Version: September 2023

Data Processing Agreement acc. Art. 28 GDPR

between the Customer

- below Client -

and

NXGEN Technology AG, Technoparkstrasse 1, CH- 8005 Zurich

- below Service Provider -

Preamble

The Service Provider supplies the Client with the NXGEN XXXX application and associated services as outlined in the agreement between the parties, comprising the contract and the general terms and conditions (hereinafter the "Main Contract"). Within this context, the Service Provider may process personal data for which the Client acts as the data controller under applicable data protection regulations (hereinafter "Order Data").

This agreement establishes the data protection rights and obligations of both parties in connection with the Service Provider's handling of Order Data under the Main Contract, ensuring compliance with the GDPR. Additionally, it addresses adherence to Swiss data protection laws under

the applicable Data Protection Act (DSG), provided these are not already satisfied by compliance with GDPR requirements.

§ 1 Scope, Subject, and Duration of Processing

1. **Application Scope:**
   This data protection agreement applies to all activities performed under the Main Contract wherein the Service Provider's employees or subcontractors may process Order Data on behalf of the Client.

2. **Purpose and Scope:**
   The Service Provider processes personal data as part of providing the NXGEN XXXX application and delivering related services. This includes data necessary for the NXGEN XXXX application's operation and data entered or collected by users during their use of the application.

3. **Duration:**
   Processing duration aligns with the Main Contract's term.

4. **Data Categories:**
   The personal data processed may include:

   - **User profile data:** Access details such as names, email addresses, and optionally other user-provided profile information (e.g., titles, locations).

   - **Data collected during NXGEN XXXX usage:** Client-related data such as names, addresses, emails, phone numbers, and video, audio, or chat data.

5. **Data Subjects:**
   The categories of individuals affected by processing include the Client, its employees, authorized personnel (e.g., freelancers, instructors), and the Client's customers.

6. **Location of Processing:**
   Processing will occur exclusively within the EU, Switzerland, or other countries within the European Economic Area (EEA).

§ 2 Responsibility for Data Processing

1. The Client retains sole responsibility for ensuring the legality of Order Data processing and the protection of data subject rights under GDPR Articles 12–22, acting as the "Data Controller" as per GDPR Article 4(7).

2. The Service Provider processes Order Data exclusively on behalf of the Client and following the Client's instructions.

§ 3 Technical and Organizational Measures

1. The Service Provider must implement appropriate measures to safeguard Order Data, in line with GDPR Article 32, and prevent unauthorized access or distribution.

2. Measures are subject to technical advancements, with the Service Provider maintaining at least the agreed-upon level of protection.

§ 4 Obligations of the Service Provider

1. The Service Provider processes Order Data solely on the Client's instructions and must correct, delete, or restrict data only as directed.

2. Requests from data subjects concerning their data must be forwarded promptly to the Client.

3. The Service Provider ensures compliance with this agreement, including sub-processors' adherence (see §9).

4. Unauthorized duplication or use of Order Data is prohibited, except as required for lawful processing or contractual performance.

5. The Service Provider assists with inspections, regulatory requests, and data protection obligations as needed, with reasonable costs reimbursed by the Client.

6. Data breaches or suspected irregularities must be reported immediately to the Client.

§ 5 Obligations of the Client

1. The Client ensures the legality of processing and exercises responsibility for data subject rights.

2. The Client informs the Service Provider of errors or irregularities identified during compliance checks.

§ 6 Authority to Give Instructions

1. The Service Provider acts solely under the Client's instructions unless legally required otherwise.

2. Additional instructions outside the agreed scope may incur costs, provided they are unrelated to rectifying Service Provider breaches.

3. The Service Provider must notify the Client if an instruction appears to violate the law.

§ 7 Support Obligations

1. The Service Provider assists the Client in fulfilling data subject requests and meeting GDPR compliance obligations, such as under Articles 32–36.

