Data Processing Agreement

Version: 1.1 · **Effective date:** 2026-11-18

This is the one standard agreement for every customer. It is not negotiated per customer.

1. Parties and scope

1.1 This Data Processing Agreement ("DPA") is between:

- **The customer** named in the signature block ("Customer"), and
- **The Next Gen (جيل الغد) Company, a private limited company (General Trading) registered in Erbil, Kurdistan Region of Iraq, under Companies Law No. 21 of 1997, trade number 20250104343449, registered 1 October 2025**, the operator of the nashir.ai service ("nashir"). Registered address: Erbil, Erbil Center, Bakhtiari, Gulan 48, 427. Contact address for notices and support: Gulan Str., Nergiz Plaza Building, 4th floor, Office 409, Erbil.

1.2 It forms part of the nashir Terms of Service (the "Agreement") and applies whenever nashir processes personal data on the Customer's behalf and that processing is subject to the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR"), the UK GDPR, or a law that imposes equivalent processor obligations.

1.3 Annexes I, II and III are part of this DPA.

2. Definitions

2.1 "Personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meanings given in Article 4 GDPR.

2.2 "Customer Personal Data" means personal data that nashir processes on the Customer's behalf to provide the service, as described in Annex I.

2.3 "Subprocessor" means a third party that nashir engages and that processes Customer Personal Data.

2.4 "SCCs" means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914.

3. Roles and instructions

3.1 The Customer is the controller of Customer Personal Data (or a processor acting for its own controller). nashir is the processor (or sub-processor).

3.2 nashir processes Customer Personal Data only on the Customer's documented instructions. The instructions are: the Agreement, this DPA, the Customer's configuration and use of the service (including the channels it connects, the features it switches on and the calls it makes through the API), and written instructions the Customer gives through support@nashir.ai.

3.3 nashir will tell the Customer if it believes an instruction breaks the GDPR or other EU or Member State data protection law.

3.4 nashir is an independent controller for the personal data of the Customer's own account users that it needs for its own purposes: account administration, billing, security and legal compliance. That processing is described in the nashir Privacy Policy and is outside this DPA.

3.5 The Customer is responsible for the lawfulness of the data it sends to nashir, for having a legal basis and any consent needed to message its end customers, and for informing them.

4. nashir's obligations

4.1 Confidentiality. On the date of this DPA, only nashir's managing director has access to Customer Personal Data, apart from the Subprocessors listed in Annex III. nashir will bind any employee or contractor in writing to confidentiality before giving them access.

4.2 Security. nashir applies the technical and organisational measures in Annex II. Annex II lists only measures that exist on the effective date. nashir may change the measures as long as the overall level of protection does not fall.

4.3 Assistance. Taking into account the nature of the processing and the information available to it, nashir assists the Customer with: responding to data subject requests (section 7), security of processing, breach notification (section 8), and data protection impact assessments and prior consultation (Articles 32 to 36 GDPR).

4.4 Records. nashir keeps a record of the categories of processing it carries out for the Customer. Annex I is that record at the level of this DPA.

5. Use of AI providers

5.1 When the Customer switches on nashir's AI assistant for a channel, the content of the conversations on that channel (message text, and images, voice notes and documents sent by the end customer) is sent to the AI providers listed in Annex III to generate replies, transcribe audio, describe images and search the Customer's knowledge base.

5.2 When the AI assistant is off, inbound messages are stored and forwarded to the Customer's own webhook without being sent to an AI provider. There is one exception, which the Customer can switch off: when the Customer sends a text message through the nashir API, nashir by default runs a product-lookup step that sends the end customer's most recent inbound message to an embedding provider (OpenAI) and, where query expansion is enabled, to a language model (Google Gemini through OpenRouter). This happens when that inbound message contains price, order, availability or photo wording or names a product in the Customer's catalog. The Customer switches the step off for a send by setting `skip_presentation` to `true` in the request, on the send-message endpoint and on the reply-to-message endpoint. nashir then sends the text exactly as given and makes no product lookup and no call to an AI provider for that send. See Annex I, section 6.

5.3 nashir does not use Customer Personal Data to train AI models. The AI providers' public terms, read on 2026-11-12, say the following about data sent through their paid interfaces (sources in Annex III, section 3):

- Anthropic: may not train models on customer content from its API services.
- OpenAI: does not use API data to train or improve its models unless the customer opts in.
- Google: does not use prompts or responses of the paid Gemini API to improve its products; content sent through the unpaid tier is used.

