GDPR Policy

Docsaway is operated by QiQ Communications PTY LTD (ACN 113 045 248) trading as Docsaway who is referred to in this GDPR Policy as "we", "us", "our" and similar grammatical forms.

By engaging us to provide the Services, you acknowledge and agree that you will act as a Data Controller; that you wish to instruct us to act as a Data Processor for Processing the Personal Data and that you agree to this GDPR Policy and the appended Standard Contractual Clauses. This GDPR policy forms a legally binding contractual agreement between us.

1. Definitions

Unless stated otherwise in this GDPR Policy,

a) **Customers** means you or your organization that is instructing and engaging Docsaway.

b) **Data Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

c) **Data Processor** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

d) **Data Protection Laws** means all laws and regulations relation to the protection of Personal Data and the Procession of Personal Data including but not limited to the EU GDPR and UK GDPR.

e) **Data Subject** means any identifiable natural person.

f) **GDPR** means the EU GDPR and/or UK GDPR as applicable.

g) **Personal Data** means 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.

h) **Processing** means 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.

i) **Services** means the mailing services we provide.

j) **Standard Contractual Clauses** means the standard contractual clauses issued by the European Commissioned on 4 June 2021 and as appended to this GDPR Policy and which are specific to customers from Europe.

k) **Subprocessor** means any person appointed by us or on behalf of us to process Personal Data on your behalf in connection with the GDPR Policy.

l) **Supervising Authorities** means an independent public authority which is established by a Member State pursuant to GDPR.

2. Processing of Personal Data

We warrant that we shall comply with all applicable Data Protection Laws while Processing the Personal Data and not process the Personal Data in any manner that is inconsistent with your written instructions. We shall process the Personal Data only for the duration of the Services. We recommend that you avoid transferring of any sensitive data unless it is absolutely necessary for the carriage of Services.

You acknowledge and agree to furnish us with all reasonable instructions required by us for Processing the Personal Data.

3. Processor Personnel

We warrant that we will not use the Personal Data in a way which is a detrimental to you. We will only disclose and grant access to the Personal Data strictly on a "need to know" basis to only such employees, agents, officers, directors and contractors as need to receive the Personal Data to give effect to the Processing of the Personal Data. We will ensure that our directors, officers, employees and any professional advisers to whom the Personal Data is disclosed comply with the Data Protection Laws.

4. Security

We use various state of the art technologies and procedures to help protect Personal Data from unauthorized access, alteration, loss, alternation, disclosure or use.

Some of the safeguards we use are physical access controls, information firewalls and access authorisation controls to where Personal Data is held in data centres. We also use data encryption while transferring the Personal Data. Our websites are password protected along with memorable numbers to provide appropriate levels of security.

Our commitment to data security means:

- We have procedures to limit access to Personal Data within our organisation;
- We use security measures and technologies, that are considered as appropriate measures under Article 32 of the GDPR within our organisation to protect Personal Data; and
- We use service providers that can establish that they have secure controls relating to software security, access security and network security, including where credit card information is being transferred.

All our employees keep up to date with all technical aspects of security and ensure the ongoing security of our servers and systems and are trained and made aware of their responsibilities under this GDPR Policy.

5. Subprocessor

We have a number of partners around the globe to assist us with the printing and posting of letters. Locations of our mailing partners are listed on our website and are updated from time-to-time.

You agree for us to appoint them as Subprocessors for the delivery of Services. We will ensure that the same data protection obligations as set out in this GDPR Policy (including, where appropriate, the Standard Contractual Clauses) shall be imposed on that SubProcessor by way of a contract.

For the purposes of section 9(c) of the Standard Contractual Clause, you agree that we may be prohibited from disclosing agreements with our Subprocessors to you. We will, however, use our reasonable efforts to require any Subprocessor to disclose the agreement to you on a confidentiality basis.

We may from time-to-time appoint or replace any Subprocessors. If we do so, we will notify you of it at least 30 days before making any appointment or replacement. If you object to any changes or have any concerns, then please write to us at support@docsaway.com.

Where the SubProcessor fails to fulfil its data protection obligations, we shall remain fully liable to you for the performance of the SubProcessor's obligations.

6. Data Subject's rights

We agree to assist you in fulfilling your obligations to respond to request to exercise Data Subject rights under the Data Protection Laws by implementing reasonable and practicable technical and organisational measures.

We agree to notify you as soon as practicable if we receive a request from a Data Subject under the Data Protection Laws in relation to the Personal Data. We will respond to such a request only in accordance with your instructions or as required by the applicable laws. In the event of inconsistency between your instructions and the applicable laws, the latter shall prevail. We will not charge the Data Subject in the process of fulfilling their request.

