Data Protection Statement Telemedicine

Status: 2026

University Clinic of Dentistry

hereinafter referred to as "UZK"

1. Data Controller

Universitätszahnklinik Wien GmbH
Sensengasse 2a, 1090 Wien, Österreich
E-Mail: office-unizahnklinik@meduniwien.ac.at | Web: https://www.unizahnklinik-wien.at/

Data protection officer:
VACE Systemtechnik GmbH, E-Mail: datenschutz-unizahnklinik@meduniwien.ac.at.

2. Purpose of Data Processing, Data Categories und legal basis

UZK processes your personal data in compliance with the **General Data Protection Regulation (GDPR)** and the **Austrian Data Protection Act (DSG)**. The fundamental principles applied by UZK are:

Lawfulness: Your personal data are processed exclusively on the basis of a valid legal basis.
Transparency: We provide clear information about how your personal data are processed.
Data minimisation: Only personal data that are necessary for the respective purposes are processed.
Security: Your personal data are protected against misuse.
Confidentiality: Your personal data are treated confidentially.

a) Purposes of Processing

UZK processes personal data of patients exclusively for the purpose of **medical treatment and administrative management in the context of telemedical services**. In particular, this includes:

- conducting telemedical consultations
- diagnosis and treatment of dental, oral and maxillofacial diseases
- fulfilment of statutory documentation obligations (maintenance of medical records)
- billing of services rendered to patients or their insurance providers (statutory health insurance or private insurers)
- scheduling of telemedical consultations and treatments
- contacting patients via email or telephone

UZK also processes patient data in the context of **scientific research and university education**. Processing is carried out exclusively on the basis of applicable legal provisions, in particular:

- Art. 6 (1) (e) GDPR – task carried out in the public interest
- Art. 9 (2) (j) GDPR – processing for scientific research purposes
- § 2d DSG – scientific research
- § 51f Austrian Medicinal Products Act (AMG) – clinical trials
- § 7 (2) (2) Austrian Research Organisation Act (FOG)

The following protective measures are implemented:

- **Pseudonymisation or anonymisation:** Personal data are processed in pseudonymised or anonymised form wherever possible in order to minimise the identifiability of the data subjects.
- **Access restriction:** Access to personal data is limited to authorised persons and is granted on the basis of a role-based access control system.
- **Transparency and information:** Patients are comprehensively informed about data processing for research and educational purposes and about their rights.

- **Consent:** Where required by law, explicit consent will be obtained prior to processing. Consent is voluntary and may be withdrawn at any time.

Documentation and monitoring: Compliance with data protection requirements is regularly reviewed and documented. Disclosure of data to external research institutions or cooperation partners takes place only in accordance with legal requirements and, where necessary, following prior consent of the data subjects.

b) Categories of Data

For the above purposes, UZK processes health data and administrative data of patients. This includes in particular:

- **Master data**: name, title, date of birth, gender, nationality
- **Contact data**: address, email address
- **Social security data**: e.g. social security number
- **Treatment data**: medical history, findings and diagnoses, therapies and medical procedures performed, medication, X-ray and CT images, laboratory results, medical reports and other documentation relating to the patient's medical history
- **Access and usage data**: IP address, date and time, browser type, operating system, referrer URL, date and time of video connection, login activities
- **Communication data**: video consultation logs, date and time of communication, telephone logs
- **Analytics data**: pseudonymised usage statistics
- **Cookie data**: technical session cookies, consent cookies where applicable
- **Billing data**: details of health insurance providers or other cost bearers, documentation of services, billing data (services rendered, fees, payment information)

c) Legal Basis

The protection of your personal data is of particular importance to us. Your data are therefore processed exclusively on the basis of statutory provisions, in particular:

- **Treatment contract** – Art. 6 (1) (b) GDPR (e.g. telemedical consultation)
- **Compliance with legal obligations within the framework of education** – Art. 6 (1) (c) GDPR
- **Task carried out in the public interest (university teaching)** – Art. 6 (1) (e) GDPR
- **Protection of vital interests** – Art. 6 (1) (d) GDPR
- **Consent** – Art. 6 (1) (a) GDPR and Art. 9 (2) (a) GDPR

Statutory retention obligations include:

- treatment data: up to **30 years** pursuant to § 1489 Austrian Civil Code (ABGB)
- billing data: at least **7 years** pursuant to § 132 Federal Fiscal Code (BAO)

Within UZK, your personal data are accessible only to those departments that require them for the fulfilment of the purposes stated above (e.g. treating physicians, assistants, billing department).

