1.

Principles of Personal Data Protection at

the Medical University

of Bialystok

Information for year prefects/students

Prepared by:

Emilia Minasz

Data Protection Officer

The materials may be used only for informational purposes at the Medical University of Bialystok.

2.

REFORM OF DATA PROTECTION RULES

GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – (General Data Protection Regulation)

3. WHAT DOES THE GDPR PROTECT?

DOCUMENTS

PERSONAL DATA

NATURAL PERSONS

FUNDAMENTAL RIGHTS AND FREEDOMS

in particular, the right to the protection of personal data

4. PERSONAL DATA

DEFINITION

Personal data is information about:

an identified natural person or an identifiable natural person who can be identified directly or indirectly, in particular on the basis of an identifier such as:

- ✓ name and surname

- ✓ identification number
- ✓ location data
- ✓ the internet identifier or
- ✓ one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person

5. THESE MAY BE PERSONAL DATA

Email address

Lists of employees, students

PESEL number

Image

Assessment grades

Student's ID number

6. CONTROLLER

Controller - a natural or legal person, public authority, agency or other entity which, alone or jointly with others, determines the purposes and means of processing personal data **of the Medical University of Bialystok**

7. DATA PROTECTION OFFICER

Emilia Minasz **MUB's** Data Protection Officer

Phone no. 85 6865215 email: iod@umb.edu.pl

Officer's tasks:

- ✓ informing and advising on the obligations arising from the GDPR,
- ✓ monitoring compliance with the GDPR and the controller's policies in the field of personal data protection, including division of responsibilities, awareness-raising activities, training and audits,
- ✓ providing recommendations on data protection impact assessments upon request and monitoring its implementation,
- ✓ cooperation and consultations with the supervisory authority,
- ✓ contact point for the supervisory authority and persons whose data we process.

8. PRINCIPLES OF PERSONAL DATA PROCESSING GDPR

- Principle of legality, reliability and transparency
- Principle of purpose limitation
- **Principle of minimization – AS LITTLE AS POSSIBLE**
- Principle of correctness **- UPDATE THE DATA**

immediately notify the appropriate dean's office and the Department of Student Affairs about the change of marital status, name, address and other data affecting your situation

- Principle of storage limitation
- **Principle of integrity and confidentiality - PROTECT DATA AGAINST LOSS AND ACCESS BY UNAUTHORIZED PERSONS**
- Principle of accountability

9. PRINCIPLES OF PERSONAL DATA PROCESSING GDPR

Principle of integrity and confidentiality - PROTECT DATA AGAINST LOSS AND ACCESS BY UNAUTHORIZED PERSONS

University employees:

- ✓ do not provide information about students
- ✓ do not provide documents with personal data

TO THIRD PARTIES

which may include, among others: family members, friends

10. PERSONAL DATA PROTECTION

Principle of confidentiality

YEAR PREFECT!

If you are in possession of students' data:

1) do not share them in conversations with other students,
2) do not send this data to other students.,
3) do not post data on the Internet, e.g. on social media
4) do not provide personal data over the phone (impersonating telephone persons) and, if necessary, verify the identity of the contacting person

11. PERSONAL DATA PROTECTION

Principle of confidentiality

Students who consent to the processing of their personal data by the year prefect do so for a specific purpose, which is the year prefect's intermediation in contacts with organisational units conducting didactic classes and dean's offices, and only in the scope of data contained in:

- in agreements/contracts on professional practice,
- on lists of students regarding the organization of the year, for example, the division into groups.

12. YEAR PREFECTS

Principle of confidentiality

YEAR PREFECT!

Remember that you have undertaken to keep confidential the personal data of students to whom you gain access in connection with the performance of the year prefect at the Medical University of Bialystok.

If you are sending a message to a group of students, use the BCC option in your university e-mail – for a hidden message (this way you will not reveal the e-mail addresses and therefore the student album numbers)

13. STUDENTS RULES

For university matters, use the university email address

Please note that the university address (idnumber@student.umb.edu.pl) is personal data

You are obliged by the Article 9 of the Regulations of studies use in all matters related to studies in electronic correspondence student university account in the domain student.umb.edu.pl and systematically check your email account and read your correspondence

In addition, the student is obliged to systematically log into the University's IT system and get acquainted with the information contained there.

