GDPR Terms: Mandatory Data Protection Agreement for Vox Media's Vendors/Suppliers

Vox Media, Inc., a corporation organized under the laws of Delaware, with offices at 1201 Connecticut Ave. NW, 11th Floor, Washington, DC 20036 ("Vox") and the Vendor Company to whom this Data Protection Annex has been sent, or to which this Data Protection Annex otherwise applies,(the "Processor") have one or more written agreements (collectively, "the Agreements") pursuant to which the Processor provides services to Vox (collectively, the "Services") that may entail the Processing of Personal Data (as defined below).

The European General Data Protection Regulation (GDPR) imposes specific obligations on Vox and other companies (controllers) with regard to their vendor relationships. The GDPR requires companies to conduct appropriate due diligence on processors and to have contracts containing specific provisions relating to data protection.

Each of the Agreements contains provisions requiring each party to comply with all applicable laws. This Data Protection Annex ("Annex Z") documents the data protection requirements imposed upon the parties by the GDPR. This Annex Z is hereby incorporated by reference into each Agreement in order to demonstrate the parties' compliance with the GDPR.

1.   For purposes of this Annex, "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation, together with any addition implementing legislation, rules or regulations that are issued by applicable supervisory authorities. Words and phrases in this Annex shall, to the greatest extent possible, have the meanings given to them in Article 4 of the GDPR. In particular:

   (a) "Personal Data" has the meaning to give it in Article 4(1) of the GDPR: "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," but only to the extent such personal data pertain residents of the European Economic Area (EEA) or are otherwise subject to the GDPR.
   (b) "Personal Data Breach" has the meaning given to it in Article 4(12) of the GDPR: "[any] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."
   (c) "Processing" has the meaning given to it in Article 4(2) of the GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"
   (d) "Subprocessor" means any processor as defined in Article 4(8) of the GDPR: "[any] natural or legal person, public authority, agency or other body which processes personal data" on behalf of the Processor (including any affiliate of the Processor).
   (e) "Transfer" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Subprocessor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

2. In accordance with GDPR Article 28(1), Processor represents that it has implemented appropriate technical and organisational measures in such a manner that its Processing of Personal Data will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.

3. In accordance with GDPR Article 28(2), the Processor shall not engage any Subprocessor without prior specific or general written authorisation of Vox. In the case of general written authorisation, the Processor shall inform Vox of any intended changes concerning the addition or replacement of other Subprocessors and give Vox the opportunity to object to such changes. The Processor shall also comply with the requirements for subprocessing as set forth in Article 28(4), namely that the data protection obligations set forth herein (and as may otherwise be agreed by the Processor in the Agreements) such be imposed upon the Subprocessor, so that the Processor's contract with the Subprocessor contains sufficient guarantees that the Processing will meet the requirements of the GDPR.

4. In accordance with GDPR Article 28(3), the following terms are incorporated by reference into the Agreements:

(a) The Processor shall only process the Personal Data only (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from Vox, including with regard to any Transfers, and (iii) as needed to comply with law (in which case, the Processor shall provide prior notice to Vox of such legal requirement, unless that law prohibits this disclosure);

(b) Processor 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) Processor shall take all security measures required by GDPR Article 32, namely:

  i. 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, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
  ii. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
  iii. The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process them except on instructions from Vox, unless he or she is required to do so by EEA Member State law.

(d) Taking into account the nature of the processing, Processor shall reasonably assist Vox by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Vox's obligation to respond to requests for exercising the data subject's rights;

(e) Taking into account the nature of processing and the information available to the Processor, Processor shall comply with (and shall reasonably assist Vox to comply with) the obligations regarding Personal Data Breaches (as set forth in GDPR Articles 33 and 34), data protection impact assessments (as set forth in GDPR Article 35), and prior consultation (as set forth in GDPR Article 36);

(f)   At Vox's discretion, the Processor shall delete or return all the Personal Data to Vox after the end of the provision of services relating to Processing, and delete existing copies unless applicable EEA member state law requires storage of the Personal Data;

(g) The Processor shall provide Vox with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by Vox or another auditor mandated by Vox; and

 (h) The Processor shall immediately inform Vox if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

5.   The Processor shall not Transfer any Personal Data (and shall not permit its Subprocessors to Transfer any Personal Data) without the prior consent of Vox. The Processor understands that Vox must approve and document that adequate protection for the Personal Data will exist after the Transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the Transfer exists (e.g., the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks).

6.   The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will notify Vox without undue delay in the event of any Personal Data Breach.

7.   The Processor shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for Vox) Processor shall make them available to Vox upon request.

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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

Name of the data exporting organisation:..

Address:...

Tel.: ....; fax: ....; e-mail: ....

Other information needed to identify the organisation:

………………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation: ....

Address:...

Tel.:...; fax:...............................; e-mail:.................................

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.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

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

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

(d)   *'the 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;

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

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

Clause 2

Details of the transfer

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

---

[1]

Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

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

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the 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.

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other

unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

(g)   to forward any notification received from the data importer or any 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).

Clause 5

Obligations of the data importer[2]

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;

---

[2]

Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(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.

Clause 6

Liability

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

2.   If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his 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 of by operation of law, in which case the data subject can enforce its rights against such entity.

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

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the 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.

Clause 7

Mediation and jurisdiction

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

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

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

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

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).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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[3]. 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.

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.

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, namely …………………………………… ……………………………………………………………………………………………

---

[3]   This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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.

Clause 12

Obligation after the termination of personal data processing services

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

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

Signature……………………………………………

(stamp of organisation)

On behalf of the data importer:
Name (written out in full):   …………………………………………………………………
Position: …………………………………………………………………………………
Address: …………………………………………………………………………………

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 your activities relevant to the transfer):
…………………………………………………………………………………………………
……………………………………………………………………………………

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
…………………………………………………………………………………………………
……………………………………………………………………………………

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
…………………………………………………………………………………………………
……………………………………………………………………………………

Categories of data
The personal data transferred concern the following categories of data (please specify):
…………………………………………………………………………………………………
……………………………………………………………………………………

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
…………………………………………………………………………………………………
……………………………………………………………………………………

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
…………………………………………………………………………………………………
……………………………………………………………………………………

DATA EXPORTER

Name:………………………………

Authorised Signature ……………………

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):
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………………………………………………
……………………………………………………………

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a)   the data exporter promptly notifying the data importer of a claim; and

(b)   the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim[4].

---

[4]   Paragraph on liabilities is optional.