3. Recipients of Data

UZK transfers personal data to external parties only in the following cases:

- **Health insurance institutions and billing entities**: Data necessary for billing (e.g. name, social security number, treatment date, services provided) are transmitted to your statutory health insurance provider or private insurance company.
- **External healthcare providers**: Medical findings or documents may be shared with co-treating physicians or external healthcare institutions (e.g. specialist referrals, hospitals), generally only with your consent or at your request. In urgent cases requiring further treatment, such data may be transferred on the basis of implied consent or, where necessary, on the legal basis mentioned above.
- **Laboratories**: External laboratories may be commissioned for diagnostic analyses (e.g. blood tests or tissue samples). For this purpose, samples and necessary personal data (e.g. sample codes, gender, date of birth for interpretation) are transmitted to the contracted laboratory.
- **Authorities and public bodies**: Where statutory reporting obligations exist or official requests are made, UZK may transmit data to competent authorities (e.g. reporting certain infectious diseases pursuant to the Epidemics Act).
- **Legal representatives**: Where patients are minors or legally incapacitated, relevant data may also be communicated to legal guardians or authorised representatives where necessary for medical decisions and consent to treatment.
- **Processors**: Cisco WebEx
  Cisco Systems, Inc., San Jose, USA
  Purpose: video conferencing for telemedical consultations and treatments.
  Data transfers to third countries (USA) may occur.
  The legal basis for such transfers is the **EU-US Data Privacy Framework** or **Standard Contractual Clauses**.

External recipients receive personal data only to the extent necessary for the respective purpose and are bound by confidentiality obligations. No further disclosure to third parties (e.g. for marketing purposes) takes place unless you have explicitly consented or UZK is legally obliged to do so.

4. Transfers to Third Countries

UZK itself does not transfer data outside the EU or EEA.

However, transfers to third countries may occur through processors. In such cases, appropriate safeguards (e.g. EU-US Data Privacy Framework or EU Standard Contractual Clauses) are implemented.

5. Storage Period

Personal data are deleted once the purpose for which they were collected has been fulfilled and no statutory retention obligations prevent their deletion.

Medical record data are generally retained by UZK for **up to 30 years from the last entry**. This extended retention period serves purposes of medical follow-up care and the defence of potential legal claims.

6. Automated Decision-Making

No automated decision-making or profiling within the meaning of **Art. 22 GDPR** takes place.

7. Online Systems and Digital Communication

Our website is operated in accordance with current security standards.

All personal data transmitted via our website are transferred exclusively through **encrypted connections (SSL/TLS)**.

Access to personal data is restricted to authorised persons, based on a role-based access concept, and all access is logged.

Technical and organisational measures in accordance with **Art. 32 GDPR** are implemented to ensure data security.

8. Confidentiality in Website Operations

All persons involved are bound by confidentiality obligations. Data access is granted according to the **“need-to-know” principle**.

9. Rights of Data Subjects

Data security is also a high priority with regard to the rights of data subjects. Therefore, data subjects can only assert their rights after they have been unequivocally identified.

Every data subject whose personal data is processed by UZK has the following rights:

- Right of access (Art. 15 GDPR): You can request information about whether and which personal data we process about you.
- Right to rectification (Art. 16 GDPR): You have the right to have incorrect or incomplete personal data corrected.
- Right to erasure (Art. 17 GDPR): You can request the deletion of your personal data, provided that no legal retention obligations stand in the way.
- Right to restriction of processing (Art. 18 GDPR): You can request that your data only be processed to a limited extent, e.g. during an examination of your objections.
- Right to data portability (Art. 20 GDPR): You have the right to receive your provided data in a structured, common format or to have it transferred to another controller.
- Right to object (Art. 21 GDPR): You can object to the processing of your data for reasons arising from your particular situation.
- Withdrawal of consent (Art. 7 para. 3 GDPR): You can withdraw consent given at any time with effect for the future.

To exercise your rights, you can contact us in writing by post or by e-mail (datenschutz-unizahnklinik@meduniwien.ac.at) at any time or visit us personally.

10. Technical and Organizational Measures

These include in particular:

- access restrictions

- encryption
- data protection training
- data minimisation
- regular security audits
- secure data transmission in online services

All UZK employees are contractually obliged to maintain confidentiality and are regularly trained in the secure handling of personal and sensitive data.

a) Data Security when Using WebEx

WebEx uses **HTTPS encryption**. You can recognise this by:

- the URL beginning with **https://**
- a **padlock symbol** in the address bar

Your personal data are transmitted in encrypted form.

WebEx is a secure video conferencing platform provided by Cisco and widely used by companies and healthcare providers worldwide.

b) WebEx collects the following technical data:

- IP address of the device
- device information (type, operating system)
- connection quality
- connection duration
- error messages

c) WebEx does not process:

- video content (unless recording is activated)
- audio content (unless recording is activated)
- health data
- medical information

d) Recording of WebEx sessions

Important: recordings are only possible with your consent.

- Sessions are **not recorded by default**
- If a recording is planned, your consent will be obtained in advance
- You may consent to or refuse the recording
- Recordings are used solely for **medical documentation or training purposes**

If recordings are made:

- they are stored with the same level of security as other data
- they are deleted promptly unless statutory retention obligations apply
- access is restricted to authorised persons only

11. Continuous Control and Improvement

Continuous improvement of quality and processes is a top priority at UZK. Compliance with data protection guidelines and applicable laws, as well as the effectiveness of data protection and data

security measures, are continuously monitored and optimized to ensure the smooth implementation of data protection measures.

12. Right to Lodge a Complaint

You have the right to lodge a complaint with the Austrian Data Protection Authority, Barichgasse 40-42, 1030 Vienna, dsb@dsb.gv.at.