DATA PROCESSING ADDENDUM

Data Processing Addendum ("**DPA**") to the agreement dated 24th May 2018 ("**Agreement**") between SRCL Limited trading as FPM Group and My Surgery Website ("**Processor**") and the website owner, ("**Controller**") (each a "**Party**", together the "**Parties**").

BACKGROUND

(1) The Processor agreed to provide the Controller with services as further specified in the Agreement and Annex 1 to this DPA (the "**Services**") and to implement the technical and organizational measures further specified in Annex 2 to this DPA; and

(2) In providing the Services, the Processor may from time to time be provided with, or have access to, information of the Controller which may qualify as personal data within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") and other applicable data protection laws and provisions.

In order to enable the Parties to carry out their relationship in a manner that is compliant with law, the Parties have entered into this DPA as follows:

1. Terminology

For the purposes of this DPA, the terminology and definitions as used by the GDPR shall apply.

Further definitions are provided throughout this DPA.

2. Responsibilities of the Controller

(a) The Controller confirms that, in respect of the processing to be carried out under this DPA, the technical and organisational measures of the Processor, as set out in Annex 2, are appropriate and sufficient to protect the rights of the data subject.

(b) The Controller confirms that the processing to be carried out under this DPA is lawful according to Art. 6 GDPR and that data subjects were informed sufficiently.

(c) The Controller warrants that all personal data provided to the Processor for its performance of the Services by the Controller has been and shall be processed (including its disclosure to Processor) by the Controller in accordance with GDPR and other applicable data protection laws at all times.

3. Instructions

(a) The Processor shall process the personal data only on behalf of the Controller and in accordance with the documented instructions given by the Controller, unless prohibited by law applicable to the Processor; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless such notification is prohibited by applicable law.

(b) The Controller's instructions are provided in this DPA and the Agreement. Any further instructions that go beyond the instructions contained in this DPA or the Agreement shall not be effective unless recorded in an amendment to this DPA or the Agreement.

(c) The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes applicable data protection provisions. In such case, the Processor is not obliged to follow the instruction until the Controller has confirmed or changed it in a way addressing the infringement.

4. Obligations and rights of the Processor

(a) The Processor shall ensure that persons authorised by the Processor to process the personal data on behalf of the Controller, in particular the Processor's employees as well as employees of any other processors engaged by the Processor, are subject to a binding obligation of confidentiality and that such persons process any personal data to which they have access in the context of performing the Services in compliance with the Controller's instructions.

(b) The Processor shall implement the technical and organisational measures as specified in Annex 2 before processing the personal data on behalf of the Controller. The Processor may amend the technical and organisational measures from time to time provided that the amended technical and organisational measures are not less protective than those set out in Annex 2.

(c) The Processor shall make available to the Controller the information necessary to demonstrate compliance with the obligations of the Processor relating to information security as required by applicable data protection law and by this DPA as applicable to the Services. The Processor shall in particular allow for and contribute to audits (e.g., providing audit reports and/or other relevant information or certificates to Controller upon Controller's request) or on-site inspections, conducted by the Controller or an auditor mandated by the Controller. The extent of the Processor's obligation to assist with such audits shall be proportionate to the nature and purpose of the processing and subject to reasonable prior notice by the Controller.

(d) The Processor shall notify the Controller without undue delay of any 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 under this DPA ("**Personal Data Breach**"). The Processor will assist the Controller with the Controller's obligation under applicable data protection law to inform the data subjects and the supervisory authorities, as applicable, by providing the necessary information taking into account the nature of the processing and the information available to the Processor.

(e) The Processor shall provide reasonable assistance to the Controller with its obligation to carry out a data protection impact assessment and prior consultation with the supervisory authorities that relates to the Services provided by the Processor to the Controller under this DPA by means of providing the necessary and available information to the Controller.

(f) The Processor shall, at the option of the Controller, delete or return to the Controller all personal data which are processed by the Processor on behalf of the Controller under this DPA after the end of the provision of the Services, and delete any existing copies unless applicable law requires the Processor to retain such personal data. For the avoidance of doubt, this obligation shall not be infringed by the destruction of personal data in the proper performance of the Services.

(g) The Processor shall designate a data protection officer and/or a representative, to the extent required by applicable data protection law. The Processor shall provide contact details of the data protection officer and/or representative, if any, to the Controller.

