INFERDAT, INC.

ABI™ Platform

END USER LICENSE AGREEMENT

Version 1.0

Effective Date: 05/06/2026

> **IMPORTANT — PLEASE READ THIS AGREEMENT CAREFULLY BEFORE DEPLOYING OR USING THE ABI™ PLATFORM. BY SUBSCRIBING VIA THE AWS MARKETPLACE, CLICKING "ACCEPT," OR DEPLOYING THE DEPLOYMENT STACK, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT ON BEHALF OF YOURSELF AND THE ENTITY YOU REPRESENT. IF YOU DO NOT AGREE, DO NOT DEPLOY OR USE THE ABI™ PLATFORM.**

This End User License Agreement ("Agreement" or "EULA") is entered into by and between Inferdat, Inc., a Nevada corporation ("Inferdat," "we," or "us"), and the entity or individual accepting these terms ("Customer," "Licensee," "you," or "your"). This Agreement governs Customer's access to and use of the ABI™ Platform through the AWS Marketplace.

This Agreement supplements, and does not replace, the AWS Customer Agreement and AWS Marketplace Terms of Service. In the event of a conflict between this Agreement and those terms solely with respect to the commercial terms of the AWS Marketplace transaction, the AWS Marketplace Terms of Service shall control.

---

1. DEFINITIONS

As used in this Agreement, the following capitalized terms have the meanings set forth below:

1.1 "ABI™ Platform" or "Platform" means the ABI™ artificial-intelligence-powered business intelligence software, including all services, features, application programming interfaces (APIs), container images, Lambda functions, CloudFormation templates, Step Functions workflows, Amazon Bedrock Guardrails, Amazon Bedrock AgentCore Memory resources, user interfaces, documentation, and associated components made available by Inferdat, including all Updates, bug fixes, and modifications thereto.

1.2 "Agreement" means this End User License Agreement, including any applicable Order Forms and addenda incorporated by reference.

1.3 "AWS" means Amazon Web Services, Inc. and its affiliates.

1.4 "AWS Customer Agreement" means the agreement between Customer and AWS governing Customer's use of AWS services, available at https://aws.amazon.com/agreement/ (as updated from time to time).

1.5 "AWS Marketplace" means the AWS Marketplace digital catalog through which Customers subscribe to and are billed for the ABI™ Platform.

1.6 "Business Hours" means 9:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday, excluding U.S. federal public holidays.

1.7 "Confidential Information" means any non-public information disclosed by one party ("Disclosing Party") to the other ("Receiving Party") that is designated as confidential or that a reasonable person would understand to be confidential given its nature or the circumstances of disclosure. Inferdat's Confidential Information includes, without limitation, the Platform's source code, object code, algorithms, model architectures, training methodologies, system designs, and pricing. Customer's Confidential Information includes Telemetry Data received by Inferdat.

1.8 "Customer Data" means any data, content, database schemas, table structures, query inputs, or other information owned or controlled by Customer that Customer inputs into, connects to, or processes through the ABI™ Platform.

1.9 "Deployment Stack" means the AWS CloudFormation stack deployed into Customer's AWS Account as part of Platform setup, provisioning and managing the Infrastructure Resources.

1.10 "Documentation" means the technical and user documentation Inferdat makes available regarding the Platform, as updated from time to time.

1.11 "Downstream End Users" means Customer's own customers or end users to whom Customer makes the Platform available under a White-Label arrangement.

1.12 "Effective Date" means the earlier of: (a) the date Customer first accepts this Agreement; or (b) the date Customer deploys the Deployment Stack.

1.13 "End Users" means Customer's employees, contractors, and agents authorized by Customer to access the Platform under Customer's account.

1.14 "Infrastructure Costs" means all AWS fees and charges incurred in Customer's AWS Account in connection with the Deployment Stack and Platform operation, including without limitation charges for Amazon ECS, Amazon Aurora, Amazon ElastiCache, AWS Lambda, Amazon Bedrock (including model inference and Guardrails), Amazon Bedrock AgentCore Memory, Application Load Balancers, AWS Certificate Manager, Amazon VPC (including NAT Gateways and data transfer), Amazon S3, Amazon CloudWatch, AWS EventBridge, AWS Step Functions, AWS Systems Manager, AWS Secrets Manager, AWS CloudTrail, AWS Security Token Service, Amazon ECR, and all data egress and ingress charges.

1.15 "Marketplace Subscription" means the active, paid subscription to the ABI™ Platform purchased through the AWS Marketplace.

1.16 "Order Form" means a separately executed written agreement specifying subscription tier, additional services, and commercial terms, applicable to Enterprise tier Customers.

1.17 "Platform Version" means a specific release of the ABI™ Platform identified by a version number published in Inferdat's release manifest.

1.18 "Telemetry Data" means the operational metadata collected from Customer's AWS Account by the Phone-Home Lambda and related Platform components and transmitted to Inferdat's systems, as fully described in Section 6.

1.19 "Third-Party Services" means any services, platforms, or infrastructure not owned or operated by Inferdat, including AWS services such as Amazon Bedrock, AWS Marketplace, Amazon ECR, and any data sources Customer connects to the Platform.

1.20 "Update" means any bug fix, patch, minor release, or major release of the Platform made generally available by Inferdat.

1.21 "White-Label Use" means Customer's permitted rebranding and offering of the Platform as part of Customer's own product or service, subject to the conditions in Section 15.

2. LICENSE GRANT

2.1 Subject to the terms of this Agreement and Customer's maintenance of an active Marketplace Subscription, Inferdat grants Customer a limited, non-exclusive, non-transferable, non-sublicensable (except as expressly permitted in Section 15) license to: (a) deploy the Deployment Stack in Customer's AWS Account; (b) access and use the Platform solely for Customer's internal business purposes and, where applicable, for White-Label Use in accordance with Section 15; and (c) permit End Users to access the Platform in accordance with this Agreement.

2.2 The license is limited to the features and capabilities of the subscription tier purchased (Build, Insights, or Enterprise). Customer may not access features that exceed its subscribed tier without upgrading.

2.3 This license is conditioned on: (a) an active Marketplace Subscription; (b) continuous compliance with this Agreement; and (c) compliance with the AWS Customer Agreement and all applicable AWS Marketplace terms. The license terminates automatically upon subscription expiration or cancellation, subject to the grace period in Section 13.2.

