Data Processing Agreement

This agreement sets out how Online50 treats client data within the scope of Data Protection Legislation. This agreement forms part of the contractual terms between Online50 and our customers.

1. Definitions

1.1. In this document the term "**we**" or "**Online50**" means Online50 Limited (company registered number 3144276) (and the use of the words "**us**", "**our**" and "**ourselves**" will be interpreted accordingly) and the term "**you**" means the party paying for Online50's services as a natural person or a business whether corporate or incorporate as the context requires (and the use of the words "**yours**" and "**yourselves**" will be interpreted accordingly) and use of the terms "**either party**" or "**other party**" will be interpreted as the context requires.

1.2. In this document the following terms shall have the following meanings:

"Data Controller"	as defined in legislation the Data Controller is the person or recognised legal entity that determines the scope and purposes of the data held or deemed to be a Data Controller by virtue of legislation.
"Data Processor"	as defined in legislation a Data Processor is a person or recognised legal entity that performs data processing activities on behalf of the Data Controller.
"Personal Data"	as defined in legislation Personal Data is any information relating to a uniquely identifiable living natural person.
"Personal Data Breach"	as defined in the legislation means 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.
"Data Subject"	as defined in the legislation means the identifiable living natural person to whom personal data relates.
"Standard Trading Data"	means Personal Data obtained and used in the course of a normal trading relationship including but not limited to names and contact details including email addresses.
"Standard Employment Data"	means Personal Data obtained and used in the course of employing, including engaging as a subcontractor or agency worker, a Data Subject including, but not limited to,

	names, gender, date of birth, nationality, national insurance number, passport or other national identification numbers, bank account details and Personal Data regarding their next of kin.
"Standard Marketing Data"	means Personal Data obtained and used in the course of the normal promotion of the goods and services of the Data Controller, including but not limited to names, contact details including email addresses, interests and records of communications.
"Special Purpose Data"	means Personal Data that the Data Controller obtains and uses which is not Standard Trading Data, Standard Employment Data, or Standard Marketing Data.
"Internet Services"	means the Internet Services that Online50 provides to you.
"Development Services"	means the software development service that Online50 provides to you.
"Consultancy Services"	means the consultancy services that Online50 provides to you.
"The Services"	means together the Internet Services Development Services and Consultancy Services.
"Authorised User"	means a natural living person authorised by the Data Controller to process data including Personal Data using the Internet Services.
"The Legislation"	means the General Data Protection Regulations as encapsulated in the Data Protection Act 2018 or any future legislation that is applicable.
"The Regulator"	means the data protection supervisory authority which has jurisdiction over the Data Controller's use of Personal Data.

2. Commencement and Term

2.1. This agreement related to the Data Processing carried out to provide The Services and is deemed to start and end with the obligations of those contracts and to be incorporated into the terms of those contracts. The terms of this Agreement may be varied from time to time to take into account changing legislative requirements or to

incorporate changing operational needs provided the agreement remains compliant with The Legislation and Online50's obligations in respect of the protection of Personal Data are not reduced.

3. Purpose and Scope of Data Processing

3.1. The Data Controller will determine the scope, use and categories of the processing of Personal Data according to their legitimate needs.

3.1.1. The Internet Services have been designed to be used to support the processing of Standard Trading Data, Standard Employment Data and Standard Marketing Data. If the Data Controller intends to use the Internet Services for any Special Purpose Data the Data Controller must advise Online50 in writing of their needs and what Personal Data will be processed to allow Online50 to meet our obligations under The Legislation and this agreement.

3.2. In providing the Internet Services Online50 will at times act as a Data Processor. In particular Online50 is responsible for the systems which allow for the storage and retrieval of information and by which Authorised Users process data including Personal Data.

3.3. Where the Internet Services include application software running on Online50 systems Online50 staff may connect to the disconnected sessions of Authorised Users to terminate running applications for the purposes of management of the Internet Services including allowing systems to reboot. When connecting to disconnected sessions Online50 personnel will be able to view any Personal Data being displayed within the session.

3.4. In the course of providing support for the Internet Services, when requested by an Authorised User Online50 personnel may undertake further actions such as connecting to the Authorised User's session to view what they are doing or to work on a software application that is used to process Personal Data without the Authorised User being connected to the session.

3.5. At the request of Authorised Users Online50 may need to engage the services of a third party in a role that is deemed a Data Processor under The Legislation. Examples of this may be resetting an application password or repairing data where data may need to be sent to a third party or to resolve email transmission problems where email information (including email addresses) may need to be disclosed to the personnel of another email provider. When Online50 needs to pass any data to a third party then Online50 personnel will request for confirmation of this action from the Authorised User by email.

4. Online50 Infrastructure

4.1. Unless explicitly specified all of The Services are provided using Online50's technical infrastructure in the United Kingdom. Online50 shall be free to maintain and enhance our infrastructure to meet the changing requirements of our clients but will not store data outside the United Kingdom without the written consent of the Data Controller.