5. Data subject rights

(a) Taking into account the nature of the processing, the Processor shall provide reasonable assistance to the Controller, including through appropriate technical and organisational measures, with the fulfilment of the

Controller's obligation to comply with the rights of the data subjects and respond to data subjects' requests relating to their rights of (i) access, (ii) rectification, (iii) erasure, (iv) restriction of processing, (v) data portability, and (vi) objection to the processing.

(b) The Controller shall determine whether or not a data subject has a right to exercise any such data subject rights and give instructions to the Processor to what extent the assistance is required.

6. Subprocessing

(a) The Processor may engage another processor without prior authorisation of the Controller.

(b) The Processor shall enter into a written contract with another processor ("**Subprocessing Agreement**") and such Subprocessing Agreement shall (i) impose upon the other processor the same obligations as imposed by this DPA upon the Processor, to the extent applicable to the subcontracted part of the Services, (ii) describe the subcontracted part of the Services, and (iii) describe the technical and organizational measures the other processor has to implement pursuant to Annex 2, as applicable to the subcontracted part of the Services.

(c) Where the other processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the other processor's obligations.

(d) In case any other processor is located outside the EU/EEA in a country that is not recognized as providing an adequate level of data protection, the Processor will (i) take reasonable measures to enable the Controller and the other processor to enter into a direct data processing agreement based on EU Model Clauses (Controller to Processor), or (ii) provide the Controller with information on the other processor's certification under the Privacy Shield program and regularly, at least annually, re-confirm that the other processor's certification under the Privacy Shield program is still valid, or (iii) provide the Controller with other information and relevant documentation on the mechanism for international data transfers pursuant to Art. 46 GDPR that is used to lawfully disclose the Controller's personal data to the other processor.

7. Term and termination

The term of this DPA is identical to the term of the Agreement (inclusive of any renewals or extensions). Save as otherwise specified herein, termination rights and requirements shall be the same as those set out in the Agreement.

8. Liability and indemnification

(a) Each Party's liability for government/authority fines and penalties and any other loss or expense whatsoever (whether direct or indirect) incurred by the other Party for failure to comply with the requirements of any laws or regulations that affect the other Party, to the extent such failure was caused by the Party's breach of the terms of this DPA, shall be subject to and limited by the limitations of liability contained in the Agreement.

(b) The limitation of liability set out in clause 8 (a) above shall not apply in case of a Party's liability for intentional or willful default and any mandatory statutory liability imposed on that Party.

(c) Subject to clause 8 (a) and clause 8 (b) above, each Party shall indemnify and hold the other Party harmless from and against all losses due to claims from third parties including government/authority fines and penalties resulting from, arising out of or relating to any material breach of this DPA by the indemnifying Party.

9. Miscellaneous

(a) Each Party shall comply with its obligations under the GDPR and under any other applicable data protection laws.

(b) This DPA shall be governed by the same law as the Agreement except as otherwise stipulated by applicable data protection law. The place of jurisdiction for all disputes regarding this DPA shall be as determined by the Agreement except as otherwise stipulated by applicable data protection law.

(c) In the event of conflict between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, the relevant provisions of this DPA shall prevail.

(d) Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or – should this not be possible – (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.

(e) Each Party has the right to request changes to this DPA to the extent required to satisfy any applicable and mandatory findings, guidance or orders issued by competent European Union or EU Member State authorities, national implementation provisions, or other legal developments concerning the GDPR requirements for the commissioning of data processors under the national laws applicable and binding to the Controller. The Party receiving such a request shall not unreasonably delay or withhold its agreement.

Annex 1 to the DPA – Description of the processing activities

1. **Categories of data subjects**
   The personal data processed concern the following categories of data subjects:

   - FPM Group customers
   - FPM Group prospective customers
   - Employees/contacts of the above
   - Any personal identifiable data from the content of the website or messages passed via it.

2. **Subject-matter of the processing**
   The subject-matter of the processing is described in the Agreement. The services that process data are set out in Annex 2.