2. Costs incurred for assistance will be reimbursed unless the need arises due to the Service Provider's breach of this agreement.

§ 8 Client Inspection Rights

1. The Client may monitor compliance with contractual and data protection obligations, including by conducting audits or on-site inspections, with reasonable notice.

2. Costs are borne by the Client unless breaches are discovered attributable to the Service Provider.

§ 9 Use of Sub-processors

1. The Client grants general consent for the engagement of sub-processors, as listed in Appendix 2.

2. Changes to sub-processors require prior notification, with a 14-day objection period for the Client.

3. Sub-processors must meet the same obligations as the Service Provider under this agreement.

§ 10 Data Deletion and Return

1. Upon termination of the Main Contract or earlier upon request, the Service Provider will delete or return all data to the Client, as specified, and provide proof of deletion if required.

§ 11 Liability

1. Liability for damages is based on respective responsibility. In external cases, the Client assumes liability unless damage results from the Service Provider's breach.

2. Internal indemnification follows proportional responsibility for damages.

§ 12 Final Provisions

1. This agreement supersedes conflicting provisions of the Main Contract. Amendments must be in writing.

2. If any provision is invalid, it will be replaced with a valid provision that fulfills its intent.

3. Swiss law applies, and the Commercial Court of Zurich has exclusive jurisdiction.

4. The Service Provider complies with Swiss laws, refraining from unauthorized foreign authority cooperation as per Swiss Penal Code Article 271.

5. Disputes will be resolved amicably or via the Zurich Commercial Court.

Attachment 1

Overview of the technical-organizational Measures

I. Confidentiality (Art. 32 Section. 1 lit . b GDPR)

1. **Access control**

Preventing Unauthorized Access to Data Processing Systems

Unauthorized individuals are prevented from accessing data processing systems where personal data is processed and used.

Measures include:

- Access Control Mechanisms: Magnetic or chip cards for authorized access.
- Video Surveillance: Monitoring access points.
- Authorization Management: Determining and documenting authorized individuals.
- Closed Shop Operation: Limiting entry to authorized personnel.
- Access Authorization Audits: Regularly reviewing and updating access permissions.
- Access Control Systems: Implementing technical and organizational controls.
- Key Management: Maintaining a current key list and regulating key usage.
- Access Logging: Recording entry and exit activities.
- Security Personnel: Employing receptionists or ushers.
- Physical Security: Ensuring office doors and windows are locked when unattended.

2. Access and Access control

Ensuring Authorized Use of Data Processing Systems

Access control mechanisms must ensure that:

- Only authorized individuals can access data processing systems.
- Personal data cannot be accessed, read, copied, modified, or removed without authorization during use or after storage.

Measures include:

- User Authentication: User ID and password protection.
- Permission Verification: Mechanical checks to validate access rights.
- Access Restrictions: Limiting access to "read-only" where applicable.
- Time Restrictions: Setting time-bound access permissions.
- Access Logging: Tracking and logging user activities, including failed access attempts.
- Encryption Methods: Employing encryption to secure data.
- Role-Based Access: Assigning user rights based on roles and responsibilities.

3. Separation control

Ensuring Data Separation for Different Purposes

Data collected for different purposes must be processed separately.

Measures include:

- System Segmentation: Separating test and production systems.
- Logical Data Separation: Using distinct directories or databases for client-specific data.
- Different Encryption Methods: Assigning separate encryption keys for distinct datasets.

4. Pseudonymization

Processing Personal Data with Limited Identifiability

Personal data is processed so it cannot be linked to an individual without additional information, which must be stored separately under secure measures.

Measures include:

- Pseudonymization Rules: Establish rules for generating pseudonyms (UUID v4).
- Authorization Management: Define individuals responsible for pseudonymization and depseudonymization.
- Random Allocation: Use random algorithms for pseudonym generation.
- Secure Storage: Protect allocation tables and pseudonymization keys against unauthorized access.

