Privacy Policy

Effective Date: 13 June 2026
Last Updated: 13 June 2026

This Privacy Policy explains how **NKLINE Technology Services Private Limited**, operating the platform known as **NDTDESK** ("NDTDESK", "we", "us", or "our"), collects, uses, stores, shares, protects, retains, exports, and deletes personal data and customer data when you use our website, application, software services, training services, certification management tools, examination tools, professional record tools, and related services.

This Privacy Policy applies to:

1. Business customers using NDTDESK to manage employee certifications, examinations, training records, qualification matrices, certificates, approvals, and related compliance activities;

2. Individual NDT professionals using NDTDESK to maintain their professional profile, certificates, expiry reminders, employment history, experience logs, training records, and related documents;

3. Visitors to our website;

4. Trial users, demo users, and users communicating with us for sales, support, or service-related purposes.

By using NDTDESK, you agree to the collection and use of information in accordance with this Privacy Policy.

1. About NDTDESK

NDTDESK is a digital platform designed for non-destructive testing (NDT) certification management, online examinations, training management, employee qualification tracking, certificate validity tracking, experience log management, approval workflows, QR-based certificate verification, and related professional record management.

Our services may be used by companies, training organizations, certifying authorities, NDT Level III personnel, managers, employees, candidates, trainees, and individual NDT professionals.

2. Data Controller and Data Processor Roles

For business customers, the customer organization normally determines what employee, candidate, certification, examination, training, and professional data is entered into NDTDESK. In such cases, the customer organization acts as the data controller, and NDTDESK acts as a data processor or service provider processing the data on behalf of the customer.

For individual professionals who create and maintain their own NDTDESK profile directly, NDTDESK may act as the data controller for the personal data collected and processed for that individual account.

Where required, specific data processing terms may be agreed separately with business customers.

3. Types of Data We Collect

We collect only the information required to provide, maintain, secure, improve, and support our services.

3.1 Account and Contact Information

We may collect:

- Name;
- Email address;
- Mobile number;
- Company name;
- Job title or designation;
- Country or region;
- Account login details;
- User role and access permissions;
- Billing contact details;
- Communication preferences.

3.2 Business Customer Data

When a company uses NDTDESK, the company or its authorized users may enter or upload data relating to employees, candidates, trainees, inspectors, technicians, certifying authorities, and other personnel.

This may include:

- Employee or candidate name;
- Employee ID or internal reference number;
- Email address and contact details;
- Company, department, branch, or location;
- NDT method, level, technique, sector, and certification scope;
- Certification issue date, expiry date, renewal date, and status;
- Written practice or procedure references;

- Training records;
- Examination records;
- Theory, practical, and vision examination results;
- Qualification matrix data;
- Approval records by Level III, certifying authority, or authorized personnel;
- Uploaded certificates, forms, practical records, vision records, training records, and supporting documents;
- Audit trail or workflow status information;
- QR verification information;
- Employment history or experience records entered or validated by the customer.

3.3 Individual Professional Data

When an individual NDT professional creates a personal account, we may collect and store:

- Name and contact details;
- Professional profile information;
- NDT certificates and expiry dates;
- Training records;
- Employment history;
- Experience logs;
- Employer validation records, where applicable;
- Uploaded professional documents;
- Notification preferences;
- Account activity and profile updates.

Individual professionals are responsible for ensuring that the information they upload is accurate and that they have the right to upload any documents or third-party information included in their account.

3.4 Examination and Training Data

When users participate in online examinations, training modules, assessments, or certification workflows, we may collect:

- Course enrollment and progress;

- Test attempts;
- Answers submitted;
- Scores and results;
- Completion status;
- Time spent in training or examination modules;
- Certificate of completion details;
- Examination approval or rejection status;
- Comments or remarks entered by authorized users.

Where remote proctoring is enabled, we may collect additional examination integrity data such as login records, activity logs, images, video, audio, screen activity, or proctoring observations, depending on the feature configuration and customer requirement.

Where AI-assisted proctoring is enabled, automated tools may assist in identifying possible examination integrity concerns. Such tools are used to support review and do not replace the responsibility of the customer, examiner, Level III, certifying authority, or authorized approver to make the final decision.

