

PRIVACY POLICY

EZKarta mobile application

Controller: Ministry of Health of the Czech Republic

Last updated: 1 September 2026

In brief: After identity verification, EZKarta enables patients to view data held in healthcare information systems established by law. Deactivating or uninstalling the application removes the data stored by the application on the phone, but not data held in source registers and systems, whose retention is governed by legislation.

1. About this Privacy Policy

This Privacy Policy explains how the Ministry of Health of the Czech Republic (hereinafter referred to as the 'Czech Ministry of Health', the 'Ministry' or 'we') handles users' personal data and health data in connection with the operation of the EZKarta mobile application. In particular, it describes the categories and sources of data, the purposes and legal bases of processing, recipients, security, retention periods and deletion options.

Pursuant to Section 27(1)(h) and Section 35a of Act No. 325/2021 Coll., on the Electronisation of Healthcare, as amended, EZKarta is a central electronic healthcare service. After unambiguous identity verification, it enables patients to view data about them held in the National Health Information System, registers established under the Public Health Protection Act, the ePrescription system, medical records and the Integrated Data Interface.

Use of EZKarta is voluntary. Not using or deactivating the application has no effect on the provision of health services or on data held in information systems established by law.

2. Personal data controller and contact details

The controller of personal data processed in connection with the provision of EZKarta is the Ministry of Health of the Czech Republic, Palackého náměstí 4, P.O. BOX 81, 128 01 Prague 2, Company ID No.: 00024341.

You may contact the Data Protection Officer by email at oia@mzcr.cz or in writing at: Data Protection Officer, Ministry of Health of the Czech Republic, Palackého náměstí 4, P.O. BOX 81, 128 01 Prague 2.

For questions about how the application works, please call 1221 or email linka1221@mzcr.cz.

3. How EZKarta obtains and displays data

Users sign in using a Citizen Identity authentication method. The application does not create a separate user password. For subsequent access, it may use the security features of the mobile device, in particular the system PIN, facial recognition or fingerprint authentication. Biometric templates are processed by the device's operating system; EZKarta receives only information indicating whether authentication was successful or unsuccessful.

After sign-in, the application obtains data from source systems established by law and displays it for the currently selected person. This may be the user, the user's minor child, a person represented by the user by operation of law, or a person who has granted the user the relevant authorisation. The scope of access is verified through the Permissions Register and other authoritative sources.

EZKarta primarily provides secure access to information and services. It does not create most of the health data; it displays data held by healthcare providers, health insurance companies, the Czech Ministry

of Health, the Institute of Health Information and Statistics of the Czech Republic (IHIS CR), the State Institute for Drug Control and other entities designated by law.

4. Data and functions processed by EZKarta

4.1 Identification, profile and authorisations

The application may display or use, in particular, the first name, surname, date of birth, address and contact details, the healthcare sector patient identifier (RID), health insurance information, registered healthcare providers, representation authorisations and a list of persons whose data the signed-in user is authorised to access. The QR code in the profile may contain the RID of the selected person.

Users may update their contact details through the available service; the new values are stored in the relevant central system. Incorrect core data, health insurance information or registered healthcare providers may be challenged using the procedure offered in the application or through designated public services.

4.2 Overview, favourite services and settings

The Overview shows the currently selected person, the status of selected preventive care entitlements and the user's selected favourite services. The application also processes user settings, such as the selected appearance, favourite items and the application's activation status on the device.

4.3 Vaccination Record and EU Digital COVID Certificates

The Vaccination Record displays vaccination information for the selected person. The data may come, in particular, from the National Register of Reimbursed Health Services (vaccinations covered by public health insurance from 2010 to 2022) and from the OCKO module of the Infectious Disease Information System (vaccinations from 1 January 2023). The displayed information may include the vaccinated person, disease, vaccine name and batch, date and sequence number of the dose, route of administration and identification of the healthcare provider.

Where the function is available in the current version, EZKarta may retrieve, store and display EU Digital COVID Certificates, their QR codes, the holder's identification details, vaccination, test or recovery information, the issuing entity, country, date of issue and unique identifier. Certificates are stored in the application's protected storage on the device, and the user may choose to display or share them.

At the user's request, a Vaccination Record or certificate may be exported, for example as a PDF, or shared with a recipient selected by the user. Data is not transferred automatically and an active action by the user is required.

4.4 Preventive care, screening programmes and other health information

EZKarta may display information about completed preventive examinations and screening tests, including their types, dates, number of visits and healthcare provider. The overview may be tailored according to age, sex and care already received.

It may also display laboratory results, including the type of test, measured values, units, reference ranges, result date and result history; medical assessments, including the type of assessment, conclusion and validity period; and information about blood or plasma donation, in particular the periods in which donations took place and indicative information about eligibility for another donation.

4.5 Shared Health Record

The Shared Health Record is a central service under Act No. 325/2021 Coll. It includes the Emergency Health Record and the results of preventive and screening examinations.

