Nateq Data Processing Agreement

Version 1.0. Last updated 11 November 2026.

1. Parties, scope and order of precedence

1.1 This Data Processing Agreement ("DPA") is between **NATEQ LLC**, a Wyoming limited liability company ("Nateq"), and the customer named in the order form or account ("Customer").

1.2 It forms part of the Nateq Terms of Service or other agreement under which Customer uses the Nateq platform (the "Agreement"). It applies whenever Nateq processes Customer Personal Data on Customer's behalf.

1.3 If this DPA conflicts with the Agreement, this DPA wins on data protection. If it conflicts with the SDAIA Standard Contractual Clauses attached under section 6, the SDAIA Standard Contractual Clauses win.

1.4 This DPA does not cover data Nateq processes as a controller in its own right (Customer's account, team and billing data). That data is covered by the Nateq Privacy Policy.

2. Definitions

- **PDPL**: the Saudi Personal Data Protection Law (Royal Decree M/19 of 9/2/1443H, as amended by Royal Decree M/148 of 5/9/1444H), its Implementing Regulations, the Regulation on Personal Data Transfer Outside the Kingdom, and SDAIA rules and guidelines issued under them.
- **SDAIA**: the Saudi Data & AI Authority, the competent authority under the PDPL.
- **Data Protection Law**: the PDPL and any other data protection law that applies to the processing, such as the UAE Federal Decree-Law 45/2021 or the GDPR.
- **Controller, Processor, Personal Data, Sensitive Data, Processing, Data Subject**: as defined in the PDPL.
- **Customer Personal Data**: Personal Data about Customer's end users, contacts and leads that Nateq processes for Customer through the platform (messages, calls, recordings, transcripts, emails, contact profiles, CRM records, bookings).
- **Sub-processor**: a third party Nateq engages to process Customer Personal Data.
- **Personal Data Breach**: a security incident that leads to unauthorised access to, or disclosure, loss, alteration or destruction of, Customer Personal Data.
- **SDAIA SCCs**: the Standard Contractual Clauses for Personal Data Transfer issued by SDAIA (version 1.0, September 2024, or any later version).

3. Roles and instructions

3.1 Customer is the Controller of Customer Personal Data. Nateq is its Processor.

3.2 Nateq processes Customer Personal Data only on Customer's documented instructions. The Agreement, this DPA, Customer's settings in the platform (channels, AI agents, retention, integrations) and Customer's written requests are those instructions.

3.3 Nateq will tell Customer promptly if it believes an instruction breaks the PDPL, and may suspend that instruction until it is confirmed or changed.

3.4 Customer is responsible for: having a lawful basis for the processing and for collecting the data; giving its end users the notices the law requires (including that they may be talking to AI and that calls may be recorded); its own risk assessment for transfers outside the Kingdom; and any registration with SDAIA that applies to it.

3.5 **Sensitive Data.** Customer will not use the platform to process Sensitive Data (such as health data) of individuals in the Kingdom, because the PDPL gives it no route to Nateq's hosting today (Annex 4). Clinics and other healthcare providers may use the platform for bookings and administration only, with their AI set not to ask for symptoms or medical details. Any other Sensitive Data needs Nateq's prior written agreement.

4. Nateq's obligations

4.1 **Confidentiality.** Only staff and contractors who need access to run or support the service may access Customer Personal Data, and they are bound by confidentiality. Support access to a Customer workspace is logged.

4.2 **Security.** Nateq applies the measures in Annex 2 and keeps them at least at that level for the term of the Agreement.

4.3 **Minimisation.** Nateq processes only the Customer Personal Data needed to provide the service, and sends each Sub-processor only what its function needs.

4.4 **Records.** Nateq keeps a record of the processing it carries out for Customer (Annex 1) and gives it to Customer or SDAIA on request.

4.5 **Assistance.** Taking into account the nature of the processing, Nateq helps Customer meet its PDPL duties: data subject requests (section 7), breach notification (section 8), impact and transfer risk assessments (section 6), and SDAIA inquiries (section 11).

5. Sub-processors

5.1 Customer approves the Sub-processors listed in Annex 3. The PDPL Implementing Regulations require the Controller's prior approval of sub-processors; signing this DPA is that approval for the listed ones.