3.5 Billing and Payment Information

We may collect billing-related information such as:

- Billing name;
- Company billing address;
- Tax details, where applicable;
- Invoice records;
- Subscription plan details;
- Payment status.

Payment processing and subscription billing may be handled through third-party payment service providers, including Paddle. We do not intentionally store full credit card or debit card details on our own servers. Payment information is processed by the relevant payment service provider subject to its own terms, privacy policy, and security controls.

3.6 Website, Device, and Usage Data

When you access our website or application, we may collect technical and usage data such as:

- IP address;
- Browser type;

- Device type;
- Operating system;
- Pages visited;
- Login time and activity;
- Session information;
- Error logs;
- Referral source;
- General usage analytics.

This information helps us maintain security, improve performance, troubleshoot issues, and understand how users interact with the platform.

3.7 Support and Communication Data

When you contact us, request a demo, raise a support request, send an email, or communicate with us through other channels, we may collect:

- Name and contact details;
- Company details;
- Message content;
- Support request details;
- Attachments shared with us;
- Communication history;
- Feedback and survey responses, where applicable.

4. How We Use Data

We use the collected data for the following purposes:

1. To create and manage user accounts;
2. To provide certification management, examination, training, qualification tracking, and professional record management services;
3. To enable employer-based certification workflows and approval processes;
4. To generate, manage, verify, and track certificates and qualification records;
5. To provide expiry reminders, alerts, and notifications;

6. To support individual professional profiles, certificate tracking, employment history, and experience logs;
7. To process subscriptions, invoices, and billing;
8. To provide customer support and technical assistance;
9. To improve platform performance, usability, security, and reliability;
10. To prevent unauthorized access, misuse, fraud, or security incidents;
11. To comply with legal, contractual, tax, regulatory, and audit obligations;
12. To communicate service updates, policy updates, product information, and support-related messages;
13. To analyze website and platform usage in order to improve our services.

We do not sell customer data or individual professional data.

5. Legal Basis for Processing

Depending on the user, service, location, and applicable law, we may process personal data based on one or more of the following legal bases:

1. **Contractual necessity:** to provide services requested by a customer or user;
2. **Consent:** where a user has provided consent, such as for optional communications or certain optional features;
3. **Legitimate interests:** to operate, secure, improve, and support our platform;
4. **Legal obligation:** to comply with applicable laws, tax requirements, regulatory obligations, or lawful requests;
5. **Customer instruction:** where we process personal data on behalf of a business customer.

6. Data Ownership

Business customers retain ownership of all data entered, uploaded, generated, or maintained by them or their authorized users within their NDTDESK account.

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

NDTDESK does not claim ownership over customer data or individual professional data. We process and store such data only for the purpose of providing and supporting the services, subject to this Privacy Policy and any applicable agreement.

7. Data Access and User Permissions

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

For business accounts, customer administrators and authorized users may access, upload, edit, approve, reject, verify, export, or manage data based on the permissions assigned within the customer account.

NDTDESK personnel do not routinely access customer data. Access by our team is restricted and may occur only where necessary for:

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

We require our personnel and service providers to handle data confidentially and only for authorized purposes.

8. Data Sharing and Disclosure

We may share data only in limited circumstances, including the following:

8.1 With Authorized Users

Data may be visible to authorized users within the same customer account, such as administrators, Level III personnel, certifying authorities, managers, trainers, examiners, or other approved roles.

8.2 With Service Providers

We may use trusted third-party service providers to operate, secure, support, and improve NDTDESK. These providers may support services such as:

- Cloud application hosting;
- Database hosting;
- Authentication and session management;
- Email delivery;
- Payment processing;

- Analytics;
- Customer support;
- File storage;
- Backup and infrastructure services;
- Security monitoring.

These service providers are permitted to process data only as required to provide their services to us and are not permitted to use customer data or personal data for their own unrelated purposes.

8.3 With Customers or Employers

Where an individual's data is created, uploaded, validated, or managed under a business customer account, the relevant customer organization may have access to such data based on its internal policies and assigned permissions.

8.4 Certificate Verification

Where QR-based certificate verification or public verification links are enabled, limited certificate-related information may be displayed to verify authenticity. The information shown may include certificate holder name, certification method, level, validity, status, issuing organization, and verification status.