7. Data Breaches

If we become aware of or reasonably suspects of data breaches, hacking or cyber-attacks (Security Incident), we will:

a) immediately and in any event within 48 hours notify you in writing of the Security Incident, and provide you with all information in relation to the Security Incident as required by you;

b) promptly investigate the cause of the Security Incident and notify you in writing;

c) mitigate the impacts of Security Incident by, amongst other things, decreasing the threat level by eliminating or intercepting the adversary before they attack, blocking opportunities through enhanced security, or reducing the consequences if an attack should occur; and

d) remedy the Security Incident as soon as possible in consultation with you.

8. Data Protection Impact Assessment and Prior Consultation

We will provide you with reasonable assistance with any data protection impact assessments and prior consultations with Supervising Authorities which you may reasonably require. Any data protection impact assessment or prior consultant will be strictly in relation to the Processing of Personal Data.

9. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), we will apply specific restrictions and/or additional safeguards.

10. Deletion or return of Personal Data

Where applicable, we agree to do the following in relation to Personal Data held by us within 10 business days from the date of termination of the Services:

a) return or destroy all hard copies and (to the extent possible) delete any electronic copies such as copies saved on our computers;

b) retain copies only to the extent required by the Data Protection Laws; and

c) provide a written declaration confirming that this clause has been complied with.

11. Audit rights

We will keep detailed records of all measures we put in place to comply with the Data Protection Laws. Where reasonable and practicable, we will assist you by providing necessary documentation and information to demonstrate compliance with the Data Protection Laws.

12. Data transfer

You agree for us to transfer the Personal Data to our servers located at:

- Lansing Data Center, Lansing, Michigan, USA

The Personal Data will be transferred to countries outside of the European Economic Area. This is because we have mailing partners across the globe. List of our mailing locations can be found on our website.

We will use data encryption when Personal Data is transferred. We will take all measures that are necessary to ensure the transfer is in compliance with applicable Data Protection Laws.

We will implement appropriate technical and organisational measures to ensure the security of the Personal Data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

This includes but is not limited to:

- 24/7/365 manned facilities;

- CCTV Security Cameras covering inside, outside and all entrances of data centres;
- Site entrances are controlled by Electronic Perimeter Access Card System;
- Sites are remotely monitored by a 3rd Party security company;
- Entrances secured by Mantraps with Interlocking Doors;
- SSAE-16 & HIPAA Compliant;
- Safe Harbor Certified; ==> What is the source for this? Not 100% sure this is correct.
- Restricting remote admin access to our servers to key personnel within our technical support team; and
- Limiting access to server only to resolve an issue or to ensure that managed hosting services are met.

13. Accuracy of the Personal Data

If we become aware that the Personal Data we has received is inaccurate, or has become outdated, we shall inform you without undue delay. In this case, you shall cooperate with us to erase or rectify the data.

14. Confidentiality

Each Party will not at any time divulge or in any way communicate confidential information to any third party including the media except as far as may be necessary or required in connection with the proper performance the party's obligations and duties unless the party is specifically authorised or directed by the other party to do so or is compelled by the laws to do so and this obligation extends beyond the termination of this GDPR Policy.

15. Transparency

On request, you can make a copy of this GDPR Policy available to the Data Subject free of charge.

16. Third-party beneficiaries

Data Subjects where appropriate and applicable may invoke and enforce clauses of this GDPR Policy as third-party beneficiaries against you or us.

17. Redress

We shall inform Data Subjects in a transparent and easily accessible format, through individual notice or on our website, of a contact point authorised to handle complaints. We shall deal promptly with any complaints it receives from a Data Subject.

18. Categories

The parties agree that the categories of Data Subjects include but are not limited to the following and may vary according to a party's business and request: Employees; Suppliers; Customers; Job applicants; Consultants; Visitors; Prospects and Contractors.

The parties agree that the categories of Personal Data transferred include but are not limited to the following and may vary according to a party's business and request: First name, Last name, Address, Email address, Date of birth, Telephone number and Age.

19. Data Protection Officer

If you have any questions in relation to this GDPR Policy, please can contact us by writing to:

Peter Harris
QiQ Communications PTY LTD
PO Box 62
Kyneton
Victoria 3444
Australia

Email: support@docsaway.com

20. Governing Laws

Without prejudice to the Governing Law of the Standard Contractual Clauses, this GDPR Policy will be governed by and construed in accordance with the laws of Australia.