4.2. Online50's infrastructure is connected to a number of other networks for the purposes of data transmission. All of these connections are physically within the UK but due to the nature of the Internet we cannot guarantee how data is transmitted once it has left our network.

5. Supporting the Exercise of Data Subjects' Rights

5.1. If a Data Subject makes a Data Subject Request to the Data Controller (as defined in the legislation) Online50 will assist the Data Controller in fulfilling that request. Online50 reserve the right to charge for their time spent doing so at the prevailing rates for time used where such actions are outside the scope of normal provision of the Internet Services.

5.2. If a Data Subject makes a Data Subject Request to Online50 that is clearly intended to be made to a particular Data Controller for whom Online50 is a Data Processor then Online50 will refer the Data Subject to the Data Controller as quickly as is reasonably practical.

6. Responding to a Personal Data Breach

6.1. Where Online50 becomes aware of a Personal Data Breach we will notify the Data Controller as soon as possible.

6.2. A Personal Data Breach is a type of Information Security Incident and will be investigated and responded to in accordance with our systems to manage Information Security.

6.2.1. At the conclusion of the investigation we will identify if there are further actions that Online50 should take to improve our Information Security which will be part of our Information Security Incident Report.

6.2.2. Information Security Incident Reports can be provided to affected parties on request but may need to have sensitive information redacted.

6.3. The Data Controller is responsible for notifying The Regulator of a Personal Data Breach where required to do so by the Legislation.

6.3.1. Online50 will provide assistance to the Data Controller in fulfilling their obligation to report the Personal Data Breach. Where such assistance falls outside the normal scope of providing the Services Online50 reserves the right to charge for this assistance at the prevailing rates.

7. Obligations of Online50

7.1. Online50 will –

7.1.1. only process Personal Data as required to provide the Internet Services in accordance with the requirements of the Data Controller or as required to do so by a court of competent jurisdiction;

7.1.2. only disclose information to a third party where necessary to do so to supply the Internet Services or to comply with applicable legislation or after receiving written consent from the Data Controller;

7.1.3. notify the Data Controller as soon as possible if we are ordered to disclose data by a court of competent jurisdiction unless it is lawfully prohibited from doing so;

7.1.4. notify the Data Controller if we are of the opinion that their instruction violates applicable law unless legally exempted or prohibited from doing so;

7.1.5. not engage any sub-processors except after receiving written authority from the Data Controller and only where sub-processors are bound by a Data Processing Agreement which meets the legislative requirements and maintains the same level of obligations in regard to the safe guarding of the Data Controllers data with Online50 liable to the Data Controller for the performance of the sub-processors obligations;

7.1.6. not store information outside the United Kingdom except with the written consent of the Data Controller;

7.1.7. ensure that our personnel are bound by a duty of confidentiality and understand their obligations in this regard;

7.1.8. ensure our personnel receive ongoing training in regard to Information Security and Data Protection;

7.1.9. maintain appropriate Information Security to support the confidentiality of all data including Personal Data.

8. Your Obligations

8.1. All Online50 Customers will –

8.1.1. ensure that Authorised Users understand their individual role in protecting Personal Data;

8.1.2. ensure that Authorised Users do not share their access credentials so that any Personal Data Breach can be properly investigated;

8.1.3. ensure that Authorised Users cooperate with the directions of Online50 personnel to maintain proper operation of the systems and maintenance of Data Protection mechanisms;

8.1.4. ensure that Authorised Users do not attempt to bypass any Information Security mechanisms implemented from time to time by Online50;

8.1.5. fulfil your obligations under The Legislation;

8.2. Where You are the Data Controller you will –

8.2.1. ensure we have appropriate contact details for any Data Protection issues;

8.2.2. communicate any requirements for Special Purpose Data to us;

8.3. Where You are a Data Processor you will –

8.3.1. ensure that the Data Controller has approved Online50's role as Data Processor;

8.3.2. ensure that the Data Controller is satisfied with the terms of this agreement;

8.3.3. facilitate communication between Online50 and the Data Controller to allow Online50 to fulfil our obligations with regard to Data Protection;

9. Information Security

9.1. Online50 are responsible for the Information Security of our systems which covers ensuring the confidentiality, integrity and availability of information stored and processed on our systems in the course of providing The Services. Online50 are not responsible for the information security of other systems, including those used by Authorised Users to access our systems.

9.2. Online50 operate an Information Security regime that is accredited to the International Standard for Information Security. To maintain accreditation Online50 must submit to an independent audit. Details of our accreditation including the scope of our system and audit report can be provided on request.

9.3. Online50 are happy to respond to information requests about our Information Security Regime including requests regarding the details of technical controls we have implemented however we will not supply information which we believe could assist unauthorised or malicious access to or actions against our systems.