Data Processing Agreement

DETAILS

Parties

    Data Importer

Australian entity	Name	Paperform Pty Ltd
	ACN	615 732 682
	Address	54 Ingham Avenue
		Five Dock NSW 2046

US entity		Paperform
		C4620794
		16830 Ventura Bld Ste 601
		Encino, California 91436, USA

Data Exporter	Company name	
	Company Number or identifier	
	Business address	
	Individual name	
	Title	
	Email address	

Background	A	Paperform and the Data Exporter intend to work together as set out in the Paperform General Terms and Conditions.
	B	There will be, or is likely to be, an exchange of data between the parties.
	C	The parties have agreed to handle and transfer any data in accordance with the terms of this Data Processing Agreement.

Date of Agreement

AGREED TERMS

1. Agreement

This Data Processing Agreement (**the Agreement**) supplements, amends and forms part of the General Terms and Conditions (**Terms**) between Paperform and the Data Exporter.

(a) This Agreement will be effective as of the date Paperform receives a complete and executed Agreement from the Data Exporter indicated in the signature block below (**the Effective Date**).

(b) The scope and duration, as well as the extent and nature of the collection, processing and use of Personal Data under this Agreement will be as defined in the Terms.

(c) The term of this Agreement corresponds to the duration of the Terms. This Agreement will terminate automatically upon termination of the Terms or as earlier terminated pursuant to the terms of this Agreement.

(d) This Agreement will only be effective if executed and submitted to Paperform accurately and in full accordance with any directions provided by Paperform. Upon receipt of the Agreement by Paperform, the Agreement will become legally binding.

(e) If the Data Exporter makes any deletions or other revisions to this Agreement, then this Agreement with be null and void.

(f) The Data Exporter signatory represents to Paperform that they have the legal authority to bind Customer and is lawfully able to enter into contracts.

2. Relationship between the parties

(a) The Data Exporter acts as a data controller under the GDPR.

(b) It is a requirement of the GDPR that any data processors engaged by the Data Exporter to process the Data Exporter's Personal Data must put a contract in place that governs the transfer of Personal Data between the parties in accordance with the requirements of the GDPR.

(c) Paperform agrees and acknowledges that:

(i) it is considered a data processor of the Data Exporter and must comply with the requirements of the GDPR for data processors; and

(ii) it has implemented appropriate technical and organisational measures to meet the requirements of the GDPR insofar as they apply to Paperform and the Data Exporter's Personal Data, including any appropriate Supplementary Measures.

3. Transfers

(a) Subject to section 4(c), the Data Exporter and Paperform, and their respective Representatives, hereby enter into the Standard Contractual Clauses set out in Schedule 1 to this Agreement in respect to any Restricted Transfer from the Data Exporter to Paperform, with:

(i) the Data Exporter acting as the data controller; and

(ii) Paperform acting as the data processor.

(b)   The Standard Contractual Clauses will come into effect under section 3(a) on the commencement of a Restricted Transfer.

(c)   For the purposes of clause 8.1 of the Standard Contractual Clauses, the processing described in section 4 is deemed an instruction by the Data Exporter to process Data Exporter Personal Data, subject to Paperform's compliance with Applicable Laws.

(d)   Section 3(a) shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, does not include obtaining direct consent from Data Subjects), is to allow the Restricted Transfer to take place without breach of applicable Data Protection Laws.

(e)   The parties warrant that they have no reason to believe that the laws and practices of the third country of destination applicable to the processing of the Data Exporter Personal Data by Paperform will prevent Paperform from fulfilling its obligations under this Agreement.

(f)   Without limitation of any obligation under the Terms, Paperform undertakes that it will take all reasonable steps to ensure the reliability of any employee, agent or contractor of Paperform who may have access to the Data Exporter Personal Data, ensuring that:

     (i)   all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and

     (ii)   ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Data Exporter Personal Data,

as strictly necessary for performance of the Terms and to comply with Applicable Laws in the context of that individual's duties to Paperform.

4.   Data processing

(a)   Data Exporter hereby instructs Paperform (and authorises Paperform to instruct each Approved Subprocessor) to:

     (i)   process the Data Exporter Personal Data; and

     (ii)   transfer Data Exporter Personal Data to any country or territory only in accordance with section 3,

as reasonably necessary for the provision of the Services and consistent with the Terms.

