Groq, Inc., ("**Groq**") and you ("**Customer**" or "**you**") enter into this Order Form under the GroqCloud Terms of Sale listed at https://console.groq.com/docs/terms-of-sale to initiate committed billing as of the date of the Customer's signature below ("**Effective Date**").

Groq, Inc.
P.O. Box 1778 Mountain View, CA 94042

Customer Information	
Billing company name	aiio GmbH
Billing contact name	Jobst von Heintze
Billing email address	jobst.von.heintze@aiio.de
Order Information	
Quote Offer Date	Effective Date (Date Quote is signed)
Quote Onboard Date	Effective Date (Date Quote is signed)
Package Pricing Billing	https://groq.com/pricing/
Currency	USD
Payment Information	
Payment Term	Automatically charged for usage at the end of each calendar month to payment on file.
Payment method	Credit Card

SIGNATURE			
BY	DocuSigned by: Jobst von Heintze 4153C03E3EF24DD...	DATE	6/24/2025 | 7:01 AM PDT
NAME	Jobst von Heintze	TITLE	CMO

This **Data Processing Agreement** is made effective on the date you execute the Order Form.

BETWEEN:

(1) **Groq, Inc.** whose place of business is at 301 Castro St, Suite 200, Mountain View, California, 94041, USA ("**Groq**"); and

(2) The Customer referred to in the Order Form ("**Customer**")

(together "**the parties**")

BACKGROUND:

(A) Customer and Groq have entered into the Groq Terms and Conditions (the "**Terms**") which defines Groq's obligations with respect to the provision of services to Customer ("**Services**").

(B) Since, as part of receiving and delivering the Services, the Customer is a controller subject to the GDPR and Groq will process personal data as a processor, the parties are required to enter into an appropriate data processing agreement which reflects the roles of the parties and their obligations under applicable data protection law including for international data transfers.

(C) Accordingly, the parties hereby enter into this Data Processing Agreement ("**DPA**") in order to comply with the applicable obligations under data protection law.

The parties hereby agree that:

1. Definitions

1.1 The following definitions shall apply in this DPA:

(a) "**Data Protection Law**" means, as applicable, the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the UK's implementation of the GDPR into UK law by virtue of section 3 of the UK's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and any other applicable data protection law as may be amended or superseded from time to time; and

(b) "**C2P Clauses**" means the European Commission's standard contractual clauses in Commission Implementing Decision (EU) 2021/914 dated 4 June 2021, incorporating module 2 for controller to processor transfers.

(c) "**Schedule**" means the schedule appended to this DPA which includes the relevant annexes for the C2P Clauses.

(d) The terms 'processor', 'controller' and 'personal data' shall have the meanings given to them under Data Protection Law.

1.2 All other defined terms used in this DPA shall have the meanings given to them in the Terms.

2. Groq as processor

2.1 The parties hereby confirm that Groq is a processor and Customer is a controller under Data Protection Law for the processing of personal data in connection with the provision of the Services.

2.2 The Customer hereby confirms that Groq can process personal data that it receives from Customer in order to convert that personal data into anonymized data ("**Anonymized Data**") which Groq can use for its own purposes. The parties agree that Anonymized Data is not subject to Data Protection Law.

3. **Reliance on Standard Contractual Clauses**

3.1 Subject to section 3.2, the C2P Clauses shall apply and are hereby incorporated into this DPA, where Customer is the data exporter and Groq is the data importer for any personal data transferred outside of the European Economic Area or UK.

3.2 The parties shall enter into the C2P Clauses with the following specification to the clauses in the C2P Clauses:

(a) Clause 7 (Docking clause) is excluded.

(b) If the Customer wishes to exercise its rights under Clause 8.9 (Documentation and compliance), the Customer shall first request a copy of the annual third party audit report of Groq's facilities and data processing ("**Annual Audit Report**") subject to any reasonable confidentiality assurances (up to and including a non-disclosure agreement) that Groq seeks. It is only where Customer reasonably considers that the Annual Audit Report does not provide Customer with reasonable reassurances about Groq's compliance with the C2P Clauses that Customer shall request to conduct an audit by itself or mandate an independent auditor as permitted under Clause 8.9.

(c) Audits in accordance with Clause 8.9 (Documentation and compliance) shall: (i) be on no less than ten (10) working days' prior written notice to Groq (ii) be conducted during normal business hours; (iii) not unreasonably interfere with Groq's business activities; (iv) be limited to once a calendar year unless required by law; (v) be subject to Groq's reasonable security restrictions (e.g., sign-in requirements, badge requirements, escort requirements); (vi) be subject to a non-disclosure agreement between the auditor and Groq, where requested by Groq; and (vii) be at Customer's cost (including reimbursing Groq for its reasonable costs associated with the audit) unless the parties agree otherwise.

