DR FACE
by Osuch

ANNOUNCEMENT
CONCERNING A PERSONAL DATA BREACH

published pursuant to Article 34(3)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR)

Dear Patients,

We would like to inform you that, as a result of a cyberattack on the Medyc system in which our clinic keeps patient records, the confidentiality of our patients' personal data has been breached. On 8 October 2026 we sent individual notifications to the patients whose e-mail addresses we held. This announcement is addressed to everyone affected by the incident, in particular to those we are unable to contact individually because we do not hold their current contact details or because the message sent to them could not be delivered.

Key information at a glance

- The Medyc system operated by Qbusoft sp. z o.o., in which our clinic keeps patient records, was the target of a cyberattack. The data of our patients registered in the system up to 21 August 2026 was copied.
- The scope of the copied data depends on the information recorded about each person. It has been confirmed that identification and contact data were copied: first name and surname, PESEL number (Polish national identification number), home address, telephone number and e-mail address.
- For patients who attended a consultation or underwent a procedure, it is highly likely that photographs and PDF files stored in the system were also copied, including photographs sent before the procedure, consent forms and scans of medical records.
- So far there is no evidence that the data has been published, but this cannot be ruled out.
- We recommend restricting your PESEL number (if you have one) and exercising caution with messages and calls that refer to the data breach.
- Information: clinic reception, tel. +48 501 093 653; Data Protection Officer, e-mail: agata.szwed@asprotectis.pl.

Who is affected?

The breach concerns the data of all persons registered in our clinic's Medyc system up to 21 August 2026, covering the entire period in which we have used the system, including:

– patients who underwent a procedure;

– patients who attended a consultation without a procedure;

– persons who booked an appointment but did not attend it;

– persons who contacted the clinic and were recorded in the system with only a telephone number or an e-mail address.

Persons registered after 21 August 2026 are not affected.

What happened?

The system of our data processor, Qbusoft sp. z o.o. with its registered office in Gdańsk (the developer of the Medyc software), was the target of a cyberattack. According to Qbusoft's findings, during the

night of 22 to 23 August 2026 an unauthorised person exploited a previously unknown security vulnerability in the system (an SQL injection vulnerability), copied the patient data of clinics using the Medyc system and transferred it outside the system. Qbusoft confirmed the breach on 9 September 2026. On 2 October 2026 we received confirmation from Qbusoft that the breach covered the data of all our clinic's patients, together with information on the scope of that data, and on 6 October 2026 we received supplementary information.

The perpetrator encrypted the copied data with their own tool and is therefore able to read it. It must be assumed that they have access to the data in readable form.

What data is involved?

The scope of the data depends on the information recorded about each person in the system. For some persons all of the data listed below was recorded, for others only some of it, for example only a name with a telephone number, or only an e-mail address. If you would like to know what data was recorded in your case, please contact our reception.

Data confirmed to have been copied

First name and surname, PESEL number, home address, telephone number and e-mail address, to the extent that they were recorded in the person's profile.

Data highly likely to have been copied

Photographs and PDF files stored in the system in connection with a consultation or procedure, in particular photographs sent by patients before the procedure, consent forms for the procedure and anaesthesia, and scans of medical records. They contain information about health and, in the case of photographs, also the person's image. Photographs taken after the procedure are not stored in this system. This data concerns only persons who attended a consultation or underwent a procedure at our clinic.

Data whose copying cannot be ruled out

Qbusoft has neither confirmed nor ruled out that the breach also covered other data stored in the system, for example date of birth, information on visits and appointment dates, diagnoses, prescriptions and referrals issued, billing data, and information entered in the notes field of the patient profile. For some foreign patients who do not have a PESEL number, the passport number was recorded in the notes.

According to Qbusoft (as of 6 October 2026), the data has not so far been published or offered for sale. The perpetrators have made no demands and no threats to disclose it. However, it cannot be ruled out that the data may be used or disclosed in the future; the breach therefore poses a high risk to the rights and freedoms of the persons concerned.

What are the possible consequences?

A PESEL number or passport number combined with a name, address and contact details may be used by unauthorised persons to:

- take out a loan or credit, or conclude other contracts, without your knowledge;
- gain access to your health data at healthcare providers that verify identity by PESEL number;
- impersonate you, for example when concluding contracts at a distance.