(b)   The Data Exporter is duly and effectively authorised to give the instruction set out in section 4(a) on behalf of itself.

(c)   Paperform will ensure that each Approved Subprocessor will:

     (i)   comply with all applicable Data Protection Laws when processing the Data Exporter's Personal Data; and

     (ii)   only process the Data Exporter's Personal Data in accordance with the Data Exporter's documented instructions unless processing is required by Applicable Laws to which the Approved Subprocessor is subject.

## 5.	Approved Subprocessors

(a)	Pursuant to clause 9 of the Standard Contractual Clauses, the Data Exporter hereby provides Paperform with general written authorisation to engage the Approved Subprocessors from the agreed list https://paperform.co/subprocessors to carry out processing on behalf of Paperform to the extent necessary for Paperform to provide the Services.

(b)	Notwithstanding section 5(a), Paperform will give the Data Exporter prior written notice of any changes to the above agreed list of Approved Subprocessors at least 14 days before the intended appointment of any new Approved Subprocessor, including full details of the processing to be undertaken by the Approved Subprocessor, or the removal of any current Approved Subprocessor. If, within two weeks of receipt of that notice, the Data Exporter notifies Paperform in writing of any reasonable objections to the intended appointment:

   (i)	Paperform will not appoint (or disclose Data Exporter Personal Data to) that proposed Approved Subprocessor until the Data Exporter and Paperform have agreed on reasonable steps to address the objections raised by the Data Exporter; and

   (ii)	Data Exporter has been provided with a reasonable written explanation of the steps to be taken.

(c)	In the event that no such reasonable steps can be agreed between the Data Exporter and Paperform, either:

   (i)	Paperform may elect not to appoint the proposed Approved Subprocessor; or

   (ii)	if Paperform provides written notice to the Data Exporter that it intends to appoint the proposed Approved Subprocessor irrespective of the Data Exporter's written objections, the Data Exporter may by written notice to Paperform with immediate effect terminate the Terms to the extent that it relates to the Services which require the use of the proposed Approved Subprocessor.

(d)	With respect to each Approved Subprocessor, Paperform will ensure that the:

   (i)	Approved Subprocessor will be required to meet the terms of the Standard Contractual Clauses insofar as they apply to that Approved Subprocessor;

   (ii)	ensure that the arrangement between Paperform and the Approved Subprocessor is governed by a written contract including terms which offer at least the same level of protection for the Data Exporter Personal Data as those set out in this Agreement and meet the requirements of article 28(3) of the GDPR; and

   (iii)	the agreement with the Approved Subprocessor contains an agreed third party beneficiary clause where in the event Paperform has factually disappeared, ceased to exist in law or has become insolvent, the Data Exporter will have the right to terminate the agreement with the Approved Subprocessor and instruct the Approved Subprocessor to erase or return the Data Exporter Personal Data.

(e)	Paperform acknowledges that it:

(i)   is liable to the Data Exporter for an Approved Subprocessor's compliance with its obligations under this section 5; and

(ii) Paperform acknowledges that it will provide, at the Data Exporter's request, a copy of each agreement with an Approved Subprocessor and any subsequent amendments to that agreement, with any relevant parts of the agreement redacted to the extent necessary to protect business secrets or other confidential information, including Personal Data, prior to sharing the copy with the Data Exporter.

6.   Data Subject rights

(a) Each party will implement appropriate technical and organisational measures, as appropriate, to assist the other party in responding to requests to exercise Data Subject rights under the Data Protection Laws.

(b) Paperform will promptly notify the Data Exporter if Paperform or an Approved Subprocessor receives a request from a Data Subject under any Data Protection Law in respect of Data Exporter Personal Data.

(c) Paperform and the Data Exporter acknowledge that Data Subjects may invoke and enforce the Standard Contractual Clauses as third party beneficiaries against Paperform and / or the Data Exporter under clause 3(a) of the Standard Contractual Clauses.

(d) Paperform will not, and will ensure that any Approved Subprocessor does not, respond to that request except:

(i)   on the documented instructions of the Data Exporter; or

(ii)   as required by Applicable Laws to which Paperform is subject, in which case Paperform will, to the extent permitted by Applicable Laws, inform the Data Exporter of that legal requirement before Paperform or the Approved Subprocessor responds to the request.

