PRIVACY POLICY

How we collect, use, share and protect personal data

Controller: HB Digital Consultancy Limited, trading as Treated Digital Solutions
Company number: 698680 (Ireland)
Version: 1.1
Effective date: 18 August 2026
Privacy contact: info@treatedds.com

Privacy at a glance

Topic	What it means
Who controls your data	HB Digital Consultancy Limited (company number 698680), trading as Treated Digital Solutions, is controller for its website, professional accounts, business administration,
Patient and clinical data	The dental practice or other client is ordinarily the controller. TDS ordinarily acts as its processor and follows documented instructions under the Client Services
Selling data	We do not sell personal data.
Advertising cookies	The public website and portal do not intentionally use advertising or cross-site marketing cookies. Non-essential tracking will require an appropriate choice
Your contact	Email info@treatedds.com. Patients should normally contact their treating clinic first about clinical records.

About this policy

This policy explains how HB Digital Consultancy Limited, trading as Treated Digital Solutions ("TDS", "we", "us" or "our"), handles personal data when you visit treatedds.com, contact us, use dashboard.treatedds.com or receive our professional digital dental planning and design services.

It applies to website visitors, clients, clinicians, client staff, approved named-user accounts, professional contacts, suppliers and others whose data we handle. Portal accounts are invitation-only; public self-registration is disabled. It also covers client-submitted patient or clinical data.

This policy does not replace a dental practice's patient privacy notice and does not change the controller–processor allocation in the Client Services Agreement or Data Processing Addendum. Service-specific, regional or legally required notices may supplement it.

Our privacy commitment

We treat patient and clinical data as highly sensitive. We are committed to handling personal data lawfully, fairly and transparently and to protecting its confidentiality, integrity and availability through data protection by design and by default.

We use appropriate, proportionate and risk-based technical and organisational measures, review them as law, threats, services and technology evolve, and improve them where reasonable and necessary. This is a commitment to responsible care and continuous improvement, not a promise that any internet-connected system can be completely risk-free.

Who we are

The controller for the TDS website and TDS's own business-administration processing is:

HB Digital Consultancy Limited, trading as Treated Digital Solutions
Irish company number: 698680
Website: https://www.treatedds.com
Privacy contact: info@treatedds.com

TDS provides digital planning, design, case-management and related professional support for dental professionals. TDS does not provide direct patient care, and the treating clinician remains responsible for diagnosis, prescription, informed consent, suitability, clinical decisions and final approval.

When TDS is a controller and when it is a processor

TDS as controller

TDS acts as controller where it decides why and how personal data is used for its own purposes. This includes website enquiries, account and organisation administration, service communications, fraud prevention, security logs, billing and tax records, legal-publication and acceptance evidence, legal claims and compliance records.

TDS as processor

For patient and clinical data submitted by a client so TDS can provide services on the client's documented instructions, the client will ordinarily be controller and TDS will ordinarily be processor. The client is responsible for the applicable Article 6 legal basis, Article 9 condition, patient-facing information, data accuracy, minimisation, retention decisions and lawful instructions.

If you are a patient and your data was submitted by a dental practice or clinician, contact that practice first. If you contact TDS directly, we will normally refer or forward the request to the relevant client, unless law requires TDS to respond directly.

Important submission rule
Do not send patient records or patient-identifying information through the public enquiry form, ordinary email or social media. Submit clinical records only through the approved secure portal or another route specifically agreed by TDS.

Personal data we handle

The data depends on how you interact with us and which authorised service features you use. It may include:

- Website and enquiry data: name, professional role, practice or organisation, business contact details, enquiry type, message content and correspondence.
- Account and organisation data: name, contact details, role, clinic or employer, professional profile, account status, authorised permissions, named-user invitation records and acceptance records.
- Authentication and device data: password hashes, multi-factor authentication status and counters, trusted-device tokens, session identifiers, sign-in history and account-recovery or reset events. TDS does not store your authenticator app's current one-time code.
- Patient and case data submitted by clients: identifiers, age or date-of-birth information where necessary, treatment objectives, prescriptions, clinical notes, dental records, scans, photographs, radiographs, CBCT/DICOM data, STL or other digital models, case messages, approvals, quality-control records, outputs and revision history. These records may include health and other special-category data.
- File and integrity data: name, declared and detected type, size, SHA-256 checksum, private key, immutable non-null VersionId, upload status and exact-version access and audit events.
- Commercial and billing data: service orders, quotes, prices, currencies, purchase-order references, invoice and tax details, payment status, refunds, provider references and accounting records. Where a payment provider is enabled, TDS is not intended to store full payment-card numbers or card security codes.
- Communications and support data: portal messages, notifications, appointment or consultation information, support requests, feedback, complaints and service correspondence.
- Technical and security data: IP address, browser and device information, timestamps, requested pages, error and diagnostic information, rate-limit events, security alerts, access-control decisions and audit logs.
- Preference and browser-storage data: theme choice, navigation state, optional trusted-device choice and temporary resumable-upload state, as described in the Cookies and browser storage section.

