена на нивоата

Член 4

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

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

Технички и организациски мерки кои се класифицирани на основно, средно и високо ниво се применуваат и на други документи утврдени со закон или акт донесен врз основа на закон.

Правила на обработка на личните податоци надвор од работните простории на факултетот

Член 5

Обработката на личните податоци надвор од работните простории на Факултетот треба да се врши врз основа на писмено овластување од Факултетот и во согласност со соодветното ниво на технички и организациски мерки кои се применуваат за обработка на податоците содржани во документите.

Евидентирање и чување на документација за софтверски програми

Член 6

Факултетот треба да ја евидентира и да ја чува целокупната документација за софтверските програми за обработка на личните податоци и за сите негови промени.

Одржување на информацискиот систем

Член 7

Физичките или правните лица кои вршат одржување на информацискиот систем на Факултетот треба да ги применуваат прописите за заштита на личните податоци и документацијата за техничките и организациските мерки донесена од Факултетот.

Технички мерки

Член 8

Факултетот ги обезбедува следниве технички мерки за обезбедување тајност и заштита на обработката на личните податоци:

1. Единствено корисничко име.
2. Лозинка креирана од секое овластено лице, 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 овластеното лице до информацискиот систем во целина, на поединечните апликации и/или поединечни збирки на лични податоци потребни за извршување на неговите работни задачи.

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 3 неуспешни обиди за најавување (внесување на погрешно корисничко име или лозинка) и автоматизирано известување на овластеното лице дека треба да се побара инструкција од администраторот на информацискиот систем.

6. Инсталирање хардверска/софтверска заштитна мрежна бариера („firewall“) 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-спајвер заштита на информацискиот систем, која постојано ќе 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.

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

Организациски мерки

Член 9

Факултетот ги обезбедува следниве организациски мерки за обезбедување тајност и заштита на обработката на личните податоци:

1. Ограничен пристап или идентификација на пристапот до личните податоци.

2. Организациски правила за пристап на овластените лица до интернет кои се однесува 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 обезбедување физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци.

5. Почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци.

Писмено известување до администраторот на информацискиот систем на Факултетот, од страна на вработениот кој ги врши работите за човечки ресурси, за:

- вработувањето или ангажирањето на секое овластено лице 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;

- било кои други промени во работниот статус или статусот на ангажирањето на овластеното лице што има влијание врз нивото на дозволеният пристап до информацискиот систем.

Физичка сигурност на работните простории и на информатичко комуникациската опрема

Член 10

Факултетот воспоставува и применува мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема, вклучително и серверите каде што се собираат, обработуваат и чуваат лични податоци.

Просториите во кои е сместена информатичко комуникациската опрема со која се обработуваат личните податоци се заштитуваат од ризиците во опкружувањето со примена на мерки и контроли за намалување на ризикот од потенцијални закани вклучувајќи кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

Информирање за заштитата на личните податоци

Член 11

Лицата кои се вработуваат или се ангажираат на Факултетот, како и надворешните соработници, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со документацијата на Факултетот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци.

За лицата кои се ангажираат за извршување работа на Факултетот, во договорот за нивно ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

Лицата кои се вработуваат или се ангажираат на Факултетот, како и надворешните соработници, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

Изјавата од ставот 3 на овој член особено содржи:

- дека 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 Факултетот, освен ако со закон поинаку не е уредено и
- ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита.

Образецот на Изјавата за тајност и заштита на обработката на личните податоци е дадена во Прилог, кој е составен дел на овој правилник.

Изјавата од ставот 3 на овој член задолжително се чува во досиејата на вработените или ангажираните лица на Факултетот.

Факултетот задолжително врши континуирано информирање на овластените лица за непосредните обврски и одговорности за заштитата на личните податоци.

Обврски и одговорности на администраторот на информацискиот систем

Член 12

Обврските и одговорностите на администраторот на информацискиот систем се дефинираат и утврдуваат со Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема.

Факултетот задолжително врши периодични контроли над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.

