TMS (ANALYSIS) LTD

SECURITY POLICY

Processing of Personal Data

We will process the personal data only on behalf of the Customer and for the sole purpose of performing the services or as otherwise instructed by the Customer.

We use a sub-Processor (Descartes Systems Group Inc) who have developed the software that handles the personal data for compliance to EC Driver's Hours legislation.

Access to the data is via unique usernames and passwords given to authorised personnel of the Customer. Instructions for obtaining usernames and passwords must be in writing by the Customer. It is the customer's responsibility to ensure that usernames and passwords that are no longer needed are removed from the system by emailing support@tmsanalysis.co.uk and detailing the users that need to have their access removed.

All employees of TMS (Analysis) Ltd., and our Sub Processor are subject to a contractual obligation to keep the personal data confidential. We regularly train individuals that have access to personal data in data security and data privacy measures in order to ensure compliance. Access to personal data is strictly on a need-to-know basis to carry out their tasks in accordance with the service we provide the customer.

All paper documents and emails handled within the office that contain personal data are destroyed once work has been completed on them e.g. if printed the documents are shredded and if documents are emailed they are deleted from inbox/sent items/folders including the deleted folder.

Security of Personal Data

We have put in place measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those who have a business need to know. They will only process your personal data on our instructions and where they have agreed to treat the information confidentially and to keep it secure. We have put in place procedures to deal with any suspected data security breach and will notify you and the ICO of a suspected breach where we are legally required to do so.

We will act in respect of personal data to comply with the six principles of the General Data Protection Regulation (GDPR), which are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

You have rights in respect of how your personal data can be processed; these include the right to request:

- A copy of your personal data
- That inaccurate data is rectified; and
- That your personal data is, in certain circumstances, erased or restricted

You have the right to complain to the Information Commissioner, which you can do by contacting the Information Commissioner's Office (ICO) directly.

Breach Management

Our SubProcessor (Descartes Systems Group Inc) have put measures in place with regard to ensuring the security of personal data whilst the personal data is being processed and stored on their systems and they state:

"Unless prohibited by applicable law, upon becoming aware of the Security Breach, Descartes will:

i. Within 48 hours or sooner as required by applicable law, provide to Customer a notification of the occurrence of the Security Breach
ii. Within 5 business days, provide to Customer a summary report of the Security Breach containing details of the Security Breach, its impact on the services under the Agreement and the personal information and the initial steps taken by Descartes to address the Security Breach
iii. Within 15 business days, provide to Customer a detailed incident report analysing the Security Breach and a rectification plan which sets out what steps, if any are appropriate, will be taken to stop and further prevent the Security Breach occurring in the future.

In investigating any Security Breach, Descartes will work to provide to Customer a root cause analysis in order to prevent a recurrence. In addition, unless prohibited by applicable law, Descartes will provide Customer with a summary of the Security Breach and share information about the Security Breach as it becomes available.

At the office of TMS we do not store personal data but should a Security Breach occur whilst processing personal data, all staff are aware of the need to immediately notify the Data Protection Officer and a full investigation will take place. The Customer will be notified within 48 hours and a detailed explanation will be provided to the Customer and a statement of action to be taken to avoid a recurrence.