Information on the Processing of Personal Data by the Provider

1. Legal Basis for Processing under the GDPR

The data processing is based on the performance of a contract pursuant to Article 6(1)(b) of the GDPR.

The purpose of processing personal data is effective communication during the provision of healthcare services to users—patients who do not speak the official language of the Czech Republic—via the Application. These data are provided voluntarily, and the Application remains fully functional without their submission.

Roles of the Parties in the Processing of Personal Data

The healthcare service provider acts as the *Controller* of personal data, deciding on the purposes and means of processing.

The company *Language solutions s.r.o.*, as the provider of the Galenio Application, acts as the *Processor* of personal data, processing data on behalf of the Controller based on a data processing agreement in accordance with the GDPR.

---

2. Data Retention Period

Patients' personal data (including chat history) are retained for 24 hours from the moment they are submitted by the patient and are then automatically deleted.

The data are deleted from the Application as well as from third-party services. A list of these third parties is available below.

User account data of doctors are retained for the duration of the contractual relationship and further in accordance with statutory archiving obligations.

---

3. Data Processor

Personal data are processed on behalf of the Controller by a Processor, in accordance with Article 28 of the GDPR.

The Processor is *Language solutions s.r.o.*, with its registered office at Nové sady 988/2, 602 00 Brno, Company ID: 19590024.

The Processor processes personal data solely on behalf of and according to the instructions of the Controller and may not use the data for its own purposes.

Key responsibilities of the Provider as Processor include:

- Processing personal data solely for the purpose of operating the Application and delivering its functionalities.
- Ensuring a high level of personal data security, including data encryption and restricted access.
- Notifying the Controller of any security incidents and cooperating in their resolution.
- Maintaining records of processing activities and allowing the Controller to perform audits.
- Upon termination of cooperation, deleting or anonymizing personal data as instructed by the Controller.

4. Commitment to Processing Only Necessary Data

The Provider processes only the personal data that are essential for the operation of the Application and the fulfillment of the contractual purpose. Processing is carried out to the minimum extent necessary to enable communication between the patient and the doctor.

Data Minimization

- The Provider processes only the personal data necessary to enable communication between doctors and foreign patients, ensure the operation of the Application, and maintain its security.
- No data that are not required for the above purposes will be collected, processed, or stored.

Types of Processed Data

- **Identification data** – patient's first name, last name, date of birth, nationality, gender, doctor's first name and last name.

- **Contact data** – doctor's email address.

- **Sensitive data (Article 9 of the GDPR)** – patient's health-related information, if entered into the chat or forms.

Purpose Limitation

- Personal data are processed exclusively to enable communication between the doctor and the patient and to manage doctors' user accounts.

- The data will not be used for marketing or analytical purposes.

---

5. Method of Processing

The Provider processes personal data exclusively in electronic form, with an emphasis on security and privacy protection. The technologies used comply with the requirements of the GDPR and ensure a high level of personal data protection against unauthorized access, loss, or misuse.

Infrastructure and Data Storage

- Personal data are stored in a database hosted on the servers of the cloud service provider HostArmada.com, with physical server locations in Frankfurt am Main, Germany.

- Data are processed and stored exclusively within the European Union, ensuring their protection in accordance with the GDPR.

- Servers are protected against unauthorized access through multi-level security measures, including firewalls and network traffic monitoring.

Security

Detailed information on data security and encryption is provided below in the section **“Data Security.”**

6. Controller’s Obligations in Managing Personal Data

The **hospital**, as the **data controller**, undertakes to ensure that personal data processing within the Application complies with the GDPR and other relevant legal regulations. The main responsibilities of the controller include:

Ensuring Lawful Processing

- The controller is responsible for ensuring that all processing of patients' personal data is based on a legal basis, especially pursuant to Articles 6 and 9 of the GDPR.

- The controller will ensure that patients are properly informed about the processing of their personal data and that, if required, their explicit consent is obtained.

Use of the Application

- The controller is obliged to use the Application in accordance with its intended purpose.

---

7. Processor’s Obligations in Managing Personal Data

The **Provider**, as the **data processor**, acts based on the controller’s instructions and undertakes to ensure that the processing of personal data complies with the GDPR. Its main obligations include:

Processing Data Only Based on the Controller’s Instructions

- The processor may process personal data only to the extent and for the purposes defined in the agreement.

- The processor may not use the personal data for its own purposes.

- If the controller requests deletion or modification of personal data, the processor must fulfill the request without delay.