(e) Paperform will assist the Data Exporter in fulfilling its obligations to respond to Data Subjects' requests for the exercise of their rights under the GDPR.

(f) Paperform will inform Data Subjects in an easy accessible format on its website of a contact point authorised to handle complaints, and it will deal with any complaints it receives from a Data Subject.

7.   Personal Data Breach

(a) Each party will cooperate with the other party to investigate, mitigate and remediate Personal Data Breaches.

(b) In respect of any Personal Data Breach, Paperform will:

(i)   take such appropriate measures to address the breach, including measures to mitigate its adverse effects;

(ii)   notify the Data Exporter of the Personal Data Breach without undue delay upon becoming aware of the Personal Data Breach; and

(iii) provide the Data Exporter, without undue delay, with such details as the Data Exporter reasonably requires to consider the Personal Data Breach. This may include, depending on the nature of the Personal Data Breach, information regarding:

A. a contact point where more information can be obtained;

B. the nature of the Personal Data Breach, including the categories and approximate numbers of Data Subjects and Personal Data records concerned;

C. any investigations into such Personal Data Breach;

D. the likely consequences of the Personal Data Breach; and

E. any measures taken, or that Paperform recommends be taken, to address such Personal Data Breach, including to mitigate its possible adverse effects.

(c) Paperform will promptly inform the Data Exporter if it receives a complaint or request relating to either party's obligations under Data Protection Laws relevant to this Agreement, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority.

8. Technical and organisational measures and security

(a) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity involved in the processing for the rights and freedoms of natural persons, Paperform will, and will obtain that each Approved Subprocessor will, implement and maintain appropriate technical and organisational measures in relation to the processing of Personal Data by Paperform or Approved Subprocessor to ensure a level of security appropriate to that risk including, as appropriate, the measures referred to in article 32 of the GDPR, Annex II to Schedule 1, and any Supplementary Measures.

(b) In assessing the appropriate level of security, Paperform will take into account all risks that are presented by processing the relevant Personal Data, in particular the risk associated with the occurrence of a Personal Data Breach, and any transfer assessments completed as part of the assessment for any appropriate Supplementary Measures.

9. Deletion or return of data

(a) Paperform will, at the Data Exporter's written request, either securely delete or securely return all the Personal Data to the Data Exporter in such form as the Data Exporter reasonably requests after the earlier of:

(i) the end of the provision of the relevant Services related to processing; or

(ii) once processing by Paperform of any Personal Data is no longer required for the purpose of Paperform's performance of its relevant obligations under the Terms and this Agreement,

and securely delete existing copies (unless storage of any data is required by Applicable Law and, if so, the Data Exporter will inform Paperform of any such requirement).

(b)   Paperform shall provide written certification to the Data Exporter that it, and each Approved Subprocessor, has fully complied with this section 9.

10.   Audit rights

(a)   Without limiting any other right of the Data Exporter under the Terms, Paperform will maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of the Data Exporter, containing such information as the Data Exporter may reasonably require, including:

(i)   the name and contact details of Paperform's representative and data protection officer (if any);

(ii)   the categories of processing carried out on behalf of the Data Exporter;

(iii)   where applicable, details of transfers of Data Exporter Personal Data to a third country or an international organisation; and

(iv)   a general description of the technical and organisational security measures employed by Paperform.

(b)   Paperform will make available to the Data Exporter on request:

(i)   copies of the records under section 10(a); and

(ii)   such other information as the Data Exporter reasonably requires to demonstrate Paperform's compliance with its obligations under Data Protection Laws and this Agreement.

(c)   Paperform will allow for and contribute to audits, including inspections, conducted by the Data Exporter or another auditor mandated by the Data Exporter for the purpose of demonstrating compliance by Paperform with its obligations under Data Protection Laws and this Agreement provided that the Data Exporter provides Paperform with reasonable prior notice.

(d)   Paperform will resolve, at its own cost and expense, all data protection and security issues discovered by the Data Exporter that may constitute a breach or potential breach by Paperform of its obligations under this Agreement.

