RSM Partners

GDPR Data Protection Policy

Prepared by:

Mark Banwell

Business Operations Director

MarkB@rsmpartners.com

Authored Date:

19th January 2018

Policy Status:

Issued

Date of Last Revision:

19th April 2018

Version:

2.0

Table of Contents

1 GDPR Data Protection Policy

1.1 Introduction

We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our daily business as described below. It also covers our response to any data breach and other rights under the GDPR.

1.2 Definitions

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.3 Data protection principles

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a. Processing will be fair, lawful and transparent
b. Data be collected for specific, explicit, and legitimate purposes
c. Data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d. Data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e. Data is not kept for longer than is necessary for its given purpose
f. Data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g. We will comply with the relevant GDPR procedures for international transferring of personal data

1.4 Types of data held

We keep several categories of personal data on our clients in order to carry out effective and efficient processes. We keep this data in a secure and encrypted professional services software application 'Sage CRM' and hosted marketing automation system 'Communigator'.

Specifically, we hold the following types of data:

a. Business contact details such as name, address, email, phone numbers, job title, IP addresses
b. Information relating to a client's contract with us

All of the above information is required for our processing activities and to provide contracted services and support. More information on those processing activities are included in our privacy statement on our website www.rsmpartners.com

1.5 Data subject rights

You have the following rights in relation to the personal data we hold on you:

a. The right to be informed about the data we hold on you and what we do with it
b. The right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests"
c. The right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification'
d. The right to have data deleted in certain circumstances. This is also known as 'erasure'
e. The right to restrict the processing of the data
f. The right to transfer the data we hold on you to another party. This is also known as 'portability'
g. The right to object to the inclusion of any information
h. The right to regulate any automated decision-making and profiling of personal data

1.6 Responsibilities

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

1.7 Lawful bases of processing

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the data subject's consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Data subjects will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

1.8 Access to data

As stated above, data subjects have a right to access the personal data that we hold on them. To exercise this right, data subjects should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the data subject making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

1.9 Data disclosures

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

a. Any company initiatives operated by third parties where consent has previously been provided by the data subject
b. To assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty

These kinds of disclosures will only be made when strictly necessary for the purpose.

1.10 Data security

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a. Ensuring that data is recorded on such devices only where absolutely necessary
b. Using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
c. Ensuring that laptops or USB drives are not left where they can be stolen

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

1.11 Third party processing

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

1.12 International data transfers

The Company does not transfer personal data to any recipients outside of the EEA.

1.13 Requirement to notify breaches

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

1.14 Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

1.15 Records

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its Data Record Book. These records will be kept up to date so that they reflect current processing activities.

1.16 Data protection compliance

Our appointed compliance officer in respect of our data protection activities is:

Mark Banwell

01527 837767

markb@rsmpartners.com

The Courtyard, Buntsford Drive,
Stoke Pound, Bromsgrove B60 3DJ
T +44 (0)1527 837767
e info@rsmpartners.com
www.rsmpartners.com

RSM PARTNERS
MAINFRAME