Data Processing Addendum

Effective Date: _____

This Data Processing Addendum ("Addendum") forms part of the Agreement between GetOnline Ltd trading as 'AuthSMTP' ("Vendor") acting on its own behalf and as agent for each Vendor Affiliate and _____ ("Company") acting on its own behalf and as agent for each Company Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

1.1. In this Addendum, other than Capitalized defined terms, words and expressions have their normal English meaning as they would be understood by a reasonable person in the context of the Agreement and this Addendum.

> 1.1.1. **Applicable Laws** means (a) European Laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) English Laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws.
>
> 1.1.2. **Company Affiliate** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise
>
> 1.1.3. **Company Group Member** means Company or any Company Affiliate
>
> 1.1.4. **Company Personal Data** means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Agreement
>
> 1.1.5. **Contracted Processor** means Vendor or a Sub-processor
>
> 1.1.6. **Data Protection Laws** means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country
>
> 1.1.7. **EEA** means the European Economic Area
>
> 1.1.8. **EU Data Protection Laws** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR
>
> 1.1.9. **GDPR** means EU General Data Protection Regulation 2016/679
>
> 1.1.10. **Restricted Transfer** means:
>
>> 1.1.10.1. means a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or
>>
>> 1.1.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor.

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 below.

For the avoidance of doubt:

(a) without limitation to the generality of the foregoing, the parties to this Addendum intend that transfers of Personal Data from the UK to the EEA or from the EEA to the UK, following any exit by the UK from the European Union shall be Restricted Transfers for such time and to such extent that such transfers would be prohibited by Data Protection Laws of the UK or EU Data Protection Laws (as the case may be) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12; and

(b) where a transfer of Personal Data is of a type authorised by Data Protection Laws in the exporting country, for example in the case of transfers from within the European Union to a country (such as Switzerland) or scheme (such as the US Privacy Shield) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer;

1.1.11. **Services** means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Agreement

1.1.12. **Standard Contractual Clauses** means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 13.4

1.1.13. **Sub-processor** means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Agreement

1.2. The terms, **Commission**, **Controller**, **Data Subject**, **Member State**, **Personal Data**, **Personal Data Breach**, **Processing** and **Supervisory Authority** shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3. The word **include** shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. This Document

2.1. Where Company has a) determined that they are operating within the scope of GDPR, and b) Vendor is operating as a Processor in respect of Processing of Company Personal Data, Company should sign this Data Processing Addendum and return to dpo@authsmtp.com before processing begins.

2.2 Vendor shall acknowledge receipt by reply to that email within 2 (two) business days.

3. Processing of Company Personal Data

3.1. Vendor shall:

3.1.1. comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

3.1.2. not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2. Each Company Group Member:

3.2.1. instructs Vendor (and authorises Vendor to instruct each Sub-processor) to:

3.2.1.1. Process Company Personal Data; and

3.2.1.2. in particular, transfer Company Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement; and

3.2.2. warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate.

3.3. Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Vendor Personnel

4.1. Vendor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1. 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, Vendor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2. In assessing the appropriate level of security, Vendor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Sub-processing

6.1. Each Company Group Member authorises Vendor to appoint (and permit each Sub-processor appointed in accordance with this section 6 to appoint) Sub-processors in accordance with this section 6 and any restrictions in the Agreement.

6.2. Vendor may continue to use those Sub-processors already engaged by Vendor as at the date of this Addendum, subject to Vendor in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3. Vendor shall give Company prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. If, within 30 (thirty) calendar days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

> 6.3.1. Vendor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and

> 6.3.2. where such a change cannot be made within 30 (thirty) calendar days from Vendor's receipt of Company's notice, notwithstanding anything in the Agreement, Company may by written notice to Vendor with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

6.4. With respect to each Sub-processor, Vendor shall:

> 6.4.1. before the Sub-processor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection for Company Personal Data required by the Agreement

> 6.4.2. ensure that the arrangement between the Vendor the Sub-processor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR

> 6.4.3. if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the Vendor and the Sub-processor, or before the Sub-processor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

> 6.4.4. provide to Company for review such copies of the Contracted Processors' agreements with Sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.5. Vendor shall ensure that each Sub-processor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Company Personal Data carried out by that Sub-processor, as if it were party to this Addendum in place of Vendor.

7. Data Subject Right

7.1. Taking into account the nature of the Processing, Vendor shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2. Vendor shall:

> 7.2.1. promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

> 7.2.2. ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1. Vendor shall notify Company without undue delay upon Vendor or any Sub-processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2. Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

9.1. Vendor shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to the Contracted Processors.

10. Deletion or return of Company Personal Data

10.1 Vendor will periodically delete and procure deletion of any Company Personal Data in order to comply with the Vendor Data Retention Policy.

10.2. Subject to sections 10.3 and 10.4 Vendor shall cease promptly and in any event within 4 (four) calendar months of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of Company Personal Data to comply with the Vendor Data Retention Policy.

