Privacy Policy

For Drivers and Contractors Using the Zerity Platform

Version: 1.0

1. Introduction

Zerity Limited (**"Zerity"**, **"we"**, **"us"**, or **"our"**) is a private limited company registered in England and Wales (Company No. 14348190) with its registered office at Elizabeth House, Victoria Street, Openshaw, Manchester, M11 2NX.

Zerity provides a cloud-based platform (the **"Platform"**) that enables logistics, courier, and delivery companies (**"Clients"**) to manage contractor onboarding, compliance, fleet management, invoicing, payments, health and safety, and asset tracking.

This Privacy Policy explains how we collect, use, store, and share your personal data when you use the Zerity Platform as a **driver, courier, or contractor** (referred to as **"you"** or **"your"**) engaged through one of our Clients. It applies to your use of the Zerity web application, mobile-optimised portal, and any associated services including WhatsApp or SMS notifications.

We are committed to protecting your personal data in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

2. Data Controller and Data Processor

When you use the Zerity Platform, the **logistics company or agency that engages you** (our Client) is typically the **data controller** — they determine the purposes and means of processing your personal data as part of your engagement.

Zerity acts as a data processor on behalf of the Client, processing your personal data under the Client's instructions to deliver Platform services such as onboarding, compliance verification, and payment processing.

In certain limited circumstances, Zerity acts as an **independent data controller**, for example when we:

- Process data for Platform security, fraud prevention, and system administration
- Communicate with you about service updates or critical security notices
- Comply with legal obligations directly applicable to Zerity (e.g., tax or regulatory reporting)

Your Client's own privacy policy may also apply to you. We recommend reviewing it alongside this policy.

3. Personal Data We Collect

We collect personal data that is necessary to onboard you, verify your compliance, manage your engagement, and process your payments. The categories of data we collect are set out below:

Category	Data Elements
Identity Data	Full name, date of birth, town of birth, mother's maiden name, National Insurance number, profile photograph, next of kin details
Contact Data	Email address, telephone number, postal address (including 7-year address history)
Employment & Tax Data	Employment status (sole trader / limited company), UTR number, VAT registration number, IR35 status determination, company registration details (if applicable)
Right to Work Data	Citizenship status, passport or birth certificate copies, naturalisation certificate, visa documentation, right to work verification results
Driving & Licence Data	Driving licence (front and back copies), licence number, entitlements, endorsements, penalty points, DVLA verification results
DBS & Background Data	DBS check consent and results, criminal records data (where legally required and permitted)
Vehicle Data	Vehicle registration, make/model, MOT status, road tax status, insurance certificate, daily inspection records, defect reports, GPS verification data, damage photographs
Financial Data	Bank account number, sort code, payment history, invoice records, dispute details
Health & Safety Data	Risk assessment responses, incident reports (including photographs and GPS location), training records, certificates, food handling qualifications
Performance Data	Delivery completion data, performance scores, achievement milestones, leaderboard rankings
Asset Data	Equipment assigned to you (scanners, devices, uniforms), custody records, QR code scan logs
Technical Data	IP address, browser type, device information, login timestamps, session data, cookies and similar tracking technologies
Communication Data	Messages sent via WhatsApp, SMS, email, or in-app messaging in connection with your onboarding or compliance tasks

4. How We Collect Your Data

We collect personal data from the following sources:

Directly from you

- When you complete the onboarding process via the Zerity portal
- When you upload documents (driving licence, passport, insurance certificates, etc.)
- When you complete daily vehicle inspections or submit incident reports

- When you sign agreements or contracts electronically
- When you communicate with us or your Client via WhatsApp, SMS, or in-app messaging

From your Client (the logistics company)

- Your engagement details, depot assignment, and role-specific onboarding requirements
- Delivery data used for invoice generation and performance tracking

From third-party verification services

- DVLA — driving licence status, entitlements, endorsements, and penalty points
- HMRC — UTR and VAT number validation
- DBS — criminal record check results (where applicable)
- Right to work verification providers
- Vehicle MOT and road tax status via DVLA/DVSA databases

Automatically when you use the Platform

- Technical data collected via cookies, server logs, and similar technologies
- GPS location data during vehicle inspections (where enabled by your Client)

5. Legal Bases for Processing

Under the UK GDPR, we must have a lawful basis for processing your personal data. The legal bases we rely on depend on the specific purpose of processing:

