

## Information for Clients using Road Tech as a Data Processor

### Target Audience

- Transport Operators who use Road Tech's Systems and Services
- Employees of Road Tech helping Clients answer questions around GDPR and our role as Data Processor

### Road Tech Computer Systems - Data Processor

Among our portfolio of products are a number that are offered as a service. With regard to these services, Road Tech Computer Systems, is classed by the by the DPA 1998, and the new GDPR as a "Data Processor", with the transport operation using the service as the "Data Controller."

If you are using us as a service provider, then you will need to declare this on your submissions to the Information Commissioner in your role as Data Controller.

You will also need to show us as "Data processor" in your "privacy notice" to your staff, or clients, the "Data Subjects".

The information below should cover the areas you need as per GDPR recital 81,83,85,86 GDPR article [28](#) and [30](#).

### Company Details

Road Tech Computer Systems Ltd is a provider of software services, based at Shenley Hall, Rectory Lane, Shenley, Hertfordshire, WD7 9AN.

Road Tech have a registered office at c/o Hillier Hopkins, Radius House, 51 Clarendon Road, WATFORD, WD17 1HP, Company Registration Number 2017435. Registered in England and Wales

ICO Registration Number Z9023540 since 15/04/2005.

Contact details Main Telephone 01923 460000, Fax 01923 462222, email contact [info@roadtech.co.uk](mailto:info@roadtech.co.uk)

For the purposes of the GDPR we are a small company with less than 250 employees. We do not fall within the groups listed in Article 37.1 of the GDPR and therefore will not be appointing a DPO at this time.

Rationale: Road Tech Computer Systems Ltd is not a public authority so 37.1a does not match. Our core activity is selling software solutions to the transport industry. Population of EU as of January 2017 was 512 million.

Customers, and transport organizations who have expressed an interest amount to approximately 25,000. Ignoring the fact that we trade on a business to business basis, and assuming that all had provided details of a natural person this would amount to less than 0.005% of the EU population. Therefore does not meet the "large scale" item in 37.1b, or 37.1c.

We do not engage in the regular or systematic monitoring of customers article 37.1b, or in their criminal activity; 37.1c.

The transport operations that are our customers, use us as a data processor to process event data on their drivers. In aggregate as of January 2017 this amounts in total to data on 110,000 drivers. Presuming no duplicates this represents 0.023% of European population. This may grow significantly and therefore will need to be reviewed.

## Parties

Where a customer (usually a Transport Operation) deals with Road Tech Computer Systems Ltd on a Customer/Supplier basis, the Customer is the Data Subject, and Road Tech Computer Systems Ltd are the Data Controller for the records that we keep with regards to the contracted supply of goods and services to the transport operation. Where a transport operation uses our software purchased or hosted to keep track of information on their drivers, vehicles, customers, suppliers, etc. The transport operation is the data controller. For Software as a services SaaS, hosted in our data centres we are a data processor.

## Trading Basis

Road Tech Computer Systems Ltd, and related companies, are making the reasonable assumption that this is a “business to business” transaction. You must contact us immediately if that is not the case.

## Data Protection

Information for customers where Road Tech Computer Systems Ltd, or other group companies operate as a “Data Processor” as defined in data protection legislation (DPA 1998/GDPR 2016). both use a very broad definition of “data protection”.

This includes :-

- Service and data availability
- Security of data in transit
- Resistance of service to attack
- Audit, and detection of misuse of the data

See [GDPR](#) recital 81, 83, 85, and 86 Information for clients using us as a Data Processor.

### **Service and data availability**

The GDPR includes the availability of a service, within the scope of security.

This includes :-

1. Planned service availability
  2. Risks that contribute to unplanned interruptions,
  3. Steps to mitigate these.
- Our site has a utility power supply with Server rooms power fed from N+1 UPS systems with battery extended runtime and generator backed with external extended fuel tanks. Units can be shut down for maintenance work such as battery replacement without interrupting service.
  - We also run regular on-load testing with simulated mains failure in order to test our systems. We also have the ability to use portable power generation.
  - Site has a single utility supply, the risks of a power supply failure are mitigated by each of the three main buildings having an associated generator, with cross feed capabilities between buildings. Each building is pre-wired with external connection that can be fed from a portable generator, in the event that one or more of the fixed generators fail.
  - Our server rooms are protected by Access Control, 24Hour CCTV and we also have security personnel with patrol dogs in some periods out of normal working hours.
  - The environment is controlled with resilient air conditioning units with temperature sensors, and a fully maintained Fire Detection and Suppressant system. The server rooms are integrity tested yearly.
  - We also have Level 1 Lightning protection with ESP(Electrical Surge Protection).
  - Gated private grounds - with CCTV
  - Remotely monitored intrusion alarm
  - Remotely monitored Fire alarm

