

# **Rules for the processing of personal data**

**Data Protection Officer Klaudia Goclik**

**E-mail:[iod@pulmonologia.olsztyn.pl](mailto:iod@pulmonologia.olsztyn.pl)**

# Applicable legal acts

- By writing and saying "GDPR", we mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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). This is a legal act adopted by the European Union regulating the principles of personal data protection - it replaces Directive 95/46 / EC of 1995.
- Act of 10 May 2018 on the protection of personal data

# What are personal data - art. 4 GDPR?

- Personal data - means any information about an identified or identifiable natural person ("data subject"); an identifiable natural person is a 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, online identifier or one or more specific physical, physiological, genetic, mental factors, the economic, cultural or social identity of the natural person;
- Name and surname, address of residence, PESEL number, ID card number, telephone number, e-mail address, constitute personal data;

## Special data - data of a special category in accordance with art. 4 GDPR

- Revealing racial or ethnic origin, political views, religious or ideological beliefs, trade union membership and genetic data, biometric data, data concerning health, sexuality or sexual orientation.
- "health-related data" means personal data about the physical or mental health of a natural person, including the use of healthcare services, revealing information about his/her health;

# Other important definitions from Art. 4 GDPR:

- Administrator - means a natural or legal person, public authority, unit or other entity that, alone or jointly with others, determines the purposes and methods of personal data processing; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- Processing - means an operation or a set of operations performed on personal data or sets of personal data in an automated or non-automated manner, such as collecting, recording, organizing, organizing, storing, adapting or modifying, downloading, viewing, using, disclosing by sending, disseminating or otherwise such as sharing, matching or combining, restricting, erasing or destroying;
- Each action on personal data is their processing, the mere fact of storing personal data means that we process them.

# The most important definitions of Art. 4 GDPR:

- Pseudonymization - means the processing of personal data in such a way that they can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and is subject to technical and organizational measures that prevent its attribution to an identified or an identifiable natural person;
- consent - of the data subject means a voluntary, specific, informed and unambiguous indication of will, by which the data subject, in the form of a statement or a clear affirmative action, consents to the processing of personal data concerning him;
- breach of personal data protection - means a breach of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed

# When can personal data be processed?

Personal data can only be processed if there is a so-called the legal basis for data processing. Typical grounds for processing ordinary data are:

- a) consent of the data subject (Article 6(1)(a) of the GDPR);
- b) data processing is necessary to perform the contract with the data subject or to take steps prior to concluding the contract, at the request of that person (Article 6(1)(b) of the GDPR);
- c) processing is necessary to fulfill the legal obligation to which the administrator is subject (Article 6(1)(c) of the GDPR);
- d) processing is necessary to protect the vital interests of the data subject or another natural person (Article 6(1)(d) of the GDPR);
- e) processing is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the administrator (Article 6(1)(e) of the GDPR)
- f) processing is necessary for the purposes of legitimate interests pursued by the administrator or by a third party (Article 6(1)(f) of the GDPR)

# By implementing the rights of data subjects, we mean the rights indicated in art. 15-22 GDPR, i.e. the right to:

- access to data,
- rectification of data,
- deletion of data ("right to be forgotten"),
- data processing restrictions,
- data transfer,
- objection,
- not to be subject to decisions based solely on automated processing.




# How should personal data be secured?

The GDPR departs from the practice of indicating in the law specific measures to protect personal data to be implemented by the controller or processor. Instead, the GDPR introduces the so-called risk-based approach.

The essence of the risk-based approach boils down to the fact that each entity processing personal data should independently determine what specific data security measures should be implemented. The selection of security measures should be based on:

- a) nature, scope, context and purposes of processing,
- b) the risk of violating the rights or freedoms of natural persons with varying probability of occurrence and severity of the threat,
- c) state of technical knowledge,
- d) implementation cost.



The GDPR does not specify any specific data security measures. The GDPR only indicates exemplary technical and organizational measures that may serve to achieve this goal, i.e. ensuring a level of security adequate to the risk. These are in particular:

1. pseudonymization and encryption of personal data;
2. the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services at all times;
3. the ability to quickly restore the availability and access to personal data in the event of a physical or technical incident;
4. regularly testing, measuring and assessing the effectiveness of technical and organizational measures ensuring the security of processing.