(d) Option 2 (general written authorization) is selected under Clause 9 (Use of sub-processors) and the time period for Groq informing Customer of any changes to its sub-processors is 30 (thirty) working days in advance. Any objection by Customer of Groq's appointment or replacement of a sub-processor shall be based on reasonable grounds relating to data protection. The agreed list of subprocessors is set out in Annex III of the Schedule. Where the Customer objects, it shall notify Groq in writing of such objection prior to the appointment or replacement of the sub-processor. In such event, Groq will use reasonable efforts to provide the Services to Customer in accordance with the Agreement without using the sub-processor that Customer has objected to. If Groq reasonably requires use of the sub-processor and is unable to satisfy Customer as to the suitability of the sub-processor within thirty (30) days of Customer’s objection, the Customer may elect to terminate only the part of the Services which cannot be provided by Groq without the use of the objected-to sub-processor.

(e) Clause 11 (a) (Redress) is not included.

(f) Clause 17 (Governing Law) The parties agree that Irish law shall govern the C2P Clauses.

(g) Clause 18 (Choice of Forum and Jurisdiction) The parties agree that the courts of Ireland shall resolve disputes relating to the C2P Clauses.

(h) Any assistance provided by Groq to Customer under Clause 8.6 (Security of processing), Clause 8.9 (Documentation and compliance) and Clause 10 (Data Subject Rights) shall be at Customer's sole cost and expense except for those circumstances where Groq is not complying with its obligations under the C2P Clauses.

3.3 The parties acknowledge that Annex I to this DPA sets out the list of parties, description of transfers and competent supervisory authority, governing law and choice of forum and jurisdiction, Annex II sets out the relevant security measures, and Annex III sets out the approved third party subprocessors.

3.4 For the avoidance of doubt, the parties also rely on the C2P Clauses for compliance with the requirements of Article 28 GDPR and UK GDPR.

4. UK Transfers

4.1 The parties acknowledge that international data transfers may be made by Customer in the European Economic Area or the UK to Groq. Consequently, and as further specified in Clause 4.2, in the event of such data transfers the parties hereby incorporate into this DPA the template Addendum Version B.1.0 issued by the UK's Information Commissioner's Office ("**ICO**") and laid before the UK Parliament in accordance with s. 119A of the UK's Data Protection Act 2018 on 2 February 2022 ("**UK Addendum**"), as amended by the ICO from time to time.

4.2 The parties hereby agree that in relation to the UK Addendum:

(a) The details required for Tables 1, 2 and 3 of the UK Addendum are set out in Clause 3.2 above and in Annex I;

(b) The parties shall comply with their respective obligations under the Mandatory Clauses (as those clauses are identified in the UK Addendum) of the UK Addendum issued by the ICO and laid before Parliament in accordance with s. 119A of the UK's Data Protection Act 2018 on 2 February 2022, as it is revised under s. 18 of those Mandatory Clauses; and

(c) Pursuant to Table 4 of the UK Addendum and in the event that the UK Addendum is revised by the ICO ("**Revised UK Addendum**"), Groq shall be entitled to terminate the UK Addendum and any underlying services associated with international data transfers from Customer to Groq, pursuant to s. 19 of the Mandatory Clauses and on no less than 30 (thirty) days' prior written notice before the start date of the Revised UK Addendum.

5. Security Requirements

5.1 The parties shall comply with the obligations set out in Annex II (Technical and Organisational Measures).

6. Limitation of Liability

6.1 Groq's liability to Customer under this DPA shall be subject to the limitations of liability set out in the Terms.

7. General

7.1 In the event of any conflict between the Terms and this DPA, this DPA shall prevail.

7.2 This DPA shall be governed by and construed in accordance with English law.

The parties' execution of the Order Form has the effect of the parties entering into this DPA.

Schedule

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: The Customer as identified in the DPA

Address: As identified in the DPA

Contact person's name, position and contact details: As identified in the Order Form.

Activities relevant to the data transferred under these Clauses:

As described in Annex I.B

Signature and date: On executing the Order Form.

Role (controller):

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Groq, Inc.

Address: 301 Castro St, Suite 200, Mountain View, California, 94041, USA

Contact person's name, position and contact details: As identified in the Order Form

Activities relevant to the data transferred under these Clauses:

As described in Annex I.B

Signature and date: On executing the Order Form

Role (processor):

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of the Services, Customer personnel, any other categories of data subjects about whom personal data is inputted by Customer into the Groq platform or hosted model when it uses the Services.