8.5 Legal and Regulatory Requirements

We may disclose data where required to comply with applicable law, court orders, government requests, law enforcement requests, regulatory obligations, or to protect our legal rights.

8.6 Business Transfer

If NDTDESK or NKLINE Technology Services Private Limited is involved in a merger, acquisition, restructuring, investment, or sale of business assets, relevant data may be transferred as part of that transaction, subject to confidentiality and applicable law.

8.7 Subprocessors

NDTDESK may use third-party infrastructure and service providers, commonly referred to as subprocessors, to deliver the service.

Our current subprocessors may include, as applicable:

- **MongoDB Atlas** – database hosting;
- **Amazon Web Services (AWS)** – cloud infrastructure and hosting region support;
- **Netlify / Vercel** – application hosting and deployment infrastructure, where applicable;
- **NextAuth** – authentication and session management;

- **Zoho** – business email, communication, customer support, CRM, or operational tools, where applicable;
- **Paddle** – payment processing, subscription billing, invoicing, and tax-related payment administration.

We may update our subprocessors from time to time as required for service operation, security, performance, or business needs. Where required by applicable agreement or law, we will provide information about relevant subprocessors upon request.

We do not sell personal data.

9. International Data Transfers and Hosting

NDTDESK is operated by NKLINE Technology Services Private Limited, India. Our platform uses cloud-based infrastructure and third-party service providers.

At present, NDTDESK data is hosted using the following infrastructure:

- **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 to the service configuration;
- **Authentication/session management:** NextAuth;
- **Business communication and operational tools:** Zoho;
- **Payment processing and subscription billing:** Paddle.

Because our 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 personal data is transferred internationally, we take reasonable steps to ensure that such transfers are handled in accordance with applicable data protection requirements and customer agreements.

Where a customer requires a specific hosting region, dedicated cloud instance, EU-based hosting, or data residency arrangement, this must be reviewed and agreed separately in writing.

For enterprise customers, dedicated hosting or on-premise deployment may be considered subject to technical feasibility, security review, implementation scope, and separate commercial terms.

10. Data Retention

We retain personal data and customer data only for as long as necessary to provide the services, comply with legal obligations, resolve disputes, enforce agreements, maintain security, and support legitimate business purposes.

10.1 Active Accounts

For active accounts, data is retained for the duration of the subscription, account use, or applicable service period.

10.2 Trial Accounts

Data entered during a trial will be retained during the trial period.

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

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

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

10.3 Subscription Termination

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 applicable retention period, customer data may be deleted or anonymized unless retention is required by law, contract, audit requirement, dispute resolution, or agreed separately in writing.

Customers are responsible for requesting data export before the end of the retention period.

10.4 Individual Professional Accounts

Individual professionals may request correction, export, or deletion of their personal account data, subject to identity verification, legal obligations, customer ownership rights, and records that may need to be retained where the data is linked to an employer-validated or customer-controlled certification record.

10.5 Backups

Data deleted from the active system may continue to exist in protected backups for a limited period until backup cycles are completed.

Backup data is retained only for system recovery, business continuity, security, and disaster recovery purposes. Backup data is not used for ordinary business operations.

Where feasible, deleted data will be removed from backups during the normal backup rotation cycle.

11. Data Export and Portability

Business customers may request export of their data during an active subscription or before termination, subject to technical feasibility and the terms of the applicable agreement.

Individual professionals may request a copy of their personal data, subject to identity verification and applicable law.

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

12. Data Correction and Deletion Requests

Users may request correction, updating, export, or deletion of personal data by contacting us at:

support@ndtdesk.app

We may need to verify the identity and authority of the person making the request before processing it.

For business customer accounts, requests relating to employee, candidate, or certification data may need to be handled through the relevant customer organization because the customer may control that data.

We may refuse or limit a deletion request where retention is required for legal, contractual, audit, fraud prevention, dispute resolution, security, or compliance reasons.

13. Security Measures

We use reasonable technical and organizational measures to protect data from unauthorized access, loss, misuse, alteration, or disclosure.

These measures may include:

- Secure cloud infrastructure;
- Role-based access controls;
- Account authentication;
- Encrypted communication using HTTPS/TLS;
- Access restriction for internal personnel;
- Database security controls;
- Backup and recovery procedures;
- Monitoring and troubleshooting controls;

- Administrative access limitation;
- Periodic review of security practices.