2.4 All rights not expressly granted are reserved by Inferdat. No implied licenses arise under this Agreement.

3. LICENSE RESTRICTIONS

3.1 Customer shall not, and shall ensure that End Users and Downstream End Users do not, directly or indirectly:

- reverse engineer, decompile, disassemble, decrypt, or otherwise attempt to derive the source code, algorithms, model architectures, training methodologies, underlying logic, or structure of the Platform or any component thereof, by any means whatsoever;
- enable, activate, or permit the activation of AWS ECS Exec (enableExecuteCommand) on any ECS service or task deployed as part of the Deployment Stack, for any reason;
- modify, alter, tamper with, replace, or delete any IAM roles, IAM policies, ECS task definitions, container images, Lambda function code, EventBridge rules, Step Functions workflows, SSM parameter store entries, CloudFormation resources, or any other resource deployed as part of the Deployment Stack, except as expressly authorized in writing by Inferdat;
- copy, reproduce, distribute, publicly display, or create derivative works of the Platform or any component thereof;
- circumvent, disable, bypass, tamper with, or otherwise defeat any license enforcement mechanism, entitlement check, digital rights management control, or technical protection measure implemented by Inferdat;
- run, deploy, or execute any container image hosted in Inferdat's Amazon ECR repositories outside of the authorized Deployment Stack;
- access, view, copy, or extract Inferdat's source code or proprietary algorithms by any means, including enabling container shell access, exploiting vulnerabilities, intercepting network traffic, or using memory analysis tools;
- sell, resell, sublicense, assign, or transfer this Agreement or any rights hereunder to any third party, except as expressly permitted in Section 15;
- use the Platform for any Competitive Purpose as defined in Section 20;
- use the Platform in violation of any applicable law, regulation, or third-party rights;
- remove, alter, or obscure any proprietary notices, labels, or trademarks displayed within the Platform; or
- permit or enable any third party to do any of the foregoing.

3.2 Customer acknowledges that the restrictions in this Section are reasonable and necessary to protect Inferdat's legitimate proprietary interests. Any breach of this Section constitutes a material breach entitling Inferdat to immediate termination of this Agreement without notice or opportunity to cure, in addition to all other remedies at law or in equity, including injunctive relief.

3.3 PROPRIETARY CODE PROTECTION. Customer expressly acknowledges that Inferdat's proprietary source code, compiled binaries, container images, model weights, prompt templates, system prompts, and algorithmic logic (collectively, "Protected Code") are deployed within Customer's AWS Account solely as a technical necessity of the Platform's architecture and NOT as a delivery of source code or a grant of access rights to that code. The physical proximity of Protected Code to Customer's infrastructure does not diminish Inferdat's intellectual property rights or grant Customer any right to access, inspect, copy, or analyze Protected Code. Without limiting the generality of Section 3.1, Customer specifically shall not:

(a) use AWS Systems Manager Session Manager, ECS Exec, SSH, or any other remote access mechanism to obtain shell access to any container or compute resource running Platform code;

(b) attach debugging tools, profilers, memory analyzers, or instrumentation agents to any Platform process or container;

(c) mount, copy, export, or snapshot any container filesystem, EBS volume, or storage layer containing Platform code;

(d) capture, inspect, or reconstruct container images from ECR layer caches, Docker layer storage, or ECS task storage;

(e) use AWS CloudTrail, VPC Flow Logs, Application Load Balancer access logs, or any network monitoring tool to reverse-engineer the Platform's internal API calls, service-to-service communication patterns, or data flows for the purpose of understanding or replicating Platform functionality;

(f) use Amazon Bedrock invocation logs, CloudWatch Logs Insights, or any logging mechanism to capture, store, or analyze the system prompts, tool definitions, agent configurations, or orchestration logic used by the Platform;

(g) create AMIs, EBS snapshots, or container image exports of any resource containing Platform code; or

(h) engage any third party, including security researchers, penetration testers, or consultants, to perform any of the foregoing on the Platform or Deployment Stack components on Customer's behalf. For the avoidance of doubt, this subsection does not prohibit Customer from conducting general security assessments of its own AWS Account environment, provided such assessments are not directed at the Platform or Deployment Stack components.

Customer acknowledges that any violation of this Section constitutes misappropriation of trade secrets under the Defend Trade Secrets Act (18 U.S.C. § 1836) and the Nevada Uniform Trade Secrets Act (NRS 600A), in addition to breach of contract, and that Inferdat shall be entitled to immediate injunctive relief, statutory damages, and recovery of attorneys' fees without the requirement of posting bond.

3.4 ENHANCED REMEDIES FOR IP VIOLATIONS. In addition to all other remedies available at law or in equity:

(a) LIQUIDATED DAMAGES. Customer agrees that any breach of Sections 3.1, 3.3, or 20.2 causes damages that are inherently difficult to quantify, including loss of competitive advantage, cost of re-engineering, and lost future revenue. Accordingly, in the event of a confirmed breach of any such Section, Customer shall pay Inferdat liquidated damages equal to the greater of: (i) three (3) times the total fees paid or payable under this Agreement during the twelve (12) months preceding the breach; or (ii) $250,000 USD. The parties acknowledge and agree that this amount represents a reasonable pre-estimate of Inferdat's damages, arrived at through negotiation, and is not a penalty. This clause shall not limit Inferdat's right to seek actual damages if they exceed the liquidated amount.

(b) DISGORGEMENT. Customer shall disgorge and pay to Inferdat all profits, revenue, and economic benefit derived from any unauthorized use, access, or exploitation of Inferdat's intellectual property or Protected Code.

(c) INJUNCTIVE RELIEF. Customer acknowledges that monetary damages alone would be inadequate to compensate Inferdat for breach of this Section. Customer consents to the entry of immediate injunctive relief without the necessity of proving actual damages or posting bond, including emergency ex parte relief under 18 U.S.C. § 1836(b)(3) of the Defend Trade Secrets Act where applicable.

(d) ATTORNEYS' FEES. In any action to enforce this Section, the prevailing party shall be entitled to recover reasonable attorneys' fees, expert witness fees, and costs of litigation. Notwithstanding Nevada's American Rule, this clause constitutes the express contractual exception required to permit fee recovery.

4. DEPLOYMENT AND INSTALLATION

4.1 The ABI™ Platform is deployed exclusively within Customer's AWS Account via a single AWS CloudFormation stack provisioned through the AWS Marketplace. Customer is solely responsible for providing an AWS Account in good standing with sufficient service limits, IAM permissions, and configurations required for the Deployment Stack to be created and operated.

4.2 Customer acknowledges that the Deployment Stack provisions and manages a significant number of AWS resources within Customer's AWS Account, which may include without limitation: Virtual Private Cloud (VPC) with subnets, route tables, internet gateways, and NAT Gateways; Amazon ECS cluster, services, and task definitions; Application Load Balancer (ALB); AWS Certificate Manager (ACM) certificates; Amazon ElastiCache cluster; Amazon Aurora database cluster; Amazon Bedrock Guardrails; AWS Lambda functions (including the Phone-Home Lambda, Deployment Notification Lambda, and Upgrade Helper Lambda); AWS EventBridge rules and schedules; AWS Step Functions state machines; AWS Systems Manager (SSM) Parameter Store entries; Amazon S3 buckets; AWS IAM roles and policies; ; Amazon CloudWatch alarms, dashboards, and log groups; and Amazon ECR repositories. The provisioning and ongoing operation of these resources will generate substantial Infrastructure Costs for which Customer is solely responsible.

