

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: Research Research Limited

Address: Unit 111, 1340146 Curtain Road

London EC2A 3AR, ENGLAND

Tel.: +44 20 7216 6500; fax: +44 20 7216 6501; e-mail: WOCB@RESEARCHRESEARCH.COM

Other information needed to identify the organisation

NONE

(the **data exporter**)

And

Name of the **data importing** organisation: SendGrid, Inc.

Address:

1451 Larimer Street

Denver CO 80202

United States of America Tel.: 303-552-0653; fax: 720-479-8678; e-mail: legal@sendgrid.com

Other information needed to identify the organisation

.....

(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.

1. Definitions

For the purposes of the Clauses:

'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;

'the data exporter' means the controller who transfers the personal data;

'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;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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;

'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;

'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.

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.

3. Third-party beneficiary clause

3.1 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.

3.2 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.

3.3 The data subject can enforce against the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

- 3.4 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.

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 subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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).

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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

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

6. Liability

- 6.1 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 subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
- 6.2 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 subprocessor 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 or by operation of law, in which case the data subject can enforce its rights against such entity.
- 6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
- 6.4 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

- 7.1 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.

- 7.2 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.

8. Cooperation with supervisory authorities

- 8.1 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.
- 8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, 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.

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

9. Governing Law

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

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.

11. Subprocessing

- 11.1 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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

- 11.2 The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

- 11.3 The provisions relating to data protection aspects for subprocessing 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.

- 11.4 The data exporter shall keep a list of subprocessing 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.

12. Obligation after the termination of personal data processing services

- 12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor 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.

12.2 The data importer and the subprocessor 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.

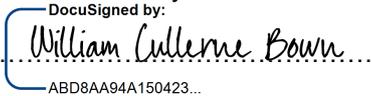
On behalf of the data exporter:

Name (written out in full): William Cullerne Bown

Position: EXECUTIVE CHAIRMAN

Address: UNIT 111, 134-146 CURTAIN ROAD, LONDON EC2A 3AR, ENGLAND

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

Signature.....ABD8AA94A150423...

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Michael Tognetti for SendGrid, Inc.

Position: SVP and General Counsel

Address: 1451 Larimer St., Denver, CO 80202 USA

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

Signature.....

(stamp of organisation)

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 (please specify briefly activities relevant to the transfer):

a UK company providing cloud services including file storage, collaboration, email notification,

and information to customers around the world

Data importer

The data importer is a US headquartered provider of cloud-based transactional and marketing email delivery, management and analytics services.

Data subjects

The personal data transferred concern any data subject who is a sender, recipient or copy recipient of an email which the data exporter instructs the data importer to deliver and manage. Data subjects may also include individuals who are mentioned within the body of emails sent by the data exporter using the data importer's services.

Categories of data

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

- Sender, recipient and copy recipient identification information (first and last name), contact information (address, telephone number (fixed and mobile), e-mail address, fax number), employment information (job title); and
- Any other personal data that the data exporter chooses to include within the body of an e-mail that it sends using the data importer's services.

The personal data transferred to the data importer for processing is determined and controlled by the data exporter in its sole discretion. As such, the data importer has no control over the volume and sensitivity of personal data processed through its service by the data exporter.

Special categories of data (if appropriate)

The data importer does not intentionally collect or process any special categories of data in the provision of its service.

However, special categories of data may from time to time be inadvertently processed by the data importer where the data exporter chooses to include this type of data within the communications it sends through the data importer's service.

As such, the data exporter is solely responsible for ensuring the legality of any special categories of data it may choose to process through the data importer's service.

Processing operations

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

- Personal data will be transferred from the data exporter to the data importer for the data importer to perform transactional and marketing email delivery and management services on behalf of the data importer.
- These services will consist primarily of sending and delivering e-mail communications on behalf of the data exporter, to such recipients and containing such content as are determined by the data exporter in its sole discretion. The data importer will also provide the data exporter with analytic reports concerning the e-mail communications it sends on the data exporter's behalf.
- Full details about the data importer's service can be found at <https://sendgrid.com/email-solutions>

DATA EXPORTER

Name: William Cullerne Bown

Authorised Signature
DocuSigned by:
William Cullerne Bown
ABD8AA94A150423...