Во извештајот од ставот 2 на овој член треба да се содржани констатираните неправилности и предложените мерки за отстранување на тие неправилности.

Обврски и одговорности на овластените лица

Член 13

Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем се дефинираат и утврдуваат со Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема.

Факултетот задолжително ги информира овластените лица од ставот 1 на овој член со документацијата за техничките и организациски мерки кои се однесуваат на извршувањето на нивните обврски и одговорности.

Овластените лица од ставот 1 на овој член задолжително го применуваат правилото „чисто биро“ при обработката на личните податоци.

Евидентирање на инциденти

Член 14

Постапките за евидентирање и санирање на инцидентите поблиску се утврдуваат со Правилата за пријавување, реакција и санирање на инциденти на Факултетот.

Идентификација и проверка

Член 15

Факултетот задолжително води евиденција на овластените лица кои имаат авторизиран пристап до документите и информацискиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

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

Лозинките треба автоматски да се менуваат по изминат временски период што не може да биде подолг од три месеци утврден со овој правилник.

Контрола на пристап

Член 16

Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информатичко комуникациска опрема кои се неопходни за извршување на нивните работни задачи.

Факултетот воспоставува механизми за да се оневозможи пристап на овластените лица до личните податоци и информатичко комуникациска опрема со права различни од тие за кои се авторизирани.

Во евиденцијата на овластените лица утврдена во член 12 став 1 на овој правилник се внесуваат и нивоата на авторизиран пристап за секое овластено лице.

Администраторот на информацискиот систем кој е овластен согласно со Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користењето на документите и информатичко комуникациската опрема може да доделува, менува или да го одзема авторизираниот пристап до личните податоци и информатичко комуникациска опрема само во согласност со критериумите кои се утврдени од страна на Факултетот.

Управување со медиуми

Член 17

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 овластени лица утврдени во овој правилник.

Пренесувањето на медиумите надвор од работните простории се врши само со претходно писмено овластување од страна на Деканот на Факултетот.

Факултетот воспоставува 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.

Одредбите од ставот 3 на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на Факултетот.

За пренесените медиуми надвор од работните простории на Факултетот се преземаат неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив. Медиумите можат да се пренесуваат надвор од работните простории само со претходно писмено овластување од страна на деканот на Факултетот и 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.

Уништување, бришење или чистење на медиум

Член 18

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.

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

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

Уништувањето и бришењето или чистењето на медиумот го врши комисија составена од 3 (три) члена формирана од деканот на Факултетот. Комисијата составува записник за уништувањето и бришењето или чистењето на медиумот. Записникот ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци снимени на истиот.

Сигурносни копии и повторно враќање на зачуваните лични податоци

Член 19

Факултетот врши проверка на примената на Правилата за начинот на правење на

сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци со кои поблиску се утврдуваат начинот на правење на сигурносни копии, нивното архивирање и чување, како и повторното враќање на зачуваните лични податоци.

Во Правилата од ставот 1 на овој член се утврдуваат постапки за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

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

Сигурносни копии се прават на начин кој ќе овозможи реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите или персоналните компјутери и се физички и криптографски заштитени за да се оневозможи нивна модификација.

Контрола на информацискиот систем и информатичката инфраструктура

Член 20

Информацискиот систем и информатичката инфраструктура подлежат на внатрешна и надворешна контрола, со цел да се провери дали постапките и упатствата содржани во документацијата за техничките и организациските мерки на Факултетот се применуваат и се во согласност со прописите за заштита на личните податоци.

Факултетот врши надворешна контрола на информацискиот систем и на информатичката инфраструктура на секои 3 години, а внатрешна контрола секоја година.

Надворешната контрола од ставот 1 на овој член се врши од страна на независно трето правно лице.

Со посебна одлука на Деканатската управа на Факултетот се утврдува тим овластен да врши внатрешна контрола.