10.3. Subject to section 10.4, Company may in its absolute discretion by written notice to Vendor within 30 (thirty) calendar days of the Cessation Date require Vendor to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Vendor shall comply with any such written request within 30 (thirty) calendar days of the Cessation Date.

10.4. Each Contracted Processor may retain Company Personal Data to the extent required by:

  10.4.1. the Applicable Laws and only to the extent and for such period as required by Applicable Laws

  10.4.2. the Vendor Data Retention Policy

10.5. Vendor shall ensure the confidentiality of all such retained Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in requiring its storage and for no other purpose.

10.6. Upon request, Vendor shall provide written certification to Company that it has fully complied with this section 10 within 4 (four) calendar months of the Cessation Date.

11. Audit Rights

11.1. Subject to sections 11.2 to 11.4, Vendor shall make available to each Company Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2. Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3. Company or the relevant Company Affiliate undertaking an audit shall give Vendor reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

11.4 A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

>11.4.1. if the Vendor believes the audit or inspection is not properly requested, scoped or justified;

>>11.4.1.1. if the Vendor declines a request to perform an audit or inspection, the Company is entitled to terminate this DPA and the Agreement.

>>11.4.1.2. if the Standard Contractual Clauses apply, nothing in this Section 11 varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

>11.4.2. to any individual unless he or she produces reasonable evidence of identity and authority;

>11.4.3. outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiliate undertaking an audit has given notice to Vendor that this is the case before attendance outside those hours begins; or

>11.4.4. for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

>>11.4.4.1. Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's compliance with this Addendum; or

>>11.4.4.2. A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor of the audit or inspection.

12. Restricted Transfers

12.1. Subject to section 12.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

12.2. The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

>12.2.1. the data exporter becoming a party to them;

12.2.2. the data importer becoming a party to them; and

12.2.3. commencement of the relevant Restricted Transfer.

12.3. Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4. Vendor warrants and represents that, before the commencement of any Restricted Transfer to a Sub-processor, Vendor's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, as agent for and on behalf of that Sub-processor will have been duly and effectively authorised (or subsequently ratified) by that Sub-processor.

13. General Terms

Governing law and jurisdiction

13.1. Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1. the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2. this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

Order of precedence

13.2. Nothing in this Addendum reduces Vendor's obligations under the Agreement in relation to the protection of Personal Data or permits Vendor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3. Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4. Company may:

13.4.1. by at least 30 (thirty) calendar days written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2. propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5. If Company gives notice under section 13.4.1:

> 13.5.1. Vendor and shall promptly co-operate (and ensure that any affected Sub-processors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and

> 13.5.2. Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 and/or 13.5.1.

13.6. If Company gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

13.7. Neither Company nor Vendor shall require the consent or approval of any Company Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum 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, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

Company

Signature   _____

Name   _____

Title   _____

Date Signed   _____

Vendor

Signature   _____

Name   _____

Title   _____

Date Signed   _____

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Agreement and this Addendum.

The nature and purpose of the Processing of Company Personal Data

The Vendor provides a service whose primary purpose is to relay email messages via the SMTP protocol from the Company to the recipients named in the message.

Any Personal Data collected, stored and processed by the Vendor is only done so to carry out the Service effectively, provide supporting functions or support the Company in relation to the Service.

The types of Company Personal Data to be Processed

- **Message data** including (but not limited to):
  - Sender IP
  - From Address
  - Recipient Addresses
  - Message Subject

- The **Message Body** and any Personal Information within the message body and any attachments will be temporarily stored, virus scanned and transmitted across the Vendor network - once the message has been delivered or returned to the sender, the message body will be discarded.

- **Message delivery data** including (but not limited to) recipient address and delivery response.

- **Personal Information** collected, transmitted or stored by the Vendor via means other than those listed above, but in relation to providing the service. This includes but is not limited to spam complaints, diagnostic messages and quarantined messages.

The Personal Information transferred to the Vendor network is entirely controlled by the Company, therefore the Company is responsible for ensuring that any data transferred is permitted under the Agreement and the Applicable Laws.

The Company agrees not to transfer any Sensitive Personal Information or Special Category Personal Information to the Vendor network at any time.

The categories of Data Subject to whom the Company Personal Data relates

The applicable data subjects are any natural persons named as a sender (From) or recipient (to, cc, bcc) of a message sent via the Vendor network.

Any natural persons named within the body of any message sent via the Vendor network may also be considered a data subject within the scope of GDPR.