- OpenRouter: does not itself use inputs or outputs for training. nashir limits which model providers OpenRouter may send data to through the privacy settings of its OpenRouter account: every provider that trains on inputs or publishes prompts is switched off, the 1% data discount is off, and input and output logging is off (confirmed in the account settings on 2026-11-12). These settings apply to every request made with the account, including requests made by nashir's automation workflows. Every model nashir uses through OpenRouter is served by a provider that OpenRouter lists as not training on inputs. Some of these providers keep prompts for a limited period for their own operation; see the subprocessor list.
- Microsoft (Azure AI Speech): real-time speech audio and text are not stored. Microsoft's Data Protection Addendum, which applies to Azure Speech, limits Microsoft's use of customer data to providing the service and the business operations it lists.

6. Subprocessors

6.1 The Customer gives nashir a general authorisation to engage Subprocessors. The current list is in Annex III and is published at https://nashir.ai/legal/subprocessors once that page is live.

6.2 nashir will give the Customer at least 30 days' notice before a new Subprocessor starts processing Customer Personal Data, by updating the published list and by email to every active account owner. nashir keeps a log of each notice: the date, the change and the recipients.

6.3 The Customer may object in writing within those 30 days on reasonable data protection grounds. If the parties cannot resolve the objection, the Customer may end the affected service and receive a refund of prepaid fees for the unused period. This refund applies in this case only; here it overrides the rule in the Terms of Service that no refund is issued for a partial period.

6.4 nashir puts data protection obligations on each Subprocessor that are in substance the same as those in this DPA, and remains responsible to the Customer for each Subprocessor's performance. Data processing agreements are in place as follows. The data processing terms of Anthropic, OpenAI, OpenRouter, Hostinger, Cloudflare and Resend apply automatically as part of their service terms. The data processing agreement with Zoho was signed on 2026-11-12. Microsoft's Data Protection Addendum is incorporated by reference into its Product Terms and applies to Azure Speech without a separate signature.

6.5 Messaging platforms (Meta for WhatsApp, Messenger and Instagram; TikTok) carry the Customer's messages under the Customer's own agreements with those platforms. Whether they are nashir's Subprocessors, the Customer's own processors or independent controllers is set out in Annex III.

7. Data subject requests

7.1 If a data subject contacts nashir about Customer Personal Data, nashir will pass the request to the Customer without undue delay and will not answer it itself, unless the Customer instructs otherwise or the law requires it.

7.2 The service gives the Customer these tools on the effective date:

- read a person's conversation in the inbox;
- export contact lists as CSV (contact fields only, not messages);
- delete a WhatsApp audience contact (removes the contact record only);
- archive a CRM contact (hides it; the record is kept and can be restored).

7.3 There is no self-service tool that exports or erases all data held about one person. On the Customer's written request, nashir will carry out that export or erasure within 30 days, following its internal data-subject-request procedure, which lists the records it covers and those it does not. Data in backups is not altered and expires with the backup (Annex II, section 9).

7.4 The erasure of one person covers, in the Customer's account: contacts, messages and attachments, assistant and knowledge-search logs, CRM records, bookings, consent history, send and call logs, webhook delivery logs, raw webhook records from the messaging platforms (also after the channel was disconnected), webhook records from a connected store, staged contact-import rows, the person's questions in the "unanswered question" lists, and the matching runs in nashir's automation engine for workflows nashir hosts. The do-not-message entry (phone number only) is kept unless the Customer asks otherwise.

7.5 nashir cannot delete: notifications already delivered to the phones and browsers of the Customer's team, Telegram alerts and emails already sent, messages already delivered to the Customer's own webhook or systems, and the copies held by the messaging platforms and the AI providers.

8. Personal data breach

8.1 nashir will notify the Customer without undue delay, and no later than 72 hours after it becomes aware of a personal data breach affecting Customer Personal Data. nashir follows a written incident procedure and sends the notice with an internal tool that records, for each recipient, when the notice was sent. Its security contact is security@nashir.ai, published at https://nashir.ai/.well-known/security.txt.

8.2 The notice is sent by email to the account owner's address, with security@nashir.ai as the reply address, and contains what nashir knows at the time: what happened, the categories and approximate number of people and records affected, the likely consequences, the measures taken or planned, and a contact point. nashir sends further information as it becomes available.

8.3 nashir will take reasonable steps to contain the breach and will cooperate with the Customer's own notification duties. A notice under this section is not an admission of fault.

9. Retention and deletion during the term

9.1 nashir keeps Customer Personal Data for the periods in Annex I, section 7. Those periods describe what the system does on the effective date, including the records that are currently kept for the life of the account.