- We follow accepted ISO standards to store and protect the personal data we collect, including the use of encryption if appropriate.
- We employ server grade machines with SSD and dual power supplies where applicable.
- Our servers are monitored 24/7/365 by a trained team of our in house engineers and system specialists, using automated checks and remote alerts.
- All information you provide to us is stored on our secured servers within the EEA. As the transmission of information via the internet is not completely secure - for example email - , we cannot guarantee the security of your data transmitted to our site and any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access. Where we have given you a password or where you have chosen a replacement which enables you to access certain parts of our website, you are responsible for keeping the password confidential. We ask you not to share a password with anyone, ever.
- Data availability is paramount in our service provision. We employ RAID, disk replication, delayed replication, clustering
- Data within Road Tech SaaS applications are stored in a highly available system. This utilises a crash resistant database system from a leading supplier, sitting on a RAID system, ensuring redundant disks are in place to recover from lost storage media. Hardware sourced from the leading server manufacturer and highly resilient. Data is replicated in real time using DRBD to storage in a separate data centres, utilising separate power supply, buildings, backup generators and UPS systems. This allows for sub-second fail over on loss of server, power, or entire data centre structure.

#### **Maintenance:-**

- Planned - Second Tuesday of every Month there is a planned maintenance event between 10pm and midnight GMT/BST.
- Additional - When necessary to carryout upgrade or security protection measures as necessary.
- Emergency - If some unforeseen failure occurs, and it is necessary for our infrastructure engineers to carry out urgent measures which means the limiting of some services, these actions will be managed and service downtime will be kept to a minimum.

#### **Security of data in transit**

- Our Internet connectivity is managed across 2 separate providers with diverse routing, firewalled and load balanced.
- We employ TLS (Transport Layer Security) , HTTPS (Hyper Text Transfer Protocol - Secure) and VPN ( Virtual Private Network) using AES 256 encryption technology whilst data is in transit to mitigate against interception of data.

#### **Resistance of service to attack**

As a company Road Tech Computer Systems Ltd has always taken security seriously. We hold to the old parable that "it is a bad idea to put all of your eggs in one basket". We have our own AS number, and one part of the business uses this to function as an ISP providing network services to the other parts of the business. With each business area having its own separately secured network. Traffic entering from the internet, a private circuit, or a VPN. Will always transit at least two layers of firewall, before arriving at the network for the target business area

- Multi layered Firewalling
- Protection against cross site scripting, and SQL injection.
- Reduction of attack surface area
- Network separation, with our own AS number so we are able to supply Internet services to our internal business divisions.

#### **Network Security**

Applications use a variety of techniques to discourage attacks.