5.2 Nateq will give Customer at least **30 days' notice** by email and on nateq.io/subprocessors before adding or replacing a Sub-processor. Customer may object in writing on reasonable data protection grounds within that period. If the parties cannot resolve the objection, Customer may end the affected part of the service and receive a pro-rata refund of prepaid fees for it.

5.3 Nateq binds each Sub-processor by written contract to data protection terms that protect Customer Personal Data at least as well as this DPA, and remains liable to Customer for its Sub-processors.

5.4 **Customer-enabled integrations** (Annex 3, part B) are services Customer chooses to connect, such as its CRM, help desk, store or mailbox. They receive data only on Customer's instruction and under Customer's own contract with that provider. They are not Nateq's Sub-processors, and deleting data in Nateq does not delete it there unless Customer turns on deletion for that integration.

6. Transfers outside the Kingdom

6.1 Customer acknowledges that Nateq stores Customer Personal Data in AWS eu-central-1 (Frankfurt, Germany) and that some Sub-processors process it in transit in the European Union and the United States (Annex 4). Nateq does not offer hosting inside the Kingdom today.

6.2 **SDAIA SCCs, Controller to Processor.** For Customer Personal Data of individuals in the Kingdom, the parties enter into the SDAIA SCCs (Controller-to-Processor version) as an appendix to this DPA, with Customer as exporter and Nateq as importer. The SDAIA SCCs are attached unchanged, because SDAIA does not allow them to be modified.

6.3 **Onward transfers.** The SDAIA SCCs require onward transfers outside the Kingdom to go only to Sub-processors that have acceded to them. Nateq will ask each Sub-processor in Annex 3 to accede, and shows on nateq.io/subprocessors which have done so and the data protection terms each relies on until then. Where section 6.5 offers an option for a Sub-processor, Customer may ask Nateq to use it. Otherwise, if Customer does not accept a Sub-processor on that basis, Customer may object and end the affected part of the service as set out in section 5.2.

6.4 **Exemption case and risk assessment.** The parties rely on the exemption for transfers that provide a service directly to the data subject (Transfer Regulation article 4(2)(D)), as set out in Annex 4. Customer carries out the risk assessment the Transfer Regulation requires before transferring. Nateq gives Customer the information it needs (Annexes 1, 2 and 4) and answers reasonable follow-up questions.

6.5 **Workspace options.** On request, Nateq will turn off for Customer's workspace AI routing by TypeSafe AI (Jev), and AI voice calls with live call transcription (ElevenLabs). Nateq will tell Customer which features stop working as a result.

6.6 If SDAIA publishes a list of adequate countries, new SCCs, or amendments to the transfer rules, the parties will update this section and Annex 4 in good faith.

6.7 **Accreditation certificate.** Nateq will apply for an SDAIA accreditation certificate once SDAIA publishes licensed certification bodies, and will tell Customer when it holds one.

7. Data subject requests

7.1 Customer can handle most requests itself in the dashboard: export everything about a contact, erase a contact (with an erasure certificate), and set retention periods.

7.2 If a data subject contacts Nateq directly about Customer Personal Data, Nateq will pass the request to Customer within **48 hours** and will not answer it itself unless Customer asks or the law requires.

7.3 Where a request cannot be met in the dashboard (for example a correction in a system field), Nateq will help within **10 business days** of Customer's written request, so Customer can meet the PDPL response deadline.

7.4 An erasure in Nateq does not erase copies in Customer-enabled integrations unless Customer turned on deletion for them. The erasure certificate lists any records that remain there.

8. Personal data breach

8.1 Nateq will notify Customer of a Personal Data Breach affecting Customer Personal Data **without undue delay and no later than 24 hours** after becoming aware of it. This leaves Customer time to meet its own 72-hour notice to SDAIA.

8.2 The notice goes to the workspace owner's email and includes, as far as known: what happened and when; the categories and approximate number of data subjects and records; the likely consequences; what Nateq has done and will do; what Customer should do; and a contact. Nateq sends updates as facts become known.

8.3 Nateq will help Customer with its notices to SDAIA and to data subjects. Customer decides whether and how to notify them.

8.4 Notice of a breach is not an admission of fault or liability.

9. AI processing

9.1 Nateq does not use Customer Personal Data to train or fine-tune AI models, its own or anyone else's.

9.2 Nateq sends Customer Personal Data to AI and speech Sub-processors only to produce the service for Customer (replies, routing, summaries, transcription, speech). Nateq uses those providers under terms that do not allow them to train on the data, and lists any provider where this is not yet confirmed on nateq.io/subprocessors.