# What is the data breach notification obligation?


The GDPR imposes a legal obligation on entities processing personal data to inform about security incidents regarding personal data. This is a very significant change compared to the Act of August 29, 1997, which did not contain such a solution at all.

A security incident is referred to in the provisions of the GDPR as a breach of personal data protection and may consist of:

- a) breach of security leading to accidental or unlawful destruction, loss, modification of personal data
- b) breach of security leading to unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.

Examples:

- loss of the carrier with personal data,
- obtaining access to data by an unauthorized person,
- hacking into the system used to process personal data.



The supervisory authority (PUODO) should be informed about the incident. The information should be provided immediately, but not later than within 72 hours of finding the breach. In certain cases, data subjects should also be informed about the incident - this will be the case when the breach is likely to result in a high risk to the rights and freedoms of the data subject.

Examples:

- unauthorized persons gaining access to logins and passwords of customers of the electronic banking system,
- loss of a carrier containing patients' medical records.

# GDPR sanctions - financial

## **ENTREPRENEURS**

up to 2% of the total annual global turnover from the previous financial year or up to EUR 10,000,000

or

up to 4% of the total annual global turnover from the previous financial year or up to EUR 20,000,000

## **PHYSICAL PEOPLE**

up to EUR 10,000,000

or

20,000,000 euros

# GDPR sanctions - other

- **Criminal liability** - criminal provisions have been included in the Act on the Protection of Personal Data and provide for - depending on the type of act - a fine, restriction of liberty or imprisonment for up to three years.
- **Civil liability** - the data subject has the right to compensation for material or non-material damage resulting from the violation of the GDPR.
- **Employee liability** - in extreme cases, an employee's insubordination may be considered a serious violation of basic employee duties and even result in termination of the contract in disciplinary mode, due to the employee's fault.



# **PRACTICAL ISSUES**

## **Can the medical entity provide information by phone about the fact of hospitalization of patients with the identity indicated by the interlocutor?**

- When there is no certainty as to the identity of the interlocutors, but providing such information may affect the patient's health or life - yes, but it may take place in exceptional cases.
- If the refusal to provide information about the patient's hospital stay may prevent the exercise of the right of family members or close relatives to information about the patient's health condition, the entity should provide such information in emergency situations (e.g. road accident) and in life-threatening situations for the patient.
- However, the institution should make it sufficiently probable that the interlocutor is a person authorized to obtain this information by asking control questions, e.g. PESEL number, address of residence;
- In accordance with the principle of minimization, only the information that is necessary to act in a state of emergency should be provided over the phone.



## Can a medical entity use an established method of disclosing information about the patient's health condition in terms of the patient's temperature?

- ▶ On the so-called bedside cards, yes. A medical entity may use bedside cards in its practice. Resigning from them, however, is a good practice.
- ▶ In many cases, a sudden deterioration in the patient's health may require immediate access to his/her identification data.
- ▶ The bedside card gives such a guarantee. The healthcare entity may completely resign from bedside cards, taking into account the obligations arising from the provisions of art. 36 sec. 3, 5 and 6 of the Act of 15 April 2011 on medical activity.
- ▶ If the use of cards is necessary, they should be secured by:
  - ▶ the use of frames for bedside cards that protect personal data contained in the cards;
  - ▶ the construction of the frame should make it impossible to read the data;
  - ▶ the use of an overlay protecting the patient's data on the bedside card;
  - ▶ reversal of bedside cards;
- ▶ **The above was pointed out by NIK during inspections of medical entities in terms of the GDPR as inconsistent with Art. 24 sec. 1 of the GDPR, in which the implementation of appropriate technical and organizational measures to ensure the protection of personal data is indicated as one of the obligations of the ADO.**

## Can the medical entity make access to the medical records of a third party conditional?

- The authorization granted by the patient to whom the documentation relates, bearing a handwritten signature or submitted in electronic form, bearing a qualified electronic signature or a signature confirmed by a trusted profile, in accordance with the provisions on patient rights and the Patient Rights Ombudsman, the authorization in a given facility may be granted at any form, and limiting the form of the authorization is a violation of patient rights.
- However, it should be remembered that the institution should be sure about the identity of the person granting the authorization. If the patient grants such authorization directly in the presence of staff, this form of declaration should be acceptable.
- It should also be remembered that the entity providing health services, while fulfilling its obligations related to keeping medical records, was also obliged to keep a list with information on the provided medical records.

