SOZO's Client Data Processing Agreement

1   Definitions

1.1   "**data controller**" means a data controller or controller (as the case may be) as defined by the Data Protection Legislation (and 'controller' shall be construed accordingly). In this context it refers to SOZO Design's clients.

1.2   "**Data Processing Agreement**" means this agreement.

1.3   "**data processor**" means a data processor or processor (as the case may be) as defined by the Data Protection Legislation (and 'processor' shall be construed accordingly). In this context it refers to SOZO Deign Ltd.

1.4   "**Data Protection Legislation**" means the GDPR for as long as it is directly applicable in the United Kingdom and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the United Kingdom, and then any successor legislation to the GDPR or the Data Protection Act 1998.

1.5   "**Data Subject**" means a data subject as defined by the Data Protection Legislation.

1.1   "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.2   "**Personal Data**" means personal data as defined by the Data Protection Legislation.

2   General obligations

2.1   Both Parties shall comply with all applicable requirements of the Data Protection Legislation. This <u>clause 2.1</u> is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation.

2.2   The Parties acknowledge that for the purposes of the Data Protection Legislation and this Data Processing Agreement, the Data Controller is the data controller and the Data Processor is the data processor. The <u>Schedule</u> to this Data Processing Agreement sets out the scope, nature and purpose of processing by the Data Processor, the duration of the processing and the types of Personal Data and categories of Data Subject.

2.3   Without prejudice to the generality of <u>clause 2.1</u>, the Data Controller will ensure that it has, at all times:

    2.3.1   a valid legal basis under the Data Protection Legislation for the processing of Personal Data under this Data Processing Agreement, including, without limitation, such processing by the Data Processor as instructed or permitted by the Data Controller under clause 3.1.1 and clause 3.2 of this Data Processing Agreement;

    2.3.2   where required by law (for example, as required for the transmission by electronic means of direct marketing communications under the Privacy and Electronic Marketing Communications Regulations 2003), valid consent (under the Data Protection Legislation) for such processing; and

    2.3.3   appropriate notices in place as required by the Data Protection Legislation to enable lawful transfer of Personal Data to the Data Processor for the duration and purposes of this Data Processing Agreement.

3   Data Processing

3.1   Without prejudice to the generality of clause 2.1, the Data Processor shall, in relation to any Personal Data processed in connection with the performance by the Data Processor of its obligations under this Data Processing Agreement:

3.1.1   process Personal Data only on lawful documented instructions from the Data Controller, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by European Union or European Union Member State law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing Personal Data, unless that law prohibits such information on important grounds of public interest;

3.1.2   ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3.1.3   take all reasonable measures required pursuant to Article 32 of the GDPR, appropriate to the level of risk for the data controller's website;

3.1.4   respect the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor;

3.1.5   the data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The data processor shall endeavour to ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. However, due to the nature of the internet the data processor cannot guarantee the security or protection of all data.

3.1.6   taking into account the nature of the processing, assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR;

3.1.7   assist the Data Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to the Data Processor;

3.1.8   at the choice of the Data Controller, delete or return all Personal Data to the Data Controller after the end of the provision of the services relating to processing, and delete existing copies unless European Union or European Union Member State law requires storage of Personal Data; and

3.1.9   make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the GDPR or other European Union or Member State data protection provisions.

3.2   The Data Controller hereby gives its prior consent, documented (written) instructions and written authorisation to the Data Processor to:

3.2.1   engage any of the following processors as sub processors:

- SEO Tools
    - o   Advanced Web Ranking
    - o   Raven Tools
- Email service
    - o   Campaign Monitor
    - o   Mailchimp

- o Sparkpost
- o Mailgun
- ● Hosting
    - o UK Fast
    - o Kinsta
    - o Cloudways
    - o Cloudflare (for clients with DNS on Cloudflare, they can intercept the traffic as some of their services rewrite data on the page, like email obfuscation)
- ● Project Storage
    - o Google
        - ▪ Google Drive stores client documents
        - ▪ Google Calendar may contain client details within event descriptions
    - o Teamwork
    - o Usersnap
    - o Invision
    - o Bitbucket / Gitlab
- ● Internal tools
    - o Slack
    - o Office 365
    - o Sophos
- ● Payment providers
    - o Paypal / Braintree
    - o Stripe
    - o Sagepay
    - o Worldpay
    - o Amazon Pay
    - o Barclay Card
    - o V12
    - o Decopay
    - o Pay365
- ● Server processes
    - o New Relic