11.   Access by Public Authorities

(a)   Paperform agrees to notify the Data Exporter and where possible, any affected Data Subjects (if necessary, with the help of the Data Exporter) in accordance with clause 15 of the Standard Contractual Clauses, if it:

(i)   receives a legally binding request from a public authority under the laws of the country of destination for the disclosure of Data Exporter Personal Data, with the notification including:

A.   information about the Data Exporter Personal Data requested;

B.   the requesting authority; and

C. the legal basis for the request, or

    (ii)   becomes aware of any direct access by public authorities to Data Exporter Personal Data in accordance with the laws of the country of destination with the notification including all information available to Paperform.

(b)   With respect to the legally binding requests or direct access by public authorities in section 11(a) above, Paperform agrees to:

    (i)   use its best efforts to obtain a waiver against any prohibition against notifying the Data Exporter and to document these efforts;

    (ii)   where permissible under the laws of the country of destination, to provide the Data Exporter at regular intervals as much relevant information as possible on the requests received by public authorities in the country of destination, including;

        A.   number of requests;

        B.   type of Data Exporter Personal Data requested;

        C.   requesting authorities; and

        D.   whether these requests have been challenged and the outcome of those challenges, and

    (iii)   review the legality of any requests for disclosure and to challenge those requests if there are reasonable grounds to do so, documenting any reviews or challenges and providing these to the Data Exporter where permissible, and to the relevant supervisory authority on request; and

    (iv)   pursue possibilities of appeal against the requests for disclosure.

(c)   If Paperform is required to provide any disclosures as detailed in this section 11, it will only provide the amount of information required to comply with the request.

12.   Definitions

(a)   For purposes of this Agreement only, the following terms shall have the meanings set out below and any other capitalised terms not defined herein shall retain the meaning ascribed to them in the Terms:

Applicable Laws means:

    (i)   European Union or Member State laws with respect to any Data Exporter Personal Data that the Data Exporter is subject to; and

    (ii)   any other applicable law with respect to any Data Exporter Personal Data that the Data Exporter is subject to;

Data Exporter Personal Data means any Personal Data processed by Paperform or an Approved Subprocessor on behalf of the Data Exporter pursuant to or in connection with the Agreement; and

Data Protection Laws means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the EU General Data Protection Regulation 2016/679 ("GDPR")

and laws implementing or supplementing the GDPR and any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the European Union and, only to the extent applicable, the data protection or privacy laws of any other country;

GDPR means the EU General Data Protection Regulation 2016/679;

Paperform means the applicable Paperform Entity that provides the Services, as designated in the Terms;

Paperform Entities means Paperform Pty Ltd (615 732 682) and / or Paperform (C4620794).

Representative means, in respect of a party, any person acting for or on behalf of the party and includes any director, officer, employee, agent, contractor or sub-contractor of the party;

Restricted Transfer means:

(i)   a transfer of Data Exporter Personal Data from the Data Exporter to Paperform or an Approved Subprocessor; or

(ii)   an onward transfer of Data Exporter Personal Data from Paperform or an Approved Subprocessor to another Approved Subprocessor,

(iii)   in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the appropriate safeguards as set forth in article 46 of the GDPR;

Services means the services and other activities to be supplied to or carried out by or on behalf of Paperform for the Data Exporter pursuant to the Terms;

Standard Contractual Clauses means the contractual clauses set out in the Decision of the Commission of the European Union 2021/194 and the module of these contractual clauses which is applicable to the situation between the Data Exporter and the Data Importer (or any replacement European Commission standard contractual clauses from time to time);

Approved Subprocessor means any person (including any third party, but excluding an employee or independent contractor of Paperform) appointed by or on behalf of Paperform to process Personal Data on behalf of the Data Exporter in connection with the Terms which has been authorised (through general or specific authorisation) by the Data Exporter to process Personal Data on behalf of the Data Exporter and which has agreed to a written contract with the same level of protection as under these Terms and the Standard Contractual Clauses in Schedule 1 in accordance with clause 9 of the Standard Contractual Clauses.

Supplementary Measures means any additional technical, organisational, contractual or other measures adopted by agreement between the Data Exporter and Paperform after undertaking the assessment and steps outlined in the European Data Protection Board's Recommendations 01/2020, or other similar Recommendations published by the European Data Protection Board from time to time.

(c)   The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**process/processing**", "**Processor"** and "**Supervisory Authority**" shall have the

same meaning as in article 4 of the GDPR. The words "include/including" shall be construed to mean include without limitation.