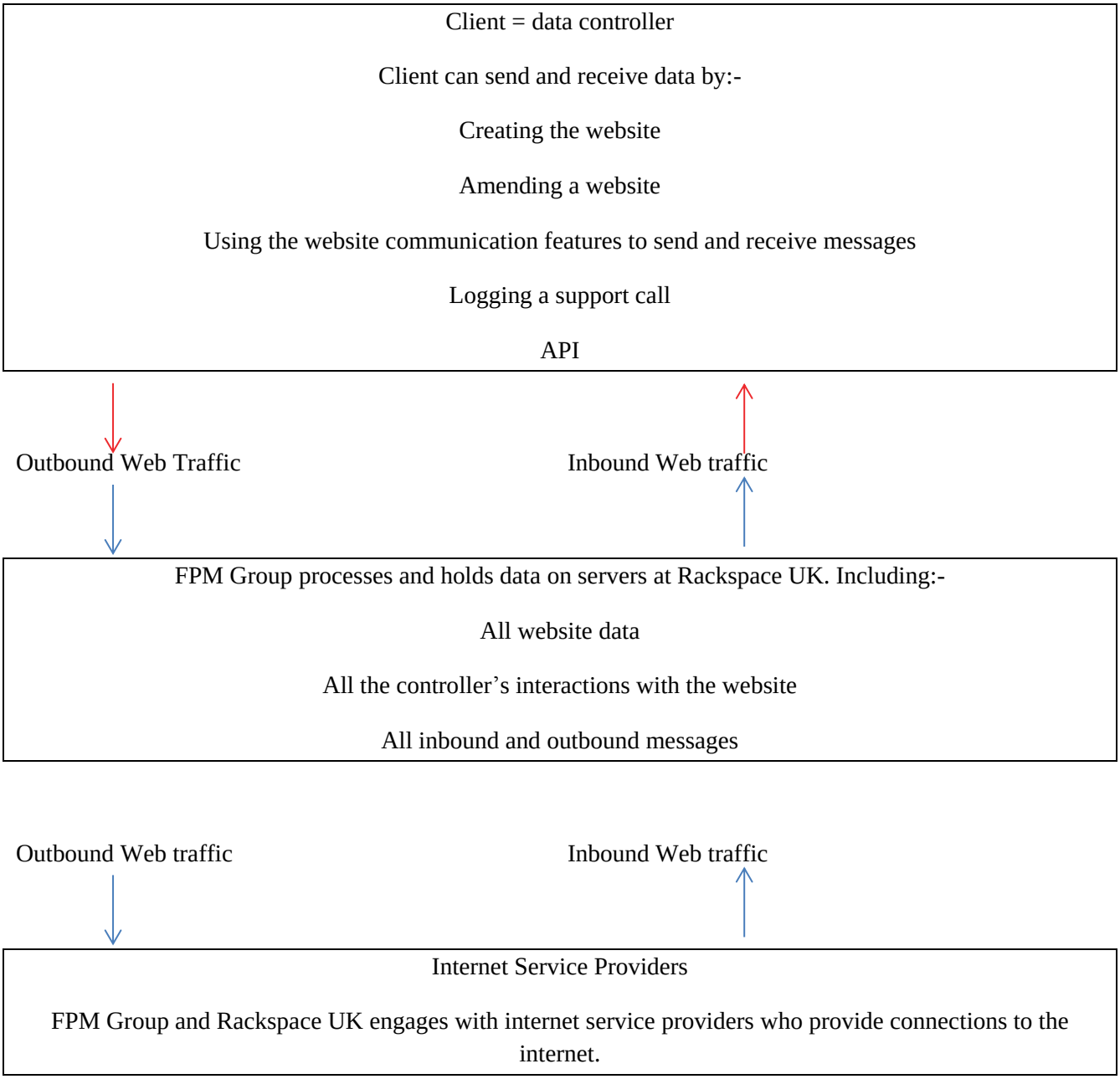
3. **Nature and purpose of the processing**
   The nature and purpose of the processing is described in the Agreement. Essentially the processing enables customers to run and maintain a website that interacts with the Controllers' customers.

4. **Type of personal data**
   The personal data processed by the Processor on behalf of the Controller is determined by the Controller and the Controller's customer who both create the content of the website through its initial setup and continued use and as a messaging platform . All categories of personal data may therefore be contained in the website.

5. **Special categories of data (if appropriate)**
   The personal data processed by the Processor on behalf of the Controller is determined by the Controller and the Controller's customer who both create the content of the website through it's initial setup and continued use and as a messaging platform. Special categories of personal data may therefore be contained in the website.

   A summary of the processing pathway is set out in the diagram overleaf.

FPM Group - My Surgery Website - Data Processing Pathway



Annex 2 to the DPA – Description of the technical and organizational measures implemented by Processor in accordance with applicable data protection law:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement the following technical and organizational measures to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons. In assessing the appropriate level of security the Controller and the Processor took account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

1. Purpose and scope of Document

To detail the technical and organisational measures undertaken by FPM Group (as a Stericycle Group company) to ensure a level of security is provided in its service delivery that is appropriate to the risks represented by the processing and the nature of the personal data being processed, as required by Article 32(1) of the General Data Protection Regulation (GDPR).