## Is it possible to label medicinal products with the patient's name?

- Yes. Due to the reduction of the risk of mistakes, marking the patient's name and surname when using the service in a medical entity is acceptable. This applies to all medicinal products. The legal basis for the processing of personal data in the above scope is art. 9 sec. 1 lit. h GDPR.
- Consequences related to the administration of the wrong medical product may have a serious impact on the health and even life of patients, the above premise is a direct legal basis for marking medical products by name.
- It would be impossible to collect consents from patients for the processing of personal data in this regard, because if they did not give such consent, the facility would have a huge problem.

# Can the doctor and medical staff in the sickroom refer to patients by their first and last names?

- ▶ The doctor should not address the patient by name in the sick room. However, you can address the patient using, for example, the phrase "Mrs. / Mr. " along with the addition of the first name, which at the same time guarantees respect for the patient's dignity. The exceptions are cases when the doctor cannot identify the patient in any other way than by using his name, or when it is necessary to undertake emergency actions to save life or health.
- ▶ According to Art. 9 sec. 2 lit. h GDPR, the processing of personal data concerning health is possible when it is necessary for the purposes of preventive health care, medical diagnosis, provision of health care, treatment or management of health care or social security systems and services on the basis of the law of a Member State.
- ▶ According to Art. 36 sec. 3 and 5 of the Act of 15 April 2011 on medical activity, patients are provided with identification marks. The identification mark contains information allowing to determine: name and surname, date of birth of the patient. Only in justified cases it may refrain from doing so. The reason, together with the refusal to use such means of identification, shall be included in the medical records.
- ▶ Information above of the mark are to be recorded in such a way as to prevent its identification by unauthorized persons.
- ▶ The purpose of the above of the provisions is therefore to prevent the identification of the patient by third parties. Thus, the adoption as a rule of addressing the patient by the medical staff by name and surname would be inconsistent with the purpose of the above-mentioned law. regulations.

# Can a doctor talk to a patient about his illness in the sick room?

- When there is no guarantee that other patients will not hear it, and the patient's health condition allows such a conversation to be held outside the patient's room, then, as a rule, the medical staff's transfer of information disclosed to the patient, data about his health, in a dormitory room should be limited to the minimum necessary to achieve the purpose for which they are processed;
- Activities that are not health monitoring, asking questions about how you feel or obtaining and providing information related to the treatment process. Undoubtedly, they may include information about obtaining informed consent for medical procedures, information about the diagnosis, treatment method, etc. If the state of health allows it, such information should be provided in a doctor's office or in another place where there are no other unauthorized persons.
- Communication with the patient directly related to the implementation of ongoing monitoring of the patient's health, including asking about the well-being, obtaining and providing basic information related to the treatment process. This includes activities related to the doctor's or nurse's rounds, information about changing medications and planned examinations. In such situations, it is possible to provide information about the patient's health in the patient's room.
- Only authorized persons may stay in the room during current medical activities. At the patient's request, a relative may also be present.
- If the conversation about the patient's health is directly related to saving life or health and failure to conduct the conversation immediately could expose the patient to harm, it is possible to conduct the conversation at any place.

# Can a health facility put the names and specializations of doctors admitting patients on the doors of doctor's offices?

- Yes, placing the doctor's names and specializations on the doors of doctor's offices does not violate the GDPR.
- Information about the doctor's name and specialty is his usual personal information. According to Art. 6 sec. 1 lit. c GDPR, the basis for the processing of ordinary data is the implementation of the obligation arising from the provisions of law.
- According to Art. 31 of the Act on health care services financed from public funds, the patient has the right to choose a doctor, and in accordance with art. 36 of the Act on Medical Activity, persons employed in a hospital or remaining in a civil law relationship with a medical entity whose treatment facility is a hospital, are required to wear in a visible place an identifier containing the name and function of that person.
- The given doctors, including in particular the name, surname, type and degree of specialization or skills in the narrower fields of medicine or providing specific health services, are included in the register kept by the competent regional medical council in accordance with Art. 8 sec. 1 of the Act of 5 December 1996 on the Professions of Physician and Dentist and in accordance with the Regulation of the Minister of 26 June 2012 on the detailed requirements that should be met by the premises and equipment of the entity conducting medical activity, determines the obligation to mark doctor's offices.

