DATA PROCESSING AGREEMENT (DPA)

pursuant to Article 28 GDPR
for the peer-to-peer communication platform CRYPE

This agreement is offered as a supplementary option. The use of CRYPE without concluding a Data Processing Agreement is carried out at the customer's own responsibility.

---

1. Contracting Parties

This Data Processing Agreement is concluded between

the Processor:
SCS-Secure Communication Services Limited
Dubai, United Arab Emirates

SCS-Secure Communication Services Limited operates the peer-to-peer communication platform "CRYPE" (hereinafter referred to as **"CRYPE"**).

EU Representative pursuant to Article 27 GDPR:
SCS Consult GmbH
Waldrebenweg
9400 Wolfsberg
Austria
Email: mail@crype.eu

The EU Representative acts as the contact point for supervisory authorities and data subjects pursuant to Article 27 GDPR.

and

the organization accepting this agreement in the course of registration for or use of the CRYPE platform
(hereinafter referred to as the **"Customer"** or **"Controller"**).

---

2. Subject Matter of the Processing

The subject matter of this agreement is the provision of the communication platform CRYPE operated by the Processor for **encrypted peer-to-peer video and messaging communication** between end users of the Controller.

Via CRYPE, the Processor provides **exclusively the technical infrastructure** required for:

- authentication,
- connection establishment (signaling), and
- operation of the platform.

Communication content is transmitted **exclusively and directly between the endpoints of the participants**.

---

3. Type and Purpose of Processing

3.1 Type of Processing

The Processor does **not** process any communication content via CRYPE, in particular:

- no audio or video data,
- no message content,
- no screen sharing or file transfers.

Processing is limited to an **absolute minimum of metadata**, in particular:

- user ID and account status,
- organizational assignment,
- technical connection information,
- security- and operations-relevant system logs.

Peer-to-peer communication is conducted primarily directly between endpoints.
In exceptional cases (e.g. NAT configurations), STUN and/or TURN servers may be used.
TURN servers function exclusively as **encrypted data relays**.

Decryption, content analysis, or storage of communication data by the Processor via CRYPE is **technically excluded**.

3.2 Purpose of Processing

Processing is carried out exclusively for the purpose of:

- operation and provision of the platform,
- connection establishment and signaling,
- system security, stability, and abuse prevention,
- support at system and account level.

Use of CRYPE for the Processor's own purposes is excluded.

---

4. Categories of Data Subjects

- employees of the Controller,
- external communication partners (e.g. organizations, patients, customers).

Communication content of these persons is **not** processed by CRYPE.

---

5. Categories of Personal Data

- user identifiers,
- minimal profile data,
- organization-related information,
- technical metadata and system logs.

The publication of profile data in the central CRYPE contact directory takes place **solely at the decision of the respective user**.

---

6. Roles and Responsibilities

- **Controller:** the Controller within the meaning of the GDPR
- **CRYPE:** Processor, with technically excluded access to communication content

The Controller remains solely responsible for:

- the lawfulness of processing,
- the content of communications,
- informing the data subjects.

---

7. Technical and Organizational Measures (TOMs)

CRYPE implements appropriate technical and organizational measures in accordance with Article 32 GDPR.

The TOMs are described in **Annex 1** and form an integral part of this agreement.

---

8. Sub-Processors

Within the operation of CRYPE, the Processor engages sub-processors **exclusively for infrastructure services** (e.g. data center operations).

- no access to communication content,
- no content processing,
- obligation to comply with equivalent data protection and security standards.

---

9. Assistance Obligations

CRYPE assists the Controller with:

- data subject access requests, insofar as metadata is concerned,
- data protection incidents at infrastructure level.

Assistance with regard to communication content is **technically not possible**.

---

10. Notification of Personal Data Breaches

CRYPE shall notify personal data breaches without undue delay if:

- metadata is affected, or
- a security-relevant incident affects the platform.

Communication content is excluded.

---

11. Deletion of Data

Users may delete their CRYPE accounts independently at any time.

Upon account deletion, **all metadata associated with the account is deleted**, so that no personal data remains with CRYPE.

---

12. Audit Rights

Audits are limited to:

- processes,
- technical measures,
- documentation.

Inspection of communication content is excluded.

---

13. Liability

The Processor shall be liable exclusively within the scope of:

- the metadata actually processed,
- the services contractually agreed.

Any liability of the Processor for communication content is excluded.

---

14. Final Provisions

14.1 Written Form

Amendments and supplements to this Data Processing Agreement require text form.

14.2 Governing Law

The law of the country in which the Processor has its registered seat shall apply, taking into account the directly applicable provisions of European data protection law, in particular the General Data Protection Regulation (GDPR).

14.3 Severability Clause

Should individual provisions of this agreement be or become wholly or partially invalid or unenforceable, the validity of the remaining provisions shall remain unaffected.
The parties undertake to replace the invalid or unenforceable provision with a valid provision that comes closest to the economic purpose of the original provision.

14.4 Responsibility of the Controller

The assessment of whether and to what extent this Data Processing Agreement is required for the respective use of CRYPE lies exclusively with the Controller.
CRYPE does not perform any legal assessment of the Controller’s individual use or regulatory obligations.

Annex 1 – Technical and Organizational Measures (TOMs)

1. Access Control

- role-based administration system
- administrative access is logged

2. Data Minimization

- storage of minimal profile data only
- no content data

3. Encryption

- end-to-end encryption
- peer-to-peer key exchange
- no key management by CRYPE

4. Network Security

- encrypted data transmission
- TURN servers used exclusively as encrypted relays

5. Deletion

- complete deletion of all metadata upon account deletion

🇬🇧 English

The decision on whether a **Data Processing Agreement (DPA)** or a **Business Associate Agreement (BAA)** is required and whether such an agreement is concluded **rests with the customer**.

CRYPE does not assess whether and to what extent the GDPR applies to the respective use.

☐ Where required, I accept the **Data Processing Agreement (DPA)** pursuant to Art. 28 GDPR for the use of CRYPE.

CRYPE does not determine whether the customer qualifies as a healthcare provider under applicable healthcare regulations.

☐ Where required, I accept the **Business Associate Agreement (BAA)**.