Pursuant to Section 34a of that Act, the Emergency Health Record may contain, in particular:

- blood group;

- allergies;
- adverse, serious adverse and unexpected adverse reactions to medicinal products;
- adverse events and serious adverse events related to medicinal products;
- serious adverse reactions and events related to the collection of blood or a blood component, or to a transfusion;
- medicinal products dispensed during the preceding 12 months, as recorded in the medication record;
- medicinal products administered during inpatient care in the preceding 12 months.

For medicinal product data, the 12-month period is the scope of data displayed in the Shared Health Record; it is not necessarily the retention period of the original record in the source system.

4.6 Health Record Deliveries and My Documents

Health Record Deliveries comprise medical records, or parts thereof, transferred through health information exchange network services. EZKarta displays deliveries addressed to the selected person. The user may collect a delivery and download it to the phone or, where this function is available and the user has given the relevant consent, move it to My Documents.

My Documents may contain medical records or medical imaging documentation stored for longer-term availability. Users may view, download and permanently delete documents. Withdrawal of consent to automatic storage stops further deliveries from being stored; documents stored previously remain available until the user deletes them or another legal ground for their deletion arises.

4.7 Medicinal products and external services

EZKarta may offer users a link to the ePrescription application or web interface and links to public medicinal product databases. After moving to an external application or website, any further processing of personal data is governed by the privacy policy of the relevant operator. EZKarta may also display public links to healthcare institutions and services.

4.8 Technical and operational data

To ensure the application's functionality and security and to improve it, we process technical and operational data, such as the application version, crash and error data, information about features used and data required to record updates. Under the current technical configuration, Google services Firebase Crashlytics, Firebase Remote Config and Google Analytics are used.

Telemetry data sent to these services does not include a telephone number, IMEI or advertising identifier and is not linked within EZKarta to the user's name, RID or health data. It is not used for advertising, marketing profiling or the sale of personal data.

4.9 Mobile device permissions

EZKarta may request access to the camera only when the user initiates the QR code scanning function. Access to biometric authentication is provided by the device's operating system. When exporting a document, the user may select a storage location or another application; subsequent handling of the exported file is then controlled by the user and the relevant operating system or service.

5. Purposes and legal bases of processing

We process personal data primarily for the following purposes:

- to verify the user's identity and authorisation to access the selected person's data;
- to provide central electronic healthcare services and make data available to the patient;
- to securely transfer medical records and manage documents selected by the user;
- to ensure security, availability and support, detect errors and protect against misuse;
- to comply with statutory record-keeping, audit and information obligations;
- to evaluate operation and improve the application within the scope of technical telemetry.

The legal basis is primarily compliance with a legal obligation and the performance of a task carried out in the public interest or in the exercise of official authority pursuant to Article 6(1)(c) and (e) of the General Data Protection Regulation (GDPR). The processing of health data is based primarily on Article 9(2)(h) and (i) of the GDPR and the relevant healthcare legislation.

Where the application requests consent for an optional function, such as the automatic storage of deliveries in My Documents, the consent may be withdrawn. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal or data that must continue to be held under legislation. Viewing health data held by law through EZKarta is not based solely on the user's consent.

6. Who may have access to the data

Only authorised persons have access to personal data, to the extent necessary for their tasks. The following entities, in particular, may participate in the operation of the application:

- the Ministry of Health of the Czech Republic, as controller;
- the Institute of Health Information and Statistics of the Czech Republic, as the operator of selected systems and a processor;
- the National Agency for Communication and Information Technology, state enterprise, as an integrator or technical supplier of selected services;
- other contracted IT, support, connectivity and security suppliers bound by confidentiality, the controller's instructions and data protection requirements;
- public authorities or other entities where disclosure is required by law;
- a recipient selected by the user when sharing or exporting data or a document.

When services provided by international suppliers are used, technical data may, depending on the service configuration, also be processed outside the European Economic Area; in such cases, appropriate safeguards under the GDPR are applied.

7. Data security

Data is protected by technical and organisational measures appropriate to its sensitivity. These include, in particular, identity verification through Citizen Identity, authorisation management, encrypted communication, protected application storage, access secured by a PIN or the device's biometric authentication, separation of health data from technical telemetry, access management for authorised staff and the logging of significant activities.

Users should protect their devices, must not disclose their access PIN to another person, and should always check the recipient and the scope of the data being transferred before sharing it.

8. Data retention and deletion

Retention periods differ depending on whether data is stored only on the phone, in temporary storage, in the user's My Documents section, in a source healthcare system or in operational logs. EZKarta is neither the sole nor the original repository of most of the health data it displays.