Ensuring Data Security

- The processor commits to implementing technical and organizational measures to protect personal data against unauthorized access, loss, misuse, or leakage.

- Technical measures are detailed in the section **"Data Security"** below.

Reporting Security Incidents

- If the processor detects a personal data breach, it must inform the controller no later than **24 hours** after detecting the incident.

- The processor must provide the controller with all available information about the incident, including:

    - The **nature of the incident**

    - The **impact on personal data**

    - The **measures taken** to resolve the issue and prevent future incidents

- The processor commits to cooperating with the controller in resolving the incident and assisting in any reporting to supervisory authorities.

Cooperation in Exercising Data Subjects' Rights

- The processor must enable the controller to respond to patient requests regarding the exercise of their rights (e.g., data deletion, data access…).

Termination of Processing and Data Deletion

- After the end of the cooperation or upon the controller's request, the processor must:
    - **Immediately delete or anonymize** all personal data it processed on behalf of the controller.

8. Processor's Obligations in Case of a Security Breach

In the event of a **personal data breach** that may lead to accidental or unauthorized access, loss, or leakage of personal data, the **Provider** (Processor) commits to act in accordance with the following rules:

Immediate Notification to the Controller

- The Provider must inform the Controller **without undue delay**, and no later than **24 hours** after discovering the incident.

- The notification must include:

    1. **Description of the incident** – what happened and which data was affected.

    2. **Consequences of the incident** – potential impact on patients, doctors, or other individuals.

    3. **Corrective measures** – steps taken to resolve and mitigate the damage.

Cooperation in Incident Resolution

- The Processor must fully cooperate with the Controller in resolving the incident and provide all necessary information.

- Upon the Controller's request, the Processor must conduct an internal audit and provide a report with findings and recommendations to improve security.

Implementation of Corrective Measures

- The Provider commits to immediately implementing appropriate technical and organizational measures to prevent recurrence of the incident.

- If necessary, the Provider shall update security protocols and strengthen data access protections.

Obligation to Keep Records of Incidents

- The Processor is obliged to maintain **records of all security incidents**, including their cause, impact, and corrective measures taken, for at least **5 years**.

- Upon the Controller's request, the Processor must provide a copy of these records.

---

9. Processor's Remuneration

The **processing of personal data** by the Provider (Processor) is included as part of the services provided by the Application and **its cost is fully covered by the subscription fee** paid by the Controller.

Specification of Processed Data Types, Their Security and Lifecycle

Data Lifecycle

User Accounts of Doctors and Hospital Information

1. Data Collection:

a) From hospitals during the creation of hospital and doctor accounts.
b) From doctors when changing their passwords.

2. Data Management:

a) Data is stored in a database on servers hosted by HostArmada.com. These servers are physically located in Frankfurt, Germany.
b) Data is deleted upon the deletion of the hospital or doctor user account.

Patient Data and Chat History

1. Data Collection:

a) Patients may enter their identification data and general information into the chat and connection form.
b) Patients then send messages in the chat, which contain general and **sensitive data**.
c) Doctors also send messages in the chat that may include general and **sensitive data**.
d) Doctors can export communication and patient data into a PDF file.

Data Security

1. Technical Security:

a) All data is encrypted. Decryption keys are stored in the patient's and doctor's browsers. The key is not stored on the server.
b) Security function: When a patient sends a message, it is sent in plaintext to the server, where it is encrypted using a key stored in the authentication token (RoomToken) shared by the patient and doctor. The message is then stored

encrypted in the database and decrypted when delivered to the doctor.
c) Daily backups of the database and application code are performed at 4:30 AM.
d) Access logging: We monitor access to the application and detect suspicious behavior.
e) Password policy: Passwords must be at least 6 characters long and include at least one lowercase letter, one uppercase letter, one number, and one special character.

2. Personnel Security:

a) All employees sign a non-disclosure agreement (NDA).
b) All employees and collaborators are trained in GDPR compliance.
c) All employees use passwords that meet the above-specified password criteria.
d) A record of all vendors with access to personal data is maintained. Data processing agreements in accordance with GDPR are signed with all processors. The list of third parties is available below.

---

3. Supply Chain Security:

a) A record of all suppliers with access to personal data is maintained.
b) Data processing agreements in compliance with GDPR are signed with all data processors.
c) The list of third parties is provided below in this document.