Lawful Basis	Purpose	Legal Reference
Performance of a Contract	Processing your onboarding application, verifying your identity and right to work, managing your engagement, generating invoices, and processing payments.	Art. 6(1)(b)
Legal Obligation	Conducting right to work checks, HMRC reporting (UTR/VAT validation), IR35 compliance, DBS checks (where legally required), DVLA licence verification, RIDDOR incident reporting, and maintaining audit-ready records.	Art. 6(1)(c)
Legitimate Interests	Platform security and fraud prevention, improving our services, analysing aggregated performance data, and maintaining the integrity of the compliance system. We always balance our interests against your rights.	Art. 6(1)(f)
Consent	Sending you non-essential communications (e.g., marketing or surveys), using optional cookies and analytics, processing optional data not required for your engagement. You can withdraw consent at any time.	Art. 6(1)(a)

Lawful Basis	Purpose	Legal Reference
Substantial Public Interest	Processing special category data such as criminal records (DBS checks) and health-related data where necessary for reasons of substantial public interest under Schedule 1 of the Data Protection Act 2018.	Art. 9(2)(g) / DPA 2018 Sch. 1

6. How We Use Your Data

We use your personal data for the following purposes:

Onboarding and Verification

- Processing your application to work with a Client
- Verifying your identity, right to work, driving licence, and DBS status
- Collecting and validating tax information (UTR, VAT registration)
- Facilitating electronic signing of agreements and contracts

Ongoing Compliance Management

- Monitoring document expiry dates and sending automated renewal reminders
- Performing periodic re-verification of your driving licence and vehicle documents
- Maintaining IR35 status determinations and audit-ready compliance records
- Generating compliance reports for your Client

Fleet and Vehicle Management

- Recording daily vehicle inspections, defect reports, and maintenance records
- Tracking MOT, insurance, and road tax status for vehicles assigned to you
- Managing damage reports and recovery processes

Payments and Invoicing

- Generating invoices from delivery data provided by your Client
- Processing payments to your bank account
- Managing payment disputes

Health, Safety, and Risk Management

- Recording risk assessments, incident reports, and near-miss events
- Managing your training records and certification renewals
- Reporting notifiable incidents under RIDDOR where required by law

Performance and Engagement

- Tracking delivery performance metrics on behalf of your Client
- Administering recognition programmes, leaderboards, and milestone rewards

Platform Operations and Security

- Maintaining Platform security, detecting and preventing fraud
- Providing technical support and resolving issues
- Improving Platform functionality based on aggregated, anonymised usage data

7. Who We Share Your Data With

We do not sell your personal data. We share your data only with the parties listed below, and only to the extent necessary for the purposes described in this policy:

Recipient	Purpose and Scope
Your Client	The logistics company or agency that engages you. They receive your onboarding data, compliance status, vehicle inspection records, performance data, and payment information as required to manage your engagement.
Government Agencies	DVLA (driving licence verification), HMRC (tax validation), DBS (criminal record checks), HSE (RIDDOR reporting where required). Data is shared only as required by law or regulation.
Payment Processors	Our payment processing partners who facilitate payment transfers to your bank account. They receive only the financial data necessary to process payments.
Cloud Infrastructure	We host the Platform on secure cloud infrastructure providers based in the UK/EEA. These providers act as sub-processors under strict contractual obligations.
Verification Providers	Third-party services that assist with identity verification, right to work checks, and document validation on behalf of your Client.
Communication Providers	SMS and WhatsApp message delivery providers (e.g., Twilio) who transmit compliance reminders and onboarding notifications on our behalf.
Professional Advisers	Our legal, accounting, and insurance advisers where necessary to protect our legitimate interests or comply with legal obligations.
Law Enforcement	Where we are required by law, court order, or regulatory requirement to disclose your personal data.

All third parties with whom we share data are bound by contractual obligations to keep your personal data confidential and to use it only for the specified purposes.

8. International Data Transfers

Your personal data is primarily stored and processed within the United Kingdom. Where we use service providers located outside the UK, we ensure appropriate safeguards are in place, including:

- UK adequacy regulations recognising the destination country's data protection standards
- International Data Transfer Agreements (IDTAs) approved by the ICO

- Standard Contractual Clauses (SCCs) supplemented with additional security measures where appropriate

9. How Long We Keep Your Data

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. The retention periods below are guided by UK regulatory requirements:

Data Type	Retention Period	Basis
Onboarding records & identity documents	Duration of engagement + 6 years	Tax and employment law requirements (HMRC)
Right to work evidence	Duration of engagement + 2 years	Immigration, Asylum and Nationality Act 2006
DBS check records	Up to 6 months after check completion	DBS Code of Practice; retained data elements (type, reference, date) kept for 2 years per 2025 guidelines
Driving licence verification data	Duration of engagement + 6 years	Regulatory compliance and audit trail requirements
Vehicle inspection records	Duration of vehicle assignment + 6 years	Fleet compliance and HSE requirements
Financial and payment records	6 years from end of engagement	Companies Act 2006; HMRC tax record requirements
Health and safety records	3 years from date of incident	Limitation Act 1980 (personal injury claims); RIDDOR records kept for minimum 3 years
Performance data	Duration of engagement + 12 months	Retained for continuity; anonymised or deleted thereafter
Technical / log data	12 months	Platform security and troubleshooting
Communication records	Duration of engagement + 12 months	Dispute resolution and audit trail

When data is no longer required, it is securely deleted or anonymised. Your Client may instruct us to delete your data earlier, subject to our legal retention obligations.

