

Privacy Policy – Client Zone

Information on the processing of personal data pursuant to Article 13 of 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) (hereinafter referred to as "GDPR")

The CLIENT ZONE is a digital patient portal intended for clients of the polyclinics of the Penta Hospitals group.

1. CONTROLLER OF PERSONAL DATA

Penta Clinic s.r.o.

Registered office: Na Florenci 2116/15, 110 00 Praha 1

Identification number: 61854093

Registered in the Commercial Register maintained by the Municipal Court in Prague under file no. C 31359.

The Controller collects your personal data, disposes of it, and bears responsibility for its proper and lawful processing.

2. PURPOSES OF PROCESSING AND LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

The purpose of processing personal data is to enable patients (clients of the polyclinics) to:

- register and manage their user account,
- manage care programmes,
- record and manage payments,
- book healthcare services (examinations) and plan them,
- access an overview of services used.

Processing is necessary for the provision of these digital services and for the efficient organisation of healthcare by the provider.

The processing of personal data and health data within the Client Zone is carried out in accordance with the GDPR on the basis of the following legal grounds:

- Article 9(2)(h) GDPR (provision of healthcare),
- Article 6(1)(b) GDPR – performance of a contract (provision of services to the patient),
- Article 6(1)(c) GDPR – compliance with legal obligations of the healthcare services provider,
- Article 6(1)(a) GDPR – consent of the data subject (e.g. for marketing or supplementary services).

In the case of the provision of services to minor patients, personal data are processed to the extent necessary for the provision of healthcare services and in accordance with the relevant legislation.

3. SCOPE OF PERSONAL DATA PROCESSING

The processing of personal data is considered necessary because:

- without patient identification, it is not possible to ensure the correct assignment of services and bookings,
- without contact details, it is not possible to carry out communication (booking confirmations, notifications),
- without payment records, it is not possible to ensure the administration of purchased programmes,
- without booking data, it is not possible to plan and provide healthcare.

The scope of data processed is limited exclusively to those that are necessary for the achievement of the above-stated purposes.

In the context of the use of the mobile application, technical data relating to the device and the application may also be processed, in particular the IP address, device type, operating system, device identifiers, application logs, and diagnostic and operational data necessary for ensuring the security, stability, availability, and proper functioning of the application.

The application may send push notifications related to the provision of services, bookings, or the management of the user account. The user may change the notification settings on their device.

The application may use analytical and diagnostic tools for the purpose of ensuring functionality, security, and the improvement of services.

4. CATEGORIES OF PERSONAL DATA SUBJECT TO PROCESSING

For the above-stated purposes, the Controller processes the following categories of personal data:

- identification data (first name, surname),

- contact details (e-mail, telephone, address),
- user account data,
- technical and operational data,
- booking and service usage data,
- payment data,
- health insurance data,
- health data and healthcare services data.

5. RECIPIENTS OF PERSONAL DATA

Clients' personal data are disclosed exclusively to authorised employees of the Controller and are further transferred only to the extent necessary to external processors who ensure the operation and support of services. In the event that external processors are used, the protection of your data is always ensured by contractual and technical means. The transfer of personal data may also occur where required by law, in particular to public authorities or supervisory bodies. All transfers are carried out in accordance with applicable legislation, in particular the requirements of the GDPR.

Where the provision of services involves the transfer of personal data outside the European Economic Area, this is always carried out in accordance with the GDPR and on the basis of appropriate personal data protection safeguards.

6. SECURITY AND RETENTION PERIOD OF PERSONAL DATA

The Controller has adopted appropriate technical and organisational measures to secure personal data against unauthorised access, loss, misuse, or damage.

Personal data are retained for the duration of the user account and thereafter for the period stipulated by legislation in the field of healthcare services provision and the maintenance of medical records.

7. RIGHTS OF THE DATA SUBJECT

You have the right:

- to access personal data pursuant to Article 15 GDPR,
- to rectification of inaccurate personal data pursuant to Article 16 GDPR,
- to request the erasure of your personal data pursuant to Article 17 GDPR,
- to object to processing pursuant to Article 21 GDPR,
- to restriction of processing pursuant to Article 18 GDPR,
- to data portability to the extent stipulated by applicable legislation pursuant to Article 20 GDPR,
- to lodge a complaint with the Office for Personal Data Protection if you consider that the Controller is processing personal data in breach of the GDPR,

- to withdraw consent granted for the processing of personal data (e.g. for marketing purposes), by means of a written notice sent to the Controller's address (please mark the envelope "GDPR").

Within the Client Zone, no automated decision-making or profiling takes place that would have legal effects for the data subject.

The application does not track users for the purpose of targeted advertising and does not transfer personal data to third parties for marketing purposes without the user's consent.

8. MANNER OF EXERCISING THE RIGHTS OF THE DATA SUBJECT

The manner of exercising your rights is set out in document SP8026 – Procedure for the Exercise of Data Subject Rights on the Penta Hospitals (Poliklinika Florenc) website, where F80005 – Request for the Exercise of Data Subject Rights is also available.

Your request shall be dealt with without undue delay, and at the latest within one month. In exceptional cases, in particular due to the complexity of your request, we are entitled to extend this period by a further two months. We shall of course inform you of any such extension and the reasons therefor.

Data Protection Officer: Mgr. Renata Macková, renata.mackova@kplusm.cz, tel. 774 059 522.

This document is effective from: 1 April 2026