4.3 By deploying the Deployment Stack, Customer expressly authorizes Inferdat to deploy, configure, and operate the resources described in Section 4.2 within Customer's AWS Account solely for the purpose of providing the Platform. This authorization does not grant Inferdat direct console or credential access to Customer's AWS Account.

4.4 Customer is responsible for ensuring its AWS Account satisfies all technical prerequisites for deployment, including AWS service limit availability and regional compatibility. Inferdat makes no warranty that the Platform will be compatible with all AWS configurations or existing Customer infrastructure.

4.5 Customer bears sole responsibility for the security configuration of its AWS Account, including VPC security groups, network access control lists, IAM permission boundaries, AWS Organizations service control policies, and any other controls that may affect Platform operation or security.

5. SOFTWARE UPDATES

5.1 Inferdat may publish Updates to the Platform from time to time. Updates are published to Inferdat's central Amazon ECR repositories and made discoverable via a release manifest file (versions.json) hosted in Inferdat's central Amazon S3 bucket (abi-platform-releases). The manifest contains version numbers, release dates, ECR repository names, image digests, and changelog URLs. It does not contain source code, Customer Data, or secrets.

5.2 Customer retains full control over when to apply Updates. The Platform administrator interface displays an update notification banner when a new version is detected. Updates are applied by Customer by triggering a Step Functions workflow within Customer's AWS Account. Inferdat strongly recommends applying security-related Updates promptly.

5.3 To check for Updates, Customer's AWS Account makes a read-only cross-account S3 request to Inferdat's central account via an STS AssumeRole mechanism with a scoped ExternalId. This access is read-only and Customer expressly authorizes it as a condition of using the Update functionality.

5.4 Inferdat may designate certain Updates as required for continued technical support. Inferdat will provide at least thirty (30) days' advance written notice of such requirements. Inferdat's support obligations under Section 12 do not apply to Platform Versions that have been designated end-of-life.

5.5 The Update process may result in brief service interruptions. Customer is responsible for scheduling Updates during appropriate maintenance windows. Inferdat is not liable for any downtime, data loss, or harm resulting from Update-related interruptions.

5.6 Inferdat is not responsible for Update failures arising from Customer's unauthorized modifications to the Deployment Stack, container images, task definitions, IAM policies, or any other resources prior to Update application.

6. TELEMETRY, MONITORING, AND DATA COLLECTION

6.1 Operational Telemetry (Phone-Home Lambda). Customer acknowledges and agrees that the Platform includes a Phone-Home Lambda function deployed within Customer's AWS Account that collects operational metadata ("Telemetry Data") and transmits it to Inferdat's central API endpoint (https://phonehome.abi.inferdat.ai/phone-home) via HTTPS with AWS SigV4 authentication. The Phone-Home Lambda transmits the following Telemetry Data on each invocation:

- Customer's AWS Account ID;
- CloudFormation stack name and AWS deployment region;
- Platform Version currently deployed;
- Entitlement status result (active, expired, lockout, disabled, or unknown);
- Trigger source (scheduled, event-driven, or manual);
- For each ECS service in the Deployment Stack: service name, container image URI and digest (SHA-256), running task count, desired task count, and derived health status; and
- Tamper detection signals as described in Section 6.4.

6.2 Transmission Schedule. The Phone-Home Lambda transmits Telemetry Data: (a) on a nightly automated schedule (approximately every 24 hours via AWS EventBridge); and (b) in near-real-time upon detection of certain AWS CloudTrail events, including IAM policy modifications on roles prefixed with "ABI™-platform-", ECS UpdateService events on the Platform cluster, and ECS RunTask or StartTask events on the Platform cluster. Customer expressly consents to this event-driven, near-real-time telemetry transmission as a condition of using the Platform.

6.3 Deployment Notification Data. Upon first deployment of the Deployment Stack, and upon subsequent stack Updates that change the Platform Version, the Deployment Notification Lambda transmits the following additional data to Inferdat's central API endpoint: Customer's AWS Account ID; timestamp; Customer's configured domain; Customer administrator email address; company name; administrator username; auto-generated temporary administrator password; AWS region; CloudFormation stack name; Platform Version; health check status; and tamper detection signals. The temporary administrator password is transmitted solely to enable Inferdat's system to deliver a welcome email to the Customer administrator. This temporary password is NOT persisted in Inferdat's databases after the welcome email is delivered. CUSTOMER IS STRONGLY ADVISED TO ROTATE THE ADMINISTRATOR PASSWORD IMMEDIATELY UPON FIRST LOGIN.

6.4 Tamper Detection Monitoring. The Phone-Home Lambda performs tamper detection checks on every invocation and includes the results in Telemetry Data. These checks include: (a) IAM Role Policy Integrity — SHA-256 hashing of inline and attached policies on Inferdat-deployed IAM roles (ABI™-platform-ecs-task-role, ABI™-platform-ecs-task-execution-role, ABI™-platform-phone-home-role) compared against a baseline stored in SSM; (b) ECS Exec Status — detecting whether enableExecuteCommand is active on any Deployment Stack ECS service; (c) Unauthorized Task Definitions — detecting ECS task definitions not authorized by Inferdat that reference Inferdat's ECR image repositories; and (d) CloudFormation Stack Drift — detecting unauthorized modifications to Deployment Stack resources. The tamper detection system is purely observational. No automated remediation, access restriction, lockout, or resource modification is performed by the tamper detection system. Detection of tamper signals generates an internal alert at Inferdat, which may prompt Inferdat to contact Customer for investigation.

6.5 EventBridge Monitoring Rules. The Deployment Stack includes AWS EventBridge rules that capture CloudTrail API events in near-real-time to trigger the telemetry transmissions described in Section 6.2. These rules monitor: IAM policy changes on ABI™-platform-* roles; ECS cluster UpdateService events; and ECS RunTask/StartTask events. Customer consents to the deployment and continuous operation of these monitoring rules within Customer's AWS Account.

6.6 What Is Not Collected. Inferdat does not collect, transmit, or have access to: Customer Data; Customer's database contents or records; SQL queries generated by or executed through the Platform; dashboard content, chart data, or analytical outputs; End User conversation history; query results; any data processed by Amazon Bedrock; or any personally identifiable information of End Users beyond the administrator contact details described in Section 6.3. Telemetry Data is strictly limited to operational and integrity metadata about the Platform's configuration and health.

6.7 Bedrock Data Flows. The Platform uses Amazon Bedrock (including Bedrock model inference APIs and the Amazon Bedrock AgentCore Memory API) to process natural language queries and generate SQL and other analytical outputs. As part of normal Platform operation, the following data is transmitted to Amazon Bedrock's regional API endpoints within Customer's AWS Account: End User natural language query text; system prompts; database schema information (DDL, table and column names, SQL examples); and tool call results. No raw database data (actual data rows or records) is transmitted to Amazon Bedrock. The Amazon Bedrock AgentCore Memory API, used for conversation context persistence, operates entirely within Customer's AWS Account and transmits no data to Inferdat. Customer's use of Amazon Bedrock is governed by the AWS Customer Agreement, and Customer is solely responsible for compliance with applicable laws governing its use of AI services with Customer Data.

