DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") is made on [insert effective date] ("**Effective Date**")

BETWEEN

Doctors Without Borders/Médecins sans frontières Canada a non-for-profit corporation with its principal place of business at 551 Adelaide Street West, Toronto, ON, M5V 0N8, Canada ("**MSF**");

and

[Name of supplier] a company with its principal place of business at [address of supplier] ("**Supplier**").

RECITALS

(A) Supplier provides certain professional services ("**Services**") to MSF under the [Name of Main Agreement] (the "**Main Agreement**"). In connection with the Services, the Parties anticipate that Supplier will process Personal Data on behalf of MSF, the data controller for such Personal Data;

(B) To the extent that the provision of such Services involves the processing of Personal Data, the Parties have agreed to enter into this Addendum for the purpose of ensuring compliance with the applicable Data Protection Laws (as defined below).

THEREFORE, the parties have agreed as follows:

1. DEFINITIONS

1.1 "**(Sub)process/(sub)processing**", "**data subject**", "**data processor**, "**data controller**", "**personal data**", "**data breach**", "**data protection impact assessment**", " **technical and organisational measures**", "**recipient**" shall have the meaning ascribed to them in the Data Protection Laws;

1.2 "**Authorized Subprocessors**" means (a) those Subprocessors set out in Annex 3 (*Authorised Subprocessors*); and (b) any additional Subprocessors consented to in writing by MSF in accordance with section 5.1;

1.3 "**Data Protection Laws**" means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), as well as all laws implementing or supplementing the same, guidance related thereto and any other applicable data protection or privacy laws, as amended from time to time;

1.4 "**EEA**" means the European Economic Area;

1.5 "**Personal Data**" means the data described in Annex 1 (*Details of Processing of Personal Data*) and any other personal data processed by Supplier or any Subprocessor on behalf of MSF pursuant to or in connection with the Main Agreement;

1.6 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;

1.7 "**Subprocessor**" means any data processor (including any third party and any affiliated company) appointed by Supplier to process personal data on behalf of MSF; and

1.8 "**Supervisory Authority**" means (a) an independent public authority established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws.

2. PROCESSING OF PERSONAL DATA

2.1 Supplier undertakes to comply with the requirements of Data Protection Laws when processing Personal Data on behalf of the MSF.

2.2 Supplier shall only process the types of Personal Data enumerated in Annex 1 (*Details of Processing of Personal Data*) to this Addendum for the purposes set forth in the Agreement.

2.3 Supplier shall not process, transfer, modify, amend or alter the Personal Data, or disclose, grant access or permit the disclosure of the Personal Data to any third party other than in accordance with MSF's written instructions (whether in the Agreement or otherwise) unless otherwise required by applicable law to which Supplier is subject, in which case Supplier shall, to the extent permitted by such law, inform MSF of that legal requirement before processing that Personal Data.

2.4 [optional: For the purposes set out in section 2.1. above, MSF hereby instructs Supplier to transfer Personal Data to the recipients in the countries listed in Annex 4 (*Authorised Transfers of Personal Data*), provided that Supplier shall comply with section 5 (*Subprocessing*) and 11 (*International Transfers of Personal Data*).]

3. SUPPLIER PERSONNEL

3.1 Supplier guarantees that it shall treat all Personal Data as strictly confidential and that it shall inform all of its employees, agents, contractors and Authorized Subprocessors engaged in processing the Personal Data of the confidential nature of such Personal Data. Supplier shall ensure that persons authorised to process the Personal Data have committed themselves to confidentiality obligations (a copy of which shall be provided upon MSF's request) or are under an appropriate statutory obligation of confidentiality or secrecy.

4. SECURITY

4.1 In addition to any obligations set forth in the Main Agreement, Supplier shall implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risk and shall take all measures required pursuant to article 32 GDPR , including but not limited to, as appropriate, (i) the pseudomization of Personal Data, (ii) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (iii) restoring the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, and (iv) regularly

testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.2 Supplier shall cooperate with MSF to adapt the technical and organisational measures as needed to meet the needs of MSF. The technical and organisational measures shall include reasonable measures agreed upon by the Parties listed in Appendix 2 to the Standard Contractual Clauses and Annex 5 (*Technical and organisational measures*). These technical and organisational measures shall apply even if Supplier has self-certified under the EU-US or Swiss-US Privacy Shield programs. Supplier shall tighten, supplement, and improve its security measures on an on-going basis, as appropriate, in order to maintain compliance with Data Protection Laws.