Contact details alone (telephone number, e-mail address), even without any other data, may be used to:

- convincingly impersonate our clinic, a bank or a public authority in a telephone call, text message or e-mail in order to obtain money or further data by deception.

Unauthorised use of health data and photographs may infringe your rights, in particular if third parties attempted to use this information:

- to your detriment, including in a way that violates your privacy, personal rights or medical confidentiality;
- for fraud or to put pressure on you, e.g. by contacting you and referring to knowledge of your past treatment.

What can you do?

If you have a PESEL number

- You can restrict (zastrzec) your PESEL number free of charge in the mObywatel mobile app, online at mObywatel.gov.pl, or in person at any municipal office (urząd gminy or urząd miasta). When concluding contracts, financial institutions are required to check whether a PESEL number is restricted, which reduces the risk of liabilities being incurred in your name. Restricting your PESEL number does not prevent you from registering with a doctor, collecting a prescription or dealing with public offices. The mObywatel service also shows who checked your PESEL number and when.
- You can inform other healthcare providers you use that third parties may attempt to use your PESEL number.

If your passport number was recorded

- We recommend contacting the authority that issued your passport (e.g. the relevant consulate or the competent authority in your country) to find out whether the document can be flagged as compromised or replaced.
- Please pay attention to any correspondence concerning contracts or liabilities concluded without your knowledge and clarify it without delay.

Contact details and health data

- Please be particularly careful with unexpected telephone calls, text messages and e-mails whose sender refers to your treatment, to our clinic or to the data breach, especially if the message contains a link and invites you to “check whether your data has leaked”.
- Please do not provide passwords, codes or any additional data in response to such contacts. Our clinic does not ask for them by telephone, text message or e-mail. In messages about this incident we refer only to our website drosuch.pl. If you receive an unusual request that appears to come from us, please confirm it by calling +48 501 093 653.
- If it is confirmed that your data has been used by unauthorised persons, you may seek protection of your rights under the applicable law, including the Polish Civil Code.

Regardless of the scope of the data, if you suspect that it has been used unlawfully, you can report this to the Police.

What action has been taken?

To limit the effects of the attack, according to the information provided to us, Qbusoft sp. z o.o. has:

1. removed the vulnerability exploited by the perpetrator and other identified vulnerabilities, and tested the fixes;
2. reviewed the application's source code for further vulnerabilities;
3. changed all access credentials that may have fallen into the perpetrators' hands;
4. introduced additional monitoring of servers and applications and blocking of suspicious traffic;
5. reported the incident to the Central Cybercrime Bureau (CBZC), the President of the Personal Data Protection Office (UODO), CSIRT NASK, the e-Health Centre (Centrum e-Zdrowia) and the Social Insurance Institution (ZUS);
6. been monitoring whether the data affected by the incident has been made public;
7. announced an independent external security audit.

Our clinic, as the controller of patients' personal data, has taken the following action:

- on 2 and 6 October 2026 we requested Qbusoft sp. z o.o. to provide detailed information on the scope and causes of the breach;
- on the basis of the replies received, we determined the scope of the breach affecting our clinic;
- we notified the breach to the President of the Personal Data Protection Office in accordance with Article 33 GDPR;
- on 8 October 2026 we sent individual notifications to the patients whose e-mail addresses we held, and we are informing by text message those for whom we hold only a telephone number;
- we changed the passwords of all system users at our clinic and reviewed accounts and access rights;
- we are following the announcements of Qbusoft and the competent authorities on an ongoing basis and will publish any significant new findings here.

Where can you get further information?

Our clinic reception, tel. **+48 501 093 653**, will provide information about the incident, tell you what data was recorded in your case and, at your request, send you the full notification by e-mail or by post. The notification is available in Polish and English.

For matters concerning the protection of personal data processed by our clinic, including this announcement, you can contact our Data Protection Officer, Ms Agata Szwed, by e-mail: **agata.szwed@asprotectis.pl**.

The software provider's official announcements about the incident are published (in Polish) at medyc.pl, under "Komunikaty".

We apologise for this situation and for any concern it may cause.

Yours sincerely,
Piotr Osuch Chirurgia Plastyczna
Warsaw, 20 October 2026