INTRODUCTION

The EU General Data Protection Regulation (GDPR) 2018 replaces the prior Data Protection Acts. The GDPR applies to anyone who processes personal data 'data controllers', it includes third party companies acting on behalf of Quadratek, and the individuals that the data relates to 'data subjects'. Quadratek are responsible for meeting the GDPR obligations and have committed to adopt the best practices of the GDPR.

Quadratek must have a legal basis to justify capturing and processing personal data and be transparent about how, why and when that data is collected, processed and transferred.

As part of Quadratek's processes it is essential that certain personal information is available to us. We will only request, store and share personal data where there is a legal basis or operational requirement to do so. We will seek the employee's written consent in respect of all personal data held, stored or shared by Quadratek about them. Where a data controller wishes to process existing data for a new purpose, the data subject must be notified and further approval sort.

PERSONAL DATA

Personal data is data consisting of information, which relates to an individual who can be identified from the information. All personal data must be processed in accordance with the GDPR 2018 regulations. Quadratek has appointed a Data Controller / Data Protection Officer (DPO) to act as the data controller. They are responsible for carrying out Data Protection Impact Assessments and implementing measures that meet the principles of the GDPR which includes setting out tasks, responsibilities and reporting lines in conjunction with the technical team.

Quadratek and others acting on its behalf, will collect, retain and process information about its employees and other data subjects. The type of information which may be obtained and stored by Quadratek includes [but is not exclusive to] dates of birth, sex, health and the commission or alleged commission of any offences. The types of information and who has access to this information is documented within the Data Register. This information will be used for payroll and personnel management purposes in connection with each individual's employment with Quadratek. In addition, Quadratek shall use any personal data it holds to ensure it can monitor and comply with any current legislation, particularly in terms of equal opportunities and non-discrimination. Where the company holds any employee's personal data, it shall check this data from time to time to ensure that it remains accurate. This shall be carried out on a regular basis by contacting each employee to confirm the details held on file. Employees who become aware of a material change to their circumstances; such as their personal details/maiden names/aliases, home address, next of kin or any contact phone numbers; is required to notify Quadratek as soon as practicable.

Data subjects have the right to not be subject to a decision-making process by 'automated processing' where the decision significantly affects them (recruitment, triggers for sickness/absence, attendance bonuses, shift rostering, employee monitoring). Where exceptions are made, additional safeguarding such as the right to human intervention applies.

Data sourced from social media sites in respect of employees or third parties will be based on Quadratek having a legitimate and lawful reason for doing so. Quadratek may also collect and store data on any other persons associated with the carrying out of its business, or as part of its recruitment and/or training programme. Wherever possible, any information stored will be verified as correct and will be regularly audited for its accuracy by the Data Protection Officer (DPO)

Quadratek will accurately record details on other recipients and cross border third party service providers who sit outside the European Economic Area (EEA)

DATA SECURITY

Data breaches are a breach of security leading to destruction, loss, altering, unauthorised disclosure of or access to personal data. All breaches identified by the company must be documented and reported without delay and not later than 72 hours after their becoming aware of a breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Breaches could include a breach of data protection principles, conditions for consent, data subjects' rights and international data transfers. Significant fines can be applied if Quadratek fails in its responsibilities.

If any data is lost, or believed to be lost, then the employee MUST report this to the DPO or Director of Quadratek as soon as possible.

Quadratek encourages best practice security measures within its Technical and IT policies for deterring and restricting potential loss of data**.**

CONFIDENTIALITY

All data or information sorted or processed on Quadratek's systems or transmitted within or from Quadratek (e.g. e-mail, voice-mail) is the property of Quadratek and may be accessed, read or monitored accordingly. Any employee with access to Quadratek IT resources must ensure the confidentiality and appropriate use of any accessible data, by being aware of the security needs of equipment where such information may be held or displayed, as well as the protection of any access rights, such as passwords.

All employees are required to abide by the privacy rights of all other employees regarding the disclosure of personal information, as required by current legislation. It should also be noted that disclosure of confidential information to unauthorised persons or entities, or the use of such information for self-interest or advantage, is prohibited; as is access to non-public areas of any network drive. Breaches will be treated severely under the company disciplinary rules.

PRIVACY

All users of Quadratek's IT resources are advised to consider the open nature of information disseminated electronically and should not assume any degree of privacy or restricted access to such information. Quadratek strives to provide the highest degree of security when transferring data but cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed or misused by others.

Though it is not the intention of Quadratek to continuously monitor Internet and e-mail communications, or access data files held by an individual; Quadratek reserves the right to do so at any time. Quadratek has the right to read and/or delete any data stored on Quadratek owned or leased equipment. All employees must be aware that they therefore have no right of privacy in respect to Internet and e-mail communications, or stored data, utilising Quadratek owned or leased equipment and services.

However, it should be noted that Quadratek would not normally access an employee's data or communications without first requesting permission to do so. Although, in the event of an internal disciplinary investigation, or on the request by a Government Agency, or as a result of litigation against the individual and/or Quadratek, any e-mail or data files may be locked and/or copied to prevent destruction and loss of information. In such cases, Quadratek may revert to its right to view any data held without first requesting the permission of the individual concerned.