KPEA (UK) LIMITED

DATA PROTECTION AUDIT

This data audit was carried out in anticipation of the coming into force of the General Data Protection Regulation on 25 May 2018 to ensure that we are fully aware of, and have a clear record of, our systems and procedures for holding, processing, sharing, securely storing and wiping personal data, and of our compliance in so doing with DPA and GDPR.

We set this data audit in the context of our business and practice. We collect, process and store data in the course of our business as an enquiry agency. We are a family business owned by Lorna Bevins, with Lorna being responsible for running the business and employing only 3 members of staff, two of which have worked in the business for many years. In the course of our business, and in common with all process servers, The other employee and any future employees are usually known to us but we would still obtain two checked references before employment commences. All employees are made aware of our Data Protection policy by Lorna Bevins. We use over 250+ agents in the UK, many of whom are sole traders or small limited companies that have been used by this Company for many years and are well known to us. New agents are taken on recommendation and/or vetted by Lorna Bevins. Process serving and tracing is carried out on a nationwide basis and by its nature involves a chain of professionals acting in this field, and therefore data is commonly processed by a number of businesses on any one job.

We hold, process and store data only to enable us to carry out the transactions for which we are engaged.

Lorna Bevins is the data controller.

An external IT consultant is employed by the Company who has been recommended to us and we have worked with for over a year. They are fully compliant with GDPR and our Data Protection Policy.

1.Who provides us with Personal Data in the course of our business?

- Solicitors and other companies, acting as data holders of client information, instruct us as data processors. This is our main source of data.
- Private clients, ie data owners, also directly instruct us from time to time
- Agents, themselves acting as data processors, use our services and in doing so pass data to us

2.What personal data do we hold in the course of our business?

- We need to process a range of personal data about individuals, as part of our daily operations, as well as to maintain our own accounts and records.
- The exact information we hold and process about data subjects will depend on what we have been asked us to do or what we are contracted to do. This information could include, for example:
    - personal details
    - investigation brief, results and related information
    - family details
    - financial details
    - education and employment details
    - goods and services
    - lifestyle and social circumstances
    - images of individuals captured by camera or video
- We also collect basic personal information (name, email address, phone number and any other information provided) submitted should individuals fill out a “contact us” form on our website. We use such information solely to respond to the query raised.. Any such information collected is subject to our privacy policy available on the website.

3.How do we collect and securely store and process personal data

3.1We access, organise, store and retrieve personal data electronically within our cloud-based storage system within Microsoft Office 365 which as far as we aware is held in UK/EEU storage sites. Our active firewall is provided by AVG Internet Security which includes spyware protection and an anti-virus product.

3.2 We pay a monthly licence fee to Microsoft Office 365 for a premium business licence. Microsoft is committed to GDPR compliance across its cloud services, and provides GDPR related assurances in its contractual commitments.

3.3 Staff have a Windows laptop each for use in the business, set by default to automatically install security updates.

3.4 Accounts can be accessed remotely using secure strong passwords unique to each user, and from our offices at home the accounts can be accessed without such passwords, although access to our computer systems themselves is password protected with strong passwords.

3.5 All of our passwords are recorded in hard copy and stored securely away from the laptops.

3.6 We ordinarily collect and send out personal data via emails from and to clients, other lawyers and advisers using the email accounts set up within Microsoft Office 365 suite. Personal data in transit is encrypted.

3.7 We do not encrypt emails ourselves as this would run against standard practice within the legal profession, but on occasion we are required as part of our client engagement to send personal data by email which we consider to be sensitive eg bank account or employee details. When this is the case, our policy and practice is to attach such information to our emails in a password-protected document using passwords of more than 8 characters and not easily guessable, unless a secure portal is available as an alternative.

3.8 We are careful to select the correct email address before clicking send. In the main, recipients of our emails are sophisticated businesses, under the same data protection obligations as ourselves, whom we are confident to be secure recipients. If at any time we propose to send sensitive emails to a recipient whose server we have good cause to believe to be insecure, we will not do so without checking that their arrangements are secure enough.

3.9 Lorna's and Andy's mobile phone are set up to enable the send and receive of emails from the respective business email accounts within Outlook 365. We have configured our mobile settings so that our emails do not back up to iCloud as we do not consider this to be GDPR compliant. Lorna and Andy's phone can be remotely wiped in the event of loss or theft.

