Cover Note – Guidance for the Data Exporter

This Data Processing Addendum (DPA), together with the Standard Contractual Clauses (SCCs) and, where relevant, the UK Addendum, is provided to help you comply with GDPR and UK GDPR when using our services.

Most of the document is pre-completed by us (the Vendor).

To finalise the agreement, you as the Data Exporter need to:

- Complete the effective date on page 1
- Enter your business name on page 1
- Review Data Processing Agreement on page 2 -> 8
- Complete the DPA signature block on page 8
- Review Annex A on page 9; confirm no special category data will be sent
- Review Annex B on page 10
- Review Annex C on page 11
- Complete SCC Clauses 17/18 Member State on page 20
- Complete and sign '**Data exporter'** details of SCC Annex I.A on page 21
- Complete competent supervisory authority of SCC Annex I.C on page 22
- Complete UK Addendum Tables 1 on page 25 (if UK transfers apply)

IMPORTANT: We are unable to offer customised versions of this DPA.

If you have any questions please contact us via email using dpo@authsmtp.com.

Data Processing Addendum

Effective Date: _____

This Data Processing Agreement ("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 (a) EU General Data Protection Regulation 2016/679 with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU GDPR; and (b) UK General Data Protection Regulation with respect to any Company Personal Data in respect of which any Company Group Member is subject to UK GDPR.

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 "Module 2: Transfer Controller to Processor" of the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 as set out in full in Schedule 1 to this Agreement, including Annexes I–III thereto, amended as indicated (in square brackets and italics) in that Schedule and under section 13.4.

1.1.13. **UK Addendum** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018, as set out in full in Schedule 2 to this Agreement, including the mandatory tables and options thereto, amended as indicated (in square brackets and italics) in that Schedule and under section 13.4.

1.1.14. **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 A 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 A by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex A (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.

6.1.1 For the avoidance of doubt, where the Standard Contractual Clauses apply, Clause 9 of the Standard Contractual Clauses shall also govern the use of Sub-processors, and this Section 6 shall be read consistently with that Clause.

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 Rights

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 endeavors 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 and/or the UK Addendum (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 cooperate) 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 Mr D.M Priest

Title Managing Director

Date Signed _____

ANNEX A: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex A 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 B: Details of Technical and Organisational Security Measures

This Annex B includes certain details of the Technical and Organisational Security Measures as required by Article 28(3) GDPR.

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

Annex C: Sub-Processors

In accordance with Section 6 of this Agreement, the Controller authorises the engagement of the following Sub-processors. Each Sub-Processor may process Personal Data only for the purposes of providing the services described below and in accordance with this Agreement.

Name of Sub-processor	Registered Address	Service Provided	Processing Location(s)	Categories of Data Processed
Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA	Content delivery network, DDoS protection, traffic routing	Global (incl. US, EU, UK data centres)	IP addresses, traffic metadata, application data transiting the service
PayPal (Europe) S.à r.l. et Cie, S.C.A.	22–24 Boulevard Royal, L-2449 Luxembourg	Payment processing (Website Payments Pro)	EU, US (PayPal global infrastructure)	Customer identification data, payment details, transaction data
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Ireland	Web analytics (Google Analytics)	EU, US (Google global infrastructure)	IP addresses, online identifiers, browsing behavior, traffic data

Schedule 1: STANDARD CONTRACTUAL CLAUSES

Disclaimer: This document was generated based on the text available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012 and is provided for convenience purposes. It should not be considered an authoritative text or legal guidance.

CONTROLLER TO PROCESSOR

SECTION I

CLAUSE 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

CLAUSE 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

CLAUSE 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/ or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

CLAUSE 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

CLAUSE 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

CLAUSE 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

CLAUSE 7 – OPTIONAL

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these
(c) Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in
(d) Annex I.A.

(e) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

CLAUSE 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights.