6.8 Content Filtering. The Platform deploys Amazon Bedrock Guardrails within Customer's AWS Account to filter potentially harmful, off-topic, or unsafe inputs and outputs processed by the Platform's AI components. Guardrails may block or modify certain queries that are detected as prompt injection attempts, harmful content requests, or queries outside the Platform's intended analytical scope. Customer acknowledges that content filtering is an active component of the Platform and that Guardrails may occasionally produce false positives that block legitimate queries. Guardrail configuration is managed by Inferdat as part of the Platform and may not be independently modified by Customer. Inferdat may update Guardrail configurations as part of Platform Updates.

6.9 Data Retention and Use. Telemetry Data received by Inferdat is retained for ninety (90) days. Tamper alert data is retained as reasonably necessary for investigation and compliance. Deployment notification data (excluding the temporary password, which is not retained) is retained for Customer account management. Inferdat uses Telemetry Data solely for: (a) verifying Marketplace Subscription entitlements; (b) monitoring Platform health and integrity; (c) providing technical support; (d) detecting potential Agreement violations; and (e) improving the Platform. Inferdat will not sell Telemetry Data to third parties.

7. AWS AND THIRD-PARTY SERVICES

7.1 The ABI™ Platform operates within Customer's AWS Account and relies on numerous AWS services. Customer's use of all AWS services is governed exclusively by the AWS Customer Agreement and applicable AWS service terms. Inferdat is not a party to the agreement between Customer and AWS and has no liability for AWS service outages, performance degradation, pricing changes, service discontinuation, or any other AWS-related issues that affect Platform operation.

7.2 Inferdat's support obligations under Section 12 expressly exclude issues caused by AWS service disruptions, AWS account configuration problems, AWS service limit breaches, or Customer's failure to maintain an AWS Account in good standing.

7.3 Customer is responsible for all data source connections to the Platform, including credentials, connection security, and ensuring data sources comply with applicable data privacy laws. Inferdat is not responsible for security of Customer's data in transit from data sources to the Platform.

7.4 The Platform's Marketplace entitlement verification calls the AWS Marketplace Entitlement API (marketplace-entitlement.us-east-1.amazonaws.com), transmitting only Customer's AWS Account ID and the ABI™ Platform product code. No Customer Data is transmitted in this call.

8. MARKETPLACE BILLING AND FEES

8.1 All subscription fees for the Platform are charged by AWS through the AWS Marketplace in accordance with the pricing on the ABI™ Platform's Marketplace listing at the time of subscription. Inferdat does not directly charge, invoice, or collect payment from Customer.

8.2 All billing inquiries, disputes, refund requests, and payment issues must be directed to AWS Marketplace support. Inferdat has no access to Customer's payment information, AWS billing account data, or AWS cost and usage reports.

8.3 Inferdat may modify subscription fees through the AWS Marketplace. Fee changes will be published on the Marketplace listing and communicated in accordance with AWS Marketplace notification procedures. Continued use after the effective date of a fee change constitutes acceptance.

8.4 Customer is solely responsible for all taxes, duties, and governmental charges arising from the purchase and use of the Platform, excluding taxes based on Inferdat's net income.

9. INFRASTRUCTURE COSTS AND RESOURCE RESPONSIBILITY

9.1 Customer's Sole Responsibility for Infrastructure Costs. Customer acknowledges that the Deployment Stack provisions and operates numerous AWS resources within Customer's AWS Account and that operation of these resources generates continuous Infrastructure Costs. Customer is solely and exclusively responsible for all Infrastructure Costs, regardless of cause or origin.

> **INFERDAT HAS NO LIABILITY WHATSOEVER FOR INFRASTRUCTURE COSTS. THIS SECTION IS A MATERIAL TERM OF THIS AGREEMENT.**

9.2 Specific Exclusions. Without limiting the generality of Section 9.1, Inferdat is not responsible for Infrastructure Costs arising from:

- normal Platform operation, including Amazon Bedrock model inference calls, Amazon Aurora query processing, Amazon ElastiCache operations, ECS task execution, and Lambda invocations;
- runaway or unintended processes caused by Platform bugs, software defects, or misconfigurations, including but not limited to unintended looping queries, excessive Bedrock model inference calls, Lambda invocation loops, or unintended data transfer between AWS services or regions;
- Customer's misconfiguration, over-provisioning, failure to set appropriate AWS Budgets, cost anomaly alerts, or service quotas;
- security incidents, unauthorized access, cryptomining, or other malicious activity targeting Customer's AWS Account or the Deployment Stack, regardless of whether such activity exploits a vulnerability in the Platform;
- denial-of-service attacks, volumetric traffic attacks, or other external attacks directed at infrastructure within Customer's AWS Account;
- Customer's failure to apply Updates containing cost-related bug fixes;
- accidental or unintended resource scaling, including ECS task proliferation or Aurora auto-scaling events; or
- data transfer, data egress, or cross-region costs of any kind.

Notwithstanding the foregoing, in the event of a confirmed Platform defect that directly causes materially excessive Infrastructure Costs, Inferdat will work in good faith with Customer to identify and resolve the defect promptly. This good faith commitment does not create any obligation on Inferdat's part to reimburse, offset, or otherwise compensate Customer for Infrastructure Costs incurred, and does not limit or modify the disclaimers in Section 9.1.

9.3 Cost Control Obligations. Customer is solely responsible for implementing and maintaining AWS cost controls, including AWS Budgets and billing alerts, AWS Cost Anomaly Detection, service quota configurations, and regular review of AWS Cost Explorer. Inferdat may, at its discretion, include cost-saving recommendations in Documentation but has no obligation to do so and makes no warranty regarding the cost efficiency of any Platform configuration.

9.4 Security Responsibility. Because the Deployment Stack operates entirely within Customer's AWS Account, Customer bears full responsibility for the security of the environment in which the Platform operates. Inferdat is not responsible for:

- security vulnerabilities in Customer's AWS Account configuration that enable unauthorized access to Deployment Stack resources;

- data breaches, data loss, or unauthorized data access arising from Customer's misconfiguration of VPC security groups, IAM policies, network ACLs, or other access controls;
- security incidents arising from Customer's failure to apply security-related Updates;
- security incidents caused by unauthorized access to Customer's AWS Account credentials or IAM keys;
- Customer's compliance with data protection laws applicable to its use of the Platform, including HIPAA, GDPR, CCPA, or any other privacy regulation; or
- security of data sources, databases, or other systems Customer connects to the Platform.

9.5 Row-Level Security. The Platform provides Row-Level Security (RLS) features enabling Customer to restrict End User data access. Customer is solely responsible for correctly configuring RLS. Inferdat is not liable for unauthorized data access resulting from Customer's misconfiguration of RLS or any other access control feature.