9.2 The Customer can delete individual records with the tools in section 7.2 and can ask nashir to delete others.

10. Audits

10.1 On written request, at most once in any 12 months (and also after a personal data breach or when a supervisory authority requires it), nashir will give the Customer the information needed to show that it complies with this DPA, and will answer reasonable written questions.

10.2 nashir holds no third-party security certification and has not had an external penetration test on the effective date. If the information under 10.1 is not enough to meet the Customer's legal duty, the parties

will agree the scope, timing and cost of an audit, carried out remotely by the Customer or by an independent auditor bound by confidentiality.

11. International transfers

11.1 Customer Personal Data is stored on a server in Germany (Annex II, section 1). nashir is established in Iraq and its staff reach the data from Iraq to operate and support the service. Iraq has no adequacy decision from the European Commission. Access from Iraq is therefore treated as a transfer to a third country.

11.2 For that transfer the parties enter into the SCCs, which are incorporated by reference:

- **Module Two** (controller to processor) when the Customer is a controller;
- **Module Three** (processor to processor) when the Customer is itself a processor.

11.3 The SCCs are completed as follows.

- Clause 7 (docking clause): applies.
- Clause 9(a): Option 2, general written authorisation; notice period 30 days (section 6.2).
- Clause 11(a): the optional independent dispute resolution body is not used.
- Clause 17: Option 1; the law of the EU Member State in which the Customer is established. If the Customer is not established in a Member State, the law of Ireland.
- Clause 18(b): the courts of that same Member State.
- Annex I.A, I.B and I.C of the SCCs: Annex I of this DPA. The competent supervisory authority is the authority of the Member State in which the Customer is established.
- Annex II of the SCCs: Annex II of this DPA.
- Annex III of the SCCs: Annex III of this DPA.

11.4 For transfers subject to the UK GDPR, the UK International Data Transfer Addendum to the SCCs applies. For transfers subject to the Swiss Federal Act on Data Protection, the SCCs apply with the adaptations required by the Swiss authority.

11.5 Onward transfers from nashir to Subprocessors outside the European Economic Area are made under clause 8.8 of the SCCs. The mechanism for each Subprocessor is listed in Annex III: an adequacy decision (including the EU-US Data Privacy Framework where the provider is certified), or standard contractual clauses in the provider's own data processing terms.

11.6 nashir has documented a transfer impact assessment for the access from Iraq: the data, who accesses it and why, the laws on government access to data, the risk, and the safeguards in place. nashir gives it to the Customer on request and reviews it when the law or the processing changes.

11.7 nashir has not appointed a representative in the European Union under Article 27 GDPR. nashir has not appointed a data protection officer.

12. End of the Agreement

12.1 When the Agreement ends, the Customer chooses whether nashir deletes or returns Customer Personal Data. Return means an export of the Customer's contacts and messages in a common machine-readable format, produced manually by nashir within 30 days of the request. If the Customer does not choose within 30 days, nashir may delete.

12.2 Deletion is carried out with the account deletion process described in Annex I, section 8. On the effective date that process removes the main content immediately but leaves the records listed there. nashir will delete those remaining records on the Customer's written request, following its internal complete-deletion procedure. Billing records are kept as described in 12.4.

12.3 An account whose subscription has simply lapsed is not deleted automatically. Its data is kept until the Customer deletes the account or asks nashir to delete it.

12.4 nashir may keep data that the law requires it to keep (for example billing records), for only as long as the law requires, and keeps it confidential. Backups expire as described in Annex II, section 9.

12.5 On request nashir confirms the deletion in writing.

13. Liability

Each party's liability under this DPA is subject to the limits and exclusions in the Agreement, including the cap in the Terms of Service: a party's total liability does not exceed the fees the Customer paid in the 12 months before the claim. Nothing in this DPA limits a data subject's rights under the SCCs or the GDPR.

14. General

14.1 If this DPA and the Agreement conflict on the processing of Customer Personal Data, this DPA prevails. If this DPA and the SCCs conflict, the SCCs prevail.

14.2 This DPA applies for as long as nashir processes Customer Personal Data for the Customer.

14.3 This DPA is governed by the laws of Iraq, and disputes under it are subject to the courts of Erbil, Iraq. The SCCs are the exception: they keep the law and the courts of an EU Member State (clauses 17 and 18, as completed in section 11.3), because the SCCs require it.

14.4 nashir may update Annexes II and III as described in this DPA. Other changes need both parties' written agreement.