9.3 Nateq keeps AI request traces (prompts and responses) for debugging for no more than **14 days**, on a sample of requests.

9.4 The platform lets Customer tell its end users they are talking to AI, and that calls are recorded, on every channel. It is on by default. If Customer turns it off, Customer is responsible for giving the notice another way.

9.5 AI replies can be wrong. Customer configures what the AI may do (knowledge, actions, escalation to a human) and remains responsible for decisions it makes about data subjects.

10. Retention, deletion and return

10.1 During the Agreement, Customer sets how long messages, conversations, call recordings and transcripts are kept. Deleted data is removed from live systems by the next scheduled run.

10.2 When the Agreement ends, Customer may export its data for **30 days**. Nateq then deletes Customer Personal Data from live systems within **30 days**, and issues a deletion certificate on request.

10.3 Copies in database backups and earlier file versions are overwritten within **35 days** of deletion. Until then they are encrypted, isolated from normal use and not restored except to recover from a disaster, in which case deleted data is deleted again.

10.4 Nateq may keep data longer only where the law requires it. Nateq keeps invoices and billing records, which are its own controller data, for tax purposes.

11. Audits and SDAIA cooperation

11.1 Nateq will answer Customer's reasonable written security and privacy questionnaires once a year, and after any Personal Data Breach.

11.2 If Customer needs more, or SDAIA requires it, Customer may audit Nateq's compliance with this DPA once a year, with **30 days' notice**, during business hours, under confidentiality, and at Customer's cost. The audit may be done remotely. An independent auditor must not be a Nateq competitor.

11.3 Each party will cooperate with SDAIA on requests about the processing under this DPA. Nateq will tell Customer about any SDAIA request concerning Customer Personal Data unless the law forbids it.

11.4 If a public authority asks Nateq for Customer Personal Data, Nateq will tell Customer before disclosing unless the law forbids it, and will disclose only what is legally required.

12. Liability, term, governing law

12.1 Each party's liability under this DPA is subject to the limits in the Agreement, except where the law does not allow a limit.

12.2 This DPA lasts as long as Nateq processes Customer Personal Data. Sections 8, 10 and 11 survive until deletion is complete.

12.3 This DPA is governed by the law that governs the Agreement. The SDAIA SCCs are governed by the laws of the Kingdom of Saudi Arabia, as they themselves require.

12.4 Customer accepts this DPA by accepting the Nateq Terms of Service. A Customer that needs a signed copy may sign below and send it to legal@nateq.io.

	Customer	**NATEQ LLC**
Name		Ahmed Elsayed
Title		Founder
Signature		
Date		

Annex 1: Details of processing

Item	**Details**
Subject matter	Providing the Nateq AI customer service platform to Customer
Duration	The term of the Agreement plus the deletion period in section 10
Purpose	Receiving, answering, routing and recording Customer's conversations with its end users across chat, WhatsApp, Messenger, Instagram, email and voice calls; AI replies and summaries; search; analytics; integrations Customer turns on
Data subjects	Customer's end users, website visitors, contacts, leads, callers and email correspondents

Categories of data	Name, phone number, email, channel IDs (WhatsApp, Messenger, Instagram); message and email content and attachments; call audio, voicemails and transcripts; facts the AI extracts from conversations; contact custom fields and CRM notes; bookings and payment request references; visitor IP hash and user agent; consent records
Sensitive data	Not permitted for individuals in the Kingdom (section 3.5)
Storage location	AWS eu-central-1, Frankfurt, Germany
Retention	Set by Customer (section 10); otherwise until Customer deletes it or the Agreement ends