9.6 Data Backup and Recovery. Customer is responsible for all data backup, recovery, and retention obligations for data stored in Aurora databases and any other storage resources within the Deployment Stack. Inferdat makes no warranty regarding data durability and is not responsible for data loss.

9.7 Post-Termination Costs. Customer is responsible for removing the Deployment Stack and all associated AWS resources upon termination of this Agreement. INFERDAT IS NOT RESPONSIBLE FOR INFRASTRUCTURE COSTS INCURRED AFTER TERMINATION IF CUSTOMER FAILS TO REMOVE THE DEPLOYMENT STACK AND ALL PROVISIONED RESOURCES FROM ITS AWS ACCOUNT.

10. INTELLECTUAL PROPERTY

10.1 Inferdat Ownership. Inferdat retains all right, title, and interest in and to the ABI™ Platform, including all intellectual property rights. This includes without limitation: all source code and object code; proprietary algorithms and model architectures; training methodologies; system design and architecture; user interface and experience designs; Documentation; all trademarks and trade names including "ABI™," "ABI™ Platform," and "Inferdat"; and all improvements and derivative works made by Inferdat. Customer acquires no ownership interest in the Platform. The license granted herein is a license to use, not a sale or transfer of intellectual property.

10.2 Customer Ownership. Customer retains all right, title, and interest in Customer Data, including database schemas, dashboard configurations, reports, and other outputs generated through Customer's use that incorporate Customer's proprietary information. AI-generated outputs (SQL queries, visualizations, insights) derived from Customer Data are tools for Customer's use; their ownership follows Customer's ownership of the underlying Customer Data.

10.3 Limited License to Process Customer Data. Customer grants Inferdat a limited, non-exclusive, royalty-free license to access and process Customer Data (including Telemetry Data) solely to the extent necessary to operate the Platform, provide support, verify entitlements, detect tampering, and improve the Platform. Inferdat will not use Customer Data for any other purpose.

10.4 Feedback. If Customer provides Inferdat with feedback, suggestions, or recommendations regarding the Platform ("Feedback"), Customer grants Inferdat a perpetual, irrevocable, worldwide, royalty-free license to use, modify, and incorporate such Feedback without obligation. Inferdat has no obligation to implement any Feedback.

10.5 No Trademark License. Nothing in this Agreement grants Customer the right to use Inferdat's trademarks, trade names, or logos except as expressly authorized in writing by Inferdat or as permitted within a licensed White-Label arrangement.

11. CONFIDENTIALITY

11.1 Each Receiving Party agrees to hold the Disclosing Party's Confidential Information in strict confidence and to use it solely for exercising rights or fulfilling obligations under this Agreement.

11.2 The Receiving Party shall: (a) protect Confidential Information using at least the same degree of care it uses for its own confidential information, but no less than reasonable care; (b) not disclose Confidential Information to any third party without prior written consent; and (c) limit disclosure to employees, contractors, and advisors with a legitimate need to know who are bound by confidentiality obligations at least as protective as this Agreement.

11.3 Confidentiality obligations do not apply to information that: (a) is or becomes publicly available through no fault of the Receiving Party; (b) was rightfully known to the Receiving Party without restriction prior to disclosure; (c) is rightfully received from a third party without restriction; or (d) is independently developed without reference to the Confidential Information.

11.4 Customer specifically acknowledges that the ABI™ Platform, including its architecture, container images, algorithms, and pricing, constitutes Inferdat's Confidential Information. Customer shall not disclose, publish, or share benchmark results, technical evaluations, performance analyses, or security assessments of the Platform without Inferdat's prior written consent.

11.5 Telemetry Data received by Inferdat constitutes Customer's Confidential Information. Inferdat shall use Telemetry Data only as described in Section 6.9 and shall not disclose it to third parties except as required by law or as necessary to provide support or investigate security incidents.

11.6 Either party may disclose Confidential Information as required by law, regulation, or court order, provided it gives the Disclosing Party prompt written notice (to the extent legally permitted) and reasonably cooperates with efforts to seek a protective order.

11.7 Confidentiality obligations survive termination for five (5) years, except that obligations with respect to Inferdat's source code and proprietary algorithms survive indefinitely.

12. SUPPORT SERVICES

12.1 Build and Insights Tiers. For Customers on Build or Insights subscription tiers, Inferdat provides email-based technical support. Inferdat will use commercially reasonable efforts to respond to support requests within four (4) Business Hours of receipt. Support is available during Business Hours only.

12.2 Severity Classification. Support requests are classified as:

- Critical: The ABI™ Platform is completely inaccessible or non-functional for all End Users with no available workaround. Inferdat will use commercially reasonable efforts to provide an initial response within four (4) Business Hours and to resolve or provide a workaround for Critical issues as expeditiously as practicable.
- Non-Critical: All other support requests, including individual feature issues, performance concerns, and configuration questions. Inferdat will use commercially reasonable efforts to respond within four (4) Business Hours.

12.3 Scope of Support. Support covers: (a) defects and bugs in the ABI™ Platform application software; and (b) guidance on Platform configuration and usage. Support expressly excludes: (i) issues caused by Customer's AWS infrastructure configuration, AWS service outages, or AWS account limitations; (ii) issues caused by Customer's modifications to the Deployment Stack, container images, or IAM policies; (iii) data source connectivity or data quality issues; (iv) general AWS advisory services; (v) issues arising from Customer's use of unsupported Platform Versions; and (vi) issues outside Inferdat's reasonable control.

12.4 Customer Responsibilities. Customer shall: (a) designate at least one technically qualified contact person for support requests; (b) provide sufficient information to reproduce reported issues; and (c) maintain the Platform at a supported Platform Version. Support is provided in English.

12.5 Enterprise Support. Support terms for Enterprise tier Customers are governed by a separately executed Order Form. In the absence of an Order Form, Enterprise Customers receive the same support as Insights tier. The Order Form may specify custom SLAs, dedicated support contacts, and additional service terms.

12.6 No SLA Guarantee. The response time commitments in this Section represent commercially reasonable efforts and do not constitute a performance guarantee or service level agreement. Inferdat's failure to meet these targets does not constitute a breach of this Agreement and does not give rise to any right of termination or credit.

13. LICENSE ENFORCEMENT AND ENTITLEMENT VERIFICATION

13.1 Entitlement Checks. The Platform verifies Customer's active Marketplace Subscription by calling the AWS Marketplace Entitlement API on a nightly basis and upon certain triggering events. The entitlement status is stored in Customer's SSM Parameter Store (/ABI™-platform/entitlement-status) and read by Platform services to determine whether to serve user requests.

13.2 Grace Period. Upon the first detection of an expired or lapsed Marketplace Subscription, the Platform enters a seven (7) calendar day grace period during which Platform services continue operating normally. If the Subscription is not reinstated within the grace period, the Platform transitions to a "lockout" state, blocking access for all End Users. Inferdat may, in its sole discretion, extend the grace period.