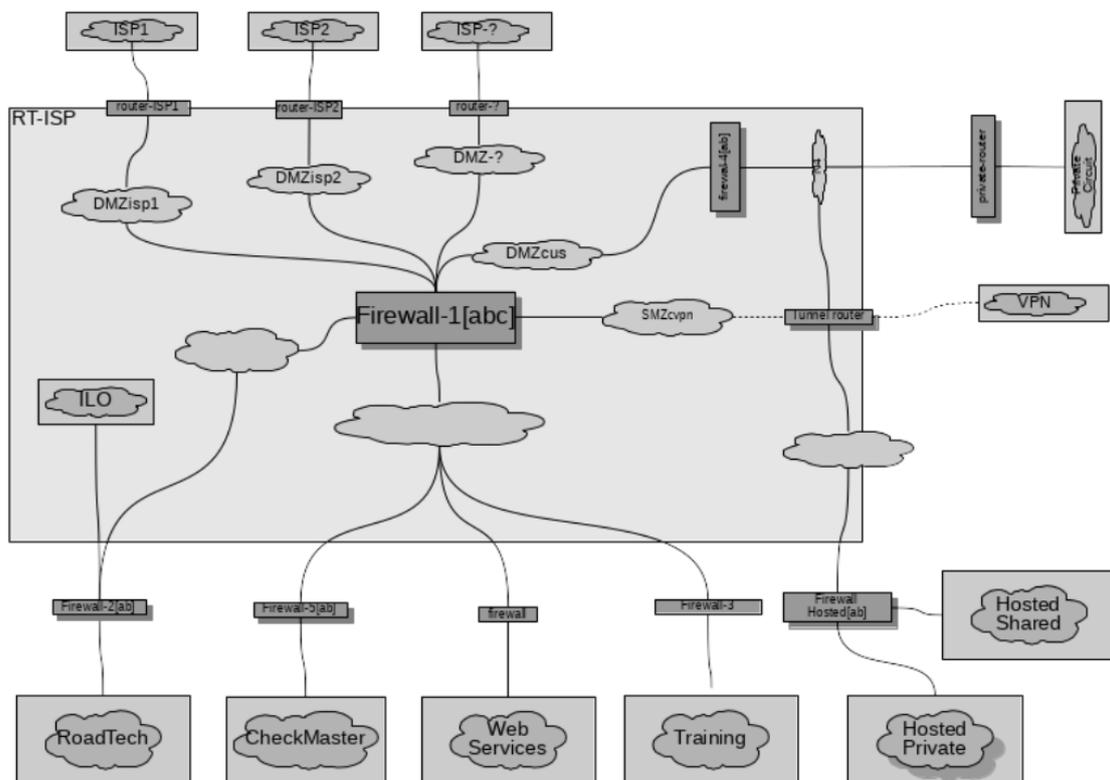
### Network security Shenley.

As a company Road Tech Computer Systems Ltd has always taken security seriously. We hold to the old parable that “it is a bad idea to put all of your eggs in one basket”. We have our own AS number(AS34099) and one part of the business uses this to function as an ISP providing network services to the other parts of the business.

With each business area having its own separately secured network. Traffic entering from the internet, a private circuit, or a VPN. Will always transit at least two layers of firewall, before arriving at the network for the target business area.

### Internet and WAN

With regard to internet connectivity one part of the business shown in the diagram below as RTisp, aggregates external connections, and acts as an ISP to the other business units. RTisp multi homes between multiple ISPs as transit providers. As indicated on the diagram its client business units, each have their own networks and firewalls.



### Audit, and detection of misuse of the data

- The Infrastructure Team run regular penetration tests and security scans using state of the art vulnerability assessment scanning software from a supplier who provides cybersecurity solutions to 24000 organisations across the globe.
- Log inspection is undertaken weekly and result are fed back into the system to make it more robust, taking any appropriate action to ensure robustness.

## Client applications

Web based services run off of our UK data centres. Client devices can cache data locally to maintain a restricted service when communication with the servers is lost.

### **Falcon**

The tracking units record period position updates while moving along with start and stop events based on GNSS (including GPS and possibly Galileo satellite signals). If out of mobile coverage, or experiencing any other communications failure they will cache data for a period. How long depends on the version and firmware.

### **Tachomaster Client and WTD console (Kiosk Mode)**

Maintains a local cache with the current authentication codes and state for each of the customers users. Will allow state changes while communications is interrupted. Can read and cache digital card data collecting binary large object files (BLOB) from both digital driver cards and vehicle units. Data is temporarily held locally, within a SQL bastion database, for store and forward whereby the data is synchronised via https to the Road Tech servers and removed from source.

### **Tachomaster Client Analogue Chart Scanning**

Authentication Login via https, station scans and stores duplex chart images locally pending hours analysis, centre-field entry and chart audit. Once audited and subject to web communications availability the charts are synchronised to the Tachomaster servers. If your broadband connection fails you can still scan and process charts, but they will not be synchronised. Full data analysis, for infringements, does not occur until uploaded to our servers. Once synchronised, charts are removed from source.

### **Checkmaster Client**

Authentication Login via https, station scans and temporarily stores Data Protection Declaration (formally mandate) locally in memory pending confirmation. Once confirmed and subject to web communications availability the Data Protection Declaration images are sent to the Checkmaster servers. If your web communications connection is lost the application will not run. Once sent images are removed from source. If the client is closed with unsent images remaining, these images are removed.