5. SUBPROCESSING

5.1 Subject to section 5.3, Supplier shall obtain MSF's prior written consent to the use of any Subprocessor to process Personal Data. As at the Effective Date, MSF hereby authorises Supplier to engage those Subprocessors set out in Annex 3 (*Authorised Subprocessors*).

5.2 With respect to each Subprocessor, Supplier shall (i) provide MSF with full details of the processing to be undertaken by each Subprocessor; (ii) carry out adequate due diligence on each Subprocessor; (iii) include terms in the contract between Supplier and each Subprocessor that are equivalent to those set out in this Addendum (also incorporating Standard Contractual Clauses or other arrangement MSF may approve) and shall supervise compliance thereof. Upon request, Supplier shall provide a copy of its agreements with Subprocessors to MSF for review. Supplier is fully liable for the acts and omissions of its Subprocessors.

6. DATA SUBJECT RIGHTS

6.1 Supplier shall notify MSF within two (2) calendar days if it receives a data subject request to exercise his/her rights under Data Protection Laws, including requests by a data subject to exercise rights in chapter III of GDPR, and shall provide full details of that request to MSF. Supplier shall direct such data subject to MSF, and shall not directly process the data subject's request, absent consent from MSF.

6.2 Supplier shall fully co-operate as requested by MSF to enable MSF to comply with any exercise of rights by a data subject regarding Personal Data. Such co-operation shall include (i) the provision of all information requested by MSF within any reasonable timescale specified by MSF, including full details and copies of the complaint, communication, or request and any Personal Data it holds in relation to a data subject; (ii) where applicable, providing such assistance requested by MSF to enable MSF to comply with the relevant request within the timescales prescribed by the Data Protection Laws; and (iii) implementing any additional technical and organisational measures as may be reasonably required by MSF to allow MSF to respond effectively to relevant complaints, communications or requests.

7. INCIDENT MANAGEMENT

7.1 In addition to any obligations set forth in the Main Agreement, Supplier shall notify MSF without undue delay, and no later than forty-eight (48) hours upon becoming aware of a data breach (unless the Main Agreement specifies a shorter timeframe), providing MSF

with all available information that allows MSF to meet any obligations to report a data breach in accordance with the Data a Protection Laws, including Article 33 and 34 GDPR. At a minimum, the notification to MSF shall include:

7.1.1 a description of the nature of the data breach, the categories and numbers of data subjects concerned, and the categories and numbers of Personal Data records concerned;

7.1.2 the name and contact details of Supplier's data protection officer or other relevant contact from whom more information may be obtained;

7.1.3 a description of the likely consequences of the data breach; and

7.1.4 a description of the measures taken or proposed to be taken to address the data breach.

7.2 Supplier shall assist MSF with notifying the data breach to any Supervisory Authority and/or the data subjects in accordance with Data Protection Laws.

7.3 Supplier shall fully co-operate with MSF and take such reasonable steps as MSF requests to assist in the investigation, mitigation and remediation of each data breach, in order to enable MSF to (i) perform a thorough investigation into the data breach, (ii) formulate a response that meets the requirements of the applicable Data Protection Laws, (iii) mitigate any harmful effect resulting from the data breach; and (iv) take suitable further action to meet any requirement under the Data Protection Laws.

7.4 Supplier shall assist MSF in remediating or mitigating any potential damage arising from a data breach. Supplier shall further provide MSF with regular status updates on the data breach including, but not limited to, actions taken to resolve such incident, at mutually agreed intervals or times for the duration of the data breach.

7.5 Within four six (6) weeks of closure of the incident, Supplier shall provide MSF a written report describing the data breach, the root cause analysis, actions taken by Supplier during its response and Supplier's plans for future actions to prevent a similar data breach from occurring.