Annex 2: Security measures

Area	Measure
Encryption at rest	Database (AWS RDS) and cache (ElastiCache) encrypted with AWS KMS; files (S3) encrypted with SSE-S3; server disks encrypted; message bodies additionally encrypted per contact so erasure destroys the key
Encryption in transit	TLS on all public endpoints and provider calls; database connections verify the server certificate; cache uses TLS; file storage accepts HTTPS only
Network	Database and cache in private subnets; file bucket blocks all public access; files served through short-lived signed links
Workspace isolation	API requests are scoped to the caller's workspace, and cross-workspace access is covered by automated tests on the endpoints that handle personal data
Access control	Role-based access inside each workspace; staff support access is logged
Logging and monitoring	Access log of who opened conversations, calls, transcripts and files, and who exported contacts; AWS CloudTrail including file reads (1 year); CDN logs (90 days); application logs in CloudWatch (90 days) with emails, phone numbers and message text masked; error tracking in Sentry (Germany) with personal data filtered
Malware	Files are scanned with ClamAV: attachments before Nateq sends them by email, and incoming files before anyone can open them. Infected files are blocked
Backups	Automated database snapshots kept 35 days, encrypted, same region
Deletion	Contact and workspace erasure across database, files, search index, AI memory, vectors and cache, with a certificate
Incident response	Written breach runbook; customer notice within 24 hours (section 8)

Annex 3: Sub-processors

This list is current on the date above. The live list, including where each provider processes data and whether it has acceded to the SDAIA SCCs, is at nateq.io/subprocessors.

A. Sub-processors (always in the data path)

Provider	Function	Data	Location
Amazon Web Services	Hosting, database, files, cache, CDN	All Customer Personal Data	Germany (eu-central-1)

Google (Gemini)	AI replies, summaries, embeddings, voice-note transcription, AI memory	Message text, conversation history, contact facts, call transcripts, voice-note audio	Global endpoint, no region set
TypeSafe AI (Jev)	AI routing decisions	Conversation text and decision context	United States
ElevenLabs	Speech-to-text and text-to-speech on calls	Caller audio, AI reply text, voicemail audio	United States
LiveKit	Real-time call media	Live call audio, phone numbers	United States
Meta Platforms	WhatsApp, Messenger and Instagram delivery	Messages, media, phone numbers and IDs	Meta data centres (global); messages kept up to 30 days
Resend	Email sending and receiving	Email content, addresses, attachments	Ireland
Postmark	Workspace email subdomains for inbound mail and campaign replies; backup email sending	Email content, addresses, attachments	United States
Sentry	Error tracking	Error events with personal data filtered	Germany
Cloudflare (Turnstile)	Bot protection on widget and forms	Visitor IP, browser signals	Cloudflare network

B. Customer-enabled integrations (only if Customer connects them; see section 5.4): Gmail and Google Workspace, Microsoft 365; HubSpot, Salesforce, Pipedrive, Zoho CRM; Zendesk, Freshdesk; Shopify, Salla, Zid, Foodics, WooCommerce, Meta catalog; Aramex, DHL, SMSA; Slack, Microsoft Teams; Notion, Asana, Jira, Trello; Google and Microsoft calendars; Customer's own webhooks.

Annex 4: Transfer basis

Transfers to Nateq rely on exemption case D of the Transfer Regulation, with the SDAIA SCCs (Template 2) as the safeguard and Customer's risk assessment. Sensitive Data from Saudi workspaces has no transfer route today and must stay out of the platform.

1. **Purpose.** Providing a service or benefit to the data subject, a permitted purpose under Transfer Regulation article 2(2).
2. **Adequacy.** Not available: SDAIA has not published its list of adequate countries, and an EU adequacy decision does not count.
3. **Exemption case.** Article 4(2)(D): the transfer provides a service directly to the data subject, within their expectations and interests. Customer's end users contact Customer for support through Nateq.
4. **Safeguard.** Case D names an accreditation certificate held by the recipient. SDAIA has not yet published licensed certification bodies, so none can be obtained. Until then the parties sign the SDAIA SCCs, Template 2, unchanged (section 6.2), and Nateq will apply for the certificate once bodies are listed (section 6.7).
5. **Risk assessment.** Customer carries it out before transferring (article 7). Annexes 1, 2 and this Annex supply the facts it needs.
6. **Sensitive Data.** Case D excludes Sensitive Data, so Saudi workspaces must not process it (section 3.5).
7. **Onward transfers.** Only to Sub-processors that accede to the SDAIA SCCs (Template 2, section 8). Each Sub-processor's status is shown at nateq.io/subprocessors.

Appendix: SDAIA Standard Contractual Clauses (Template 2, Controller to Processor)

The SDAIA Standard Contractual Clauses for Personal Data Transfer, version 1.0 (September 2024), Template 2, apply unchanged between Customer (exporter) and Nateq (importer). The official text is published by SDAIA at https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf. The details their appendices ask for are given in Annex 1 (description of the transfer), Annex 2 (security measures) and Annex 3 (sub-processors) of this DPA.