Security is a set of preventive measures taken to guard against risk and this document describes those measures.

Failure to comply with the requirements of this procedure may result in investigation and subsequent formal action in line with the Company's Capability and Disciplinary procedures.

This Document should be read in conjunction with Stericycle policies on data protection which can be found on Stericycle's website.

2. Policy Statement

Stericycle protects the company's assets from all threats, whether internal or external, deliberate or accidental.

Stericycle will meet all applicable legal, regulatory and contractual requirements and duties of care.

Stericycle is committed to the key principles of GDPR, namely that personal data are:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected and processed for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the processing;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of the processing (subject to limited exceptions); and
- processed in a manner that ensures the security of the personal data, using appropriate technical or organisational measures.

In particular, it is the policy of Stericycle and FPM Group to ensure that:

- Company and client data are protected against unauthorised access
- Confidentiality of information is assured
- Integrity of information is maintained
- Regulatory, legislative and contractual requirements are met
- All staff are familiar with security measures, procedures and standards i.e. aware and conscious of security, potential risks to security, and the value of information.
- Security standards and procedures are used, including the use of passwords and virus control.
- All parties cooperate with each other to prevent or respond quickly to breaches of security i.e. all breaches of security, actual or suspected are reported, investigated and recorded.
- There is general agreement about what is appropriate in terms of security and who is responsible for their implementation.
- Technical and organisational security measures are clear and explained to all employees.

3. Company Overview

My Surgery Website was founded in 2006 with the aim of providing first class, secure website systems; in 2013 My Surgery Website was acquired by Stericycle and currently forms part of the Stericycle Group.

4. Description of services / products provided / How we work with you

My Surgery Website provides software and services that deliver user editable websites.

5. Accreditations and Memberships

My Surgery Website has been awarded the following BSI ISO accreditations:-

- **ISO 9001: 2017** – This Quality Management certification enables My Surgery Website to demonstrate our commitment to service quality and customer satisfaction. Customers can be assured that we are continually improving our quality management system
- **ISO 14001:2017** – The environmental management certification demonstrates My Surgery Website's commitment to the environment. The standard provides guidelines on how manage the environmental aspects of our business activities more effectively.

6. Responsibilities

Managing Director / VP International

The Managing Director / VP International endorses and actively supports this Document and e security policy. The Managing Director / VP International ensures that appropriate systems security measures are implemented and adhered to and those individual responsibilities are taken seriously at every level of the organisation.

IT Director

The IT Director has direct responsibility for maintaining the Data Security Policy. This includes:

- Developing, implementing and periodically reviewing security policies and procedures
- Providing technical advice and guidance on all aspects of Data Security Policy, including legislation, standards, practice and contractual obligations affecting data security
- Ensuring the administration of security access controls
- Reviewing Data Security at regular intervals to ensure compliance with the data security policy, procedures and best practice
- Assessing new security risks as technology and systems change
- Taking reasonable steps to ensure the reliability of staff members e.g. obtaining references from previous employers
- Ensuring that only authorised individuals have access to services and information
- Approving access to secure or sensitive data
- Requiring third party data processors to contractually comply with the obligations imposed on Stericycle My Surgery Website by the Data Protection Act

Quality and Compliance Director

As part of Stericycle My Surgery Website investment in Data Security and Data protection, we have recently introduced the Quality and Compliance Director role, which amongst others, has the responsibility to ensure:

- Compliance to ISO 9001:2017
- Reviewing additional certifications required for the business
- Providing a framework to conduct Corrective and Preventative action investigations
- Providing guidance and supporting corporate with the implementation of the GDPR framework and other compliance initiatives.