7.6 Supplier shall not disclose to any third party (including, but not limited, to Supervisory Authorities and regulators) any information about a data breach without first obtaining MSF's prior written consent, unless notification is required by EU or Member State law to which Supplier is subject, in which case Supplier shall, to the extent permitted by such law, inform MSF of that legal requirement, provide a copy of the proposed notification and consider any comments made by MSF before notifying the data breach.

7.7 Supplier shall promptly notify the MSF about any legally binding request for disclosure of Personal Data by a law enforcement authority and shall refrain from disclosing same until instructed to do so by the MSF, unless otherwise prohibited from doing so.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

8.1 Supplier shall provide reasonable assistance to MSF with any data protection impact assessments that are required under Article 35 GDPR and with any prior consultations to

any Supervisory Authority required under Article 36 GDPR, in relation to processing of Personal Data by Supplier on behalf of MSF and taking into account the nature of the processing and information available to Supplier.

9. DELETION OR RETURN OF PERSONAL DATA

9.1 Supplier shall observe the data retention periods set forth in Appendix 1 and, within 10 (ten) days of the earlier of: (i) cessation of processing of Personal Data by Supplier; or (ii) expiration or termination of the Main Agreement, at the choice of MSF either (a) return a complete copy of all Personal Data to MSF and securely wipe all other copies of Personal Data processed by Supplier or any Authorised Subprocessor; or (b) securely wipe all copies of Personal Data processed by Supplier or any Authorised Subprocessor.

10. RECORDS AND AUDIT

10.1 Supplier shall maintain written records of all of the categories of processing carried out on behalf of the MSF, including (i) the name and contact details of any sub-processor; (ii) the processing activities carried out by each sub-processor, and any transfers of Personal Data outside of the EEA (including the name of the country where the recipient of such data is located and details of the legal basis for such transfer); and (iii) a description of the technical and organisational security measures applicable to each category of processing.

10.2 Upon MSF's request, and in addition to any audit rights set forth in the Main Agreement, Supplier shall make available to MSF all information necessary to demonstrate compliance with Data Protection Laws and this Addendum and allow for and contribute to audits, including inspections by MSF or another auditor mandated by MSF of any premises where the processing of MSF's Personal Data takes place. Supplier shall permit MSF or another auditor mandated by MSF to inspect, audit and copy any relevant records, processes and systems in order that MSF may satisfy itself that Supplier is in compliance with the provisions of Data Protection Laws and this Addendum.

11. INTERNATIONAL TRANSFERS OF PERSONAL DATA

11.1 Supplier shall not (permanently or temporarily) process the Personal Data nor permit any Authorised Subprocessor to (permanently or temporarily) process the Personal Data in a country outside of the EEA without an adequate level of protection as defined in Data Protection Laws other than in respect of those recipients in such countries listed in Annex 4 (*Authorised Transfers of Personal Data*), unless authorised in writing by MSF in advance.

11.2 When requested by MSF, Supplier shall promptly enter into (or procure that any relevant Subprocessor of Supplier enters into) an agreement with MSF which shall include provisions set out in Annex 2 (*Standard Contractual Clauses*) and/or such variation as Data Protection Laws might require or authorize, in respect of any processing of Personal Data in a country outside of the EEA without an adequate level of protection.

12. CHANGES IN APPLICABLE DATA PROTECTION LAWS

12.1 The Parties agree to negotiate in good faith modifications to this Addendum if changes are required to address the amendments to or legal interpretation of Data Protection Laws, including (i) to comply with any applicable Member State law; (ii) to comply with any modification or guidance on the interpretation of Data Protection Laws; or (iii) if changes

to the membership status of a country in the European Union or the European Economic Area require such modification.

13. ENFORCEMENT AND INDEMNIFICATION

13.1 Without prejudice to any other rights or remedies that the MSF may have, Supplier hereby acknowledges and agrees that a person with rights under this Addendum may be irreparably harmed by any breach of its terms and that damages alone may not be an adequate remedy. Accordingly, a person bringing a claim under this Addendum shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this Addendum.