13.3 Fail-Open on Network Errors. If the AWS Marketplace Entitlement API is unreachable due to network failure or API unavailability, the Platform will fail open (continue serving requests) and will not initiate or extend the grace period timer on the basis of network error alone. This fail-open behavior is a technical resilience measure and does not constitute a license to use the Platform beyond the period of an active Marketplace Subscription. Customer's legal obligation to cease use upon subscription expiration is not diminished by fail-open behavior.

13.4 Prohibited Circumvention. Customer shall not: (a) modify, delete, falsify, or spoof SSM parameters related to entitlement status (/ABI™-platform/entitlement-status or related paths); (b) block, intercept, or alter the Phone-Home Lambda's communications with Inferdat's entitlement endpoint; (c) modify the Phone-Home Lambda, Deployment Notification Lambda, or Upgrade Helper Lambda code or configuration; or (d) take any action intended to circumvent or defeat the Platform's license enforcement mechanisms. Any such circumvention is a material breach and an infringement of Inferdat's intellectual property rights.

13.5 Audit Rights. Inferdat may, upon reasonable prior written notice (except in cases of suspected material breach or circumvention, where no advance notice is required), audit Customer's use of the Platform to verify compliance with this Agreement. Such audits will be conducted in a manner minimizing disruption and will be at Inferdat's expense unless the audit reveals material non-compliance, in which case Customer shall bear reasonable audit costs.

14. TERM AND TERMINATION

14.1 Term. This Agreement commences on the Effective Date and continues for as long as Customer maintains an active Marketplace Subscription, unless earlier terminated under this Section.

14.2 Termination for Cause. Either party may terminate this Agreement upon written notice if the other party materially breaches this Agreement and fails to cure such breach within thirty (30) days of written notice. Either party may also terminate immediately if the other party becomes insolvent, makes an assignment for the benefit of creditors, or becomes subject to bankruptcy proceedings.

14.3 Immediate Termination by Inferdat. Notwithstanding Section 14.2, Inferdat may terminate this Agreement immediately upon written notice, without a cure period, if Customer: (a) breaches Section 3 (License Restrictions) or Section 20 (Acceptable Use and Competitive Use Prohibition); (b) circumvents or attempts to circumvent any license enforcement mechanism; (c) accesses or attempts to access Inferdat's source code or proprietary algorithms; (d) enables ECS exec on any Deployment Stack ECS service; or (e) engages in conduct Inferdat reasonably believes constitutes material infringement of Inferdat's intellectual property rights.

14.4 Automatic Termination. This Agreement automatically terminates if Customer's Marketplace Subscription expires, is cancelled, or lapses and is not reinstated within the seven (7) day grace period described in Section 13.2.

14.5 Effect of Termination. Upon termination for any reason: (a) the license granted in Section 2 immediately terminates; (b) Customer must immediately cease all use of the Platform; (c) the Deployment Stack and all resources provisioned in Customer's AWS Account will remain in Customer's AWS Account, but Platform functionality will cease upon lockout activation; (d) Customer is responsible for removing the Deployment Stack and all associated resources from its AWS Account; and (e) Customer remains liable for all Infrastructure Costs incurred until removal of the Deployment Stack. Termination does not entitle Customer to any refund of fees paid through the AWS Marketplace.

14.6 Survival. Sections 1, 3 (to the extent applicable post-termination), 9, 10, 11, 14.5, 17, 18, 19, 20 (as applicable), 22, and 23 survive termination of this Agreement.

15. WHITE-LABEL USE AND SUBLICENSING

15.1 Permitted White-Label Use. Subject to the terms of this Section and Customer's subscription to a tier that includes White-Label features, Customer may rebrand the Platform and offer it as part of Customer's own product or service to Downstream End Users. This permission is a limited authorization to present the Platform under Customer's brand, not a sublicense of Inferdat's intellectual property.

15.2 Customer's Responsibility for Downstream End Users. Customer is solely and exclusively responsible for all Downstream End Users' access to and use of the Platform, including: (a) all acts and omissions of Downstream End Users; (b) ensuring Downstream End Users are bound by terms and conditions at least as restrictive as the restrictions in Sections 3 and 20 of this Agreement; (c) all data privacy, security, and regulatory compliance obligations arising from Downstream End Users' use; and (d) all claims, liabilities, and regulatory actions arising from Downstream End Users' use.

15.3 Required Pass-Through Restrictions. Customer must include in its agreements with Downstream End Users explicit prohibitions on: (a) reverse engineering, decompilation, or disassembly of the Platform; (b) resale or redistribution of the Platform; (c) unauthorized access to infrastructure, container images, or source code; (d) enabling ECS exec or modifying Deployment Stack resources; and (e) competitive use as described in Section 20.

15.4 No Inferdat Liability to Downstream End Users. Inferdat is not a party to any agreement between Customer and Downstream End Users. Inferdat has no obligations to Downstream End Users and is not liable for any claims arising from their use of the Platform. Customer shall not make representations or warranties to Downstream End Users on Inferdat's behalf.

15.5 Branding Limitations. Customer may remove Inferdat's branding as permitted by its subscription tier. Customer may represent the white-labeled product as its own offering and is not required to disclose Inferdat as the underlying technology provider to Downstream End Users. Customer may not, however, affirmatively claim to have independently developed the underlying AI or business intelligence technology in contexts where such claim would constitute fraud or misrepresentation, including without limitation patent applications, investor representations, regulatory filings, or legal proceedings.

15.6 Indemnification for White-Label Use. Customer shall indemnify, defend, and hold harmless Inferdat from and against all claims, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising from Downstream End Users' use of the Platform or Customer's white-label product or service.

16. REPRESENTATIONS AND WARRANTIES

16.1 Customer Representations. Customer represents and warrants that: (a) if Customer is an entity, it is duly organized, validly existing, and in good standing; (b) Customer has full legal authority to enter into this Agreement; (c) Customer's use of the Platform complies and will comply with all applicable laws, including data privacy and security regulations applicable to Customer's industry; (d) Customer has the right to connect its data sources to the Platform and to process Customer Data through the Platform; (e) Customer will not use the Platform for any unlawful purpose or in any manner infringing third-party rights; and (f) Customer has reviewed and agreed to the AWS Customer Agreement.

16.2 Inferdat Representations. Inferdat represents and warrants that: (a) it is duly organized, validly existing, and in good standing as a Nevada corporation; (b) it has full legal authority to enter into this Agreement and to grant the licenses herein; and (c) to Inferdat's knowledge as of the Effective Date, the Platform does not infringe the intellectual property rights of any third party.