II. Integrity (Art. 32 Section. 1 lit . b GDPR)

1. **Distribution control**

Ensure that personal data cannot be read, copied, altered, or removed during electronic transmission, transport, or storage without authorization.

Measures include:

- Documentation: Record retrieval and transmission processes.
- Recipient Determination: Clearly define transmission or transport recipients.
- Transport Security: Use secure methods and containers.
- Encryption: Encrypt data during transmission.
- Monitoring: Oversee transport timelines and validate data accuracy upon receipt.
- VPN Usage: Use virtual private networks for secure data transfers.

2. Input control

Ensure accountability for data entry, modification, and deletion in data processing systems.

Measures include:

- Input Authorization: Define and document authorized personnel.
- Logging: Record login activities and data changes.

III. Availability and Resilience (Art. 32, Sec. 1, Lit. b & c GDPR)

1. **Availability**

Protect personal data against accidental loss or destruction.

Measures include:

- Uninterrupted Power Supply (UPS): Ensure continuous power availability.
- Redundant Power Lines and Generators: Mitigate power failures.
- Fire Safety: Fire detectors and disaster recovery plans.
- Data Backups: Storing backups in separate, secure locations.
- Server Redundancy: Employ a redundant server architecture.
- Security Measures: Protect server rooms with access controls and antivirus solutions.

2. Quick Recoverability

Ability to restore data in case of loss or corruption.

Measures include:

- Backup Systems: Ensure regular and reliable data backups.
- Restoration Testing: Periodically test data recovery procedures.
- Emergency Plans: Maintain restart plans for rapid system recovery.

3. Load capacity/ Resilience

Maintain system functionality during incidents.

Measures include:

- Patch Management: Regularly update software.
- Intrusion Detection: Use systems to detect and respond to unauthorized activities.
- Employee Training: Educate staff on incident recognition and prevention.
- Fail-Safe Modes: Transition systems to fail-safe states during incidents.

IV. Regular Examination, Evaluation, and Assessment (Art. 32, Sec. 1, Lit. d GDPR; Art. 25, Para. 1 GDPR)

1. **Order control**

Ensure contractual compliance for commissioned data processing.

Measures include:

- Contractual Clarity: Clearly define responsibilities and duties between service providers and clients.
- Provider Selection: Carefully vet service providers.
- Audit and Monitoring: Regularly review contract execution.
- Sanctions: Enforce penalties for contract breaches.
- Risk Management: Update risk analyses as new vulnerabilities emerge.

2. External Audits and Certifications

Measures include:

ISO 27001 Compliance: Use ISO 27001-certified data centers, ensuring adherence to international standards for information security, access control, incident management, and legal compliance.

Attachment 2

Service Providers used pursuant to Section 9

company SubService Providers	Address/Country	Description the acquired Partial performance

Amazon Web Services EMEA SARL	Avenue John F. Kennedy 38 1855 Luxembourg Luxembourg	**Data center (ISO 27001-certified)** **VPN Services** **Locations:** **Frankfurt (Production) Zurich (Production)** **Ireland (Development & Backup)**
Twilio Ireland Limited	3 Dublin Landings North Wall Quay Dublin 1Ireland	**VoIP (ISO 27001- certified)**
Sitasys AG	Industriestrasse 6 4513 Langendorf Switzerland	**Alarm processing and virtual receivers**

OpenVPN Inc	6200 Stoneridge Mall Rd Fl3 Pleasanton, CA 94588 USA	**VPN Services**

Octa Inc	100 Frith Street San Francisco, CA, 94105 USA	**Authentication service (ISO 27001- certified)**
Zoho Corporation BV	Beneluxlan 4B 3527 HT Utrecht The Netherlands	**Mail and Business Support Systems (ISO 27001- certified)**
Google Ireland Ltd	Gordon House Barrow Street Dublin4 Ireland	**Data center (ISO 27001-certified)**