DATA IMPORTER

Name:

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) (or document/legislation attached):

Information Security Program

SendGrid maintains an information security program focused on the security and integrity of Customer Data. SendGrid's information security program includes administrative, technical, and operational controls appropriate for the size of its business and the types of information it processes.

Physical Protection

SendGrid maintains physical and environmental controls on its corporate office spaces, including restricted access to the facility and video monitoring of ingress points.

Where SendGrid utilizes third-party hosting centers, SendGrid reviews and evaluates the physical and environmental controls of the facilities in order to meet the control requirements of the types of information it processes, including temperature and humidity regulation and monitoring, fire protection, physical and logical access controls in accordance with least privilege, video monitoring at ingress/egress points, emergency power, and redundant data circuits.

Physical access to corporate offices or data processing centers is revoked upon employee separation, and is reviewed on a semi-annual basis.

Network Security

SendGrid has implemented industry standard security controls to protect customer data from loss or unauthorized disclosure. SendGrid implements network boundary protection mechanisms to its production systems.

Access to production systems which contain customer information requires multi-factor authentication through a VPN connection.

SendGrid implements industry best-practice DDOS protection mechanisms.

Monitoring

SendGrid monitors its systems by logging security-related events, alerting on suspicious activity, and conducting further analysis on suspicious activity.

Logical Access Control

Access to customer data is restricted based on the least privilege principle; access is issued via a documented access authorization process. Access is revoked as soon as practicable of personnel separation.

Personnel Security

SendGrid ensures it hires skilled professionals who successfully complete a background screening and sign a confidentiality agreement, acceptable use of information systems agreement, and code of conduct. Personnel transfers result in access management changes based on least privilege and role.

Incident Management

SendGrid maintains an information security incident management program that provides timely response and notification as appropriate to security incidents in order to protect customer information.

Audit and Compliance

SendGrid analyzes and reviews the security controls put in place by its third party providers and sub-processors to ensure that they have implemented adequate security controls to protect customer data that may be stored or accessed by its third party providers.

Data Deletion

Customer Data will generally be deleted within 60 days, but in no event later than 365 days. This is subject to applicable legal requirements.

Appendix 3 to the Standard Contractual Clauses

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

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's confidential information as that term is defined in the data importer's terms of service found at <http://sendgrid.com/tos> (or another written and signed agreement between data importer and data exporter) and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the data importer's terms of service found at <http://sendgrid.com/tos> (or another written and signed agreement between data importer and data exporter). This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").
4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. The parties acknowledge that data importer uses internal and external auditors to assess the adequacy of its data processing, including the security of the systems and premises used by data importer to provide data processing services.
2. The parties further acknowledge that these audits:
 - (a) are performed at least once each year;
 - (b) shall be comprehensively assessed against SOC standards;

- (c) are conducted by auditors selected by the data importer, but otherwise conducted with all due and necessary independence and professionalism; and
 - (d) are fully documented in an audit report that affirms the data importer's controls meet the standards against which they are assessed ("**Report**");
3. At data exporter's written request, data importer will (on a confidential basis) provide data exporter with a summary of the Report so that data exporter can verify data importer's compliance with the audit standards against which it has been assessed and these Clauses.
 4. Data importer shall further provide detailed written responses (on a confidential basis) to all reasonable requests for information made by data exporter, including responses to information security and audit questionnaires, that data exporter considers necessary to confirm data importer's compliance with these Clauses.
 5. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in this Appendix.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in data importer's terms of service found at <http://sendgrid.com/tos> or any signed written agreement between the parties. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out below, which collectively ensure that the onward subprocessor will provide adequate protection for the personal data that it processes:
 - (a) any onward subprocessor must agree in writing:
 - (i) to only process personal data in the European Economic Area or another country that the European Commission has formally declared to have an "adequate" level of protection in accordance with the requirements of EU Directive 95/46/EC; or
 - (ii) to process personal data on terms equivalent to these Clauses or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities and whose scope extends to transfers of personal data from the territories in which the data exporter is established; and
 - (b) data importer must restrict the onward subprocessor's access to personal data only to what is strictly necessary to perform its subcontracted data processing services to data importer (which shall be consistent with the instructions issued to data importer by data exporter) and data importer will prohibit the onward subprocessor from processing the personal data for any other purpose.
3. Data importer shall maintain a list of all onward subprocessors it has engaged to process personal data pursuant to these Clauses. At present, the subprocessors are Amazon Web Services, Inc. and Softlayer Technologies, Inc.