On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time,

the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

CLAUSE 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes

to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

CLAUSE 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects 'requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

CLAUSE 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

CLAUSE 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

CLAUSE 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(c) [Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(d) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

CLAUSE 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of

(b) the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(c) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(d) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(e) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(f) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(g) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

CLAUSE 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

CLAUSE 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(a) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(b) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

CLAUSE 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (specify Member State).

CLAUSE 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

1 - STANDARD CONTRACTUAL CLAUSES - ANNEX I

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor):

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: GetOnline Ltd trading as AuthSMTP

Address: 7 Forbes Park, Bramhall, Stockport, SK7 2RE

Contact person's name, position and contact details:

Mr David Priest
Managing Director

dpo@authsmtp.com

Activities relevant to the data transferred under these Clauses:

The data importer processes personal data as necessary to perform the services described in **Annex A (Details of Processing of Company Personal Data) of the Data Processing Agreement**, which is incorporated by reference into these Clauses.

Signature and date: _____

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

The data importer processes personal data as necessary to perform the services described in **Annex A (Details of Processing of Company Personal Data) of the Data Processing Agreement**, which is incorporated by reference into these Clauses.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be:

Organisation Name: _____

GUIDANCE NOTES

(a) where the data exporter is established in the European Union, the supervisory authority of the Member State in which the data exporter is established;

(b) where the data exporter is established in the United Kingdom, the Information Commissioner's Office (ICO); and

(c) where the data exporter is established outside the European Union and the United Kingdom, the supervisory authority shall be the supervisory authority of the EU Member State in which the data importer has appointed its EU representative (or, if no representative is appointed, the Data Protection Commission of Ireland).

Schedule 1 - STANDARD CONTRACTUAL CLAUSES - ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The technical and organisational security measures implemented by the data importer are described in Annex B (Details of Technical and Organisational Security Measures) of the Data Processing Agreement, which is incorporated by reference into these Clauses.

Schedule 1 - STANDARD CONTRACTUAL CLAUSES - ANNEX III

LIST OF SUB-PROCESSORS

The authorised Sub-Processors are set out in Annex C (Sub-Processors) of the Data Processing Agreement, as updated from time to time in accordance with Section 6 of that Agreement.

Schedule 2: Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, IN FORCE 21 MARCH 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

TABLE 1: PARTIES

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name: Main address Official registration number (if any)	Full legal name: GetOnline Ltd Trading name: AuthSMTP Main address: 7 Forbes Park Bramhall Stockport SK7 2RE Official registration number: 03151203
Key Contact	Full Name: Job Title: Contact Email:	Full Name: David Priest Job Title: Managing Director Contact Email: dpo@authsmtp.com
Signature (if required for the purposes of Section 2)		

TABLE 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: 4 June 2021 Reference: Commission Implementing Decision (EU) 2021/914 of 4 June 2021 Other identifier: Module 2: Controller → Processor All clauses of Module 2, as included in Schedule 1 of this Agreement.

TABLE 3: APPENDIX INFORMATION

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See SCC Annex I (Schedule 1 to this Agreement)
Annex 1B: Description of Transfer: See SCC Annex I (Schedule 1 to this Agreement)
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See SCC Annex II (Schedule 1 to this Agreement)
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex C (Sub-Processors) of the DPA, as referenced in SCC Annex III.

TABLE 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES

Ending this Addend the Approved Adden changes	Which Parties may end this Addendum as set out in Section 19: ~~Importer~~ Exporter ~~neither Party~~

Part 2: Mandatory Clauses

ENTERING INTO THIS ADDENDUM

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

INTERPRETATION OF THIS ADDENDUM

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as s Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which Laws when you are making a Restricted Transfer relying on standard data protection c GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or el from time to time in the UK, including the UK GDPR and the Data Protection Act 2018
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties 'obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

HIERARCHY

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

INCORPORATION OF AND CHANGES TO THE EU SCCS

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:
    "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

    "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

    "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)"; j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.";

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

AMENDMENTS TO THIS ADDENDUM

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1 Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, those Mandatory Clauses.