## Service Security

### **Internet**

With regard to internet connectivity one part of the business shown in the diagram above as RTisp, aggregates external connections, and acts as an ISP to the other business units.

RTisp multi homes between multiple ISPs as transit providers. As indicated on the diagram its client business units, have their own networks and firewalls.

### **Road Tech Office Network**

Security Measures include:-

- Antivirus appliance
- Messaging Security
- Malware protection
- Intrusion Protection
- Active Directory - role based security access and privileges
- LDAP
- Multi Layer Firewalling

- Domain Controlled
- Daily Snapshot backup
- Password complexity policy
- Restriction of portable media
- Email usage policy
- Network usage policy
- Remote usage policy
- Training of all staff on GDPR and IT Security
- Rooms where customers visit have restricted network access

### **Guest WiFi**

There is a guest WiFi network primarily for visitors that is completely separate. It uses its own broadband connection.

## Applications

### **Purpose of Roadrunner (Hosted)**

Roadrunner is used to manage Transport Operations, providing operational tools to drive better performance, efficiencies and Transport Management.

### **Personal Data Held**

Driver Contact Details and phone numbers  
Customer Contact Details and phone numbers  
Subcontractor Contact Details and phone numbers  
Supplier Contact Details and phone numbers  
Invoicing and accounting information  
Financial information

All data is held to manage Transport Operations, providing operational tools to drive better performance, efficiencies and Transport Management.

### **Roadrunner Hosted - Security Measures**

- Two factor Authentication
- Certificate Installed on every client that needs access
- Segregation of networks using VLAN technology
- Firewalling on each server
- Access control
- White List
- Blacklist
- User Access control - username and password

### **Purpose of Tachomaster**

Tachomaster is used to analyse, report and manage Worker Hours in accordance with EC legislation, performance and Transport Management analysis.

### **Personal Data Held**

Worker Name	Driving Licence Nation
Worker Email	Driving Licence Expiry
Worker Date of Birth	Driving Licence Photo Expiry
Worker National Insurance Number	CPC Cycle End
Site	Passport Expiry
Department	Licence Check Due
Supervisor	Hazardous Licence Expiry
Employee Number	Medical Check Due
Employee Type	DBS Expiry
Preferred Language	Bridge Bashing Policy Issued
Mobile Worker	HIAB Expiry
Nigh Worker	Forklift Licence Expiry
Handle Hazardous	Eyesight Exam Due
Passenger Vehicle	DQC Number
Reference Period	Last Card Readings Report
Fixed Rolling Period Start Date	Last Card Readings Comment
Night Hours Agreement	Driving Licence Categories
Start of Day	Assessment Site
Finish Date	Assessment Date
Preferred Vehicle	Assessment Expiry
Optional Default Agency	Assessment Category
Optional Customer Contract	Assessment Rating
Driving Licence Number	Assessment Grade
Driving Licence Authority	Worker Prohibited

All data held is to support the process of making sure that compliance data is made available to users, in order to provide compliance and management.

### **Tachomaster - Security Measures**

- HTTPS authentication
- CA signed certificate
- Firewalling
- User Access control - username and password
- Role based access
- Session Timeout
- Brute Force Login Protection
- Cross Site Request Forgery Protection
- Web Site Session Protection

### **Purpose of Falcon Tracking**

Falcon Tracking is used to report and manage Vehicle, Trailer and plant activity, performance and Transport Management analysis.

### **Personal Data Held**

Which Vehicles were driven by which drivers

### **Falcon Tracking - Security Measures**

- HTTPS authentication
- CA signed certificate
- Firewalling
- User Access control - username and password
- Session Timeout
- Brute Force Login Protection
- Cross Site Request Forgery Protection
- Web Site Session Protection

### **Purpose of PreDrive**

PreDrive is used to report and manage Defects to resolution with full audit.

### **Personal Data Held**

Driver Name

Site

Email address

Employee Number

Employment Start Date

Employment Finish Date

User ID

PIN

Workshop Address

Workshop Email Address

Workshop Phone

All data held is to support the process of managing the process of defect resolution, in order to provide compliance and management information.

### **PreDrive - Security Measures**

- HTTPS authentication
- CA signed certificate
- Firewalling
- User Access control - username and password
- Session Timeout
- Brute Force Login Protection
- Cross Site Request Forgery Protection
- Web Site Session Protection

### **Purpose of Checkmaster**

To provide entitlement to drive management.

