

Zoorik Data Processing Agreement

For Coral · Version 1.0 · 23 October 2026

This Data Processing Agreement (the “DPA”) applies when Zoorik Private Limited (CIN U62011KA2026PTC228102), whose registered office is at Vaishnavi Signature, No. 78/9, Outer Ring Road, Bellandur, Bangalore South, Bangalore 560103, Karnataka, India (“Zoorik”), and a client (the “Client”) sign a Pilot Schedule, or another order, that names this version (the “Pilot Schedule”). The Client does not sign this DPA on its own: signing the Pilot Schedule makes it part of the agreement for the pilot, beside the Zoorik Pilot Terms that the Pilot Schedule names (the “Pilot Terms”). This DPA is the contract between a Data Fiduciary and its Data Processor that section 8(2) of India’s Digital Personal Data Protection Act, 2023 (the “DPDP Act”) requires.

How this DPA fits with the other documents:

- Where this DPA differs from the Pilot Terms or Zoorik’s Terms of Use (zoorik.com/terms) on personal data, including section 8 of the Terms of Use, this DPA wins.
- The Mutual Non-Disclosure Agreement between the parties still governs confidentiality generally.
- Zoorik’s Privacy Policy (zoorik.com/privacy) covers the personal data that Zoorik controls itself, as section 1 below sets out.
- This DPA is the same for every client. A change for one client is valid only if the Pilot Schedule states it, and on that point the Pilot Schedule wins.
- Zoorik never changes a version once a Pilot Schedule names it. A later version applies only to a Pilot Schedule that names that version.

1. Roles and scope

Cluster Data means the data the Coral agent sends to Zoorik from the Client’s clusters, as Annex 1 describes. Data Fiduciary, Data Processor, Data Principal, personal data, processing and personal data breach have the meanings the DPDP Act gives them.

- **The Client** is the Data Fiduciary for the personal data in its Cluster Data, and Zoorik processes that data as the Client’s Data Processor.
- **If the Client processes that data for its own customers**, Zoorik is the Client’s sub-processor. The Client confirms that it may appoint Zoorik, and passes on to Zoorik in writing the instructions it receives that apply to Zoorik’s processing.
- **Zoorik’s own data:** Zoorik is the Data Fiduciary for the account data of the Client’s people who use the Coral console (their names, email addresses and sign-ins) and for its own logs, under its Privacy Policy, not this DPA.
- **In the Client’s clusters:** the Coral agent, its admission webhook and the node daemon run in the Client’s clusters (Pilot Terms, section 6). What they read there and do not send to Zoorik, including the node daemon’s checkpoints of pod memory, stays in the Client’s clusters and cloud account. The node daemon has no connection to Zoorik.

2. Instructions

- Zoorik processes Cluster Data only on the Client's instructions and only to provide Coral to the Client. The instructions are this DPA, the Pilot Schedule, the Pilot Terms, the Client's settings in Coral, and the Client's written requests (email is enough).
- Zoorik does not sell Cluster Data or use it for advertising.
- Zoorik tells the Client if it thinks an instruction breaks the law.
- If the law requires Zoorik to process or disclose Cluster Data in another way, for example to a government body or court, Zoorik does only what the law requires and tells the Client first, unless the law forbids it.
- Zoorik tells the Client before a Coral release changes what Cluster Data the agent sends (Annex 1).

3. Zoorik's people

Everyone at Zoorik who can access Cluster Data is bound to keep it confidential. Zoorik limits that access to the small number of people who need it to provide Coral, and to the automated tools Zoorik uses to build and deploy Coral.

4. Security

Zoorik protects Cluster Data with the safeguards described in the Zoorik Security Overview: Coral, 23 October 2026, and in section 10 of the Privacy Policy. Annex 2 lists the main ones. Zoorik does not reduce them during the pilot.

5. Sub-processors

- The Client authorises the sub-processors in Annex 3: Microsoft Azure, Cloudflare and Google.
- At least 30 days before Zoorik adds or replaces a sub-processor of Cluster Data, it emails the Client's contacts in the Pilot Schedule, naming the company, what it will do and where.
- The Client may object by email within those 30 days. If the parties cannot resolve the objection, the Client may stop the pilot (Pilot Terms, section 9).
- Zoorik binds each sub-processor to protect Cluster Data at least as strongly as this DPA does, and stays responsible for what each sub-processor does with it.

6. Where Cluster Data is kept

- Zoorik stores Cluster Data, and backs it up, only in Microsoft Azure's Central India region. Backups are not copied to another region.
- Between the Client's clusters and Zoorik, Cluster Data passes through Cloudflare's network, which may route it outside India.
- Zoorik makes no other transfer of Cluster Data outside India without telling the Client first.