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Agreement and this Addendum.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: _____

Address: _____

                         _____

                         _____

Tel.:   _____
Email: _____

Other information needed to identify the organisation:

                         _____

(the data exporter)

And

Name of the data importing organisation: GetOnline Ltd

Address: Unit 12D, Adlington Park
                  Macclesfield
                  Cheshire, SK10 4PZ
                  United Kingdom

Email: dpo@authsmtp.com

Other information needed to identify the organisation:

AuthSMTP

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1 - Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the Sub-processor' means any processor engaged by the data importer or by any other Sub-processor of the data importer who agrees to receive from the data importer or from any other Sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data

exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the Sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the Sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any Sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 - Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the Sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any Sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 - Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or Sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his Sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a Sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the Sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the Sub-processor agrees that the data subject may issue a claim against the data Sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the Sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 - Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any Sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any Sub-processor preventing the conduct of an audit of the data importer, or any Sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 - Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on the data importer under the Clauses. Where the Sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the Sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the Sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the Sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the Sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):   _____

Position: _____

Address: _____

                                _____

                                _____

Other information necessary in order for the contract to be binding (if any):

_____

Signature:

_____

On behalf of the data importer:

Name (written out in full):   Mr David Priest

Position: Director

Address: Unit 12D, Adlington Park
                                Macclesfield
                                Cheshire, SK10 4PZ
                                United Kingdom

Other information necessary in order for the contract to be binding (if any):

_____

Signature:

_____

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is:

_____

_____

_____

_____

Data importer

The data importer is:

> GetOnline Ltd (trading as AuthSMTP)
> Unit 12d, Adlington Park
> Macclesfield
> Cheshire, SK10 4PZ
> United Kingdom

Data subjects

The personal data transferred concern the following categories of data subjects:

(For example: employees, customers, patients, pupils, elected officials, system users)

The applicable data subjects are any natural persons named as a sender (From) or recipient (to, cc, bcc) of a message sent via the Vendor network.

Any natural persons named within the body of any message sent via the Vendor network may also be considered a data subject within the scope of GDPR.

Categories of data

The personal data transferred concern the following categories of data:

- **Message data** including (but not limited to):
  - Sender IP
  - From Address
  - Recipient Addresses
  - Message Subject

- The **Message Body** and any Personal Information within the message body and any attachments will be temporarily stored, virus scanned and transmitted across the Vendor network - once the message has been delivered or returned to the sender, the message body will be discarded.

- **Message delivery data** including (but not limited to) recipient address and delivery response.

- **Personal Information** collected, transmitted or stored by the Vendor via means other than those listed above, but in relation to providing the service. This includes but is not limited to spam complaints, diagnostic messages and quarantined messages.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

The Company agrees not to transfer any Sensitive Personal Information or Special Category Personal Information to the Vendor network at any time.

The Personal Information transferred to the Vendor network is entirely controlled by the Company, therefore the Company is responsible for ensuring that any data transferred is permitted under the Agreement and the Applicable Laws.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

The Vendor provides a service whose primary purpose is to relay email messages via the SMTP protocol from the Company to the recipients named in the message.

Any Personal Data collected, stored and processed by the Vendor is only done so to carry out the Service effectively, provide supporting functions or support the Company in relation to the Service.

DATA EXPORTER

Name: _____

Authorised Signature: _____

DATA IMPORTER

Name: Mr David Priest (Director)

Authorised Signature: _____

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. Physical Security

    1.1 All physical servers and network devices that store Personal Information are physically hosted in contracted PCI compliant data centers.
    1.2 Data centers incorporate standard security features including physical access controls, CCTV, manned security and per cabinet security measures.

2. Network Security

    2.1 Network segmentation and host based firewalls to limit network access to Personal Information
    2.2 Internal access level controls to limit access to Personal Information
    2.3 Periodic scanning for network facing service vulnerabilities and unauthorized devices / connections
    2.4 Procedural management of physical network updates and changes
    2.5 Procedural review and application of firmware and device software updates carried out on a regular basis

3. Operating System & Hosting Security

    3.1 Operating system hardening and access controls including (but not limited to):

        3.1.1 Removal of default system accounts and passwords
        3.1.2 Services / ports restricted to only those required for the system's network role
        3.1.3 User based access with multiple layers of authentication

    3.2 Automated scanning for operating system vulnerabilities and updates
    3.3 Procedural application and rollback of operating system updates
    3.4 Internal systems to monitor for emerging system threats and application of fixes
    3.5 System activity logging and monitoring
    3.6 Intrusion detection systems

4. Application Security

    4.1 Observation of current secure programming standards and application security
    4.2 Procedural application of application upgrades, changes or reconfigurations
    4.3 Service and application vulnerability scanning
    4.4 Application level access controls and user access management

5. Employee Security & Access Control

    5.1 Employee access to network, systems and applications is restricted on a per-role basis
    5.2 All access and activity is logged on a per-employee basis
    5.3 Employee training and documentation on physical / network security, Personal Information handling and incident reporting procedures
    5.4 Employee network access computers and devices are provided by the company and subject to:

        5.4.1 - Current operating systems and applications
        5.4.2 - Full disk encryption
        5.4.3 - Password policies
        5.4.4 - Anti-virus where applicable
        5.4.5 - Automated software updates
        5.4.6 - Network access using secure protocols