14.5 This DPA is made in English and in Arabic. If the two versions differ, the English version prevails.

Annex I — Description of the processing

1. Parties

Data exporter: the Customer (name, address, contact person and role as given in the signature block). Role: controller, or processor for its own controller.

Data importer: The Next Gen (جيل الغد) Company, a private limited company (General Trading) registered in Erbil, Kurdistan Region of Iraq, under Companies Law No. 21 of 1997, trade number 20250104343449, registered 1 October 2025, operator of nashir.ai. Registered address: Erbil, Erbil Center, Bakhtiari, Gulan 48, 427. Contact address: Gulan Str., Nergiz Plaza Building, 4th floor, Office 409, Erbil. Contact: support@nashir.ai, +964 7706 930 930; security contact: security@nashir.ai. Role: processor.

2. Data subjects

- The Customer's end customers and prospects: people who message the Customer, comment on its posts, call it, or are on its contact and broadcast lists.

- The Customer's team members who use the service, where they appear in conversation records (for example as the agent who replied).

3. Categories of personal data

- Identifiers: phone number, WhatsApp ID, Facebook, Instagram or TikTok user ID, display name, username, profile picture.
- Message content: the text of direct messages and comments, both directions; images, video, voice notes and documents exchanged; message timestamps and delivery status.
- Contact and CRM records: tags, custom fields, lifecycle stage, notes, consent and opt-out status, deals, tasks, the ad a conversation started from.
- Bookings: name, phone, appointment time, notes.
- Broadcast records: recipient phone number, template used, delivery and read status.
- Call records for WhatsApp calling: phone number, time, duration. Call audio is processed live when the voice add-on is used and is not recorded.
- AI records, when the assistant is on: the questions asked, the knowledge used and the replies generated.
- Technical records: raw webhook payloads received from the messaging platforms, logs of messages forwarded to the Customer's webhook.

Special categories of data: the service is not designed for them and nashir does not ask for them. End customers may include them in free-text messages. The Customer must not use the service to process special categories on purpose.

4. Nature and purpose of the processing

Receiving, storing, displaying, forwarding and sending messages and comments on the channels the Customer connects; sending broadcasts; keeping contact and CRM records; handling bookings; when switched on, generating automated replies with AI providers; sending alerts to the Customer's team; technical support and security.

5. Frequency and duration

Continuous, for the term of the Agreement and until deletion under section 12.

6. Processing by AI providers

Situation	Is message content sent to an AI provider?
AI assistant on for the channel	Yes. Inbound text, images, voice notes and documents, the recent conversation and the knowledge base excerpts go to the reply, transcription, vision and embedding providers in Annex III.
AI assistant off; inbound messages	No. They are stored and forwarded to the Customer's webhook only.

Situation	Is message content sent to an AI provider?
AI assistant off; Customer sends a text message through the API without `skip_presentation`	Sometimes. The end customer's most recent inbound message is sent to OpenAI (embeddings) and, where query expansion is enabled, to Google Gemini through OpenRouter, when it contains price, order, availability or photo wording or names a catalog product.
AI assistant off; Customer sends a text message through the API with `skip_presentation` set to `true` (send-message or reply-to-message endpoint)	No. The text is sent exactly as given. No product lookup and no call to an AI provider is made for that send.
The Customer registers its own automation as a "custom chatbot" workflow in nashir	Treated as an assistant: the product-lookup step can also run on inbound messages when the Customer has a catalog with photos.
A team member starts an action that uses AI (for example importing conversation history to build a knowledge base)	Yes, for that action only.

7. Retention while the account is active

Data	Kept for	Enforced by
Messages and comments in the inbox	90 days from the message date, then deleted	Daily automatic deletion. Checked on the live system on 2026-11-11: no WhatsApp message older than the window.
Comments on old posts	Can reappear after deletion when the platform sends them again; about 3,000 such comment records older than 90 days existed on 2026-11-11	No rule
Raw webhook payloads from Meta (contain message text and phone numbers)	90 days	Daily automatic deletion
Two archives of selected raw webhook payloads	No limit	No rule
Message preview (up to 280 characters) in each contact's timeline	No limit; kept for the life of the account	No rule
End customers' questions in knowledge-search logs and "unanswered question" lists (only when the assistant or knowledge search is used)	No limit	No rule
Log of messages forwarded to the Customer's webhook (full payload)	7 days after delivery; 30 days if failed	Daily automatic deletion

