The Kay Group (UK Holdings) Ltd, The Kay Group (UK) Ltd and Intack Self Drive Ltd

Steering and Review Group

Paul Blackmore, Richard Cox, Simon Fielding, Nicola Cotton, Lee Grendall, Ashley Kay and Adam Howard

1. GDPR has been reviewed, approved and the dissemination of GDPR along with new policies and procedures to comply with the regulation at service station business level will start on 20th February well in advance of the compliance date. All employees will sign up to it.

   Copy attached.

In addition we have placed this statement; **"Under GDPR, all data communicated is lawfully collected for specified, explicit and legitimate purposes, accurately and in a transparent manner. The Company does not pass on any data or personal information for marketing or sales to outside entities",** to:

- Emails
- Accident, Incident and No Means of Payment
- Web Site on the Contact Us and Employee Application pages
- The onsite notification laminated poster of The Kay Group (UK) Ltd being the operators
- Reference request forms

2. After much research it was agreed with our size of business and HO small staffing levels we did not warrant appointing a DPO.

Instead it has been opted for a Review Group to oversee and review the effectiveness of the risks identified and improved policy, procedures and security.

Review of our current activities, security and proposed improvements for HO & Field:

This review acts as a Data and Privacy Impact Assessment.

High Risk

- Server located in the store room
- Computers and Lap Tops are all password protected
- Mobile phones are all password or fingerprint protected
- Payroll is all held electronically
- Paper processed contracts and employee details are kept in a locked cabinet

Security - High Risk

- The server is located in the store room
- All electronic devices are password or finger activated protected
- The main office door is always locked with an intercom for third parties to be welcomed by a member of staff

- The office is further protected by our; 24 hour, 365 day open, petrol service station with CCTV external coverage

- Emails receiving and web site visiting. All Kay Group devices use Microsoft Office 365 as the email provider. This is automatically kept up to date; so this minimises rogue emails – it is rare for a rogue email with a "payload" (attachment) to reach the end user.

- Our Junk Mail settings are set to "cautious" – meaning that if an email looks like it MIGHT not be quite right, then it is sent to junk …. Attachments and links cannot be activated from "junk" so the user would knowingly have to move it out of junk to interact with the email.

- A further layer of security for Head Office and Compliance Managers run an Anti-Malware program call "Webroot". Webroot is updated several times a day.

- Finally if all the above fails and if someone receives an email with a questionable attachment or gets inadvertently directed to a website that tries to upload malware – then in the majority of cases "Webroot" will block it.

Medium/Low Risk

- MD keeps his working files on a USB device attached to his car keys

- Incident, accident reports and third party claims are kept within the Accounts office or in the store room

- CCTV recordings of incidents sent in are stored openly within the accounts office

- General files and business contracts are held in general filing cabinets

- All disused paper documents are stored in identified sacks for a third party shredding

Security - Medium/Low Risk

- Again, the main office door is always locked with an intercom for third parties to be welcomed by a member of staff

- The office is further protected by our; 24 hour, 365 day open, petrol service station with CCTV external coverage

- The Company has never suffered a breach of security

- **MD's stick pen to be encrypted**

- **Proposal to have Key Pad entry locks to the Accounts Office and Store Room**

- **When HO is redeveloped, locking cabinets and freestanding cupboards will be installed**

External Risk - Low

- The company contracts bona fida contractors to:

    - Clean the offices, under a contractual condition not to touch or move any paperwork, and

    - Another who takes old admin and shreds it for security purposes

Security – External Risk

- Under contract with security conditions

- **Both companies will be contacted to see what their considered position is with GDPR**

General Data Protection Regulation (GDPR)

The company processes personal data, which is held in some circumstances manually and in others on computer for the purpose of staff Administration, Accounts, Third Party Claims and Records.

Additionally it processes personal data with the use of CCTV.

All data collected is:

- Lawfully collected for specified, explicit and legitimate purposes accurately and in a transparent manner
    - All employee's data is collected to ensure they are legitimately employed and the company complies with legislation
    - All employees are contractually obliged to inform HO of any personal changes
    - As a backup, annually prior to the tax year end, personnel send a data form to each employee to be completed and returned, this is audited by personnel to ensure it is accurate
- Processed for limited purposes to what is necessary
    - See timescales below
- Adequate, relevant and not excessive
    - This is in place
- Not kept longer than necessary
    - A maximum of six years plus the current year after the organisation or person is no longer associated with the company
    - A Maximum of three years plus the current year to meet insurance third party claims timescales for any CCTV footage, Incident & Accident Reports
    - All third party personal data collected is for the legitimate process of claims, accidents, injury and legislative notifications, such as RIDDOR and Insurance Companies
- No data is transferred outside the European Economic Area (EEA)
- All data held on computer is also held on a backup file, updated on a daily basis through a secure Cloud remote location
- Only directors and appointed personnel processors are authorised to pass on any personal data for legitimate purposes
- The Company does not pass on any employee data for marketing or sales purposes within or outside entities
- The Company does not hold any information on Minors
- Any request of information will normally be free of charge and handled quickly for most requests but all within one month
    - Any considered requests that are unfounded or excessive will be charged or refused

- On refusing to provide any information who ever makes the request will be directed to the supervisory authority for a judicial remedy

- Information will in most cases and where possible be sent electronically an paper based files scanned in

Personal Data Breach

'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Any apparent breaches of security in access to data by persons other than those appointed must be immediately reported to a Director.

Should any individual or company contact you requesting details of information about themselves held by the Company, the request must be in writing and immediately forwarded to Head Office.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data, such as references.

The conditions for erasure include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Any request will be put forward by personnel an determined by a Director

Brexit

UK organisations handling personal data still need to comply with the GDPR, regardless of Brexit. The Government has confirmed that it will follow the GDPR principles for data protection.

Remedies, Liability and Penalties

The Supervisory Authority can impose a fine of up to: 4% of annual global turnover; or €20 million whichever is the greater. The administrative fines will in each case be designed to be effective, proportionate, and dissuasive.