The Bridge
A community magazine for Bridport supported by the Anglican Church

Registered address:
Bridport Team Ministry
84 South Street
Bridport DT6 3NW

Standard Data Processing Addendum

The following terms shall apply to any agreement between a member of The Bridge magazine and another party, in which one party is a Data Controller and the other a Data Processor. **(Contract).**

DEFINITIONS

Contract has the meaning given above.

Data Controller, Data Processor, Data Subject and **Personal Data**: as defined in Data Protection Law;

Data Protection Law: (i) unless and until the GDPR is no longer directly applicable in the UK, the GDPR and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998.

GDPR: General Data Protection Regulation ((EU) 2016/679).

Group: in relation to a company, that company, any subsidiary or holding company from time to time of that company, and any subsidiary from time to time of a holding company of that company.

The Bridge: Any person paid or unpaid working for or on behalf of The Bridge magazine.

Security Incident: as defined in clause 3.1.5.

Terms: the terms of this agreement.

1. Variation

1.1 In consideration of the mutual obligations of the parties, the Contract between them is varied by the incorporation of the Terms set out below.

1.2 Except as varied hereby, the Contract shall continue in full force and effect.

1.3 In the event of any inconsistency or contradiction between these Terms and any terms of the Contract, these Terms shall prevail.

2. DATA PROTECTION

Both parties will comply with all applicable requirements of Data Protection Law.

3. DATA CONTROLLER OBLIGATIONS

3.1 Without prejudice to the generality of clause 2.1, the Data Controller shall:

3.1.1 Be solely responsible for determining the means and the lawful purpose of the processing;

3.1.2 Ensure that it implements and makes available to Data Subjects before collecting Personal Data appropriate policies and notices about the purpose of collecting and processing Personal Data and the Data Subjects' rights in Data Protection Law;

3.1.3 Implement such technical and organisational measures as are appropriate in the circumstances of the Contract for ensuring that the amount of Personal Data collected, the extent of the processing, the storage period and accessibility are no greater than necessary for the specific purpose of processing;

3.1.4 Ensure that it has in place such systems and processes to support its obligations under Article 32-36 of GDPR.

3.2 Data Controller consents to Data Processor using: (i) any member of its staff to assist in the provision of the services under the Contract, including acting as a sub-processor processing of Personal Data on behalf of the Data Controller; ii) other sub-processors to process Personal Data on behalf of the Data Controller to provide the services in the Contract, provided that Data Processor shall remain fully liable for all acts or omissions of any of its sub-processors.

4. PROCESSING OBLIGATIONS

4.1 the Contract sets out the instructions and purposes for processing Personal Data during the term of the Contract and the nature of the Personal Data being processed.

4.2 Without prejudice to the generality of clause 2.1, Data Processor shall, in relation to any Personal Data processed in connection with the performance of its obligations under the Contract:

Purpose limitation

a) Process that Personal Data only on the written instructions of Data Controller as contained in the Contract or as otherwise provided to Data Processor (**Permitted Purpose**).

Security

b) Ensure that it has in place appropriate technical and organisational measures (and shall co-operate with any review or audit thereof by the Data Controller from time to time) to protect against accidental or unlawful destruction, and loss, alteration, unauthorised processing or disclosure of, or access to the Data (**Security Incident**), and confirm that its current measures meet the requirements set out in the attached Security Measures Schedule below.

Confidentiality

c) Ensure that all personnel (including the personnel of any permitted sub-processors) who have access to and/or are authorised to process Personal Data are: (i) bound by a strict obligation to keep the Personal Data confidential; and (ii) process the Data only as necessary for the Permitted Purpose.

International transfers

d) Not transfer any Personal Data outside the European Economic Area unless: (i) Data Processor has first obtained Data Controller’s prior written consent; and (ii) Data Processor takes such measures as are necessary to ensure the transfer is in compliance with Data Protection Law, in particular that there are appropriate safeguards in relation to the transfer and the Data Subject has enforceable rights and effective legal remedies.

Co-operation and Data Subject access

e) Provide Data Controller with all timely and reasonable assistance as it may require to enable Data Controller to: (i) respond to any request from a Data Subject; (ii) comply with its obligations under Data Protection Law with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators. (In the event that any such request, complaint or other correspondence is submitted directly to Data Processor, then Data Processor shall promptly inform Data Controller, providing full details).

Security Incident

f) Notify Data Controller immediately without undue delay on becoming aware of a Security Incident and provide all such timely information and co-operation as Data Controller may require to fulfil its data breach reporting obligations under Data Protection Law within the prescribed timescales. (Data Processor shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Data Controller informed).

Deletion

g) At the written direction of Data Controller, delete or return to Data Controller on termination or expiry of the Contract all Personal Data and copies thereof (including any Personal Data passed to a third party sub-processor), unless required by Data Protection Law or any other applicable law to retain Personal Data, in which case Data Processor shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

Audit

h) Maintain complete and accurate records and information to demonstrate its compliance with this clause and allow for audits by the Customer or the Customer's designated auditor.

4.3 Data Processor must: (i) notify Data Controller of any intended appointment or replacement of a sub-processor, giving the Data Controller an opportunity to object; and (ii) impose by written agreement the same data protection obligations on any sub-processor as apply to Data Processor under these Terms.

5. FURTHER CHANGES

5.1 Where the content of the Contract (including these Terms) is insufficient to meet the requirements under Data Protection Law, the parties will at either party's request conduct negotiations to adapt the Agreement so that its content is in accordance with those requirements. For the avoidance of doubt, neither party shall be entitled to increased or additional payments in respect of these Terms or any subsequent variation to the Contract which is implemented for the purposes of legal compliance.

6. GOVERNING LAW AND JURISDICTION

6.1 These Terms and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with them or their subject matter or formation shall be governed by and interpreted in accordance with the law of England and Wales.

6.2 The parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arises out of, or in connection with, this Variation or its subject matter or formation.

SECURITY MEASURES SCHEDULE

1. Physical and environmental security of all devices, infrastructure and facilities in order to (i) protect information assets from unauthorised physical access, (ii) manage, monitor and log movement of persons into and out of the Data Processor's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

2. Management and staff responsible for the development, implementation and maintenance of information security.

3. Audit and risk assessment procedures for the purposes of periodic review and assessment of data risks, monitoring and maintaining compliance with its own policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

4. Data security controls which include at a minimum, but may not be limited to: i) logical segregation of data; ii) restricted, role-based least privileged access; iv) monitoring; v) encryption of data in transit and at rest.

5. Use of unique IDs and passwords for all users, with periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur.

6. Password controls and processes, including prohibiting authorised users from sharing passwords. Passwords must be encrypted, of sufficient length, complexity and lifespan. Password controls should also be in place to identify and negate brute force access attempts and protect against others gaining use of passwords (e.g. multiple attempt refusal and lockout, forced reset on first use etc).

7. Event and user logging in order to record user access and system activity.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Data Processor’s possession.

9. Patch management and change management procedures.

10. Incident/problem management procedures to allow the Data Processor to investigate, respond to, mitigate and notify events related to the Data Processor’s technology and information assets.

11. Network security controls that protect and monitor network and systems using a multi layered and multiple technology approach including, but not limited to: perimeter protection (firewalls, network segmentation); use of DMZ and other segmented networks where required; intrusion detection and prevention; protection against denial of service and other brute force attacks; endpoint protection systems; vulnerability testing and penetration testing.

12. if and where card payments are being processed, the Data Processor’s systems meet and comply with the Payment Card Industry Data Security Standard.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from emergency situations or disasters.