INTRODUCTION

As a business and employer we have to comply with the General Data Protection Regulation from 25 May 2018 which replaces the Data Protection Directive 1995.

The aim of the Act primarily is to give control to citizens and residents over their personal data and to simplify the regulatory environment.

JKP have taken the necessary steps to deal with GDPR and are fully aware of the content and implications. Data held by JKP as a Data Controller may include business and trading names and addresses, phone numbers email and social media contact information for accounting, invoicing, licensing and hardware registration, installation and renewal. Also for associated business and marketing activities. In this respect the company will request the following from employees.

OPTING IN AND OUT

Consent from each individual for their images, principally those currently taken for CV's or the company website, to continue to be used in marketing and day to day running of the business. We ask that each person positively opts in to this condition and this request is clearly marked on the JKP058 Induction List for new staff. Existing staff have signed request forms which are kept in their confidential staff folders. It is made clear to all staff that withdrawal of their consent will be actioned without detriment or penalty via an email to the Data Security Officer. JKP 058 is reviewed annually as part of the QA controlled documents review.

Consent is requested from each individual for consent to hold their personal data in a secure, locked filing cabinet (in the case of paper copies) where only the registered processor (office manager) and a director hold keys and in secure folders on the server. In the case of payroll information we share this with our payroll providers MGB Accountants (all emailed data is password protected) and HMRC and store any relevant emails or correspondence in a secure folder on the server and in the secure paper records held under conditions described above. Passwords are stored in secure Directors only folder.

Consent is requested from each individual that their phone number and that of an emergency contact is held in the office for all staff to see and/or use in case of emergency. This consent can be withdrawn via email to the DSO without detriment or penalty.

All staff paper records will be confidentially shredded one year after leaving employment unless otherwise requested.

EMAIL SYSTEM

JKP utilise Office 365 (using a complex user name and password for each individual) which means that data is encrypted at rest (email messages and attachments that are stored in folders in individual's Office 365 mailbox) and in transit (messages that are in the process of being delivered. Data is in transit whenever a user's device is communicating with an Office 365 server, or when an Office 365 server is communicating with another server) using several strong encryption protocols and technologies including transport layer security/secure sockets layer, internet protocol security and advanced encryption standard. Any end user device connected to an Office 365 mailbox can be remotely wiped ensuring data from unauthorised locations from any endpoint device containing personal and contact information is removed.

The use of a DataBunker (Backup System)ensures JKP complies with GDPR requirements. AES-256 bit validated encryption adheres to specific retention periods. Any outdated data from unauthorised locations from any endpoint device means that requests from data subjects to quickly remove their personal and contact information can be quickly located and actioned.

DataBunker also ensures data remains safe anywhere, anytime on any device. Data can be recovered anywhere and at any point in time to be able to recover business critical data for any regulatory compliances and the data is encrypted in flight and at rest.

WEBSITE CONTACT FORM

Under Microsoft compliance this information is held for 7 – 14 days in 'Deleted', taking 30 days to recover and then permanently deleted

IP ADDRESSES

JKP operates a secure Windows server controlled VPN connection with active directory user name and password control

GDPR COMPLIANCE

Jones King Partnership Limited is registered on the ICO website.

Signed ***Kate O'Mahony for (Data Security Officer)*** Date **September 2021**