No internet-based system is completely secure. While we take reasonable steps to protect data, we cannot guarantee absolute security of data transmitted or stored through the internet.

Users are responsible for maintaining the confidentiality of their login credentials and for ensuring that only authorized personnel access their accounts.

14. Cookies and Similar Technologies

We use cookies and similar technologies to operate our website and application, maintain secure login sessions, remember preferences, analyze usage, and improve our services.

Cookies may include:

1. **Essential cookies:** required for login, authentication, security, and platform operation;
2. **Functional cookies:** used to remember user preferences and improve user experience;
3. **Analytics cookies:** used to understand website usage and improve performance.

Users may control cookies through browser settings. Blocking essential cookies may affect the functionality of the platform.

Where required by applicable law, we will request consent before using non-essential cookies.

15. Analytics

We may use analytics tools to understand how users interact with our website and services. Analytics data may include technical information such as device type, browser type, pages visited, session duration, and general usage patterns.

Analytics tools help us improve website performance, usability, and service quality.

Where required, users may opt out of non-essential analytics cookies through available browser or cookie settings.

16. Marketing Communications

We may send service-related emails, account notifications, product updates, training updates, expiry reminders, or other relevant communications.

Users may opt out of non-essential marketing communications at any time. However, we may continue to send essential service, security, billing, legal, and account-related communications.

17. Automated Processing and Examination Results

NDTDESK may automatically calculate examination scores, certification status, expiry status, qualification matrix status, pending requirements, and workflow status based on data entered into the platform.

For employer-based certification workflows, final certification decisions, approvals, rejections, and authorizations are controlled by the relevant customer organization, Level III personnel, certifying authority, examiner, or authorized approver.

Where remote proctoring is used, proctoring information is intended to support examination integrity review.

Where AI-assisted proctoring or automated monitoring is used, it is intended to support review by identifying possible examination integrity concerns. 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.

18. Individual Rights

Depending on applicable law and location, users may have rights relating to their personal data, including:

- Right to access personal data;
- Right to correct inaccurate or incomplete data;
- Right to update personal data;
- Right to request deletion of personal data;
- Right to restrict or object to certain processing;
- Right to withdraw consent where processing is based on consent;
- Right to request data portability where applicable;
- Right to lodge a complaint with a relevant authority where applicable.

To exercise these rights, contact us at:

support@ndtdesk.app

For data controlled by a business customer, we may redirect the request to the relevant customer organization or process the request based on the customer's instruction.

19. Children's Privacy

NDTDESK is intended for professional, educational, training, certification, and business use. It is not intended for use by children without appropriate authorization, supervision, or involvement of a responsible organization.

We do not knowingly collect personal data from children where such collection is not permitted by applicable law. If we become aware that such data has been collected without proper authorization, we will take appropriate steps to delete or restrict it.

20. External Links

Our website or platform may contain links to third-party websites, tools, documents, or resources. We are not responsible for the privacy practices, content, or security of third-party websites or services.

Users should review the privacy policies of those third parties before providing any personal data.

21. Customer Responsibilities

Business customers are responsible for:

1. Ensuring they have the right and lawful basis to upload employee, candidate, trainee, and professional data into NDTDESK;
2. Informing their users, employees, candidates, or trainees about how their data will be processed;
3. Assigning appropriate user permissions;
4. Maintaining confidentiality of account credentials;
5. Ensuring that data entered into the platform is accurate and lawful;
6. Managing internal access to employee and certification records;
7. Complying with applicable employment, privacy, certification, and industry requirements.

22. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our services, legal requirements, security practices, or business operations.

The updated version will be posted on our website with the revised “Last Updated” date. Continued use of the platform after the updated policy becomes effective means that users accept the updated policy, unless applicable law requires additional consent.

23. Contact Us

For questions, requests, or concerns regarding this Privacy Policy or the handling of personal data, contact us at:

NKLINE Technology Services Private Limited
13/2958-33, Admanathasamy Nagar North,
Pattinamkathan, Ramanathapuram,
Tamil Nadu, India - 623503

Email: **contact@ndtdesk.app**