10. Data Security

We take the security of your personal data seriously and implement appropriate technical and organisational measures, including:

- Bank-level encryption of data in transit (TLS 1.2+) and at rest (AES-256)
- Role-based access controls ensuring only authorised personnel can access your data

- Regular security audits and penetration testing
- Automated monitoring for suspicious activity and unauthorised access attempts
- Secure, encrypted backup procedures with regular recovery testing
- Data processing agreements with all sub-processors
- 99.99% Platform uptime with redundant infrastructure

While we take all reasonable steps to protect your data, no system can guarantee absolute security. In the event of a data breach, we will notify the ICO and affected individuals in accordance with UK GDPR requirements (within 72 hours of becoming aware of a qualifying breach).

11. Your Rights Under UK GDPR

Under the UK GDPR, you have the following rights regarding your personal data. Where Zerity acts as a data processor, we will assist your Client (the data controller) in fulfilling these requests:

Your Right	What It Means
Right of Access	Request a copy of the personal data we hold about you.
Right to Rectification	Request correction of inaccurate or incomplete personal data.
Right to Erasure	Request deletion of your personal data where there is no compelling reason for continued processing. This is subject to legal retention obligations.
Right to Restrict Processing	Request that we limit how we use your data in certain circumstances (e.g., while we verify accuracy after a dispute).
Right to Data Portability	Request your data in a structured, commonly used, machine-readable format and transfer it to another provider.
Right to Object	Object to processing based on legitimate interests. We will stop unless we demonstrate compelling legitimate grounds.
Right to Withdraw Consent	Where processing is based on consent, you may withdraw it at any time without affecting the lawfulness of prior processing.
Rights Related to Automated Decisions	You have the right not to be subject to decisions based solely on automated processing that produce significant effects. You may request human review.

To exercise any of these rights, please contact us at **privacy@zerity.co.uk** or speak to the logistics company through which you are engaged. We will respond within **one calendar month** of receiving your request.

If you are unsatisfied with our response, you have the right to lodge a complaint with the **Information Commissioner's Office (ICO)**:

- Website: ico.org.uk
- Telephone: 0303 123 1113
- Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

12. Cookies and Similar Technologies

The Zerity Platform uses cookies and similar technologies to:

- **Essential cookies:** Enable core functionality such as authentication, session management, and security. These are strictly necessary and cannot be disabled.
- **Functional cookies:** Remember your preferences (e.g., language selection during onboarding) to enhance your experience.
- **Analytics cookies:** Help us understand how the Platform is used so we can improve it. These are only set with your consent.

You can manage cookie preferences through your browser settings or through the cookie consent tool displayed when you first access the Platform. Disabling essential cookies may prevent you from using core Platform features.

13. WhatsApp and SMS Communications

As part of the onboarding process, you may opt in to receive communications via WhatsApp or SMS. These messages may include:

- Onboarding reminders and document upload requests
- Compliance alerts (e.g., document expiry warnings, licence renewal reminders)
- Payment notifications
- Urgent operational updates from your Client

Your communication preference (WhatsApp or SMS) is recorded during onboarding. You may change your preference or opt out at any time by replying **STOP** to any message or by updating your preferences in the Platform. Opting out of non-essential messages will not affect critical compliance or safety notifications required by law.

Messages are delivered through Twilio (our communications provider), which processes your phone number and message content solely for delivery purposes under a data processing agreement with Zerity.

14. Children’s Data

The Zerity Platform is not intended for individuals under the age of 18. We do not knowingly collect personal data from children. If you believe a minor’s data has been submitted to the Platform, please contact us immediately at **privacy@zerity.co.uk**.

15. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or Platform functionality. When we make material changes, we will:

- Update the “Last Updated” date at the top of this policy
- Notify you via the Platform, email, or other appropriate communication channel

- Where required by law, seek your renewed consent before applying changes to your data

We encourage you to review this policy periodically.

16. Contact Us

If you have any questions about this Privacy Policy or wish to exercise your data protection rights, please contact us:

Zerity Limited

Elizabeth House, Victoria Street

Openshaw, Manchester, M11 2NX

United Kingdom

Email: **privacy@zerity.co.uk**

Website: **zerity.co.uk**