Where the data comes from

- directly from you, including through the website, portal, email, telephone, meetings or professional correspondence;
- from your clinic, employer, account administrator or another authorised representative;
- from a client that submits patient or clinical data on the patient's behalf;
- automatically from browsers, devices, servers and security tools when the website or portal is used;
- from payment, accounting, communications, hosting, security, laboratory or other service providers when an authorised feature is enabled and used; and
- from public registers, regulators, professional advisers or authorities where necessary and lawful.

Why we use personal data and our legal bases

The table describes TDS's own controller processing. When TDS acts only as a processor, the client determines the relevant legal basis and Article 9 condition and TDS processes on documented instructions.

Purpose	Typical data	TDS role and legal basis
Respond to enquiries and onboarding requests	Contact, practice and enquiry data	Controller: steps requested before a contract; legitimate interests in responding to professional enquiries and
Create and administer professional accounts and organisations	Account, role, organisation, acceptance and communication data	Controller: contract where the individual is a contracting party; otherwise legitimate interests in administering the client
Provide digital dental services on a client's instructions	Patient, case, clinical, file, message and output data	Ordinarily processor: the client determines the Article 6 basis and Article 9 condition and instructs TDS under the
Secure the website, portal, accounts and records	Session, device, IP, MFA, audit, file-integrity and security data	Controller: legitimate interests in preventing misuse, protecting data and maintaining reliable services; legal
Bill, account, collect payment and keep required records	Organisation, order, invoice, tax, payment-status and acceptance data	Controller: contract, legal obligation and legitimate interests in financial administration, audit and debt
Operate support, service notices and consultations	Contact, account, case and correspondence data	Controller or processor depending on context: contract and legitimate interests in delivering and supporting the service.

Purpose	Typical data	TDS role and legal basis
Quality assurance and service improvement	Workflow, support, performance and audit data; de-identified or aggregated where practical	Controller: legitimate interests in safe, accurate and reliable services. Identifiable patient data is not used to train an unrelated general-purpose external AI model without separate authorisation
Comply with law and protect legal rights	Relevant account, billing, security, clinical and correspondence records	Controller: legal obligation and legitimate interests in regulatory compliance and establishing,
Send professional marketing where permitted	Business contact and preference data	Controller: consent where required or legitimate

Health and other special-category data

Patient dental records may contain health data. TDS ordinarily processes this data as a processor, so the client must identify and document a lawful Article 6 basis and an applicable Article 9 condition. Where TDS exceptionally determines the purposes and means of limited special-category processing as controller, TDS will identify and document an applicable Article 9 condition, such as where processing is necessary for legal claims or another condition provided by law. TDS does not use patient health data for direct marketing.

What you must provide

Website enquiries are voluntary. Account, organisation, authentication, acceptance and service information marked as required is needed to establish authority, secure the account or provide the requested service. If required information is not provided, TDS may be unable to create or activate an account, accept a case, provide a service, process a payment or meet a legal obligation.

Clients should submit only the minimum patient data needed for the requested service. The public enquiry form requires confirmation that no patient record or identifying patient information is included.

Who we share personal data with

We disclose personal data only where necessary and proportionate for an authorised purpose. Recipients may include:

- authorised TDS personnel and contractors who need the data for their assigned work and are subject to confidentiality obligations;
- hosting, database, private object-storage, backup, security and support providers. The portal's protected clinical objects are stored in private, versioned Contabo object storage under controlled access;
- email, calendar, consultation and communications providers when those services are authorised and enabled;

- payment and accounting providers when the relevant payment or accounting feature is authorised, enabled and used;
- a laboratory, manufacturer, scanner or other professional recipient selected or authorised by the client for a case. Depending on the arrangement, that recipient may be the client's direct processor, an independent controller or a TDS subprocessor;
- professional advisers, insurers, auditors and prospective purchasers or investors subject to appropriate safeguards; and
- courts, regulators, law-enforcement bodies or other authorities where disclosure is required or permitted by law.

