WADE GROUP AND CONNECTED COMPANIES

DATA PROTECTION POLICY

From 25th May 2018 Data Protection is governed by the General Data Protection Regulation (GDPR) and Wade Group is committed to complying with those regulations and any revisions that may be occur from time to time. GDPR refers specifically to data relating to identifiable natural persons. Wade Group recognises its obligation to design privacy into its systems and processes.

1 Company Details

Name	Wade Group Limited
Address	Estate Office, Ravenstone Hall, Ashby Road, Ravenstone, Leicestershire, LE67 2AA
Telephone Number	01530 816060
Data Protection Registration Number	Not Required to Register
Contact Details	The Financial Director at the above address
UK Companies House Registration	4552091

Name	Wade Furniture Group Limited
Address	Estate Office, Ravenstone Hall, Ashby Road, Ravenstone, Leicestershire, LE67 2AA
Telephone Number	01530 816060
Data Protection Registration Number	Not Required to Register
Contact Details	The Financial Director at the above address
UK Companies House Registration	2043487

Name	Wade Furniture Group Investments Limited
Address	Estate Office, Ravenstone Hall, Ashby Road, Ravenstone, Leicestershire, LE67 2AA
Telephone Number	01530 816060
Data Protection Registration Number	Not Required to Register
Contact Details	The Financial Director at the above address
UK Companies House Registration	233553

Name	Wade Spring Limited
Address	Highfield Street, Long Eaton, Nottingham NG10 4HL
Telephone Number	0115 9463000
Data Protection Registration Number	Not Required to Register
Contact Details	The Financial Director at the above address
UK Companies House Registration	2745077
Additional Information on the company	www.wade-spring.co.uk

Name	Springform Technology Limited
Address	Highfield Street, Long Eaton, Nottingham NG10 4HL
Telephone Number	0115 9463000
Data Protection Registration Number	Not Required to Register
Contact Details	The Accountant at the above address
UK Companies House Registration	2785492
Additional Information on the company	www.springform.co.uk

2 Data Protection Role

Wade Group is both a Data Controller and a Data Processer within the terms of the regulations and processes data in its own systems and in the systems of authorised sub processors.

3 Definitions

Wade Group	All of the companies whose details appear in Section 1
Data Controller	The body which alone or jointly with others determines the purposes and means of the processing of personal data
Data Processor	The person or body that processes personal data on behalf of the controller
Data Processing	Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Personal Data	Any information relating to an identified or identifiable natural person
Identifiable Natural Person	A person who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

4 Data Protection Principles

Wade Group will abide by the principles of GDPR

Lawfulness, fairness and transparency	Personal data must be processed lawfully, fairly and in a manner transparent to the data subject
Purpose Limitation	Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
Data Minimisation	Personal Data must be adequate, relevant and limited to the purposes for which they are processed
Accuracy	Personal Data must be accurate and where necessary kept up to date
Storage Limitation	Personal Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they were processed or archives to be retained
Integrity and Confidentiality	Personal Data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

5 Lawfulness of Processing Personal Data

For processing of Personal Data to be lawful Wade Group must be able to satisfy one or more of the following Conditions

Consent of the Data Subject	Consent must be specific to the type of processing taking place and be a separately given consent rather than bundled or contingent on offer of services
Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract	
Necessary for compliance with legal obligations	Can be common or statutory law and may relate to multiple types of processing
Necessary to protect the vital interests of the data subject or another person where the data subject is incapable of giving consent	
Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	
Necessary for the purposes of legitimate interests	Can be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data

6 Sensitive Data and Lawful Processing

Certain types of data have been designated as being sensitive and although the controlling and processing obligations are the same as for all personal data they must be "more so" in other words there is a greater duty of care required. The sensitive categories of data are those concerned with

Racial or ethnic origin
Political opinions
Religious or philosophical beliefs
Trade Union Membership
Health including sex life and sexual orientation
Genetic data
Biometric data

Wherever possible when dealing with these types of data specific consent of the data subject should be obtained.

7 Information Asset Register

Wade Group has required each employee who controls or processes personal data to compile a personal register of information kept and used. This must be reviewed and updated on a regular basis (not less than once a year and preferable every time a change is made). A copy of this personal register must be lodged with the Financial Director who will maintain a master company register. The Financial Director or his appointed representative will audit the register by means of periodic spot checks on individual registers. A record of these audits must be maintained.