Line managers

- The implementation of the Data Security Policy within their areas of business and for the adherence to the Policy, standards and procedures by their staff
- Ensuring that their staff are familiar with the Data Security policy, and their individual responsibilities
- Ensuring that user access is restricted to what is necessary
- Ensuring that individual userids are suspended when staff members leave
- Ensuring that all staff are broadly familiar with the relevant sections of legislation
- Ensuring that adequate and reliable service restoration plans are available to deal with emergencies, disasters and other incidents to ensure continued availability of IT resources

All employees

- Be knowledgeable and informed about security practices and procedures.
- Be aware of their responsibilities and accountability with regard to security and understand the consequences of abusing their access privileges.
- Use data and IT equipment in a manner that ensures security of the same.
- Comply with all legal and contractual requirements that apply to the data that they have access to.
- Not disclose their passwords to anyone.
- Not use another individual's userid and password.
- Ensure that IT equipment and company premises are protected against physical damage, loss, theft or abuse.
- Ensure that contractual requirements relating to security are complied with.
- Call to the attention of a line manager, or the IT director those whom they feel are violating the Data Security Policy. Every effort will be made to ensure anonymity.
- Report to the systems department, flaws observed in the system or technology.
- Refrain from exploiting any lapses in security.
- Be aware that users with access to electronic mail and the Internet can put a strain on data links by downloading large files or attachments.

My Surgery Website maintains a legal register and, amongst others, recognises and complies with the following legislation:-

- Data Protection Act (1998) to be superseded with the General Data Protection requirement.
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

7. Security Awareness / Training

All My Surgery Website staff receive security training on induction and are contracted to adhere to Stericycle information security policies.

Security refresher training is performed at least annually.

8. Risk & Opportunities

My Surgery Website maintains a risk register which is regularly reviewed by the management team. Any identified risks are mitigated and opportunities for improvement are affected.

9. Sub-Processors / Third Parties

My Surgery Website may directly sub-contract data processing.

Where a third party carries out data processing of personal data for Stericycle My Surgery Website, we will ensure that:

- There is a data processing agreement in place between Stericycle and the relevant 3rd party which details the nature and purpose of processing and meets the requirements for data processing as set out in GDPR.
- That appropriate technical and organisational measures are in place to protect the data.
- That the third party is contractually obliged to process data only under instructions from Stericycle My Surgery Website.
- That the third party is obliged to comply with Stericycle My Surgery Website obligations under GDPR.

Any third parties that My Surgery Website engages with in the performance of our services are subject to due diligence and annual audits including:-

- Restrictions on copying and disclosing data
- Ownership of software and data
- Return or destruction of data
- Measures to protect against viruses /other malicious software

My Surgery Website does not transfer data outside of the EEA. Note however that a customer may choose to send a message outside the EEA.

10. Information Security

Back Ups and Retention Periods

My Surgery Website takes daily back-ups of all client data held on a rolling five-day basis. Backups are stored securely at Rackspace UK.

Business Continuity Plan

SRCL Limited maintains a Business Continuity Plan in accordance our ISO 27001 accreditation requirements. The BCP is reviewed at least annually.

Viruses and other Malicious Software

My Surgery Website runs and keeps up to date anti-virus software.

My Surgery Website runs a monthly patching program in line with industry standards.

11. Resilience

My Surgery Website runs internal monitoring systems to ensure system availability.

My Surgery Website works on multiple redundant systems and partners to ensure system continuity.

My Surgery Website ensures that all system changes are subject to test and review before being made available in the live customer environment.

12. Access Control

System access is controlled by VPN.

Staff access to data is on a need-to-know basis, all staff have unique Userids and passwords, access is controlled by an audited rights system.

My Surgery Website data and systems are hosted at Rackspace UK. Physical Security is strictly controlled in line with Rackspace policies.

13. Data

Data is processed only in accordance with My Surgery Website contractual obligations for the purpose of creating and maintaining website. My Surgery Website does not share this data with any third parties for any reason beyond processing messages unless required to by law.

My Surgery Website does not allow the storage of data on any removable devices.

Personal data processed by My Surgery Website for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

See My Surgery Website's Privacy Policy for further details, which can be found here:

14. Data Security Incidents

SRCL Limited has a fully documented data security incident which includes:-

- Reporting procedures
- Incident reporting portal
- Defined escalation procedures
- Procedures audited in line with ISO 27001 requirements.

15. Confidentiality

My Surgery Website undertakes not to use, nor disclose to any unauthorised person, any confidential information relating to or received from our Clients for any reason unless expressly authorised by the Client, or required by law.

We understand that the use and disclosure of all information about living, identifiable individuals is governed by the Data Protection Act and we will not use or disclose any personal data acquired for any purpose that beyond the purposes of providing and maintaining a website in accordance with the Client's requirements.

We understand that we are required to keep all confidential and personal data securely, and undertake to follow all relevant procedures in doing so.

Legal requirements are reviewed as part of our quality management systems and ISO 9001, ISO 27001 accreditation.