We do not sell personal data. External providers receive data only when separately authorised, configured, enabled and used. The internal Laboratory Coordinator workspace does not appoint or activate a laboratory, disclose data, send external email or webhooks, place a manufacturing order, activate credentials or create a manufacturing contract. Contact info@treatedds.com for the current material subprocessor and processing-location information.

Third-party infrastructure and shared responsibility

Parts of the service depend on third-party infrastructure and service providers. These include the production server host, domain-name, TLS and network-security services, database and backup services, Contabo private object storage, Google reCAPTCHA and, where authorised and enabled, communications, payment, accounting, laboratory or other professional providers. Contabo is used for protected object storage; it is not the portal's production server host.

Those providers operate systems and infrastructure that TDS does not directly operate or fully control. A provider outage, vulnerability, error or security incident could affect service availability or personal data despite reasonable safeguards. TDS therefore does not promise uninterrupted availability or zero security incidents.

Provider involvement does not remove TDS's own responsibilities. TDS uses governance measures appropriate to its role, including assessing and selecting providers, limiting instructions and access, applying appropriate contractual and transfer safeguards, reviewing material risks, and maintaining incident and continuity arrangements proportionate to the service. If a provider incident affects personal data, TDS will take the steps required of it under applicable law and relevant client agreements, including investigation, containment and remediation within its control, assistance to the relevant client, and required breach-notification cooperation. Nothing in this policy excludes any duty or liability that cannot lawfully be excluded.

International transfers

Our primary portal and protected object-storage arrangements are configured for European hosting, but some approved suppliers or professional recipients may process data outside the European Economic Area (EEA). Where a restricted transfer is made, we use a lawful mechanism as required, such as an

adequacy decision, the European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement or UK Addendum, together with supplementary measures where appropriate.

A client's instruction or contractual consent does not override mandatory health-data localisation or transfer restrictions. TDS may refuse or suspend a transfer until a compliant route is available. You may contact us for information about the safeguard relevant to a transfer of your personal data.

How we protect personal data

We use technical and organisational measures proportionate to the nature and risk of the processing. Depending on the service, these measures may include:

- role-based and least-privilege access controls, organisation and case ownership checks, and multi-factor authentication for privileged access;
- private versioned storage, non-null immutable VersionIds and short-lived exact-version delivery;
- secure session cookies, trusted-device rotation and revocation, rate limiting, audit logs, monitoring and security alerts;
- authenticated same-origin server-mediated upload; direct browser storage gated off;
- secure development, testing, vulnerability management, incident response and personnel confidentiality; and
- data minimisation and fail-closed feature gates for providers and higher-risk workflows.

No internet-connected system can guarantee absolute security. Clients are responsible for their own devices, networks, user administration, credentials, local copies and lawful portal use. Report suspected compromise, misdirected patient data or another security concern promptly to info@treatedds.com.

How long we keep personal data

We keep personal data only for as long as necessary for the relevant purpose, then delete, anonymise or securely place it beyond use, unless law requires or permits longer retention. We apply a documented retention decision or criteria to each record type.

Record category	Retention approach
Website enquiries and general correspondence	Until the enquiry is resolved and for a proportionate follow-up period, or longer if the correspondence becomes part of a
Accounts and organisation profiles	For the active relationship and as needed to close the account, resolve access issues, evidence authority and meet
Patient and clinical data processed for a client	For the service term and the client's documented lawful retention period. At the end of services, data is returned or deleted where instructed and feasible, except for lawful

Record category	Retention approach
Security, session, audit and integrity records	For a risk-based period needed to detect, investigate and prevent misuse, protect users and systems, demonstrate
Orders, invoices, tax, payment status and legal acceptances	For statutory accounting, tax, contract, audit and limitation periods and as necessary for legal claims. Immutable acceptance evidence is retained where required to prove
Backups	Until the relevant protected backup expires or is securely replaced in the ordinary backup cycle, unless it is preserved for an incident, legal hold or recovery

Retention may be extended for a documented legal hold, investigation, regulatory requirement or legal claim. It may be shortened where data is no longer necessary and no lawful reason to retain it remains. Clients remain responsible for determining retention required for their clinical records.

