DATA PROTECTION POLICY Reviewed 1 April 2019

PAUL HESP
Management Consultancy

Context

Paul Hesp Management Consultancy Ltd (PHMC) provides services that require the sharing of sensitive data with clients. Data frequently includes clients' financial accounts, forecasts and business plans, and during the course of client relationships additional information relating to family, lifestyle and personal circumstances, training, education and employment details and physical or mental health or condition may be received.

In addition, PHMC may from time to time manage lists of prospect details for the purposes of marketing and information provision (for example by sending informative newsletters or service offers). Details requested and managed are limited to name, email address, postcode, telephone number and company name. No details are added to any lists unless the individual has opted in.

Such information (now referred to as client data) is used by PHMC to provide holistic advice and guidance in the course of delivering consultancy, mentoring and coaching services, and is relevant in helping PHMC to understand a client's circumstances and aspirations; this understanding informs guidance and advice about business strategies, risks and options that may be appropriate to individual clients.

PHMC recognises that client data is sensitive and confidential to individual clients both personally and commercially, and undertakes to protect the security of client data and to process it fairly. PHMC is registered under the Data Protection Act 1988 (Registration Number ZA509816) as a Data Controller with the Information Commissioners Office and is compliant with the General Data Protection Regulation.

Security Arrangements

Written/ printed data. Any paper records are kept in lockable file storage and shredded as soon as they become superfluous to a client relationship. If client data is posted, a Special Delivery service is used.

Electronic data. Sensitive data is stored on desktop and mobile devices, and synchronised using the cloud-based OneDrive system. We have obtained assurance from Microsoft that OneDrive is GDPR compliant. Computers are used on premises that are locked and secured if unattended. All computers have encrypted drives and are password protected. All email transmissions are sent and received via a secure email server.
Client data is deleted from computers on a case by case basis having regard to the length of relationship and likelihood of further engagement. Data is deleted by default after three years of client inactivity. All computers have recognised firewalls and antivirus and anti-spyware protection and systems are automatically updated.

Travel. PHMC services involve considerable travel by car or public transport. Client data is kept in personal possession at all times, or if left unattended in a car for short periods is out of sight and the vehicle locked.

Third parties. PHMC never releases data to third parties unless in specific circumstances and with client permission. Examples of such circumstances are when a client agrees to

passing data to another business support professional or to an Associate who may assist with delivering services. PHMC obtains assurance from Associates that they take appropriate steps to protect the data, and delete it as soon as service is complete.

Website Privacy. Sensitive data is not collected via the PHMC website. On occasion, clients may be invited to participate in satisfaction surveys, but sensitive data is not collected and surveys are anonymous. The PHMC website uses cookies to enhance visitor experience, and an appropriate notice is displayed, together with a link to inform visitors how to manage cookies.

Access Requests

Individuals may request a copy of all client data relating to them at any time without fee. Client data will be released directly to the client, or to a third party if there is written authority for the third party to receive the data on their behalf. Data relating to other clients will not be released. If requested to release client data to the Police, PHMC will ensure the information is needed to prevent or detect crime before releasing data.

Published: 1 April 2019. Next Review Due: 1 April 2020
Person Responsible: Paul Hesp