(d)   In this Agreement references to:

(i)   a 'section' means a section within the Agreement; and

(ii)   a 'clause' means a clause within the Standard Contractual Clauses at Schedule 1.

Schedule 1: STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 46(2)(c) of Regulation (EU) 2016/679 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, the parties (each a "party") specified in ANNEX I have agreed on the following Standard Contractual 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 ANNEX I.B.

These Standard Contractual Clauses use Module Two – Controller to Processor.

The Parties (each a "party"; together "the parties") listed in ANNEX I HAVE AGREED on the following Standard Contractual Clauses (**the Clauses**).

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b)   The Parties:

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

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

(i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii)   Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii)   Clause 9(a), (c), (d) and (e);

(iv)   Clause 12(a), (d) and (f)

(v)   Clause 13;

(vi)   Clause 15.1(c), (d) and (e);

(vii)   Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfers(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

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

(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;

(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;

(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

(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.

---

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

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

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

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

Clause 9

Use of sub-processors

(a)   The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 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.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

---

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

(b)   The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its

sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

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

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

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

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

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

Clause 13

Supervision

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

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

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

(b)   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 practice 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.

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

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

    (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[4]

    (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.

(c) 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.

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

(e) 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).

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a

request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is

transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

(b)   The Parties agree that those shall be the courts of Ireland.

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

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

<p style="text-align:center;">**APPENDIX**</p>

<p style="text-align:center;">**ANNEX I**</p>

A.   LIST OF PARTIES

Parties

Data Exporter	Name		
	Address		
	Contact person's name		
	Contact person's position		
	Contact person's email		
	Contact person's telephone		
	Activities relevant to the data transferred under these Clauses		
	Other identifying information		
	Role (Controller/Processor)	Controller	
		_____	
		Name	
		_____	
		Authorised Signature	
		_____	
		Date	
Data Importer	Name	Paperform Pty Ltd	
	Address	54 Ingham Avenue	
		Five Dock NSW 2046, AU	
	Contact person's name	Dean McPherson	
	Contact person's position	Director	
	Contact person's email	dean@paperform.co	
	Contact person's telephone	+61424619055	
	Activities relevant to the data transferred under these Clauses	The data importer provides a service that allows users (the data exporter) to create customisable forms for use in their business.	

Other identifying information	ACN 615 732 682
Role (Controller/Processor)	Processor

Paperform Pty Ltd
_____
Name

Dean McPherson
_____
Authorised Signature

November 3, 2021
_____
Date

Name	Paperform
Address	16830 Ventura Bld Ste 601 Encino, California 91436, USA
Contact person's name	Dean McPherson
Contact person's position	CEO
Contact person's email	dean@paperform.co
Contact person's telephone	+61424619055
Activities relevant to the data transferred under these Clauses	The data importer provides a service that allows users (the data exporter) to create customisable forms for use in their business.
Other identifying information	C4620794
Role (Controller/Processor)	Processor

Paperform
_____
Name

Dean McPherson
_____
Authorised Signature

November 3, 2021
_____
Date

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

- end users of Paperform's Services;

- individuals whose personal data is supplied by end users of Paperform's Services; and

- current, potential and former personnel, including contractors, consultants and freelancers.

Categories of personal data transferred

The personal data transferred concern the following categories of data:

- direct identifying information (including name, phone number, email address);

- indirect identifying information (including job title, gender, residential or billing address, date of birth);

- device identification data and traffic data (including IP addresses, information gathered via cookies and web logs); and

- any personal data supplied by end users of Paperform's Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The data importer does not knowingly collect (and Paperform's or any Paperform Entities' customers or end users should not submit or upload) any special categories of data (as defined under the GDPR).

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The personal data will be transferred in bursts to the data importer from the data exporter when the data exporter communicates with Paperform, the Paperform Entities and / or uses the Paperform Service through its customisable forms.

Nature of the processing

The data importer receives information from the data exporter when the data exporter uses the Paperform Services, makes a query in relation to the Paperform Service and / or becomes a customer of Paperform or the Paperform Entities. The data exporter can then use Paperform's Service to create customisable forms for use in their business.

Purpose(s) of the data transfer and further processing

The data exporter transfers the personal data to the data importer for processing in order for Paperform and / or the Paperform Entities to provide its services to the data exporter under the Terms between Paperform and the data exporter.