Category	Retention period and method of deletion
Application data on the mobile device	For as long as the application remains activated on the device. Selecting 'Deactivate application' or uninstalling the application removes data stored by the application on the device. This does not erase data held in central source systems.
COVID-19 certificates and other locally stored outputs	Until the relevant content is deleted, the application is deactivated or it is uninstalled. Files exported outside EZKarta remain in the destination storage until they are deleted by the user or by the operator of that storage service.
Health Record Deliveries in temporary storage	Until collected by the addressee, for no longer than 30 days from the date of storage. After this period, the delivery is irreversibly deleted (Section 31(3) of Act

Category	Retention period and method of deletion
	No. 325/2021 Coll.).
Documents in My Documents	Until the user permanently deletes them or a legal ground for their deletion arises. Withdrawal of consent to automatic storage stops new deliveries from being stored, but does not itself delete documents already stored.
Core patient data	For 50 years from the date of the patient's death or from the date on which a decision declaring the patient dead becomes final (Section 8(2)(c) of Act No. 325/2021 Coll.).
Data in the Permissions Register	For 10 years from the patient's death or declaration of death (Section 32(8) of Act No. 325/2021 Coll.).
Activity log records	For 2 years from the date of creation (Section 8(2)(d) of Act No. 325/2021 Coll.).
Medicinal products in the Shared Health Record	In the Shared Health Record, EZKarta makes available medicinal products dispensed or administered during inpatient care in the preceding 12 months. Original records may be retained for longer in the source systems in accordance with the relevant legislation.
Other health data in source systems	For the period prescribed by legislation for the relevant register, information system or medical records, and for as long as necessary for the statutory purpose. Deactivating or uninstalling EZKarta does not erase this data.
Technical telemetry	For no longer than 180 days from collection, unless the specific data is deleted or aggregated earlier.

8.1 What happens upon deactivation or uninstallation

Deactivation removes EZKarta data from the device and starts a new application initialisation process. Uninstallation removes application data in the manner provided by the operating system. These steps do not cancel a Citizen Identity authentication method, delete data held in statutory registers and source systems, or by themselves cancel authorisations recorded outside the device.

8.2 Deleting a document and exported files

When a user confirms the deletion of a document in My Documents, the file is irreversibly removed from that storage, as provided by the application's functionality. Any copy previously downloaded by the user to a phone, cloud storage, email or another application is not deleted and must be removed from the relevant destination storage.

9. Sharing data under the user's control

EZKarta does not automatically transfer health data from optional functions to another recipient. Users may choose to display a QR code, export a PDF, download a document, open an external application or website, or share information with a selected recipient. Before confirming, users should check the scope of the data and the recipient's identity.

The recipient and the operator of the destination service are also responsible for any further handling of data after the user has knowingly exported or transferred it. When users share data concerning a person they represent, they may do so only within the scope of their authorisation and in that person's interests.

10. Rights of the data subject

To the extent provided for by the GDPR and applicable legislation, you have, in particular, the right to:

- obtain information about processing and access your personal data;

- request the rectification of inaccurate data or completion of incomplete data; where data has been obtained from a source system, it must be rectified by the entity authorised to amend that data;
- request erasure or restriction of processing where the statutory conditions are met; the right to erasure does not apply to the extent that retention is necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest;
- object to processing based on the performance of a task carried out in the public interest, where permitted by the nature of the processing;
- withdraw consent to an optional function where the relevant processing is based on consent;
- lodge a complaint with the Office for Personal Data Protection.

Uninstalling or deactivating EZKarta does not constitute a request to erase data from source healthcare systems. A request concerning centrally held data will be assessed according to the legal regime applicable to the relevant system and, where appropriate, referred to the competent controller or the person who entered the data.

11. Minors and represented persons

EZKarta may allow access to data concerning minors or other represented persons where such authorisation arises by operation of law or is recorded in the relevant register. The fact that a person is displayed in the application does not mean that their data may be shared further without restriction. Users must respect the scope of their authorisation, the represented person's privacy and the purpose for which they use the data.

12. Legislation

Processing is governed in particular by the following legislation, as amended:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR);
- Act No. 110/2019 Coll., on the Processing of Personal Data;
- Act No. 325/2021 Coll., on the Electronisation of Healthcare;
- Act No. 372/2011 Coll., on Health Services;
- Act No. 373/2011 Coll., on Specific Health Services;
- Act No. 378/2007 Coll., on Pharmaceuticals;
- Act No. 258/2000 Coll., on the Protection of Public Health;
- Act No. 48/1997 Coll., on Public Health Insurance.

13. Complaints and supervision

If you believe that we are processing personal data in breach of the law, you may contact the Czech Ministry of Health's Data Protection Officer or lodge a complaint with the Office for Personal Data Protection, Pplk. Sochora 27, 170 00 Prague 7.

Website of the Office for Personal Data Protection: [Office website](#)

14. Amendments to this Privacy Policy

We may update this Privacy Policy when legislation, functions, source systems or technologies change. The current version, including the date of the latest update, will be published on a publicly accessible page; material changes may also be announced in the application.