Data Processing Agreement

pursuant to Art. 28 of Regulation (EU) 2016/679 (GDPR)

between
Company: _____
Address: _____
Registration / VAT no.: _____
Represented by: _____
(hereinafter the "Controller")

and

SANICURA d.o.o.
Ulica Andrije Hebranga 8, 10000 Zagreb, Croatia
OIB 87611335623 · MBS 081712921 · VAT ID HR87611335623
represented by Martin Eckerstorfer, Director
acting under the brand "sigmacode.io"
Data protection contact: eckerstorfer@sanicura.com
(hereinafter "sigmacode" or the "Processor")

each a "Party", together the "Parties".

> Main agreement / proposal dated _____ (the "Main Agreement")

1. Subject matter and duration

This Data Processing Agreement ("DPA") governs the processing of personal data by the Processor on behalf of the Controller in connection with the services provided under the Main Agreement. Terms such as "personal data", "processing", "personal data breach" and "supervisory authority" have the meaning given to them in the GDPR.

This DPA applies for the term of the Main Agreement and, beyond that, for as long as the Processor processes personal data on behalf of the Controller, in particular until all personal data have been deleted or returned in accordance with Section 9.

2. Nature and purpose of processing; data and data subjects

The nature and purpose of the processing, the categories of personal data, the categories of data subjects, the duration and the location of processing are specified in Annex 1. The Processor shall process personal data only to the extent necessary to perform the Main Agreement.

3. Instructions of the Controller

The Processor shall process personal data only on documented instructions from the Controller, including with regard to transfers to third countries, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

The Main Agreement and this DPA constitute the Controller's initial documented instructions. Further instructions shall be given in text form (e.g. e-mail) and are to be documented by both Parties. Instructions that go beyond the scope of the Main Agreement are treated as a change request.

The Processor shall inform the Controller without undue delay if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. The Processor is entitled to suspend the execution of the instruction concerned until it is confirmed or amended by the Controller.

4. Confidentiality

The Processor shall ensure that all persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. This obligation continues after the end of their engagement. Access to personal data is granted only to the extent necessary for the performance of the Main Agreement.

5. Security of processing

The Processor shall implement the technical and organisational measures ("TOMs") required pursuant to Art. 32 GDPR, as set out in Annex 2, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects.

The TOMs are subject to technical progress and further development. The Processor may implement adequate alternative measures, provided that the level of protection of the measures set out in Annex 2 is not reduced. Material changes shall be documented and communicated to the Controller on request.

6. Sub-processors

The Controller grants the Processor general written authorisation to engage sub-processors. The sub-processors approved at the time of conclusion of this DPA, or completed per project before processing starts, are listed in Annex 3.

The Processor shall inform the Controller in text form at least 30 days in advance of any intended addition or replacement of a sub-processor. The Controller may object to the change within 14 days of receipt of the notice on reasonable grounds relating to data protection. In that case, the Parties shall seek a mutually acceptable solution in good faith. If no such solution can be found, the Controller may terminate the services affected by the change with effect from the date the change would take effect.

Where the Processor engages a sub-processor, it shall impose on it by contract the same data protection obligations as set out in this DPA, in particular sufficient guarantees to implement appropriate TOMs. The Processor remains fully liable to the Controller for the performance of the sub-processor's obligations.

Ancillary services used by the Processor that do not involve access to the Controller's personal data (e.g. telecommunications, general office services) are not sub-processing within the meaning of this Section.

7. Assistance to the Controller

Taking into account the nature of the processing and the information available to it, the Processor shall assist the Controller:

(a) in fulfilling its obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR. The Processor shall forward any such request received directly to the Controller without undue delay and shall not respond to it itself unless instructed to do so by the Controller;

(b) in ensuring compliance with the obligations under Art. 32 to 36 GDPR, including the security of processing, the notification of personal data breaches, data protection impact assessments and prior consultation of the supervisory authority.

Assistance that the Processor is obliged to provide by law or that results from its own breach of this DPA is provided free of charge. For extensive assistance beyond this, the Processor may charge reasonable costs based on the rates of the Main Agreement, provided that it has informed the Controller of this in advance.

8. Personal data breaches

The Processor shall notify the Controller without undue delay, and in any case within 48 hours after becoming aware, of any personal data breach affecting the Controller's personal data.

The notification shall contain, to the extent available, at least:

(a) a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and of personal data records concerned;

(b) the name and contact details of a contact point where more information can be obtained;

(c) the likely consequences of the breach;

(d) the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects.

Where it is not possible to provide all information at the same time, the information may be provided in phases without further undue delay. The Processor shall take the necessary measures to secure the data and mitigate possible adverse consequences for data subjects, and shall document all personal data breaches, including the facts, their effects and the remedial action taken.

9. Deletion and return of personal data

Upon termination of the services, the Processor shall, at the choice of the Controller, delete or return to the Controller all personal data processed on its behalf and delete existing copies, unless Union or Member State law requires storage of the personal data.

Personal data contained in backups shall be deleted in the regular backup rotation cycle; until then they remain protected in accordance with this DPA and shall not be actively processed. The Processor shall confirm the deletion in writing (text form sufficient) on request.

10. Information and audits

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and this DPA.

The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller who is bound to confidentiality and is not a competitor of the Processor. Audits shall be announced with reasonable notice (as a rule 30 days), carried out during normal business hours without unreasonably disrupting operations, and take place no more than once per calendar year, unless there is a personal data breach, a justified suspicion of a material breach of this DPA, or an order by a supervisory authority.