Your data-protection rights

Depending on the law and circumstances, you may have the right to:

- be informed about processing and obtain access to your personal data;
- have inaccurate data corrected and incomplete data completed;
- request erasure or restriction of processing;
- object to processing based on legitimate interests and object at any time to direct marketing;
- receive certain data in a structured, commonly used and machine-readable format and have it transmitted where technically feasible;
- withdraw consent at any time where processing relies on consent, without affecting earlier lawful processing; and
- not be subject to a decision based solely on automated processing that produces legal or similarly significant effects, subject to legal exceptions and safeguards.

These rights are not absolute. Exemptions may apply, including to protect another person's rights, comply with law or establish, exercise or defend legal claims.

How to make a request

Email info@treatedds.com and describe the right you wish to exercise. Use a secure method and do not send unnecessary patient records by ordinary email. We may request proportionate information to verify your identity and authority before disclosing or changing data.

We will respond without undue delay and normally within one month. Where legally permitted because a request is complex or numerous, we may extend by up to two further months and will explain the extension within the first month. Rights requests are normally free of charge, subject to the limited exceptions provided by law.

For patient or clinical data controlled by a dental practice, contact the practice first. TDS will assist the client with valid requests as required by the Data Processing Addendum and applicable law.

Automated tools and artificial intelligence

TDS may use automation, algorithms, software-assisted design, machine learning or AI-enabled tools as components of internal workflow or an approved service. Their use remains subject to the agreed service scope, access controls, applicable data-protection terms and human review requirements.

The portal is not intended to make a solely automated decision about a person that produces legal or similarly significant effects. Automated suggestions do not replace the treating clinician's judgement or responsibility to review and approve the final clinical output.

TDS will not use identifiable patient data to train an unrelated general-purpose external AI model unless the client has separately authorised that use and TDS has established a lawful and contractually appropriate arrangement. Where an external AI or automation provider processes client personal data for TDS, it will be treated as a subprocessor where required.

Cookies and browser storage

The public website and portal use, or may use, the following strictly necessary or user-requested browser technologies. Names and duration can change where an equivalent security or usability control replaces them.

Technology	Purpose	Typical duration / control
sid session cookie	Authenticates the current portal session and supports security controls. Secure, HttpOnly and SameSite=Lax in	Session cookie; normally removed when the browser session ends, subject to server-side timeout.
tds_remember cookie	Optional trusted-device sign-in. The token is rotated after successful use and can be	Up to 30 days, only when the user chooses the trusted-device function.
Theme local storage	Remembers light or dark display preference on the device.	Until the user clears browser storage or changes the preference.
Navigation session storage	Maintains sidebar position and route state within a browser tab.	Normally until the tab or browser session ends.
Resumable-upload local storage	Stores a temporary upload-session token and file metadata so an interrupted authorised upload can	Removed on completion or cancellation, or when the user clears browser storage.
Google reCAPTCHA technologies	Helps protect sign-in and registration from automated abuse when configured.	Controlled by Google and used only where the security challenge is active; see Google's privacy information.

The public website does not intentionally use advertising or cross-site marketing cookies. External font, security or content-delivery services may receive ordinary network request data such as IP address, browser information and request time when their resources are loaded. If we introduce non-essential

analytics, preference or marketing technologies, we will update our notice and obtain consent before use where required. It will be as easy to withdraw consent as to give it.

For more information, see the TDS Cookie Notice and Google Privacy Policy.

Patients and children

The public website and professional portal are directed to dental professionals and authorised business users, not to children or patients for self-service. However, a client may lawfully submit patient data relating to a child where needed for professional dental services. In that situation, the client remains responsible for the lawful basis, Article 9 condition, age-appropriate information, authority or consent requirements and clinical record obligations. TDS processes the data on the client's documented instructions.

Complaints

Please contact info@treatedds.com first so we can try to resolve the issue. You also have the right to raise a concern with the supervisory authority in the country where you live or work or where the alleged infringement occurred.

TDS's Irish supervisory authority is the Data Protection Commission, 6 Pembroke Row, Dublin 2, D02 X963, Ireland. Individuals in the United Kingdom may also contact the Information Commissioner's Office where it has jurisdiction.

Changes to this policy

We may update this policy to reflect changes in law, services, providers or processing. Each published version will identify its version and effective date. Where a change materially affects active users or client-controlled patient data, we will provide additional notice where required and will obtain a new acceptance where the portal's legal gate or applicable law requires it.

Contact

Privacy and security contact
Email: info@treatedds.com
Website: https://www.treatedds.com

For privacy requests, use the subject line “Privacy request”. For a suspected security incident or misdirected patient data, use the subject line “Urgent security report” and do not include unnecessary patient information in the email.