Categories of personal data transferred

Any personal data inputted by Customer when it uses the Services, and any personal data in the generated output.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Any special category personal data input by Customer, and any personal data in the generated output.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis*).*

Continuous

Nature of the processing

The collection, storage and processing of the personal data for the purpose of providing the Services.

Purpose(s) of the data transfer and further processing

Provision of the Services, which include AI solutions.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the period stated in the Order Form.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Processing to provide data storage, online payment processing, cloud hosting and cybersecurity services, for the duration of the service to the Customer.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Ireland

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES

INTRODUCTION

Groq maintains an information security program designed to safeguard its systems, data, and Customer Data. This Exhibit describes the information security program and security standards that Groq maintains with respect to the Services and handling of data submitted by or on behalf of Customer of the Services (the "Customer Data"). Capitalized terms not defined in this Exhibit have the meanings given in the DPA or Agreement.

To learn more about Groq's technical and organizational security measures to protect Customer Data, see Groq's Trust Portal at https://trust.groq.com/ (the "Trust Portal"). The Security Measures below include the subset of the information available in the Trust Portal which applies to this DPA.

SECURITY MEASURES

Corporate Identity, Authentication, and Authorization Controls. Groq maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:

- Groq uses single sign-on (SSO) to authenticate to third-party services used in the delivery of the Services. Role Based Access Controls (RBAC) are used when provisioning internal access to the Services;
- Mandatory multi-factor authentication is used for authenticating to Groq's identity provider;
- Unique login identifiers are assigned to each user;
- Established review and approval processes for any access requests to services storing Customer Data;
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
- Established procedures for promptly revoking access rights upon employee separation;
- Established procedures for reporting and revoking compromised credentials such as passwords and API keys); and
- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

Customer Identity, Authentication, and Authorization Controls. Groq maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning Groq does not store user-provided passwords on users' behalf; and
- Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported.

Cloud Infrastructure and Network Security. Groq maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:

- Primary backend resources are deployed behind a VPN.
- The Services are routinely audited for security vulnerabilities.
- Application secrets and service accounts are managed by a secrets management service;
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked; and
- Services logs are monitored for security and availability.

System and Workstation Control. Groq maintains industry best practices for securing its corporate systems, including laptops and on-premises infrastructure, including:

- Endpoint management of corporate workstations;
- Endpoint management of mobile devices;
- Automatic application of security configurations to workstations;
- Mandatory patch management; and
- Maintaining appropriate security logs.

Data Access Control. Groq maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
- Customer Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

Disclosure Control. Groq maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using strong encryption algorithms;
- Encryption of data in transit;
- Audit trail for all data access requests for production datastores;
- Full-disk encryption required on all corporate workstations;
- Device management controls required on all corporate workstations; and
- Customer Data can be deleted upon request.

Availability control. Groq maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption;
- Ensuring that systems are functioning and faults are reported; and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment.

Segregation control. Groq maintains industry best practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data;
- Restriction of access to data stored for different purposes according to staff roles and responsibilities; and
- Segregation of business information system functions.

Risk Management. Groq maintains industry best practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation;
- Penetration testing is conducted on the Services at least annually, and any remediation items identified are resolved as soon as possible on a timetable commensurate with the associated risk;
- Annual engagements of a qualified, independent external auditor to conduct periodic reviews of Groq's security practices against recognized audit standards, including SOC 2 Type II certification audits. Upon reasonable request, Groq will provide summary details; and
- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

Personnel. Groq maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:

- Annual security training for employees, and supplemental security training as appropriate.

Physical Access Control. Groq maintains industry best practices for preventing unauthorized physical access to Groq facilities, including:

- Physical barrier controls including locked doors and gates;
- 24-hour video surveillance and alarm systems, including video surveillance of facility entrance and exit points;
- Logging of facility exits and entries.

Third Party Risk Management. Groq maintains industry best practices for managing third party security risks, including with respect to any subprocessor or subcontractor to whom Groq provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data; and
- Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by Groq's Security team.

Security Incident Response. Groq maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data including the following:

- Groq aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
- If Groq becomes aware that a Personal Data Breach has occurred, Groq will notify Customer in accordance with the DPA.

Security Evaluations. Groq performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and its policies and procedures and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of Groq's information systems.

ANNEX III

APPROVED SUB-PROCESSORS

Subprocessors can be found here:
https://trust.groq.com/subprocessors