

УНИВЕРЗИТЕТ СКОПЈЕ

ПРОЦЕДУРИ ЗА ОБРАБОТКА И БЕЗБЕДНОСТ НА ПОДАТОЦИ

I. Цел на процедурите

Целта на овие процедури е да се обезбеди правилна, сигурна и законска обработка на податоците на Универзитет СКОПЈЕ, како и заштита на личните податоци на студенти, вработени, соработници и трети лица.

II. Опсег

Овие процедури се однесуваат на:

- Лични податоци на студенти (име, презиме, адреса, оценки, студиски информации)
- Лични податоци на вработени (име, презиме, матичен број, плата, здравствени информации)
- Податоци поврзани со истражувања и академски активности
- Дигитални и хартиени податоци кои се обработуваат од Универзитет СКОПЈЕ

III. Основни принципи при обработка на податоци

1. **Законитост, правичност и транспарентност** – обработката се врши во согласност со Законот за заштита на лични податоци.
2. **Намалување на податоците** – собираат се само податоци кои се неопходни за конкретната намена.
3. **Точност** – податоците се редовно ажурираат и проверуваат.
4. **Чување ограничено на време** – податоците се чуваат колку што е потребно за исполнување на целите.
5. **Интегритет и доверливост** – се преземаат мерки за заштита од неовластен пристап, губење, уништување или оштетување.

IV. Процедури за обработка на податоци

1. **Собирање на податоци**
 - Секој оддел или канцеларија мора да има јасно дефинирана намена за собирање на податоците.
 - Личните податоци се собираат само со согласност на лицето или на законска основа.
2. **Чување на податоците**
 - Дигитални податоци: се чуваат на заштитени сервери со пристап за авторизирани лица.
 - Хартиени податоци: се чуваат во заклучени архиви, со ограничен пристап.
3. **Пристап до податоците**

- Само овластени лица (административни работници, ИТ техничари, раководители) имаат пристап.
 - Преглед на податоците од страна на трети лица се овозможува само со писмена согласност.
- 4. Пренос и споделување на податоци**
- Податоците се споделуваат само ако постои законска основа или писмена согласност.
 - За пренос на податоци се користат сигурни канали (енкрипција, VPN, заштитени платформи).
- 5. Евиденција на обработката**
- Секој оддел води евиденција за собраните податоци, целта на обработка и лицата кои имаат пристап.

V. Мерки за безбедност на податоците

- 1. Технички мерки**
- Антивирус и заштита на мрежата.
 - Редовно резервирање на дигитални податоци.
 - Енкрипција на чувствителни податоци.
 - Контрола на пристап (кориснички акаунти, лозинки, двоен фактор на автентикација).
- 2. Организациски мерки**
- Обука на вработените за заштита на лични податоци.
 - Политика за одговорност при неовластен пристап или инциденти.
 - Контрола на физичкиот пристап до серверски соби и архиви.
- 3. Мерки при инциденти**
- Секој инцидент се пријавува на Одговорното лице за заштита на лични податоци.
 - Веднаш се преземаат корективни мерки за заштита на податоците.
 - Водење евиденција за сите инциденти.

VI. Контрола и евалуација

- Одговорното лице за заштита на лични податоци врши редовна контрола на спроведување на овие процедури.
- Процедурите се ревидираат најмалку еднаш годишно или по потреба при промена на законската регулатива.

VII. Одговорности

- **Раководители на единици:** осигуруваат спроведување на процедурите во своите сектори.
- **Одговорно лице за заштита на лични податоци:** координира, контролира и известува за ризици или инциденти.
- **Сите вработени:** ги почитуваат процедурите и ја чуваат доверливоста на податоците.