Data	Kept for	Enforced by
Stored inbox media	Deleted after the message it belongs to is deleted; documents after 30 days. Applies only to accounts on the newer media storage. Media re-hosted from Facebook and Instagram for other accounts has no limit.	Daily automatic deletion
Profile pictures of people who message through Facebook or Instagram	No limit; kept in publicly readable storage at a predictable address	No rule
Contacts, CRM records, deals, bookings, consent records, conversation status	Life of the account, or until the Customer deletes them. Archived CRM contacts are not erased.	No rule
Broadcast recipient records	365 days	Daily automatic deletion
Broadcast send log (recipient phone)	No limit	No rule
AI processing traces	90 days	Daily automatic deletion
Activity logs (sign-ins, billing actions, IP address)	90 days	Daily automatic deletion
Audit log of changes (IP address, browser)	No limit	No rule
Run history of nashir's automation engine, which contains message content when the assistant is on	Finished runs: at most 14 days. Runs that did not finish are not removed automatically; 48 such runs, the oldest from January 2026, were stored on 2026-11-16. All are removed when the workflow they belong to is deleted.	The engine's automatic deletion
Backups	According to the hosting provider's rotation (Annex II, section 9)	Hosting provider

8. Deletion of the account

When the account owner deletes the account, nashir immediately and permanently deletes: connected channels and their tokens, messages, WhatsApp contacts, CRM contacts and deals, bookings, broadcasts, templates, knowledge base, posts, workflows and API keys. Tokens are revoked at the providers on a best-effort basis.

Not deleted by that process on the effective date: the team record and the user record (kept in a deactivated state; the user's email address remains recognisable), activity logs (deleted 30 days later), the audit log, billing records, and a set of secondary records including Facebook and Instagram contact profiles, consent and suppression records, the broadcast send log, call logs, support chat with nashir, and some stored media. The run history in nashir's automation engine is removed together with the account's workflows.

nashir then completes the deletion with its internal procedure, which also removes the account's raw webhook records from the messaging platforms and from a connected store, and the run history of the

workflows nashir hosted for it. Records about a channel account that another active customer also uses are kept.

Deleting a single business inside an account does not delete its messages and WhatsApp contacts; they move to the account's "Unassigned" business.

9. Subprocessors

See Annex III.

Annex II — Technical and organisational measures

Only measures that were confirmed in the code or on the live system on the effective date are listed.

1. Hosting and location

- The application, nashir's database, file storage and nashir's automation engine run on nashir's servers in Germany, rented from Hostinger.
- Public traffic reaches the server through Cloudflare.

2. Encryption

- In transit: HTTPS for all public traffic, enforced with HSTS at the Cloudflare edge.
- Channel access tokens (Meta, TikTok, Google, LinkedIn, Telegram bot tokens) are encrypted in the database with AES-256-GCM. Checked on the live system on 2026-11-11: all stored tokens are encrypted.
- Passwords are stored as bcrypt hashes. API keys are stored as SHA-256 hashes and shown once.
- The database and the server disk as a whole are not encrypted at rest.

3. Access control in the application

- Each customer's data is separated by team in every query.
- Roles for team members (owner, manager, agent, viewer) with per-member permissions.
- Sign-in is rate limited per IP address and per email address. A password reset ends all existing sessions.
- A verified email address is required before API keys or webhooks can be created.
- Two-step verification with an authenticator app (time-based one-time codes) is available. No codes are sent by SMS or email. It is required for nashir administrator accounts: until an administrator has set it up and passed it, the account has no administrator rights, in the admin panel, in the admin interfaces and for "log in as customer". For customers' users it is optional and off by default: each user can turn it on in their own account settings, and the mobile app then asks for the same code at sign-in. If one of the user's phones runs a version of the app that cannot ask for the code, setup waits until that app is updated. It is also required for the accounts of regional partners: a partner account that has not set it up cannot open any partner page or use "log in as customer".
- A user sets it up by scanning a QR code and receives 10 single-use recovery codes, stored as hashes; the authenticator secret is stored encrypted. A user can mark a browser as remembered for 30 days; remembered browsers are listed in the account settings and can be removed, and all of them are removed when the password is changed or reset or when two-step verification is turned off or reset. Wrong codes are rate limited.

