

NDTDESK Data Security & Privacy Statement

Effective Date: 13 June 2026

Last Updated: 13 June 2026

This Data Security & Privacy Statement provides a summary of how **NDTDESK**, operated by **NKLINE Technology Services Private Limited**, handles customer data, personal data, access control, data storage, retention, export, and security practices.

This statement is intended to support customer IT, quality, compliance, and procurement review. It should be read together with our **Privacy Policy**, **Terms of Service**, **Cookies Policy**, and **Refund and Cancellation Policy**.

1. Platform Overview

NDTDESK is a cloud-based platform for NDT certification management, online examinations, training management, employee qualification tracking, certificate validity tracking, approval workflows, QR-based certificate verification, experience log management, and professional record management.

The platform may be used by business customers, employers, NDT Level III personnel, certifying authorities, training providers, employees, candidates, trainees, and individual NDT professionals.

2. Data Ownership

All data entered, uploaded, generated, or maintained by a customer within NDTDESK remains owned by the customer.

Individual professionals retain ownership of their personal profile data, certificates, employment history, experience logs, training records, and uploaded documents.

NDTDESK does not claim ownership over customer data or individual professional data.

NDTDESK does not sell customer data or personal data.

3. Data Storage and Hosting

At present, NDTDESK uses cloud-based infrastructure.

Current hosting details:

- **Database provider:** MongoDB Atlas
- **Hosting infrastructure / region:** AWS / N. Virginia, United States — **us-east-1**

- **Application hosting / deployment providers:** Netlify, Vercel, AWS, or related cloud infrastructure as applicable
- **Authentication / session management:** NextAuth
- **Business communication and operational tools:** Zoho
- **Payment processing and subscription billing:** Paddle

Because the current hosting region is **AWS / N. Virginia (us-east-1), United States**, customer data may be stored or processed outside the customer's country of residence, including outside the European Economic Area.

Where a customer requires EU-based hosting, dedicated cloud hosting, specific data residency, or on-premise deployment, this can be reviewed separately subject to technical feasibility, implementation scope, security review, and commercial agreement.

4. Security Measures

NDTDESK uses reasonable technical and organizational measures to protect customer data and personal data.

These measures may include:

- Secure cloud infrastructure;
- Encrypted communication using HTTPS/TLS;
- Role-based access control;
- Account authentication;
- User permission management;
- Restricted internal access;
- Database security controls;
- Backup and recovery procedures;
- Controlled support access;
- Session-based authentication;
- Monitoring and troubleshooting controls;
- Periodic review of security practices.

No internet-based system can be guaranteed to be completely secure. However, NDTDESK takes reasonable steps to protect data from unauthorized access, misuse, loss, alteration, or disclosure.

5. User Access and Role-Based Permissions

Access to data within NDTDESK is controlled through user roles and permissions.

Business customers can assign different roles such as administrator, manager, examiner, trainer, Level III, certifying authority, employee, candidate, or trainee.

The customer organization is responsible for assigning and reviewing user permissions within its account.

NDTDESK is not responsible for internal access decisions made by customer administrators or authorized users.

6. NDTDESK Internal Access

NDTDESK personnel do not routinely access customer data.

Access by NDTDESK personnel may occur only where necessary for:

1. Technical support;
2. Troubleshooting;
3. Customer-requested assistance;
4. Onboarding or implementation support;
5. System maintenance;
6. Security investigation;
7. Legal or regulatory compliance.

Internal access is limited to authorized personnel and only for legitimate service-related purposes.

7. Data Processing and GDPR-Aligned Practices

NDTDESK is operated by an Indian company, NKLINE Technology Services Private Limited.

For business customers, the customer organization normally acts as the data controller, and NDTDESK acts as a data processor or service provider processing data on behalf of the customer.

For individual professional accounts, NDTDESK may act as the data controller for the personal data collected directly from the individual.

NDTDESK follows GDPR-aligned principles such as:

- Transparency;
- Purpose limitation;

- Data minimization;
- Access control;
- Data security;
- Data retention control;
- Data export and deletion support.

NDTDESK does not currently claim ISO 27001, SOC 2, or similar formal security certification unless expressly stated in a separate written document.

8. Subprocessors and Service Providers

NDTDESK uses third-party service providers to operate, secure, support, and improve the platform.

Current subprocessors or service providers may include:

- **MongoDB Atlas** – database hosting;
- **AWS** – cloud infrastructure / hosting region support;
- **Netlify / Vercel** – application hosting and deployment infrastructure, where applicable;
- **NextAuth** – authentication and session management;
- **Zoho** – business email, communication, support, CRM, or operational tools, where applicable;
- **Paddle** – payment processing, subscription billing, invoicing, and tax-related payment administration.

These service providers are used only as required to deliver, support, secure, or operate the NDTDESK service.

9. Data Retention

Data retention depends on account status and service type.

Unless otherwise agreed in writing:

- **Active accounts:** Data is retained during the active subscription or service period.
- **Trial accounts:** Trial data may be retained for up to **60 days** after trial expiry.
- **Terminated subscriptions:** Customer data may be retained for up to **90 days** after subscription termination.
- **Backups:** Deleted data may remain in protected backups for a limited period until normal backup rotation is completed.

After the applicable retention period, data may be deleted or anonymized unless retention is required by law, contract, dispute resolution, audit, security, or agreed written arrangement.

10. Data Export

Customers may request export of their data during an active subscription or before account closure.

Export may be provided in commonly used electronic formats where technically feasible.

Customers are responsible for requesting export before the end of the applicable retention period after cancellation or termination.

Individual professionals may request export of their personal account data, subject to identity verification and applicable legal or customer-controlled record limitations.

11. Trial Data Handling

Data entered during a trial remains owned by the customer or user.

If the customer does not continue after the trial, trial data may be retained for up to **60 days** after trial expiry to allow review, reactivation, export, or follow-up.

Upon customer request, trial data may be deleted earlier, subject to legal, security, backup, and technical limitations.

12. Subscription Discontinuation

If a customer discontinues the subscription, the customer may request export of its data before account closure.

After subscription termination, customer data may be retained for up to **90 days** to allow reactivation, export, account closure, legal compliance, dispute resolution, or backup processing.

After the retention period, data may be deleted or anonymized unless retention is required by law or agreed separately in writing.

13. Remote Proctoring and AI-Assisted Proctoring

Where remote proctoring or AI-assisted proctoring is enabled, NDTDESK may process examination integrity data such as activity logs, images, video, audio, screen activity, or proctoring observations depending on the enabled feature and customer requirement.

AI-assisted proctoring is intended to support review. It should not be treated as the sole basis for certification approval, rejection, disciplinary decision, or employment-related decision without human review by the customer or authorized personnel.

Customers are responsible for informing candidates and obtaining any required consent before using remote or AI-assisted proctoring features.

14. Dedicated Hosting and Deployment

NDTDESK's standard deployment is cloud-based.

For enterprise customers, the following options may be reviewed separately:

- Dedicated cloud deployment;
- EU-based hosting;
- Customer-specific data residency;
- Private cloud deployment;
- On-premise deployment;
- Custom infrastructure arrangement.

These options are subject to technical feasibility, customer IT requirements, security review, implementation scope, support model, and separate commercial terms.

NDTDESK is not obligated to provide dedicated or on-premise deployment.

15. Contact

For questions about data security, privacy, hosting, retention, export, or customer data handling, contact:

NKLINE Technology Services Private Limited

13/2958-33, Admanathasamy Nagar North,
Pattinamkathan, Ramanathapuram,
Tamil Nadu, India - 623503

Email: contact@ndtdesk.app