8 Company Data Map

The Information Asset Register will be used to compile a record of personal data held, the reasons for its processing, the name of the processor or sub processor. The Financial Director or his appointed representative will audit the register on an annual basis. A record of these audits must be maintained.

9 Data Retention

As a general principle information should be retained for the shortest time possible however in practice it may be necessary to retain some information for considerable periods. The company has a "Document and Electronic Data Retention Policy" This sets out the retention periods required by the business and should be adhered to by all staff. Retention of any records beyond these timescales must be approved by the Financial Director.

Destruction of records containing personal data must be by secure means
Physical records must be shredded and not binned.
Computer records must be deleted by whatever means the software provides but when computers reach the end of their useful life the hard drive must additionally be securely wiped.

10 Data Security

Files and documents containing personal data should be kept, when not in use, in locked cabinets or locked rooms when cabinets are not locked.
Computers with access to personal data must be password protected at log on and files containing sensitive personal data should additionally be individually password protected wherever possible.
Files and documents containing personal data should not be left on unattended desks.
Computers with access to personal data should not be left open when unattended. As a failsafe they should have a password protected screensaver set to operate after a suitable period of inactivity.

11 Data Protection Impact Assessments (DPIA)
As part of the Data Mapping process all existing systems have been subject to a DPIA however all new systems or changes/upgrades to existing systems must have a DPIA before installation. This must be recorded and lodged with the Financial Director.

12 Data Access Requests

All data access requests should be referred to the Financial Director.

Wade Group is obliged, within one month of receiving a data access request, to supply the following information without cost to the data subject

Confirmation of whether or not the company processes an individual's personal data
Provide a copy of the data (in commonly used electronic form if requested)
Provide an explanation of - - The purposes of processing - The categories of data processed - The recipients or categories of recipients of data - The envisaged retention period or criteria used to determine it - The individual's rights of erasure - The source of the information if not the data subject

13 Rectification

Data subjects have the right to require the company to rectify inaccuracies in personal data held. The company should attempt to verify and correct and such inaccuracies drawn to its attention.

14 Rights to Object

There are rights for individuals to object to specific types of processing for

1	Direct Marketing
2	Processing based on legitimate interests
3	Processing for research or statistical purposes

Processing for types 1 and 3 is not carried out by Wade Group.
Objections to type 2 processing must be passed to the Financial Director who must establish if the company has sufficient grounds to continue processing data on this basis.

15 Right to Erasure and Right to Restriction of Processing

Individuals have the right to have their data erased in certain specified situations – in essence where the processing fails to satisfy the requirements of GDPR.
Request for erasure must be referred to the Financial Director who must respond to the data subject within 1 month and action the request if it is valid and none of the exemptions apply.
The right to erasure applies in the following circumstances

When data are no longer necessary for the purpose for which they were collected or processed
If the individual withdraws consent to processing (and if there is no other justification for processing)
If the individual objects to processing based on legitimate interests and the company cannot demonstrate overriding legitimate grounds for the processing
When the data are otherwise unlawfully processed
If there is a legal requirement to erase the data

The right to erasure does not apply if processing is necessary for

The exercise of the right of freedom of expression and information
Compliance with a legal obligation
Performance of a public interest task or exercise of official authority
Public health reasons
Archival, research or statistical purposes
If required for the establishment, exercise or defence of legal claims

The individual also has the right to request restriction of processing of data in the following situations

When an individual disputes data accuracy restriction will apply until the data can be verified
When an individual has objected to processing based on legitimate interests processing should be restricted until the grounds for processing can be verified
When the processing is unlawful but the individual objects to erasure and requests restriction instead
When there is no further need for the data but the individual requires its retention to establish, exercise or defend legal claims

Request for erasure must be referred to the Financial Director who must ensure the data is retained but not processed until the dispute is resolved or a legitimate basis for processing established.

16 Personal Data Breaches and Notification

GDPR defines this as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

All sub processors and employees must immediately report any such data breach to the Financial Director.

The Financial Director will maintain an internal breach register detailed the facts relating to the breach and the remedial action taken.

The Financial Director will report the breach to both the Supervisory Authority and the data subjects concerned unless one of the following exemptions applies

The breach is unlikely to result in a high risk for the rights and freedoms of data subjects
Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data)