За извршената контрола од став 1 на овој член се изготвува извештај кој содржи:

- мислење во колкава мера постапките и упатствата утврдени во документацијата за техничките и организациските мерки на Факултетот се применуваат и се во согласност со прописите за заштита на личните податоци;

- констатирани недостатоци;

- предлог за неопходни корективни или дополнителни мерки за отстранување на констатираните недостатоци;

- податоци и факти врз основа на кои е изготвено мислењето и се предложени мерките за отстранување на констатираните недостатоци.

Извештајот за извршената контрола се анализира од страна на тимот на офицери за заштита на личните податоци, кој доставува предлози за преземање на потребните мерки за отстранување на констатираните недостатоци.

Идентификација и проверка

Член 21

Факултетот треба да воспостави механизми кои ќе овозможуваат јасна идентификација на секое овластено лице кое пристапило до информацискиот систем и можност за проверка на авторизацијата за секое овластено лице.

Евидентирање на авторизираниот пристап

Член 22

Факултетот води евиденција за секој авторизиран пристап која треба да ги содржи особено следните податоци:

- име и презиме на овластеното лице;
- 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 потребното 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 личните податоци, кој ќе биде определен од тимот на офицери за заштита на личните податоци и истите не може да се деактивираат.

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

Офицерот 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.

Контрола на физички пристап

Член 23

Пристап до просториите каде што е сместен информацискиот систем имаат само овластените лица.

Евидентирање и санирање на инциденти

Член 24

Постапките за евидентирање и санирање на инцидентите, како и 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, поблиску се утврдуваат со Правилата за пријавување, реакција и санирање на инциденти на Факултетот.

Факултетот за повторно враќање на личните податоци издава писмено овластување на овластените лица за да ги извршат операциите за враќање на податоците.

Тестирање на информацискиот систем

Член 25

Факултетот 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.

Пренесување на личните податоци преку електронска комуникациска мрежа

Член 26

Личните податоци можат да се пренесуваат преку електронска комуникациска мрежа само ако се криптирани или ако се посебно заштитени со други соодветни методи кои оневозможуваат податоците да бидат читливи при преносот.

Примена на одредби при друга рачна обработка на личните податоци

Член 27

Одредбите од членовите 3, 4, 5, 9, 11, 13 и 14 од овој правилник соодветно се 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.

Пристап до документите

Член 28

Пристапот до документите е ограничен само за овластените лица на Факултетот.

Овластувањето за пристап до документите ги содржи и категориите на лични податоци до кои се пристапува, како и работното место согласно Систематизацијата на Факултетот, на кое е распоредено овластеното лице.

Друго лице до документите може да има пристап само со писмено овластување на деканот на Факултетот, кое ги содржи податоците од став 2 од овој член, како и образложение на причините за давање на овластувањето за пристап.

Правило „чисто биро“

Член 29

Факултетот 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.

Чување и уништување на документи

Член 30

Документите се чуваат на начин кој ќе оневозможи нивно отворање или пристап од страна на неовластени лица.

Документите се уништуваат по истекот на рокот за нивно чување.

Уништувањето на документите се врши со ситнење така што тие не можат повторно да бидат употребливи.

Уништувањето го врши комисија составена од 3 члена формирана од деканот на Факултетот, после спроведена постапка согласно прописите за архивско и канцелариско работење.

Комисијата составува записник за уништувањето на документите. Записникот содржи податоци за целосна идентификација на документот и за категориите на личните податоци кои тој ги содржи.

Начин на чување на документи

Член 31

Плакарите (орманите), картотеките и другата опрема за чување на документи е сместена во простории заклучени со соодветни заштитни механизми. Просториите се заклучуваат и во периодот кога документите не се обработуваат од овластените лица.

Одржувањето на хигиената во просториите се врши само во присуство на овластените лица.

Копирање или умножување на документи

Член 32

Копирањето или умножувањето на документи може да се врши само од овластени лица или под контрола од овластено лице.

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

Пренесување на документи

Член 33

Документите кои содржат лични податоци можат физички да се пренесуваат надвор од објектот само од овластени лица.