The Processor may first provide suitable evidence such as existing certifications, audit reports or completed questionnaires, where these are sufficient to demonstrate compliance. Each Party bears its own costs of an audit, unless the audit reveals a material breach of this DPA by the Processor, in which case the Processor bears the reasonable costs of the audit.

11. International data transfers

The Processor shall not transfer personal data to a country outside the European Union or the European Economic Area ("third country") or to an international organisation, including by way of a sub-processor, unless the Controller has given documented instructions or approval (including by listing the recipient in Annex 3) and the requirements of Chapter V GDPR are met.

Transfers are permitted in particular on the basis of:

(a) an adequacy decision of the European Commission pursuant to Art. 45 GDPR, including the EU-U.S. Data Privacy Framework for recipients certified under it; or

(b) the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 in the appropriate module, together with supplementary measures where these are required following a transfer impact assessment.

12. Liability

The liability of the Parties towards data subjects is governed by Art. 82 GDPR. In all other respects, the liability provisions of the Main Agreement apply to this DPA, to the extent permitted by mandatory law.

13. Term and termination

This DPA enters into force upon signature by both Parties and ends with the termination of the Main Agreement. Obligations under this DPA continue to apply for as long as the Processor holds personal data of the Controller. A separate termination of this DPA is only possible together with the Main Agreement or the services concerned.

14. Final provisions

In the event of conflict between this DPA and the Main Agreement, this DPA prevails with regard to the protection of personal data. Amendments and supplements to this DPA and its Annexes must be made in writing or in text form; electronic signatures (including qualified and advanced electronic signatures under eIDAS) and the exchange of signed scans are sufficient.

Should any provision of this DPA be or become invalid, the remaining provisions remain unaffected; the invalid provision shall be replaced by a valid provision that comes closest to the Parties' intention and the requirements of the GDPR.

This DPA is governed by the law applicable to the Main Agreement; failing such choice of law, by the laws of the Republic of Croatia. This DPA is available in English and German; in case of doubt, the English version prevails.

Annexes

Annex 1 — Details of processing
Annex 2 — Technical and organisational measures
Annex 3 — Sub-processors

For the Controller (Client)	For the Processor (SANICURA d.o.o.)
Place, date	Place, date
Name, position	Name, position
Signature	Signature

Annex 1 — Details of processing

To be completed per project before processing starts.

Subject matter / project	*e.g. development and operation of the web application "…"*
Nature of processing	*e.g. hosting, development, testing with production data, support and maintenance, AI processing*
Purpose of processing	*e.g. provision of the platform to the Controller's customers*
Categories of data subjects	*e.g. customers, employees, end users, prospects — to be completed*
Categories of personal data	*e.g. contact data, account data, usage and log data, communication content*
Special categories of data (Art. 9 GDPR)	*none, unless specified here*
Duration / retention	*term of the Main Agreement; retention periods as instructed by the Controller*
Location of processing	*e.g. EU/EEA; otherwise see Annex 3*

Annex 2 — Technical and organisational measures

The Processor implements the following baseline measures pursuant to Art. 32 GDPR. Project-specific measures may be added below.

Encryption

- Encryption in transit using TLS 1.2 or higher for all connections carrying personal data.
- Encryption at rest as provided by the hosting and cloud providers used.
- Full-disk encryption on all work devices.

Access control

- Multi-factor authentication on all administrative, code-hosting and cloud accounts.
- Least-privilege and role-based access; access granted only as required for the task.
- Personal accounts only — no shared credentials; credentials stored in a password manager.
- Access rights reviewed regularly and revoked at the end of the engagement or on offboarding.

Separation

- Separate environments for development, staging and production.
- Production data used in development or testing only with the Controller's consent; pseudonymised or anonymised test data preferred.

Logging and monitoring

- Access and administrative actions logged in the providers' audit logs where available.
- Application logs designed to minimise personal data.
- Error monitoring configured to scrub personal data.

Availability and resilience

- Backups of the Controller's data per project with the hosting provider; restore procedures tested.
- Infrastructure defined as code where applicable, allowing reproducible recovery.

Secure development

- Code review for every change before deployment.
- Dependency and vulnerability scanning.
- Secrets kept in secret managers, never in source code repositories.
- Automated tests in continuous integration; security testing appropriate to the project.

Data minimisation and AI

- Only the personal data required for the respective purpose are processed.
- For AI features: no training of models on the Controller's data; AI provider selected per project, with an EU region where possible; redaction of personal data where feasible.

Hosting location

- Hosting in the EU/EEA where possible; otherwise as listed in Annex 3 with appropriate transfer safeguards.

Incident management

- Documented incident response process; notification of personal data breaches to the Controller within 48 hours.

Personnel

- Written confidentiality undertakings; regular security awareness.
- Work devices with automatic screen lock and current operating system and security updates.

Deletion

- Secure deletion of personal data at the end of the engagement in accordance with Section 9.

Project-specific additional measures:

Annex 3 — Sub-processors

The Controller authorises the following sub-processors. The list is completed per project before processing starts.

Sub-processor (name, address)	Service / processing activity	Location of processing	Transfer mechanism (if outside EU/EEA)

Changes to this list follow Section 6: the Processor informs the Controller in text form at least 30 days before adding or replacing a sub-processor; the Controller may object on reasonable data protection grounds within 14 days of receipt of the notice.