17. DISCLAIMER OF WARRANTIES

> **THE ABI™ PLATFORM IS PROVIDED "AS IS" AND "AS AVAILABLE." TO THE MAXIMUM EXTENT PERMITTED BY LAW, INFERDAT EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE.**

17.1 General Disclaimer. Without limiting the foregoing, Inferdat expressly disclaims all warranties of: (a) merchantability; (b) fitness for a particular purpose; (c) non-infringement; (d) accuracy, completeness, reliability, or suitability of any AI-generated outputs, including SQL queries, dashboards, insights, anomaly detections, and analytical conclusions; (e) uninterrupted, error-free, or secure operation; (f) freedom from bugs, defects, or harmful components; and (g) compatibility with any particular data source, AWS configuration, or Third-Party Service.

17.2 AI-Generated Output Disclaimer. CUSTOMER ACKNOWLEDGES THAT THE PLATFORM USES ARTIFICIAL INTELLIGENCE AND LARGE LANGUAGE MODELS, WHICH MAY PRODUCE INACCURATE, INCOMPLETE, MISLEADING, BIASED, OR OTHERWISE UNSUITABLE OUTPUTS. CUSTOMER IS SOLELY RESPONSIBLE FOR INDEPENDENTLY VALIDATING ALL AI-GENERATED SQL QUERIES, DASHBOARDS, INSIGHTS, AND OTHER OUTPUTS BEFORE RELYING ON THEM FOR BUSINESS, FINANCIAL, MEDICAL, LEGAL, OR ANY OTHER CONSEQUENTIAL DECISIONS. INFERDAT EXPRESSLY DISCLAIMS ALL LIABILITY FOR CUSTOMER'S RELIANCE ON AI-GENERATED OUTPUTS.

17.3 Third-Party Services Disclaimer. INFERDAT MAKES NO WARRANTIES REGARDING THE AVAILABILITY, PERFORMANCE, SECURITY, OR FITNESS OF ANY THIRD-PARTY SERVICES, INCLUDING AWS SERVICES, AMAZON BEDROCK, AND CUSTOMER'S DATA SOURCES. INFERDAT IS NOT RESPONSIBLE FOR ANY FAILURE OR DEGRADATION OF THIRD-PARTY SERVICES AFFECTING PLATFORM OPERATION.

18. LIMITATION OF LIABILITY

> **THESE LIMITATIONS REFLECT A REASONABLE ALLOCATION OF RISK AND ARE AN ESSENTIAL BASIS OF THE BARGAIN. INFERDAT WOULD NOT HAVE ENTERED THIS AGREEMENT WITHOUT THEM.**

18.1 Aggregate Liability Cap. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, INFERDAT'S TOTAL AGGREGATE LIABILITY TO CUSTOMER FOR ALL CLAIMS ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PLATFORM, WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR ANY OTHER THEORY, SHALL NOT EXCEED THE TOTAL FEES PAID OR PAYABLE BY CUSTOMER FOR THE ABI™ PLATFORM THROUGH THE AWS MARKETPLACE IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

18.2 Exclusion of Consequential Damages. IN NO EVENT SHALL INFERDAT BE LIABLE FOR ANY: (a) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES; (b) LOSS OF PROFITS, REVENUE, BUSINESS, GOODWILL, OR ANTICIPATED SAVINGS; (c) LOSS OR CORRUPTION OF DATA OR RECORDS; (d) COST OF SUBSTITUTE SERVICES OR TECHNOLOGY; (e) INFRASTRUCTURE COSTS OR AWS CHARGES OF ANY NATURE WHATSOEVER; (f) BUSINESS INTERRUPTION OR LOST BUSINESS OPPORTUNITY; OR (g) LOSS OR DAMAGE ARISING FROM CUSTOMER'S RELIANCE ON AI-GENERATED OUTPUTS; IN EACH CASE WHETHER OR NOT INFERDAT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE THEORY OF LIABILITY.

18.3 Exceptions. The limitations in Sections 18.1 and 18.2 do not apply to: (a) death or personal injury caused by Inferdat's gross negligence or willful misconduct; (b) Inferdat's fraud or fraudulent misrepresentation; or (c) liability that cannot be excluded or limited under Nevada law or other applicable law.

19. INDEMNIFICATION

19.1 Customer Indemnification. Customer shall indemnify, defend, and hold harmless Inferdat and its officers, directors, employees, agents, and successors ("Inferdat Parties") from and against all third-party claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to: (a) Customer's use of the Platform in violation of this Agreement; (b) Customer's breach of any representation, warranty, or obligation hereunder; (c) Downstream End Users' use of the Platform; (d) Customer Data, including claims that Customer Data infringes third-party intellectual property or violates applicable law; (e) Customer's failure to comply with applicable data privacy, security, or regulatory laws; or (f) Customer's negligence or willful misconduct.

19.2 Inferdat Indemnification. Subject to Sections 18.1 and 19.3, Inferdat shall indemnify, defend, and hold harmless Customer and its officers, directors, and employees from third-party claims alleging that the ABI™ Platform, as delivered by Inferdat and used in strict accordance with this Agreement, directly infringes a valid U.S. patent, copyright, or trademark. This obligation does not apply to claims arising from: (a) Customer's modification of the Platform; (b) Customer's combination of the Platform with other products; (c) Customer's use in violation of this Agreement; or (d) open-source software components included in the Platform.

19.3 Indemnification Procedures. The Indemnified Party shall: (a) promptly notify the indemnifying party in writing (failure to provide timely notice does not relieve the obligation except to the extent materially prejudiced); (b) grant the indemnifying party sole control over defense and settlement; and (c) provide reasonable cooperation at the indemnifying party's expense. The Indemnified Party may participate with its own counsel at its own expense. The indemnifying party shall not enter into any settlement imposing obligations on the Indemnified Party without prior written consent.

20. ACCEPTABLE USE AND COMPETITIVE USE PROHIBITION

20.1 Permitted Use. Customer may use the Platform solely for its internal business purposes and, where applicable, for White-Label Use in accordance with Section 15. All use must comply with applicable law, this Agreement, and the AWS Customer Agreement.

20.2 Competitive Use Prohibition. Customer shall not, and shall ensure its End Users do not, directly or indirectly, use the Platform or any information obtained through use of the Platform (including its features, architecture, user experience, data models, query logic, prompt structures, or AI capabilities) to engage in any "Competitive Purpose," meaning:

- designing, developing, building, training, improving, or commercially offering any software, service, product, or tool that competes with or is intended to compete with the ABI™ Platform or any other Inferdat product or service;
- training or fine-tuning any machine learning model, large language model, embedding model, or AI system using the Platform's outputs, behavior, response patterns, generated SQL, or any other Platform-derived information;
- conducting competitive intelligence analysis, reverse-engineering the Platform's approach to NL-to-SQL conversion, feature benchmarking, or technical evaluation for the purpose of developing or improving a competing product;
- publishing, sharing, or disclosing performance benchmarks, security assessments, or technical evaluations of the Platform without Inferdat's prior written consent; or
- facilitating or permitting any third party to do any of the foregoing.

systematically querying, probing, or interacting with the Platform for the purpose of cataloging, documenting, or reproducing its behavior, response patterns, prompt engineering techniques, SQL generation logic, chart recommendation algorithms, or any other functional behavior, whether manually or through automated means ("Behavioral Extraction"). For the avoidance of doubt, normal business use of the Platform to generate analytics does not constitute Behavioral Extraction; however, any pattern of use that a reasonable person would conclude is designed to understand how the Platform works rather than to obtain legitimate analytical outputs constitutes a violation of this Section; or

using any output, behavior, or observable characteristic of the Platform — including generated SQL queries, natural language responses, chart recommendations, or any other Platform output — as training data, fine-tuning data, evaluation data, or benchmark data for any machine learning model, large language model, or AI system, regardless of whether such model is intended to compete with the Platform or any Inferdat product.