7. Personal data breaches

- Zoorik tells the Client's contacts in the Pilot Schedule about a personal data breach affecting Cluster Data without undue delay, and within 24 hours of becoming aware of it. The first notice gives what Zoorik knows then, and Zoorik sends updates as it learns more.
- The notices cover, as far as Zoorik knows them: what happened, when and where; how and why it happened; the data and the Data Principals affected; the likely impact; what Zoorik has done to contain the breach; any findings about who caused it; and what it is doing to stop it happening again.
- Where the law requires it of Zoorik, Zoorik reports the breach to CERT-In and to the Data Protection Board of India. Zoorik helps the Client meet its own duties to tell the Board and the affected Data Principals.

8. Help with requests and the Client's duties

- Zoorik helps the Client answer requests and grievances from Data Principals about personal data in Cluster Data, and meet its other duties under data protection law, such as impact assessments and requests from regulators with authority over the Client.
- If a Data Principal asks Zoorik about Cluster Data, Zoorik refers them to the Client and tells the Client.
- Coral has no self-service tool to delete or export Cluster Data. The Client sends requests about Cluster Data to founders@zoorik.com, and Zoorik carries out deletion requests as section 10 sets out.

9. Information, audit and logs

- Once a year, on written request, Zoorik answers the Client's reasonable security questionnaire and gives the information the Client needs to show that Zoorik meets this DPA.
- Where a regulator with authority over the Client, for example the Reserve Bank of India, requires it, Zoorik gives that regulator and the Client access to information and records about the processing of Cluster Data, on reasonable notice. Zoorik cannot extend this to Microsoft Azure or Cloudflare beyond what they offer under their own terms.
- Zoorik keeps the logs the law requires it to keep.

10. Deletion

- Zoorik deletes the Cluster Data within 30 days after the pilot ends or the Client disconnects Coral (Pilot Terms, sections 6 and 9), or within 30 days after the Client asks in writing, and confirms the deletion in writing.
- Zoorik deletes Cluster Data by hand, at the end of the pilot or on request. Coral itself removes only short-lived data, such as workload signals after 24 hours. Disconnecting a cluster neither deletes its data nor tells Zoorik, so the Client tells Zoorik by email when it disconnects one.
- Copies in Zoorik's database backups expire within 7 days after the deletion.

- Zoorik keeps only what the law requires it to keep, for the period the law sets, uses it for nothing else, and then deletes it.

11. The Client's duties

- The Client has a lawful ground under the DPDP Act for any personal data in its Cluster Data, and gives Data Principals the notices the law requires.
- Where it can, the Client keeps personal data, and in particular passwords, financial details and payment data, out of resource names, labels and the `coral.zoorik.com/configuration` annotation.
- The Client is responsible for its own cloud identities and cluster access, including the identity Coral uses (Pilot Terms, section 6), and for the people it lets into its Coral organisation.

12. Liability

The limits in section 10 of the Pilot Terms, and in sections 13 to 15 of the Terms of Use that it applies, cover claims under this DPA. Nothing in them limits a liability that the law does not allow to be limited.

13. Term

This DPA applies from the Start date in the Pilot Schedule, including to any Cluster Data Zoorik already holds for the Client then, for as long as Zoorik processes Cluster Data. Zoorik's duties to keep Cluster Data confidential (section 3) and to delete it (section 10) continue after the pilot ends, until the data is deleted.

14. Law

- The parties apply the DPDP Act and the Digital Personal Data Protection Rules, 2025 to this processing from the Start date, even where a provision has not yet come into force, except the one-year retention of personal data and logs in rules 6(1)(e) and 8(3). That applies only once it is in force; until then, section 10 sets how long Zoorik keeps Cluster Data.
- If the GDPR or the UK GDPR applies to any Cluster Data, the parties will sign the European Commission's standard contractual clauses (and, for UK data, the UK addendum), as section 8 of the Terms of Use provides.
- This DPA is governed by the laws of India. The courts at Bengaluru, Karnataka have exclusive jurisdiction over any dispute arising out of or in connection with it, as section 11 of the Pilot Terms provides.

15. Notices

Notices under this DPA go by email: to Zoorik at founders@zoorik.com, and to the Client's technical and escalation contacts in the Pilot Schedule, or to another address the Client gives Zoorik by email.

Annex 1: Processing details for Coral

Item	Details
Subject-matter	Zoorik's provision of Coral to the Client for the pilot.
Duration	The pilot, then until Zoorik deletes the Cluster Data (section 10). Backup copies expire within 7 days after that.
Nature	Collection over outbound HTTPS, storage, analysis to work out Coral's recommendations and the instructions the agent fetches, display to the Client's users in the Coral console, and deletion.
Purpose	Measuring and reducing the cost of the Client's Kubernetes clusters, as the Pilot Terms describe.
Data Principals	Anyone whose personal data the Client puts in resource names, labels, the <code>coral.zoorik.com/configuration</code> annotation or Kubernetes messages, such as a person's name in a namespace. Most Cluster Data describes machines and software, not people.
Sensitive data	None intended. Coral is not built to receive passwords, financial details, or health, medical or biometric data.
Not included	Secrets; ConfigMaps other than the cluster autoscaler's status; pod logs; environment variables, Java options, commands, arguments, image names and annotations other than <code>coral.zoorik.com/configuration</code> , which the agent looks at only inside the cluster (a Kubernetes or cloud message in the table below can still quote them); the data inside the Client's applications; and pod memory.