21. Notices

Any notice, demand, consent or other communication given or made under this GDPR Policy must be in writing, signed by an appropriately authorised representative of the party, and addressed to the other party's email address.

22. Clauses specific to European customers

A. Notification of personal data breach

In the event of a personal data breach, we shall cooperate with and assist you to comply with your obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to us.

A.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by you, we shall assist you:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay you have become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679/ or Article 34(3) of Regulation (EU) 2018/1725, shall be stated in the Data Controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate

number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 or Article 35 of Regulation (EU) 2018/1725, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

A.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by us, we shall notify you without undue delay after having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

B. Non compliance and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that we are in breach of our obligations under this GDPR policy, you may instruct us to suspend the processing of personal data until we comply with this GDPR policy or the contract is terminated. We shall promptly inform you in case we are unable to comply with these Clauses, for whatever reason.

(b) You shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with this GDPR if:

(1) the processing of personal data by us has been suspended by you pursuant to point (a) and if compliance with this GDPR Policy is not restored within a reasonable time and in any event within one month following suspension;

(2) we are in substantial or persistent breach of this GDPR or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) we fail to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) We shall be entitled to terminate the contract insofar as it concerns processing of personal data under this GDPR Policy where, after having informed you that your instructions infringe applicable legal requirements, and you insist on compliance with the instructions.

(d) Following termination of the contract, we shall, at your choice delete all personal data processed on your behalf and certify to you that it has done so, or, return all the personal data to you and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, we shall continue to ensure compliance with this GDPR Policy.

C. Assistance to data controller

(a) We shall promptly notify you of any request we have received from the data subject. We will not respond to the request itself, unless authorised by you to do so.

(b) We shall assist you in fulfilling your obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), we shall comply with your instructions

(c) In addition to our obligation to assist you, we shall furthermore assist you in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to us:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679/ or Articles 33 and 36 to 38 of Regulation (EU) 2018/1725.

23. Changes to this GDPR Policy

If we decide to change this GDPR Policy, we will inform you about it in writing via email. If you continue to instruct us to provide the Services, it will be assumed that you have agreed to the modifications.

Standard Contractual Clauses

For the purposes of the Standard Contractual Clauses QiQ Communications PTY LTD trading as Docsaway will be the “data importer” and the Customer will be the “data exporter”.

Module Two: Transfer Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(a) The Parties:

(a.1.i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

(a.1.ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

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

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

Clause 2

Effect and invariability of the Clauses

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

(c.1.i.1.b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

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

(c.1.ii) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(c.1.iii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(c.1.iv) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(c.1.v) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(c.1.vi) Clause 13;

(c.1.vii) Clause 15.1(c), (d) and (e);

(c.1.viii) Clause 16(e);

(c.1.ix) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(d) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(i) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

(l.1.i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(l.1.ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(l.1.iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(l.1.iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

Clause 10

Data subject rights

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

(t) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

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

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

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

(v.1.i)lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(v.1.ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

(ag.1.i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ag.1.ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(ag.1.iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

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

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

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

(ak) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses.

If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

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

(ak.1.i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ak.1.ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

<u>SECTION IV – FINAL PROVISIONS</u>

Clause 16

Non-compliance with the Clauses and termination

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

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

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

(as.1.i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(as.1.ii) the data importer is in substantial or persistent breach of these Clauses; or

(as.1.iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

(f) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed in accordance with theGoverning Laws clause of the GDPR Policy. If that clause does not specify an EU Member State, then these Clause shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.

Clause 18

Choice of forum and jurisdiction

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

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

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

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

UK AND SWISS ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

In case of data transfers from the United Kingdom and/or Switzerland, this addendum amends the Standard Contractual Clauses to the extent necessary so they operate for data transfers from the United Kingdom and/or Switzerland,.

The Standard Contractual Clauses shall be amended in a manner that references and obligations contained in the Standard Contractual Clauses shall have the same meaning as the equivalent references in the UK GDPR or Swiss Data Protection Laws as applicable.

The amendments referred in the clause abovve include but are not limited to the following:

(a) references to “Regulation (EU) 2016/679” or “that Regulation” are replaced by “UK GDPR” or “Swiss Data Protection Laws” and references to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article of the UK GDPR or Swiss Data Protection Laws;

(b) references to Regulation (EU) 2018/1725 are removed;

(c) references to the “Union”, “EU” and “EU Member State” are all replaced with the “UK” or Switzerland;

(d) to the extent the UK GDPR applies to the processing, Clause 18 shall be replaced to state:

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

(e) to the extent the Swiss DPA applies to the processing, Clause 18 shall be replaced to state:

> “*Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts*”.