## How can you ensure anonymity when calling patients to doctor's offices when the facility does not have the funds to implement an electronic patient identification system (numbers) and there are sometimes a huge number of patients in the corridor?

- Efforts should be made to minimize the risk of disclosure of information to third parties, in particular health data, taking into account specific technical, organizational and premises conditions in the facility. The applied solutions may in no way interfere with the provision of healthcare services or put the health or life of patients at risk.
- Exemplary methods of calling a patient in a medical entity:
- call using the identification number. Given in accordance with the indication of art. 36 sec. 5 of the Act on Medical Activity of the sign/numerical pseudonym. Entering these numbers into the medical records takes place simultaneously with their transfer to the patient. The patient is then called to the office by this number.
- call after the number assigned during registration. This solution does not require financial outlays, and is only associated with assigning a unique number during registration in a way that ensures that the number is provided to the doctor in the surgery and to the patient.
- Call after an hour of visit. Making an appointment for a specific time in a way that prevents overlapping of hours.
- Call after an hour + name (Mr Michał from 11.30) + possibly office number.

# How to ensure patient anonymity during registration before a doctor's visit?

Possible methods of registering a patient in a medical entity with confirmation of identity:

- in the entity, a place should be designated for the registration process, place markings should clearly indicate the area where only the patient being serviced can be.
- a) Sticking on the floor in front of the registration station a tape in bright colors marking the area in which only the serviced person is present;
- b) Posting a message about the need to stay at one reception desk only for one patient;
- c) Separating the registration area with a wall. Plexiglass plate - a single seat or standing place in the zone. Unauthorized persons remain outside the physical barrier;
- d) Separation of the registration zone with a barrier - unauthorized persons remain outside the registration zone behind the barrier;
- e) Introducing the appropriate distance between stations;
- f) Introduction of a registration zone in a separate room outside the corridor, a place for waiting;
- g) Introduction of electronic/telephone registration.
- h) It is possible to designate a separate, isolated position for telephone registration, separate from the main reception, where personal data is read



## How to verify a patient?

- a) The registrant asks the patient to show a document verifying identity;
- b) If the patient refuses to present a document verifying his identity, he may be asked to provide identification data, i.e. PESEL or other identification number;
- c) It is possible to use cards/forms on which the patient enters the required identification data. Pages must be destroyed immediately after use, in a way that allows the recorded content to be reproduced. If it is not possible to destroy them immediately, they should be put away in a safe place and destroyed immediately after finishing work;
- d) If the patient voluntarily, without being summoned, presents a document verifying identity or provides existing information enabling identification, the acceptance of the data provided voluntarily should not be refused.
- e) Introduction of the possibility of secure electronic registration

## Conclusions from the audit carried out by the Supreme Chamber of Control in hospitals.

- The development and implementation of appropriate documentation and procedures regarding the protection of personal data was positively assessed;
- The staff was informed about the provisions of the GDPR and the internal regulations of the hospital.
- Conducting an analysis of data processing processes.
- Granting permissions in IT systems adequate to the workplace and tasks performed.
- Fulfillment of the obligation to conclude contracts for entrusting the processing of personal data.
- Sharing of medical data was carried out in accordance with applicable regulations.
- Statement that the method of marking patients' identification wristbands and the use of frames for bedside cards adopted in hospitals were inconsistent with applicable regulations
- Appropriate security measures were not applied during the doctor's absence in one of the surgeries, which posed a risk of unauthorized access to patients' personal and medical data.
- Untimely informing the President of the Office for Personal Data Protection about the appointment of the DPO.

# Simple rules

## **1. Lock your computer**

Lock your computer every time you leave your desk. This will minimize the risk of data disclosure to unauthorized persons.

## **2. Follow the rule of a clean desk**

Documents containing personal data left unattended on desks may fall into the hands of unauthorized persons. There is a risk of unauthorized disclosure of data.