14. EMAIL POLICY

Take care of the confidentiality of passwords to university IT systems, including mail:

- do not share your password with others
- do not write your password on the cards, because you may lose them

If you notice something unusual while using the mail – immediately change the password and report this fact to the IT Department

Do not use university mail in private matters, including not providing University mail for private purposes, e.g. in online stores, on social media, etc.

15. EMAIL POLICY

Watch out for messages that force you to enter your login and password – DO NOT ENTER, DO NOT RESPOND, DELETE OR/AND NOTIFY THE IT DEPARTMENT

Be very careful when providing data over the Internet

Beware of suspicious email attachments

Beware of suspicious links. If you receive an e-mail or text message, and you are not sure that their sender is real - do not respond and do not click on the links in the messages

16. EXAMPLES OF EXTORTION IN EMAILS

17. EXAMPLES OF EXTORTION IN EMAILS

18. EMAIL POLICY

WHEN SENDING AN EMAIL, PAY ATTENTION TO THE CHOSEN RECIPIENT – IT'S EASY TO BE MISTAKEN

CHECK THE ATTACHED FILES TO SEND BY E-MAIL OR ATTACHED FILES ON THE WEBSITE (WHETHER THEY ARE THE ONES YOU WANTED TO SEND)

IF YOU DON'T HAVE TO, DON'T EMAIL THE PERSONAL DATA.

19. EMAIL POLICY

Do not store personal data in the University mail if it is not necessary.

Delete unnecessary messages on an ongoing basis.

The above will protect the University from data leakage, at the moment when your university mail is hacked.

If you suspect a hack on your university mail - immediately change your password and report this fact to the IT Department.

20. GOOD PRACTICES

Please note that names, surnames, album numbers, e-mail addresses of students, grades/credits of students are personal data

- don't keep notes with students' personal data in plain sight
- do not leave students' personal information unattended, e.g. in the hallway

- do not hand over documents containing students' personal data to, e.g. to another person to deliver them to the dean's office, if you are not sure that this is the person authorized to access students' personal data

21. GOOD PRACTICES

YEAR PREFECT!

Attention to the transfer of information about the student to another student, the transfer of documents to another student, e.g. information about pass/fail, information about the need to provide confirmation of payment for a condition, etc.

Another student is not authorized to receive information about other students/documents of other students

22. GOOD PRACTICES

If you see something disturbing, such as data in the trash, data in the hallway, data left UNATTENDED, etc. notify the Data Protection Officer

Remember that even the data left in view does not entitle you to get acquainted with them and pass this information on to other persons

23. INFORMATION ABOUT GRADES

Do not publish exam/credit results (e.g. do not publish in public places, including the Internet, do not send the student list with grades and student ID numbers with grades – if you do not have the consent of the students)

Individual transmission of grades and any form that does not identify a person is permitted

24. STUDENTS' RESPONSIBILITIES

Teacher / MUB's employee has the right to legitimize a student who, for example,:

- ✓ came for exam/assessment
- ✓ came to the dean's office

The student is obliged to present a document confirming their identity for inspection

Each student is required to self-report to the dean's office in order to renew their ID

25. STUDENTS' RESPONSIBILITIES

Before settling the matter, a University employee may ask the student to show his/her student ID or ID card

The documentation requested by the student is not transferred to other people - you must collect your documents in person (applies to documents with personal data)

The teacher/other University's employee has the right to address the student by name and has the right to read the list of attendance at classes or to hand it over for signature

26. DATA PROTECTION OFFICER

Questions and concerns regarding the protection of personal data should be addressed to the Data Protection Officer (DPO)

Emilia Minasz

DATA PROTECTION OFFICER

Phone no. 85 686 5215

email: emilia.minasz@umb.edu.pl

iod@umb.edu.pl