13.2 Supplier agrees that it will (in addition to, and without affecting, any other rights or remedies that MSF may have whether under statute, common law or otherwise) indemnify and hold harmless MSF, on demand from and against third party claims, liabilities, fines, costs, expenses, loss or damage payable by MSF (including all interest, penalties and legal and other professional costs and expenses) arising directly from a breach of this Agreement by Supplier.

14. CONTACT

Any notification of question relating to this Addendum or pertaining to Data Subject's requests to exercise their rights shall be addressed to:

- For MSF: [privacy@toronto.msf.org]
- For Supplier: [insert contact email address]

15. MISCELLANEOUS

15.1 Subject to section 15.2, the Parties agree that this Addendum and the Standard Contractual Clauses shall terminate automatically upon termination or expiration of the Main Agreement or of any service contracts entered into by Supplier with MSF pursuant to the Main Agreement, whichever is later.

15.2 Any obligation imposed on Supplier under this Addendum in relation to the processing of Personal Data shall survive any termination or expiration of this Addendum.

15.3 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 but not limited to the Main Agreement, the provisions of this Addendum shall prevail with regard to the Parties' data protection obligations for Personal Data. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

15.4 Compliance by Supplier with the provisions of this Addendum will be at no additional cost to MSF.

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

SIGNED for and on behalf of **DOCTORS WITHOUT BORDERS/MÉDECINS SANS FRONTIÈRES**	**SIGNED** for and on behalf of **[NAME OF SUPPLIER]**
By:	By:
Name:	Name:
Title:	Title:

ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA

- *Subject matter of the processing of Personal Data*

[Include description here]

- *Duration of the processing of Personal Data*

[Include description here]

- *Nature and purpose of the processing of Personal Data*

[Include description here]

- *Types of Personal Data to be processed*

[Include description here]

- *Categories of data subject to whom the Personal Data relates*

[Include description here]

- *Special categories of Personal Data*

[Include description here]

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

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: Panasonic Avionics Corporation

Other information needed to identify the organisation

……
(the data **exporter**)

And

Name of the data importing organisation: [name of Supplier]

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.

Background

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

Clause 1

Definitions

For the purposes of the Clauses:

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

(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.

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

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.

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.

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. 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.

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……

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 ……

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual 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: Doctors Without Borders/Médecins sans frontières

Data importer
The data importer is: [name of Supplier]

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

- [Employees of MSF]
- [Donors of MSF]
- [Subscribers of MSF's newsletters]
- [insert other relevant category]

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

- [list types of personal data]

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

- [list types of special categories of data]

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

- [To be completed]

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):

The Processor shall undertake the following technical and organisational measures for data security in accordance with Art. 32 GDPR.

[NTD: to be adapted as necessary]

1. Confidentiality
    a. Access Control
    b. System Access Control
    c. Data Access Control
    d. Separation
    e. Pseudomization & Encryption
2. Integrity
    a. Data Entry Control
    b. Transmission Control
3. Availability and resilience
4. Procedure for the regular review, assessment and evaluation

ANNEX 3: AUTHORISED SUBPROCESSORS

[*Include details of (i) full legal name of each Subprocessor; (ii) details of the processing to be undertaken by each entity; (iii) address of Subprocessor.*]

Full Legal Name	Details of processing activity	Address

ANNEX 4: AUTHORISED TRANSFERS OF PERSONAL DATA

[*Include details of (i) all service locations of the Processor and each Subprocessor, including those within the EEA and outside of the EEA; (ii) full legal name of each recipient entity to whom data will be transferred; (iii) details of the processing to be undertaken by each entity.*]

Legal name	Locations	Details of processing activity

ANNEX 5: TECHNICAL AND ORGANISATIONAL MEASURES

Supplier shall implement and maintain the following technical and organisational measures for data security:

[NTD: To be adapted as necessary]

1. Confidentiality
    a. Access Control
    b. System Access Control
    c. Data Access Control
    d. Separation
    e. Pseudomization & Encryption
2. Integrity
    a. Data Entry Control
    b. Transmission Control
3. Availability and resilience
4. Procedure for the regular review, assessment and evaluation