3.10 We will not access any of our business online services using unsecure public wifi networks

3.11 We may also collect and very occasionally send personal data by post. Data received by post or printed from our computers may be kept in physical folders in accordance with paragraph 3.12 below.

3.12 We aim to keep as little personal data in paper form as possible. However, where we do hold such data, it is kept in files within filing cabinets in our office at home, each of which is separate and secure, fitted with lockable doors. Access to the offices is restricted to Staff. The windows in the offices are secure with locks and the premises have a modern alarm which is switched on when the house is empty. All confidential paper waste is shredded. 27 Prospect Lane is covered by 24 hour recorded CCTV.

3.13 We maintain a website https://www.keithparsons.co.uk. This contains contact forms, enabling visitors to leave their name and other details should they wish us to contact them. Data entered and sent access the Internet via the contact forms is encrypted via a secure 256-bit (2048 bit-key) Encryption Level SSL certificate for which we pay for on a yearly renewal basis.

3.14 Our website deploys cookie technology. The cookies used on our website contain no personal information and do not identify anyone. The privacy policy available on our website explains to users how cookies are deployed.

3.15 Our website server is kept up to date with security patches. Software updates are applied when available and to any underlying operating systems to keep them up to date.

3.16 Updates to our website CMS are applied after successful testing along with any required plugin or theme updates to ensure they are always kept up to date and running with the latest patches or software.

3.17 Our website CMS has its own running firewall to protect against hack attempts by unauthorised users.

3.18 We use Google's Invisible reCAPTCHA security on website contact forms to stop spam coming through the contact forms on the website. Use of this security makes you subject to the Google Privacy Policy and Terms of Use.

3.19 In the course of our business we regularly send personal data by post or email to our agents, correctly addressed."

3.20 We do not carry out penetration testing due to cost and size of our business.

4. How and why do we process personal data?

We must ensure at all times that personal data which we collect is used only for the specific purposes for which it is collected. In this way, we collect the minimum amount of personal data required to enable us to service our clients' needs.

We collect and process Personal Data for the following purposes:

Carrying out client instructions as set out in more detail in our privacy notice;

IT security and operations including enabling our external IT advisors in the UK, to remotely access and manage KPEA's IT systems when necessary to resolve IT problems. They do so using a GDPR-compliant programme, which generates a one-time only code, and denies them access once the session has ended. Our IT advisor has a full GDPR policy.

We provide a data protection notice to all data subjects, setting out in clear and plain language how we process their personal data in a concise and transparent format, by placing it on our website and providing a link to it by email at the time of accepting client instructions.

5. How do we ensure documents given to our agents are kept secure?

In line with common practice within our profession, a significant amount of our processing activity is carried out by third parties engaged by us. This is always subject to us satisfying ourselves that personal data will be kept securely in accordance with data protection laws and our specific directions.

6. Data Protection Impact Assessment

We have carefully considered the data protection risks of transactions undertaken in the course of our business and the safeguards we have in place. We do not carry out processing likely to result in high risk to individuals' interests. Therefore we do not need to do a data protection impact assessment under DPA or GDPR.

7. Breaches

Lorna Bevins is the person responsible for data protection at KPEA and has made her staff fully aware of data protection laws, and of their obligation to report any breach to her immediately upon becoming aware of the same, and Lorna fully understands his reporting obligations as data protection officer, as set out in our data protection and privacy policy. There is a data protection breach data form to be completed if required and sent to the Commission at the earliest opportunity.

8. How do we Ensure that our Procedures cover Individuals' Rights under GDPR?

Our Privacy Notice sets out in full the rights that individuals have under GDPR.

Lorna Bevins manages KPEA's policy for deletion, erasure, archiving and ultimately destroying data. .If an individual were to exercise his or her rights under GDPR, our file storage system would enable us to provide data manually, or to delete it.

9. Retention of Documents and Records

As set out in our privacy notice, personal information will be retained only for as long as necessary to fulfil the purposes for which the information was collected; or as required by law; or as long as is set out in any relevant contract a client may hold with us. In most cases, we expect to hold information for a period of ten years after a file is closed, as this is the period necessary to fulfil our legal and regulatory requirements.

KPEA (UK) LIMITED

Created 25th May 2018

Updated 7th June 2020