4. Access by nashir staff and partners

- Only accounts flagged as administrator can open the admin panel. "Log in as customer" sessions last 1 hour and their start and end are logged.
- Every time an administrator or a partner views a customer's conversations, contacts or account, a record is written to an internal access log. This covers the admin panel, the partner portal and every "log in as customer" session; for those sessions the start, the end, each page opened and each conversation, contact, export or import read are recorded. Each record holds who viewed, which customer account, what was opened (a reference to the item, never message content), when, the IP address and the browser. Repeated reads of the same item by the same person within 60 seconds are recorded once.
- Records in the access log cannot be changed, and cannot be deleted for 12 months; the database enforces this. Only nashir's administrator can read the log, in the internal admin panel; customers and partners cannot.
- The access log does not cover direct access to nashir's database, the automation engine's own editor and run history, or the administration consoles of the servers and file storage.
- Direct access to nashir's database is possible only through a restricted, authenticated channel, with an account that has no standing privileges; statements that change data are logged.
- In some markets, a regional partner confirms customers' subscription payments and provides support to customers in that market, including refund requests. It has access only to customers in its own market and none to customers in other markets.
- Internal operations alerts name an end customer's phone number only in masked form (country code and last 2 digits).

5. Database exposure

- Anonymous access to nashir's database is blocked for every table, and database-level access rules are enabled on most tables (checked 2026-11-11). The application enforces the separation between customers in its own code.

6. Protection of interfaces

- Incoming webhooks from Meta, TikTok, the payment gateways, Resend and Salla are verified with a signature before they are processed.
- Requests to addresses supplied by customers are restricted to public addresses.
- A content security policy is set on all pages.

7. Files

- Inbox attachments, knowledge base files and catalog images are in private storage and are served through signed, time-limited links.
- Post images, WhatsApp template media and profile pictures are in publicly readable storage; listing their contents is blocked.

8. Logging

- Changes made through the application are written to an audit log with the user, IP address and browser.
- Sign-ins, password changes and billing actions are written to an activity log.

- Views of customer data by nashir administrators and partners are written to the internal access log described in section 4.
- Two-step verification events of users, administrators and partner accounts are written to the same internal log: turned on, turned off, reset, recovery code used, recovery codes regenerated, remembered browser added or removed.

9. Backups

- The hosting provider (Hostinger) makes automated daily and weekly backups of the whole server, which includes the database and the stored files.
- The backups are stored separately from the server, inside the EU (Lithuania), and are kept according to the provider's rotation.
- A restore from these backups has not been tested yet.

10. Organisation

- Secrets are kept in protected configuration, separate from the code, and code changes are scanned for secrets before they are saved.
- nashir has a written incident response procedure (detection, severity, containment, customer notice within 72 hours, incident log), a published security contact, security@nashir.ai, and an internal tool that sends the breach notice and logs each recipient.
- nashir has written internal procedures for a data-subject request (export or erasure of one person's records) and for completing the deletion of an account.
- nashir has no written information security policy, staff confidentiality undertakings, security certification or penetration test on the effective date.

Annex III — Subprocessors

The current list, with the purpose, data, location and transfer mechanism for each provider, is in the Subprocessor list (https://nashir.ai/legal/subprocessors). The notice and objection process is in section 6 of this DPA.

Signatures

	Customer	nashir
Legal name		The Next Gen (جيل الغد) Company — private limited company (General Trading); trade number 20250104343449
Registered address		Erbil, Erbil Center, Bakhtiari, Gulan 48, 427
Contact address		Gulan Str., Nergiz Plaza Building, 4th floor, Office 409, Erbil
Signed by (name)		أُبي مجيد صالح / Ubai Majeed Salih
Title		Managing Director
Contact email for notices		support@nashir.ai
Date		
Signature		

DPA version 1.1.

Annex III — Subprocessor list

Subprocessors

Version: 1.1 · **Effective date:** 2026-11-18

This page lists the third parties that process personal data when The Next Gen (جيل الغد), Erbil, Iraq, provides nashir.ai, the service it operates, to customers. It is Annex III of the nashir Data Processing Agreement.

How to read this list

- "Customer data" means data about a customer's own end customers: phone numbers, names, messages and media.
- A provider receives data only when the feature named in its section heading or its row is used.
- The processing locations and transfer mechanisms below are taken from each provider's public terms, read on 2026-11-12. The data processing terms of Anthropic, OpenAI, OpenRouter, Hostinger, Cloudflare and Resend apply automatically with their service terms; the agreement with Zoho was signed on 2026-11-12; Microsoft's addendum applies to Azure Speech without a separate signature.