Физичкиот пренос на документи се врши со преземање мерки кои оневозможуваат неовластен пристап или ракување со личните податоци содржани во документите кои се пренесуваат.

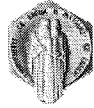
Завршни одредби

Член 34

Овој Правилник влегува во сила со денот на донесувањето.

Универзитет "Св. Кирил и Методиј" во Скопје
Машински факултет - Скопје
Декан





Универзитет „Св. Кирил и Методиј“ во
Скопје



Машински факултет - Скопје

Врз основа на член 14 став 4 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ број 38/09 и 158/10) и член 11 став 3 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на Машинскиот факултет во Скопје, ја давам следнава

ИЗЈАВА

за обезбедување тајност и заштита на обработката на личните податоци на
Универзитетот „Св. Кирил и Методиј“ во Скопје
Машински факултет - Скопје

Јас, _____ вработен/а на Машинскиот факултет во Скопје во состав на Универзитетот „Св. Кирил и Методиј“ во Скопје (во понатамошниот текст – Факултетот) на работното место _____, во согласност со Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ број 38/09 и 158/10) и со Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на лични податоци на Факултетот, изјавувам дека:

- обработката на личните податоци ќе ја вршам согласно со закон и со подзаконските акти од оваа област;
- ќе ги почитувам начелата за заштита на личните податоци;
- ќе ги применувам техничките и организациските мерки на Факултетот за обезбедување тајност и заштита на обработката на личните податоци и ќе ги почитувам сите други правила и процедури за обезбедување тајност и заштита на обработката на личните податоци воспоставени со акти на Факултетот;
- ќе вршам обработка на личните податоци и согласно упатствата добиени од одговорните лица на Факултетот;
- секој личен податок до кој ќе имам пристап во текот на работењето на Факултетот ќе го чувам како доверлив и нема да го пренесувам, оддавам, ниту на било кој друг начин ќе го ставам на располагање на било кое друго лице и во било која форма надвор од системот на пропишани и воспоставени технички и организациски мерки според кои на Факултетот се врши обработката на личните податоци;
- сум запознаен со прописите за заштита на личните податоци и документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци на Факултетот.

Во Скопје, на ден

Изјавил:



Универзитет „Св. Кирил и Методиј“ во
Скопје



Машински факултет - Скопје

Врз основа на член 14 став 4 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ број 38/09 и 158/10) и член 11 став 3 од Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на Машинскиот факултет во Скопје, ја давам следнава

ИЗЈАВА

за обезбедување тајност и заштита на обработката на личните податоци на
Универзитетот „Св. Кирил и Методиј“ во Скопје
Машински факултет - Скопје

Јас, _____ ангажиран/а на Машинскиот факултет во Скопје во состав на Универзитетот „Св. Кирил и Методиј“ во Скопје (во понатамошниот текст – Факултетот) за вршење _____ работи, во согласност со Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ број 38/09 и 158/10) и со Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на лични податоци на Факултетот, изјавувам дека:

- обработката на личните податоци ќе ја вршам согласно со закон и со подзаконските акти од оваа област;
- ќе ги почитувам начелата за заштита на личните податоци;
- ќе ги применувам техничките и организациските мерки на Факултетот за обезбедување тајност и заштита на обработката на личните податоци и ќе ги почитувам сите други правила и процедури за обезбедување тајност и заштита на обработката на личните податоци воспоставени со акти на Факултетот;
- ќе вршам обработка на личните податоци и согласно упатствата добиени од одговорните лица на Факултетот;
- секој личен податок до кој ќе имам пристап во текот на работењето на Факултетот ќе го чувам како доверлив и нема да го пренесувам, оддавам, ниту на било кој друг начин ќе го ставам на располагање на било кое друго лице и во било која форма надвор од системот на пропишани и воспоставени технички и организациски мерки според кои на Факултетот се врши обработката на личните податоци;
- сум запознаен со прописите за заштита на личните податоци и документацијата за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци на Факултетот.

Во Скопје, на ден

Изјавил:
