Privacy Policy

1. Who we are

Test Driven Solutions Limited ("TDS", "we", "us") is a technology consultancy. This policy explains how we collect and use personal data about people who visit our website, contact us, work with us as clients or suppliers, or apply for a job with us. It also explains your rights and how to use them.

TDS is the controller of your personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Our details

- Legal entity: Test Driven Solutions Limited
- Company number: 12552433, registered in England and Wales
- Registered office: Suite 14, 2nd Floor, The Spire, Pilgrim Street, Newcastle upon Tyne, NE1 2DS
- Head office: The Spire, Pilgrim Street, Newcastle upon Tyne, NE1 2DS
- Offices: Newcastle, Edinburgh, Wrocław, Warsaw and Calgary

Contacting us about your data

For questions about this policy or to exercise your rights, contact us:

- Email: privacy@testdrivensolutions.co.uk
- Post: Data Protection, Test Driven Solutions Limited, The Spire, Pilgrim Street, Newcastle upon Tyne, NE1 2DS
- Phone: 0191 406 8300

Our website is aimed at businesses and professionals and is not intended for children. We do not knowingly collect data about children.

Our website links to other sites, such as LinkedIn. We are not responsible for how those sites handle your data, so please read their privacy policies.

2. The personal data we collect

What we collect depends on how you interact with us.

Who you are	Data we may collect
Website visitor	IP address, browser and device type, pages visited, how you reached our site, and cookie identifiers (see section 7)
Someone who contacts us	Name, job title, organisation, email address, phone number and the content of your message
Client or prospective client contact	Name, job title, organisation, business contact details, meeting notes, correspondence and your communication preferences
Supplier or partner contact	Name, job title, organisation, business contact details and, for sole traders, payment details
Insights or newsletter subscriber	Name, email address, organisation and your subscription preferences
Job applicant	See section 5

We do not collect special category data (such as health, ethnicity or religion) through our website. The only exceptions are set out in section 5 for job applicants.

We may also create aggregated statistics, such as the number of visitors to a page. These do not identify you.

3. How we collect your data

- **From you:** when you fill in a form on our website, email or call us, meet us, subscribe to our Insights, or apply for a role.
- **Automatically:** when you browse our website, through cookies and similar technologies (see section 7).
- **From your organisation:** when your employer is our client or supplier and shares your contact details with us.
- **From public and professional sources:** such as Companies House, your organisation's website and professional networking sites like LinkedIn.
- **From recruitment sources:** such as job boards, recruitment agencies and people who refer you (see section 5).

4. How we use your data and our lawful basis

We only use your data where the law allows it. The table sets out what we do and why.

What we do	Lawful basis
Reply to your enquiry	Legitimate interests (responding to people who contact us)
Set up and manage client and supplier relationships, including contracts, invoicing and payments	Contract, where you are a party to it; otherwise legitimate interests (running our business)
Deliver services to our clients, including working with client staff	Legitimate interests (delivering what we have agreed with your organisation)
Send Insights, event invitations and updates about our services	Consent, or legitimate interests for existing business contacts (see section 6)
Run, secure and improve our website	Legitimate interests (keeping our website working and secure)
Measure website use with analytics cookies	Consent (see section 7)
Recruit people to work at TDS	See section 5
Keep financial records and meet tax, regulatory and legal duties	Legal obligation
Establish, exercise or defend legal claims	Legitimate interests
Prepare for a sale, merger or restructure of our business	Legitimate interests

Where we rely on legitimate interests, we have balanced our interests against your rights. You can ask us for details of that assessment.

We do not make decisions about you based solely on automated processing, including profiling, that have legal or similarly significant effects.

5. Job applicants

If you apply for a role with us, we use your data to assess your application, make a hiring decision and, if successful, prepare your employment.

What we collect

- Your CV, cover letter, contact details, work history, qualifications and skills
- Notes and scores from interviews and technical assessments
- References, once we have made an offer
- Right-to-work documents, as required by law

- Security vetting information, such as BPSS or SC checks, which may include criminal records data, for roles that require it
- Optional equal opportunities information, which may include special category data. This is used only for anonymised monitoring and does not affect your application

Lawful basis

We rely on legitimate interests to assess applications, steps before entering a contract when we make an offer, and legal obligation for right-to-work checks. Equal opportunities data is processed with your explicit consent or for equality monitoring as permitted by the Data Protection Act 2018. Vetting data is processed where required by our clients' security requirements and as permitted by the Data Protection Act 2018.

Systems and sources

We manage applications through Rippling, our applicant tracking system. We may also receive your details from recruitment agencies, job boards or a colleague who refers you.

How long we keep it

If you are unsuccessful, we keep your data for 6 months after the role closes so we can respond to any queries, then delete it automatically. If you agree to be considered for future roles, we keep it for up to 12 months. You can withdraw that agreement and ask us to delete your data at any time. If you join us, your data moves to your employee record and our employee privacy notice applies.

6. Marketing and Insights

We send our Insights, event invitations and service updates to people who have signed up, and to business contacts we have worked with or who have shown interest in our services. We follow the Privacy and Electronic Communications Regulations (PECR) when we do this.

- Every email includes an unsubscribe link. You can also email privacy@testdrivensolutions.co.uk to opt out at any time.
- We do not sell your data or share it with third parties for their own marketing.
- Opting out of marketing does not affect messages we need to send about services we are delivering for your organisation.

7. Cookies and analytics

Cookies are small files stored on your device when you visit a website. We use strictly necessary cookies to make our website work. We only set analytics or marketing cookies if you agree to them through our cookie banner.

Type	Purpose	Consent needed
Strictly necessary	Make the website work and remember your cookie choices	No
Analytics	Google Analytics (via Google Tag Manager) and Hotjar, to understand how visitors use our site	Yes
Marketing	Google Ads conversion tracking, to measure how well our advertising works	Yes

Our cookie banner is provided by CookieYes, which keeps a record of your choices. You can change or withdraw your consent at any time using the cookie settings button on every page. The banner also lists each cookie we use, who sets it and how long it lasts.

8. Who we share your data with

We share data only where needed for the purposes in section 4. Our service providers act on our instructions under written contracts and cannot use your data for their own purposes.

Recipient	Why
IT, email and collaboration providers (Google Workspace and Slack)	Running our business systems
Website hosting (Cargo Creative, using ServerPilot) and analytics providers (Google and Hotjar)	Running and measuring our website
HR and recruitment platform (Rippling)	Managing applications and onboarding
Finance, payroll and accounting systems	Invoicing, payments and records
Other TDS offices	Delivering services and recruiting across our locations
Professional advisers, auditors and insurers	Legal, accounting and insurance purposes
Clients	Sharing consultant profiles and CVs when proposing people for client work, with the consultant's knowledge
HMRC, regulators, law enforcement and courts	Where the law requires us to

Recipient	Why
A buyer or merger partner	If we sell, merge or restructure part of our business

9. International transfers

Some of your data is processed outside the UK, because we have offices in Poland and Canada and some of our service providers are based in, or host data in, the EEA and the United States.

When we transfer data outside the UK, we make sure it is protected by one of these safeguards:

- **UK adequacy regulations**, which recognise that a country gives adequate protection. These currently cover the EEA (including Poland) and Canada for commercial organisations.
- **The UK Extension to the EU-US Data Privacy Framework** (the UK-US Data Bridge), for US providers certified under it.
- **The International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses**, for other transfers.

Contact us if you would like more information about the safeguards for a particular transfer.

10. Security and how long we keep your data

We protect your data with technical and organisational measures, including access controls, encryption, managed devices and staff training. We hold Cyber Essentials and ISO 27001 certification. Only people who need your data for their role can access it. If a data breach occurs, we will notify you and the ICO where the law requires us to.

We keep data only for as long as we need it. These are our standard periods:

Data	How long we keep it
Website enquiries that do not lead to a relationship	Until your enquiry is resolved and any follow-up has ended
Client and supplier contact data	For as long as we work with you or your organisation, then only as long as needed to meet legal and contractual obligations

Data	How long we keep it
Contracts, invoices and financial records	6 years after the end of the financial year they relate to
Marketing subscribers	Until you unsubscribe, or once you stop engaging with our communications
Unsuccessful job applicants	6 months after the role closes, or up to 12 months if you agree to be considered for future roles
Analytics data	14 months

We may keep data longer if we need it for a legal claim or complaint. Data we anonymise may be kept indefinitely.

11. Your rights

You have the right to:

- **Access** a copy of the data we hold about you
- **Correct** data that is inaccurate or incomplete
- **Erase** your data where there is no good reason for us to keep it
- **Restrict** how we use your data in certain circumstances
- **Object** to us using your data based on legitimate interests, and to stop direct marketing at any time
- **Transfer** data you gave us to another organisation, where we process it by consent or contract
- **Withdraw consent** at any time, where we rely on consent

To use any of these rights, contact us using the details in section 1. There is usually no fee. We may ask you to confirm your identity, and we will respond within one month. If your request is complex, we may extend this by up to two more months and will tell you why.

12. Complaints

If you are unhappy with how we have handled your data, please contact us first using the details in section 1. We will acknowledge your complaint within 30 days and tell you the outcome.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK regulator for data protection, at ico.org.uk or on 0303 123 1113.

13. Changes to this policy

We review this policy regularly and will post any changes on this page. This version was last updated on 29 October 2026.