1. Infrastructure (always used)

Provider	Purpose	Data	Location	Transfer mechanism
Hostinger	The servers that run the application, nashir's database, file storage and nashir's automation engine; automated daily and weekly backups, stored separately from the servers	All customer data	Server: Germany. Backups: Lithuania.	None needed; data stays in the EU. Hostinger's group is based in the EU.
Cloudflare	Network proxy in front of the website, API and file storage; protection against attacks; secure channel for database administration	All traffic passes through it, including message content in API calls and stored media that it caches	Global network; requests are handled at the nearest location	Cloudflare's data processing terms with SCCs; Cloudflare is certified under the EU-US Data Privacy Framework

2. Messaging platforms (when the customer connects the channel)

Provider	Purpose	Data	Location	Transfer mechanism
Meta (WhatsApp Business Platform, Messenger, Instagram, Threads)	Delivering and receiving the customer's messages, comments, broadcasts and calls	Recipient phone numbers and user IDs, message content, media, templates	Meta's global infrastructure	Under the customer's own terms with Meta. Meta's role (processor for the customer, or independent controller) follows Meta's terms.
TikTok	Receiving and answering TikTok direct messages and comments; publishing	TikTok user IDs, message and comment content	TikTok's servers; its privacy policy names Singapore, Malaysia, Ireland and the United States	Under the customer's own terms with TikTok
Google (YouTube), LinkedIn, Telegram	Publishing the customer's posts to its own channels	Post content; no end-customer data	Provider's infrastructure	Under the customer's own terms with each platform

3. AI providers (when the AI assistant or an AI feature is on)

Provider	Purpose	Data	Location	Transfer mechanism
Anthropic	Writing the assistant's replies; reading images and documents sent by end customers	Message text, recent conversation, knowledge base excerpts, images and documents	Stored in the United States; Anthropic may route processing through the United States, Europe, Asia and Australia	Anthropic's data processing addendum, part of its Commercial Terms, with SCCs (Modules Two and Three)
OpenRouter	Routes requests to the model providers below; fallback replies	Same data as the model it routes to	United States	OpenRouter's data processing agreement, incorporated into its terms, with SCCs (Module Two). It passes data on to the model providers under their own terms; nashir restricts which providers it may use (see the training table below).
Google (Gemini models, reached through OpenRouter)	Transcribing voice notes, reading documents, expanding search queries, matching product photos	Voice notes, documents, images, the customer question being searched	Any country where Google or its agents maintain facilities	nashir has no direct agreement with Google for these models; the data reaches Google through OpenRouter (see the OpenRouter row)

Provider	Purpose	Data	Location	Transfer mechanism
OpenAI (direct and through OpenRouter)	Search embeddings for the knowledge base and for end-customer questions; describing images; comment moderation; fallback replies; live voice on the website widget	Customer questions, knowledge base text, images, comment text; live audio when web voice is used	OpenAI's infrastructure; its public API pages name no default location	OpenAI's data processing addendum, incorporated into its services agreement
Microsoft (Azure AI Speech)	Speech recognition and speech output for the WhatsApp voice-call add-on	Live call audio and the reply text	United Arab Emirates (Azure region UAE North)	Microsoft Products and Services Data Protection Addendum (version of 1 November 2026). It is incorporated by reference into Microsoft's Product Terms and applies without a separate signature; the Product Terms list Azure Speech as a core online service; transfers out of the EEA are under the 2021 SCCs.

Use of API data for model training

From each provider's public terms, read on 2026-11-12.

Provider and product	Used for training by default?	Retention stated	Source and page date
Anthropic — Claude API (Commercial Terms)	No. Anthropic may not train models on customer content from the services. Exceptions: feedback the customer explicitly submits, or an opt-in.	Inputs and outputs deleted within 30 days, longer where needed to enforce its usage policy or by law	https://www.anthropic.com/legal/commercial-terms (effective 2025-06-17); https://privacy.claude.com/en/articles/7996868
OpenAI — API platform, including audio and realtime	No, unless the customer opts in	Abuse-monitoring logs up to 30 days	https://developers.openai.com/api/docs/guides/your-data (no date shown)
Google — Gemini API, paid services	No. Prompts and responses are not used to improve Google's products.	Logged for a limited period for abuse detection; no number given	https://aistudio.google.com/docs/terms (effective 2026-03-23)
Google — Gemini API, unpaid services	Yes, and human reviewers may read the content	Not stated	Same page