### **Personal Data Held**

Driver Name

Driver Date of Birth

Driver Licence Number

Licence Expiry Date

Driver Personal Address

Vocational Entitlements

Entitlements and Convictions (*relating to driving licence offences*)

Scanned Mandate - digitally signed

Audit Records

DVLA Check Schedule

DVLA Check Results – Retained for Current month + 2 Years.

All data held is to support the process of making sure up to date entitlement to drive data is available to users, in order to provide compliance and management

### **Checkmaster - Security Measures**

- HTTPS authentication
- CA signed certificate
- Firewalling
- Data Encrypted at rest
- User Access control - username and password
- Strong password structure and expiry policy
- Session Timeout
- Brute Force Login Protection
- Cross Site Request Forgery Protection
- Web Site Session Protection

### **Retention**

Data is retained in the system and may be removed by you in line with your policies at any time.

Mandates are kept for current year +6 along with all data necessary to audit the performance of the system.

Data returned from the DVLA in response to an entitlement to drive check is retained for current month + 2 years.

## RoadrunnerLIVE

When you sign up for RoadrunnerLive, and subscribe to one of the tariffs, a process is setup that synchronizes data from your "on-premises" or "hosted" Roadrunner solution to Road Tech's RoadrunnerLIVE data storage facility at its HQ in Shenley – as detailed in the "**Service and data availability**" section.

### **Purpose/Activity:-**

The synchronised data is used for the purposes of providing one or more of the following RoadrunnerLIVE services to you:-

- Inbound EDI interfaces to create orders/bookings in Roadrunner/ RoadrunnerLive
- Outbound EDI interfaces to provide the entities defined in the Relationship section with electronic status updates.
- Web based bookings entry – allowing your customers to give you jobs over the Internet
- Service Delivery Management and Reporting
- Subcontract Portal – offering jobs to subcontractors that you have a Relationship with or post publicly if you choose
- Performance Dashboards – giving business metrics to your internal users.

All service provision is controlled by RoadrunnerLive '**Relationships**', managed by you in the RoadrunnerLive interface.

Each user will have a defined login and password.

EDI interfaces are undertaken by commission, and often involve satisfying a 3<sup>rd</sup> party's requirements. The method of data transfer between the systems is often dictated by the 3<sup>rd</sup> party and security of the data in-transit may not align with best practice. Road Tech strongly recommends the use of secure protocols employing robust authentication and TLS (Transport Layer Security) protection. If you chose to exchange data with a 3<sup>rd</sup> party using insecure methods, such as email, you do so at your own risk.

### **EDI Transactional files and data**

Any files/messages sent and received during the EDI transaction are held in a temporary area awaiting processing. Once processed these files/messages are stored for analysis and historic interrogation – or re-processing when necessary. These files will be held for a period of 3 months unless otherwise agreed in writing.

### **Data synchronised**

The data synchronised is all the necessary data to support the functions that are available through RoadrunnerLIVE from time to time. It is a subset of the complete data set in Roadrunner, this is not to be considered a backup of data. The data will include customer, vehicle, driver, trailer, contractor, pricing, invoicing, rating and service execution details.

**Personal Data Held**

Some records will contain personally identifiable data.

**Driver Record** includes:-

Member Code	Reference Period Date
Surname	Employment Start Date
Forename	Employment Finish Date
Date of Birth	Licence Authority
Employee Number	Licence Nation
Employee Type	Licence Number
Mobile Worker	Licence Expiry
Night Worker	Passport Expiry
Under EUR Regs	Hazardous Licence Expiry
Hazardous Worker	Medical Check
Reference Period	Licence Photo Expiry
	Driver CPC Expiry
	Tacho Card Last Read

**Contact Details** includes:-

Name	Department
Title	Contact Info
Name	Telephone
Surname	Mobile
Role	Email
Job Title	Fax
	Notes

**Customer Details** includes:-

Contact Details attached to customer  
Name  
Address  
Email  
Phone

**Haulier Details** includes:-

Contact Details attached to Haulier  
Name  
Address  
Email  
Phone  
Fax

**Consignment** includes:-

Driver Name  
Haulier Name  
Collection and Delivery addresses  
Collection and Delivery Address contact details  
Name  
Email  
Phone

### **Users**

Forename  
Surname  
Email  
Phone  
Mobile

### **Retention**

Data is retained in the system and may be removed by you in line with your policies at any time.