Secured Data Includes:

a) Identification data
b) General information
c) Contact information
d) Sensitive data

Categories of Personal Data

To ensure proper functioning of the Galenio web application, the following categories of personal data are processed:

1. **Identification Data** – Patient's first name, last name, date of birth, nationality, gender; Doctor's first name and last name

2. **Contact Information** – Doctor's email address

3. **General Information** – Non-health-related information shared during communication in the chat interface

4. **Sensitive Data** – All health-related information shared by the patient with the doctor and vice versa during communication

---

Level of Personal Data

The application processes both general personal data (identification and contact data) and **special categories of personal data** under Article 9 of the GDPR, which includes sensitive health-related information.
An **explicit consent** is required from the patient for processing sensitive data. The patient gives this consent by checking a box after being informed about data processing practices within the application. The consent is specific, informed, and given for the clear purpose of using the application and sharing data with the doctor.

Processing Operations

All processing operations are described in detail in the section below.

List of Third Parties

1. **OpenAI**
   a. Technology for translations
   b. Provider is located at: 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper,
   Dublin 1, Ireland
   c. In case of sharing information with companies within the OpenAI group, the data processing terms include Standard Contractual Clauses for the transfer of personal data to third countries approved by the European Commission.

2. **HostArmada.com**
   a. Server hosting
   b. Database hosting
   c. Provider is located at: 501 Silverside Rd, Wilmington, Delaware, 19809, USA
   d. The data processing terms include Standard Contractual Clauses for the transfer of personal data to third countries approved by the European Commission.
   e. The servers on which the application is hosted are located in Frankfurt am Main, Germany

3. **Google LLC IPA**
   a. Technology for speech to text and text to speech
   b. Provider is located at: 1600 Amphitheatre Parkway, Mountain View, California, 94043, USA
   c. The provider is a certified entity under the EU-U.S. Data Privacy Framework. In any case, the data processing terms also include Standard Contractual Clauses for the transfer of personal data to third countries approved by the European Commission.

4. **Translated S.r.l.**
   a. Technology for translations
   b. Provider is located at: Via Indonesia 23, 00144 Rome, Italy
   c. In case of information sharing, the data processing terms include Standard Contractual Clauses for the transfer of personal data to third

countries approved by the European Commission.

Table of Personal Data Processing Operations

Type	Category	Operation and purpose of processing	Who processes the information	Security
Patient's first name	Identification data	For the purpose of identifying the patient by the doctor and enabling the use of the application	Language solutions s.r.o. operating the web application galenio.cz, third-party services	Information on the processing of personal and health data – section: Data Security
Patient's last name	Identification data	For the purpose of identifying the patient by the doctor and enabling the use of the application	Language solutions s.r.o. operating the web application galenio.cz, third-party services	Information on the processing of personal and health data – section: Data Security
Patient's date of birth	Identification data	For the purpose of identifying the patient by the doctor and enabling the use of the application	Language solutions s.r.o. operating the web application galenio.cz, third-party services	Information on the processing of personal and health data – section: Data Security
Patient's nationality	Identification data	For the purpose of identifying the patient by the doctor and enabling the use of the application	Language solutions s.r.o. operating the web application galenio.cz, third-party services	Information on the processing of personal and health data – section: Data Security
Patient's	Identification	For the purpose of	Language solutions s.r.o.	Information on the

gender	data	recognizing the patient's gender by the doctor and identifying them	operating the web application galenio.cz, third-party services	processing of personal and health data – section: Data Security
Doctor's first name	Identification data	Serves to enable the registration of the doctor in the application and their identification	Language solutions s.r.o. operating the web application galenio.cz, third-party services	Information on the processing of personal and health data – section: Data Security
Doctor's last name	Identification data	Serves to enable the registration of the doctor in the application and their identification	Language solutions s.r.o. operating the web application galenio.cz, third-party services	Information on the processing of personal and health data – section: Data Security
Doctor's email address	Contact information	For the purpose of creating a doctor’s account in the application	Language solutions s.r.o. operating the web application galenio.cz, third-party services	Information on the processing of personal and health data – section: Data Security
Information recorded in the chat that is not sensitive personal data	General information	For the purpose of providing general information to the doctor. For the purpose of communication	Language solutions s.r.o. operating the web application galenio.cz, third-party services	Information on the processing of personal and health data – section: Data Security
Information recorded in the chat that qualifies as	Sensitive data	For the purpose of enabling treatment of the patient. For the purpose of determining	Language solutions s.r.o. operating the web application galenio.cz,	Information on the processing of personal and

sensitive data under Article 9 of the GDPR and concerns the patient's health condition		diagnosis. For the purpose of communication	third-party services	health data – section: Data Security