Provider and product	Used for training by default?	Retention stated	Source and page date
OpenRouter — its own processing	No, unless the account opts in to prompt logging. Logging is off on nashir's account (confirmed in the account settings, 2026-11-12).	Prompts and responses are not stored unless the account opts in; metadata is stored	https://openrouter.ai/privacy and https://openrouter.ai/terms (2026-08-31)
OpenRouter — requests routed to Google and OpenAI models	No. Routing is restricted to providers that OpenRouter lists as not training on inputs. On nashir's account all training and prompt-publishing endpoints, the 1% data discount, and input and output logging are off (confirmed in the account settings, 2026-11-12). The settings apply to every request made with the account, including requests from the automation workflows. The providers that serve the models in use are Google AI Studio, Google Vertex, OpenAI, Azure and Amazon Bedrock, each listed as not training (read 2026-11-12).	Set by the upstream provider. OpenRouter lists Google AI Studio as keeping prompts for 55 days and OpenAI as keeping prompts; it lists Google Vertex, Azure and Amazon Bedrock as not keeping them.	https://openrouter.ai/docs/features/provider-routing and OpenRouter's public provider list (read 2026-11-12)
Microsoft — Azure AI Speech (speech to text, text to speech)	Microsoft publishes no express statement on training for standard speech. Its Data Protection Addendum limits its use of customer data to providing the service and the business operations it lists. Real-time audio and text are not retained or stored.	None for real-time processing	https://learn.microsoft.com/en-us/azure/foundry/responsible-ai/speech-service/speech-to-text/data-privacy-security (2026-03-31); Microsoft Products and Services Data Protection Addendum (2026-11-01)

On the official EU-US Data Privacy Framework list, read on 2026-11-12, Cloudflare, Google and Microsoft are active participants and Resend is listed as active with its re-certification under review. Anthropic, OpenAI, OpenRouter and Zoho are not active participants. Anthropic's data processing addendum (https://www.anthropic.com/legal/data-processing-addendum, effective 2025-02-24) is part of its Commercial Terms and includes standard contractual clauses, Modules Two and Three. OpenAI's data processing addendum (effective 2026-01-01) is incorporated into its services agreement.

With the AI assistant off, one path still reaches OpenAI and possibly Google Gemini: a text message sent through the nashir API can trigger a product lookup on the end customer's last inbound message. The

customer switches this off for a send by setting `skip_presentation` to `true` in the request. See the Data Processing Agreement, Annex I, section 6.

4. Notifications and email

Provider	Purpose	Data	Location	Transfer mechanism
Resend	Sending email to the customer's team (account email, alerts)	Team members' email addresses; alert emails can contain an end customer's name and phone number (for example a new booking)	United States	Resend's data processing addendum, part of its terms, with SCCs
Zoho	Hosts the nashir.ai mailboxes (support@)	Emails the customer sends to nashir, which can contain customer data	United States (Zoho's US data centre)	Zoho's data processing addendum, signed on 2026-11-12
Telegram	(a) Alerts to the customer's own Telegram chat when it links one. (b) nashir's internal operations alerts.	(a) End customer's display name, masked phone number and a message preview of up to 140 characters. (b) Error alerts; an end customer's phone number appears only masked (country code and last 2 digits).	Telegram's data centres. Telegram states a location (the Netherlands) only for users who sign up from the United Kingdom or the EEA	None. Telegram offers no data processing agreement.
Google (Firebase Cloud Messaging), and the push services of Apple, Google and Mozilla browsers	Push notifications to the team's phones and browsers	Sender name and a message preview, unless previews are switched off	Provider's infrastructure	Firebase Data Processing and Security Terms, which provide for SCCs and the Data Privacy Framework

5. Regional partners

In some markets, a regional partner confirms customers' subscription payments and provides support to customers in that market, including refund requests. It has access only to customers in its own market and none to customers in other markets.

6. Store integrations (when the customer connects a store)

Provider	Purpose	Data	Location	Transfer mechanism
Salla	Receives order notifications from the customer's store to send over WhatsApp; product import	Shopper phone number and message text, received from Salla	Salla is established in Saudi Arabia	Under the customer's own terms with Salla

7. Payment providers (not subprocessors)

Wayl (Iraq), Paymob (Saudi Arabia), EasyKash (Egypt), Switch (legacy) and Binance Pay handle the customer's own subscription payments. They receive the account holder's billing details (amount, email; EasyKash also name and mobile number). They do not receive data about the customer's end customers, and nashir uses them as a controller of its own billing. They are listed for transparency.

8. Not used

- No third-party error tracking service.
- No advertising or product analytics service.
- Cohere was removed from the service in 2026.

9. Changes to this list

nashir gives at least 30 days' notice before a new subprocessor starts processing customer data, by updating this page and by email to account owners. Customers can object as described in section 6 of the Data Processing Agreement. nashir keeps a log of each notice sent.

Change log

Date	Change
2026-11-12	Version 1.0
2026-11-18	Version 1.1. No subprocessor added or removed. The API product lookup can now be switched off per send (`skip_presentation`).