### **RoadrunnerLive - Security Measures**

- HTTPS authentication
- CA signed certificate
- Firewalling
- User Access control - username and password

## **Retention periods**

As a supplier we must retain accounting records etc for defined periods of time, this includes data to cover the contractual requirements from our contract with a transport operation.

Where the transport operation is the data controller, and we are a processor. at the termination of the contract for whatever reason [article 28.3g](#) applies.

During the life of a contract each application has its own schedule for purging old data.

Where a service is billed on a purely transactional basis it is possible for a contract to enter an inactive phase where no new data is entered, but enquires on the remaining data can still be made. In this case the existing data will continue to be expired and be purged, according to the normal schedule for the application.

Personal data is kept for the duration of the period you are a customer of Road Tech. We shall retain your data only for as long as necessary in accordance with applicable laws. We may keep your data for up to 7 years from the point at which you cease using our products or services. We may not be able to delete your data before this time due to our legal contractual and/or accountancy obligations. We assure you that your personal data shall only be used for these purposes stated herein.

Checkmaster data returned from a DVLA entitlement to drive check is retained for current month + 2 Years.

When the contract ends the Data Controller has the right to request that the personal data is removed or provided to them.

## Data Subject rights

### **Right to be Informed**

#### What the ICO says

We aim to provide enough information on the services we provide to enable a Data Controller using our services to fully comply with requirements to inform data subjects.

### **Access**

#### What the ICO says

GDPR does not change this very much, as most subject data relates to driver activity, and the Tachograph legislation required employers to provide a minimum of a year's worth of tachograph data and two years of working time data on request.

In Tachomaster and Falcon if the user of the service assigns logins to their data subjects, the data subject can access most services relating to driver activity in worker mode.

In all systems the data can be amended and deleted if the role allows.

### **Data Portability**

#### What the ICO says

Data can be extracted from our systems using suitable output functions. In Tachomaster the original digital card data is available and completely portable. All other static data have extracts to commonly used file formats to enable portability.

### **Rectification**

#### What the ICO says

All functions to amend records are available in the systems if roles allow.

Manual entries for WTD/RTD, holidays, sick days, and similar can all be edited by a user with the appropriate authority.

Tachograph data reads from driver card, or tachograph head as a digitally signed unalterable blob. The legislation makes provision for adding manual notes, not making changes to the evidence.

You can update licence entitlement information provided by a driver, but if there is a discrepancy between what a driver thinks, and what the licensing authority says on a check, the driver must take the issue up with the licensing authority.

### **Object**

If you are using "public task" or "legitimate interest" to cover processing for purposes outside of legislative requirements, or for a longer period, data subject has the right to object.

#### What the ICO says

### **Restrict processing**

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

#### What the ICO says

### **Erase**

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

#### What the ICO says

## Use of cookies

Our Websites may use "cookies" to enhance User experience. User's web browser places cookies on their hard drive for record-keeping purposes and sometimes to track information about them. User may choose to set their web browser to refuse cookies, or to alert you when cookies are being sent. If they do so, note that some parts of the Site may not function properly.

Our Websites uses the web analytics tool Google Analytics to aggregate information used to improve the user experience, you can view the Google Analytics Privacy Policy [here](#). You can opt-out of these cookies by following this link: <http://tools.google.com/dlpage/gaoptout>

Our cookies policy is available to view here <https://www.roadtech.co.uk/cookie/>

## Data Breaches

In the event that Road Tech Computer Systems Ltd become aware of a data breach, relating to data held as processor for a transport operation as controller. We will notify them

In the event of a data breach, we will use the contact details that were provided at point of sign-up, unless other arrangements have been made.

## Contacting us

If you have any questions about this Privacy Policy, the practices of this site, or your dealings with this site, please contact us at:

Road Tech Computer Systems Ltd.  
Shenley Hall  
Rectory Lane  
Radlett  
Hertfordshire  
WD7 9AN  
**tel:**01923 460000  
**email:**[crm@roadtech.co.uk](mailto:crm@roadtech.co.uk)  
**website:**[www.roadtech.co.uk](http://www.roadtech.co.uk)

This document was last updated on 29<sup>th</sup> July 2019 ( v26)