20.3 Prohibited Technical Actions. In addition to the restrictions in Section 3, Customer shall not:

- enable AWS ECS Exec (enableExecuteCommand) on any ECS service that is part of the Deployment Stack, for any reason;
- intercept, inspect, modify, replay, or record any API call, network traffic, or data transmission made by the Platform, including calls to Inferdat's endpoints, AWS services, or Amazon Bedrock;
- modify, delete, or falsify any SSM parameter prefixed with /ABI™-platform/, including entitlement status, tamper baselines, or update availability signals;
- deploy ECS tasks using Inferdat's proprietary container images outside the authorized Deployment Stack;

- use container introspection, memory analysis, network inspection, or any other technique to analyze, extract, or reproduce the Platform's internal logic; or
- share Platform access credentials, URLs, or authenticated sessions with any person or entity that has not agreed to terms at least as restrictive as this Agreement.

20.4 Compliance with Laws. Customer shall not use the Platform to process data in violation of applicable privacy laws without appropriate safeguards, facilitate fraud or illegal activity, or violate the rights of any third party.

21. EXPORT COMPLIANCE

21.1 The ABI™ Platform may be subject to U.S. export control laws and regulations, including the Export Administration Regulations (EAR) and economic sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). Customer represents and warrants that: (a) Customer is not located in, organized under the laws of, or a resident of any country subject to U.S. embargo or comprehensive sanctions; (b) Customer is not identified on any U.S. government restricted party list, including the Specially Designated Nationals (SDN) list, Entity List, or Denied Persons List; and (c) Customer will not re-export or transfer the Platform to any prohibited destination or party in violation of applicable U.S. export laws.

21.2 Customer is solely responsible for complying with all export control and trade compliance laws applicable to its use of the Platform and its own products and services.

22. GOVERNING LAW AND DISPUTE RESOLUTION

22.1 This Agreement shall be governed by and construed in accordance with the laws of the State of Nevada, without regard to its conflict of laws principles or the United Nations Convention on Contracts for the International Sale of Goods.

22.2 Exclusive Jurisdiction. Any dispute, claim, or controversy arising out of or relating to this Agreement, or the breach, termination, enforcement, interpretation, or validity thereof, shall be subject to the exclusive jurisdiction of the state courts of Clark County or Washoe County, Nevada, or, if federal jurisdiction exists, the U.S. District Court for the District of Nevada. Each party irrevocably submits to the personal jurisdiction of such courts and waives any objection to venue therein.

22.3 JURY TRIAL WAIVER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY HEREBY IRREVOCABLY WAIVES ITS RIGHT TO A JURY TRIAL IN ANY LEGAL PROCEEDING ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE PLATFORM.

22.4 Limitation Period. Any claim or cause of action arising under this Agreement must be filed within one (1) year after the claim or cause of action arose. Claims not filed within this period are permanently barred, regardless of any statute of limitations to the contrary.

22.5 Equitable Relief. Notwithstanding the foregoing, Inferdat may seek injunctive or other equitable relief in any court of competent jurisdiction, without posting bond, to protect its intellectual property rights, Confidential Information, or to enforce Sections 3 or 20 of this Agreement. Customer acknowledges that any breach of these sections would cause irreparable harm for which monetary damages would be an inadequate remedy.

23. GENERAL PROVISIONS

23.1 Entire Agreement. This Agreement, together with any applicable Order Form and the AWS Marketplace listing terms for the ABI™ Platform, constitutes the entire agreement between the parties regarding the subject matter hereof and supersedes all prior and contemporaneous negotiations, representations, agreements, and understandings, whether written or oral.

23.2 Amendments. This Agreement may be amended only by a written instrument signed by authorized representatives of both parties, except that Inferdat may update this Agreement by posting a revised version through the AWS Marketplace listing. Continued use of the Platform following the effective date of any update constitutes acceptance of the updated terms.

23.3 No Waiver. Failure of either party to enforce any provision shall not constitute a waiver of the right to enforce such provision or any other provision in the future.

23.4 Severability. If any provision is held invalid, illegal, or unenforceable, it shall be modified to the minimum extent necessary to make it enforceable. The remaining provisions shall continue in full force and effect.

23.5 Assignment. Customer may not assign, delegate, or transfer this Agreement or any rights or obligations hereunder (by operation of law or otherwise) without Inferdat's prior written consent. Inferdat may assign this Agreement without Customer's consent in connection with a merger, acquisition, or sale of all or substantially all of the assets to which this Agreement relates. Any unauthorized assignment is void.

23.6 Notices. Legal notices required under this Agreement shall be in writing and delivered by: (a) certified mail, return receipt requested; or (b) nationally recognized overnight courier, addressed to Inferdat, Inc., [Address], Nevada [ZIP] (for Inferdat) or to Customer's address on file with the AWS Marketplace (for Customer). Operational notices (support requests, update notifications) may be sent by email.

23.7 Force Majeure. Neither party is liable for delays or failures in performance resulting from causes beyond its reasonable control, including natural disasters, pandemics, government actions, or internet or telecommunications failures. Force majeure does not excuse any payment obligation.

23.8 Independent Contractors. The parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, agency, franchise, employment, or fiduciary relationship.

23.9 No Third-Party Beneficiaries. This Agreement is for the sole benefit of the parties and their permitted successors and assigns. No other person or entity, including Downstream End Users, has any legal or equitable right under this Agreement.

23.10 Headings. Section headings are for convenience only and do not affect interpretation of this Agreement.

23.11 Counterparts and Electronic Signatures. This Agreement may be accepted electronically, including by clicking "Accept" on the AWS Marketplace. Such electronic acceptance is legally binding. Inferdat may maintain electronic records of Customer's acceptance.

23.12 Legal Review Recommendation. INFERDAT STRONGLY RECOMMENDS THAT CUSTOMER REVIEW THIS AGREEMENT WITH QUALIFIED LEGAL COUNSEL — PARTICULARLY COUNSEL FAMILIAR WITH NEVADA LAW — BEFORE DEPLOYING OR

USING THE ABI™ PLATFORM, ESPECIALLY IF CUSTOMER OPERATES IN REGULATED INDUSTRIES SUCH AS HEALTHCARE, FINANCE, OR GOVERNMENT.