Categories of data and frequency: the agent sends the following while a cluster is connected:

What	When	What it contains
Registration	When the agent registers	The agent's id and version; the cluster's name and resource id (an AKS resource id, which includes the Azure subscription id, or an EKS ARN); the capabilities it detected; the cloud account (Azure subscription id and resource group, or AWS account id and region)
Heartbeat	Every 60 seconds	The agent's id; the cluster's name and resource id; its capabilities; the images of Zoorik's components it runs and whether an update worked; the cluster autoscaler's status; and, for each node pool Coral may empty, its name, node count and the names of the nodes Coral has tainted
Usage	Read every 30 seconds, sent as 5-minute summaries	CPU, memory, out-of-memory kills, probe failures and CPU pressure per container, tagged with the namespace, the workload's kind and name, and the container's name
Inventory	Every 5 minutes	Nodes (name, id, cloud provider id, pool, VM size, zone, region, capacity and requests); workloads (namespace, kind, name, replicas, each container's requests and limits, whether probes are set, scheduling facts, PodDisruptionBudgets, autoscalers); namespaces, LimitRanges, ResourceQuotas and NodePools; up to 64 labels per workload and namespace; the value of the <code>coral.zoorik.com/configuration</code> annotation; the names of pods that hold a node

What	When	What it contains
Events	When they happen	Out-of-memory kills, memory-pressure evictions and startup failures, with the pod's name and id and its memory figures; node notices such as spot interruptions, with the node's name and id; what Coral did to a workload (resized or replaced pods, deleted a stuck pod, took over or handed back an autoscaler) and why, with the pod's name and id; the pods Coral moved off a node
Kubernetes messages	When Kubernetes refuses or cannot carry out a change Coral makes to a workload	The message text, cut to 1,024 characters
Node actions	While Coral works on a node or node pool	The node and pool; the pods moved (namespace, name and id) and how; the outcome; and a message, not shortened, that can name pods and quote the reason Kubernetes or the cloud gave for refusing a step

Annex 2: Security measures

The Zoorik Security Overview: Coral, 23 October 2026, and section 10 of the Privacy Policy, describe these measures in full. The main ones:

- **Location:** Coral's servers, database, backups and key vault run in Microsoft Azure, Central India. Database backups are kept for 7 days, in that region only.
- **In transit:** every connection to Zoorik from the internet uses HTTPS: plain HTTP is redirected, and browsers are told to use HTTPS only (HSTS). Cloudflare re-encrypts traffic to Zoorik's servers and checks their certificate, and Zoorik's web gateway accepts connections only from Cloudflare. Coral reaches its database over TLS 1.2 or later and checks the server's certificate.
- **At rest:** Microsoft Azure encrypts Zoorik's database and disks.
- **Separation:** row-level security in the database keeps each organisation's data apart, and every agent upload is tied to the organisation of its authenticated credential.
- **Credentials:** Zoorik holds no credential for the Client's cloud account and no kubeconfig. A connect token works once and expires after 60 minutes; the agent's cluster credential lasts 90 days and is replaced automatically before it expires. Both are stored only as SHA-256 fingerprints.
- **Sign-in:** no passwords. The Client's people sign in with Microsoft or Google through OpenID Connect with PKCE and a nonce; a session ends after 30 minutes idle or 12 hours.
- **In the Client's clusters:** the agent runs as a non-root user, with a read-only root file system and all Linux capabilities dropped. It sends data only to Zoorik, over outbound HTTPS, and accepts no inbound connection. It does not read the Client's Secrets, or any ConfigMap except the cluster autoscaler's status. The node daemon has no connection to Zoorik.
- **Access:** only a small number of people at Zoorik, and the automated tools Zoorik uses to build and deploy Coral, can access or change the systems that run it.

Annex 3: Sub-processors

Zoorik's sub-processors for Cluster Data, which Zoorik changes only as section 5 sets out:

Sub-processor	What it does for Zoorik	Where	Cluster Data it handles
Microsoft Azure	Hosts Coral: its servers, database, backups and key vault	Central India region	All Cluster Data Zoorik stores, and its backups
Cloudflare	Runs DNS and the secure proxy in front of Coral	Cloudflare's global network; a request can be handled outside India	Every request between the Client's clusters or browsers and Coral, in transit, including agent uploads; it decrypts and re-encrypts each request
Google (Workspace)	Zoorik's email	Google's data centres, which can be outside India	Emails between the parties, such as the pilot report and support replies, which can name the Client's clusters, nodes and workloads

Signing the Client's people in to Coral with Microsoft or Google, and GitHub serving the Coral agent's images to the Client's clusters, pass no Cluster Data to those companies. The Privacy Policy covers what they handle.