The purpose of the data importer's processing for the data exporter under the Terms includes providing customisable forms which collect the personal data of the data exporter's customers as required by the data exporter. Some purposes of these forms include customer intake, customer management, task management, marketing, lead generation, taking payments, providing quotes, scheduling meetings or any other purpose as specified by the data exporter.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
3 years after the date of termination of the Terms with the data exporter, unless otherwise agreed by the parties.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See the current list of sub-processors at https://paperform.co/subprocessors

C.   COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

If the data exporter is based in the EU, the competent supervisory authority will be the relevant supervisory authority in the EU member state where the data exporter is based.

If the data exporter is not based in the EU, the competent supervisory authority will be the relevant supervisory authority in the EU member state the data exporter's GDPR representative is based.

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TEHCNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. **Organisational Security**

    (a)   Responsibility – the data importer will assign responsibility for information security management to appropriately skilled personnel.

    (b)   'Need to Know' Access – the data importer will restrict access to information systems used in connection with the Services to personnel who are reliable, have sufficient technical expertise for the role assigned and know his or her obligations.

    (c)   Confidentiality – the data importer's personnel who have accessed or otherwise been made known of Data Exporter Personal Data, will maintain the confidentiality of such information.

2. **Handling of data**

    (a)   Media Destruction – Service Provider shall destroy removable media and any mobile device (such as discs, USB drives, DVDs, back-up tapes, printers, laptops and tablets) containing Data Exporter Personal Data or render Data Exporter Personal Data on such physical media unintelligible and not capable of reconstruction by any technical means prior to any reuse of the media, if such media or mobile device is no longer intended to be used.

    (b)   Data Encryption – If deemed appropriate by the data importer given the sensitivity of the Data Exporter Personal Data, the data importer will encrypt or protect by other technical means Data Exporter Personal Data in Service Provider's possession or control so that it cannot be read, copied, changed or deleted by unauthorised personnel while in storage.

    (c)   Data Loss Prevention – the data importer will implement comprehensive data leakage controls that automatically identify, detect, monitor, document and either alert or prevent said Data Exporter Personal Data from leaving the data importer's control without authorisation in place.

    (a)   Malicious Code – the data importer will detect the introduction or intrusion of malicious code on information systems handling or holding Data Exporter Personal Data to prevent the unauthorised access, disclosure or loss of integrity of any Data Exporter Personal Data and remove and eliminate any effects.

3. **Physical Security**

    (a)   Securing Physical Facilities – the data importer will maintain all systems hosting Data Exporter Personal Data in a physically secure environment that restricts access to only authorised individuals, detects any unauthorised access or access attempts, and reports incidents and non-conformance of security policy to management.

    (b)   Secure Physical Processing Locations – the data importer will keep an up-to-date record of the location of where Data Exporter Personal Data is stored or processed in connection with the provisions of services and the owner of such data location.

(c) Paper Destruction – the data importer will dispose of all physical documentation containing Data Exporter Personal Data in a secure and confidential manner so as to render all paper waste unreadable.

4.   Measures to assist the data controller

(a)   The data importer has the following organisational measures in place to provide assistance to the data controller:

(i)   a point of contact for the data exporter;

(ii)   an internal data processing register;

(iii)   a data breach response plan;

(iv)   a data subject rights policy;

(v)   a data processing policy;

(vi)   a data security policy;

(vii)   a form for data subjects to fill out to exercise their rights; and

(viii)   a request register where the data importer will record any data subject requests.

(b)   The data importer has the following technical measures in place to provide assistance to the data controller:

(i)   measures for ensuring data minimisation;

(ii)   measures for ensuring data quality;

(iii)   measures for ensuring limited data retention;

(iv)   measures for secure transmission of personal data;

(v)   measures for restricting the processing of personal data;

(vi)   measures for ensuring accountability; and

(vii)   measures for allowing data portability and ensuring erasure.

The controller has authorised the use of the following sub-processors:

Sub-processor	Name
	Address
	Contact person's name
	Contact person's position
	Contact person's email
	Contact person's telephone
	Description of processing and responsibilities
	Other identifying information

DATA EXPORTER

Name: ....

Authorised Signature ....

DATA IMPORTER

Name: Paperform Pty Ltd

Dean McPherson

Authorised Signature ....