3.2.2   engage any other processors as the Data Processor deems fit in the course of its provision of the services under this Data Processing Agreement; and

3.2.3   transfer Personal Data to a third country or an international organisation, provided that the Data Processor satisfies all legal obligations under the Data Protection Legislation and any other applicable laws for doing so, including: (i) ensuring appropriate safeguards are in place in relation to the transfer; (ii) the Data Subject has enforceable rights and legal remedies; (iii) the Data Processor provides an adequate level of protection to any Personal Data transferred; and (iv) the Data Processor complies with reasonable instructions notified to it in advance by the Data Controller with respect to its processing of Personal Data.

3.3   Where the Data Processor engages another processor for carrying out specific processing activities on behalf of the Data Controller, the Data Processor shall ensure that the same data protection obligations as set out in this contract or other legal act between the Data Controller and the Data Processor as referred to in paragraph 3 of Article 28 of the GDPR are imposed on that processor by way of a contract or other legal act under European Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Data Protection Legislation. Where the other processor fails to fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the performance of that other processor's obligations.

3.4   Any contract or other legal act referred to in this clause 3 shall be in writing, including in electronic form.

3.5   The Data Controller agrees that it has considered the Data Processor's obligations under Article 32 of the GDPR and considers that the Data Processor is in compliance with such obligations, in particular the obligation to implement appropriate technical and organisational

measures to ensure a level of security appropriate to the risk of the Data Controller's processing of Personal Data.

3.6   Either party may, at any time on not less than one month's prior written notice, revise clause 3 by replacing it with any applicable Data Controller to Data Processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when replaced by attachment to this Data Processing Agreement).

3.7   The Parties shall make such amendments to this Data Processing Agreement as are required to ensure that this Data Processing Agreement complies with any applicable legislation, including any applicable Data Protection Legislation from time to time.

4   Limitations and exclusion of liability

4.1   The Data Processor excludes any and all liability to the Data Controller to the maximum extent permitted by law.

4.2   In any event, the Data Processor's total aggregate liability to the Data Controller in any given calendar year shall not exceed an amount equal to fifty per cent. (50%) of any fees or charges paid by the Data Controller to the Data Processor for any services provided by the Data Processor to the Data Controller in that calendar year.

5   Costs

5.1   Where the Data Controller exercises any of its rights under this Data Processing Agreement, the Data Processor reserves the right to charge the Data Controller for any costs it reasonably incurs in complying with its corresponding obligations under this Data Processing Agreement.

5.2   The Data Processor shall only exercise its rights under clause 5.1 where it considers it just and equitable to do so.

Schedule

Subject matter of the processing

Any Personal Data processed by the Data Processor on behalf of the Data Controller in the course of the Data Processor providing Services (as defined below) to the Data Controller.

Duration of the processing

The duration of the provision of the Services (as defined below) by the Data Processor to the Data Controller.

Nature of the processing

The provision of website services, website and domain hosting, e-newsletter management services (the "**Services**") by the Data Processor to the Data Controller as agreed between the Parties.

Purpose of the processing

The provision of the Services by the Data Processor to the Client.

Types of personal data processed

- Names

- Titles

- Email addresses

- Company and legal entity names

- Phone numbers

- Addresses

- Server log information (including IP addresses, pages accessed, information requested, the date and time of the request, the source of access to the Data Controller's website, browser version and operating system).

- Online identifiers (including cookies and similar technologies)

- VAT numbers

- Client login details for specific related online services

- Client's customer data, such as contact form data and transactional data

- Any other Personal Data processed by the Data Processor on behalf of the Data Controller from time to time

Categories of data subjects

- Natural person who visit and/or interact with the Data Controller's website (including submitting messages via any contact form on the Data Controller's website from time to time and data relating to transactional orders).

- Natural persons who access the Data Controller's website other than as visitors.

- Natural persons who receive e-newsletters from data controller.

Obligations and rights of the data controller

The obligations and rights of the data controller are set out in clauses 2 and 3 of this Data Processing Agreement.