### **3. Receive documents from the printer**

Documents containing personal data printed and not collected from the printer may be taken over by unauthorized persons. Avoid such situations and always pick up printed documents.

### **4. Store documents containing personal data in lockable furniture.**

Documents stored, e.g. in a cupboard without a lock, are not properly protected because every person has access to them.

### **5. Delete document scans from your computer's hard drive.**

### **6. Do not disclose patient data to unauthorized persons**

### **7. Work on company equipment.**

# Rules for safe use of e-mail

## ➤ 1. Do not save your email password in your browser

Treat email like a banking system. Never save your email password in your web browser. This will protect you against unauthorized access or password stealing by viruses directly from the browser system.

## ➤ 2. Always remember to log out

Make it a habit to log out of your email. Many systems, especially on-line, have a very long session set. This means that once you log in, you stay logged in for days. It is very dangerous.

## ➤ 3. Use a strong and unique mailbox password

Cybercriminals have access to millions, if not billions, of standard passwords. By using simple passwords, you enable them to break into your account using Brute Force methods. Do not use your own or your loved ones' first names or surnames in your passwords. Do not use identification numbers, e.g. PESEL or dates of birth. The password should be long, contain special characters, spaces and be in the form of a sentence rather than a single phrase. Use different, unique passwords for sensitive services such as mailboxes. Breaking the password on other services where you have accounts will not automatically intercept further service accounts.

# Rules for safe use of e-mail

## ➤ 4. Never share your password

Never share your e-mail account password with any third party. This is very dangerous and what's more, you won't have any information about what this person has viewed in your mail.

## ➤ 5. Always verify the sender

Always check the sender of the message and the domain from which it is sent. Although a skilled hacker is able to impersonate any address, an increasing number of postal service providers are able to detect such messages and block them. Nevertheless, when sending fake messages, cybercriminals use email addresses with a similar name to banks or large service providers, which can lull your attention. When verifying the sender, check the e-mail address from which the message came, not the name.

## ➤ 6. Check the spelling of the message

Many messages are sent automatically by robots. Often these messages are automatically translated from other languages. As a result, the content of the message contains mainly stylistic and grammatical errors. If you receive a message with broken Polish, you can be almost sure that it was generated by a translator. Be careful with such messages.

# Rules for safe use of e-mail

## ► 7. Do not reply to SPAM

Replying to SPAM confirms the existence of an e-mail address and thus may generate another dose of unwanted messages.

## ► 8. Do not click on links in e-mails

Never click on links in e-mails. If the messages are in the form of HTML, you may be redirected to a different page than stated in the body of the message. It is better to paste the link into the address bar in the browser and check what form it has before running it. Linking to a strange unknown site should be a warning to you.

## ► 9. Beware of suspicious attachments even from friends

Hackers often send SPAM and viruses from compromised accounts to your contact list. Receiving a message from family, friends or known contractors, your vigilance is dormant. Be especially careful with ZIP, RAR, 7-ZIP, etc. zipped files and PDF documents, which very often transport viruses, Trojans, worms and other spyware.

# Rules for safe use of e-mail

## ➤ 10. Use email providers that scan attachments for viruses

When choosing your postal service provider, be guided by quality, not price. Choose providers that apply virus scanners to the attachments you receive. This will reduce the risk of a virus being installed on your device.

## ➤ 11. Beware of suspicious attachments even from friends

Hackers often send SPAM and viruses from compromised accounts to a list of kantaks. Receiving a message from family, friends or known contractors, your vigilance is dormant. Be especially careful with ZIP, RAR, 7-ZIP, etc. zipped files and PDF documents.

## ➤ 12. Use two-step verification

It's hard to get used to and a bit of a pain, but use 2-Step Verification whenever possible. It consists in the need to enter an additional code (token) sent via SMS or to the mobile application during each login. This will increase the security of your account and prevent you from accessing it even if your password is compromised.

## ➤ 13. Don't send sensitive data unencrypted

Never send sensitive data via email in unsecured form. All information, PESEL number, age, place of residence, scans of documents, etc. are sensitive. If you need to provide such documents or information, enter them in a separate document, pack them into a zip, rar, 7z or other archive with a password, and then send them encrypted. Always deliver the password via another channel, e.g. via SMS or messenger.