

Psychological Consultancy Limited Standard Contractual Clauses

The Standard Contractual Clauses are between an EEA Controller and a non-EEA Data Processor.

Where applicable, these Standard Contractual Clauses ("SCCs") form part of the arrangement, purchase order, statement of work, written or electronic agreement or agreements between Psychological Consultancy Limited ("PCL") (the "Data Importer") and the Data Exporter described in the SCCs for the purchase of products or services from the Data Importer (the "Agreement") to reflect the parties' agreement with regard to the processing and transfer of data, including personal data, in accordance with the requirements of the applicable data protection law.

HOW TO EXECUTE THE SCC:

1. The SCCs have been pre-signed by PCL as the Data Importer.
2. The file can be downloaded to your computer and opened with Adobe Acrobat to enable the signature feature. If preferred, simply print, complete, and scan.
3. To complete the SCCs, the Data Exporter must provide the following on the attached SCCs:
 - a. Complete the information as the Data Exporter on Page 2.
 - b. Provide a brief description of Data Exporter's business on Page 10.
 - c. Complete the information in the signature blocks and sign on pages 9 and 10.
4. Submit the completed and signed SCCs to PCL at info@psychological-consultancy.com.

Upon PCL's receipt of the validly completed and signed SCCs at the above email address, the SCCs will be in effect.

HOW THE SCCs APPLY:

If the entity signing the SCCs is a party to the Agreement, the SCCs are an addendum to, and form part of, the Agreement.

If the entity signing the SCCs has executed a Purchase Order or Scope of Work with PCL pursuant to the Agreement as an affiliate of the entity who is a party, but is not itself a party to the Agreement, the SCCs are an addendum to that Purchase Order or Scope of Work and applicable renewals thereof, and the entity that is a party to such Purchase Order or Scope of Work is party to this DPA.

If the entity signing the SCCs is not a party to an Agreement with PCL directly, but is instead a customer of an authorised PCL distributor or partner of PCL, the SCCs stand alone and govern only the data importer/exporter relationship between PCL and the entity signing the SCCs and create no other contractual obligations on the part of PCL.

The SCCs shall not replace any comparable or additional rights relating to processing of data, including person data, contained in any existing Agreement.

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

Data Exporter

Name	
Address	
Telephone	
Email	

Other information needed to identify the organisation:

--

(the data exporter)

And

Data Importer

Name	Psychological Consultancy Limited ("PCL")
Address	8 Mount Ephraim, Tunbridge Wells, TN4 8AS
Telephone	+ 44 (0) 1892 559540
Email	info@psychological-consultancy.com

Other information needed to identify the organisation:

PCL

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

(d) 'the sub processor' means any processor engaged by the data importer or by any other sub processor of the data importer who agrees to receive from the data importer or from any other sub processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract.

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

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

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

(g) to forward any notification received from the data importer or any sub processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information.

(i) that, in the event of sub processing, the processing activity is carried out in accordance with Clause 11 by a sub processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer:

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub processor agreement it concludes under the Clauses to the data exporter.

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

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data

subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub processor agrees that the data subject may issue a claim against the data sub processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8

Cooperation with supervisory authorities

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Sub processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub processor which imposes the same obligations on the sub processor as are imposed on the data importer under the Clauses. Where the sub processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.³
3. The provisions relating to data protection aspects for sub processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

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

On behalf of the data exporter:

Name (written in full)	
Position	
Address	

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

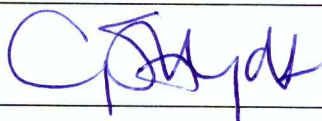
Signature:

On behalf of the data importer:

Name (written in full)	Gillian Hyde
Position	Director
Address	8 Mount Ephraim, Tunbridge Wells, TN4 8AS

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

Signature:



APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

_____ is a _____.

Data importer

The data importer is Psychological Consultancy Limited a publisher of psychometric assessments and provider of consultancy services.

The data importer's activities to the restricted transfer are previewing results of psychometric assessments for analysis, scoring and profiling of assessment responses to produce reports to assist the data exporter in providing services usually related to the HR or L&D function.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify): Data subjects may include employees, contractors, business partners, potential employees, or other individuals utilising the services.

Categories of data

The personal data transferred concern the following categories of data: Personal data transferred may concern system user IDs, name, email, company identification, responses to assessment items, results garnered through assessment process.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data: Data subject may provide ethnicity information on an optional basis only.

Processing operations

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

Personal data may be processed for the following purposes:

- (a) to provide the services, including the detection, prevention and resolution of security and technical issues, backup of data, processing, transmission, retrieval and access;
- (b) to respond to support requests; and
- (c) otherwise, to fulfil the obligations under the agreement between the parties.

DATA EXPORTER

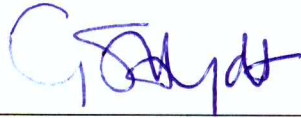
Name:

Authorised Signature:

DATA IMPORTER

Name: Gillian Hyde

Authorised Signature:



APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

PCL has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect the data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

1.Data Centre & Network Security

1.1. Data Centre

Infrastructure. PCL stores all production data in a physically secure co-location data centre. All servers and other hardware used in the Production and Testing environments are owned by PCL, although the data centre is not.

Redundancy. Data centre systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data centre equipment is scheduled through a standard change process according to documented procedures. Server Operating Systems. Data centre servers use a Microsoft-based implementation customized for the application environment, primarily the Psy-Key assessment platform.

PCL employs an internal code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

1.2. Networks & Transmission.

Data Transmission. The data centre is connected via high-speed private links to provide secure and fast data transfer. This is designed to prevent data from being read, copied, altered, or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. PCL transfers data via Internet standard protocols.

External Attack Surface. PCL employs multiple layers of network devices and intrusion detection to protect its external attack surface. PCL considers potential attack vectors and incorporates appropriate purpose-built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. PCL intrusion detection involves: tightly controlling the size and make-up of server attack surface through preventative measures; employing intelligent detection controls at data entry points; and employing technologies that automatically remedy certain situations.

Incident Response. PCL monitors a variety of communication channels for security incidents, and PCL will react promptly to known incidents.

Encryption Technologies. PCL utilises HTTPS encryption (also referred to as SSL or TLS) on its production and testing environments.

2. Access and Site Controls.

2.1. Site Controls.

On-site Data Centre Security Operation. The data centre maintains an on-site security operation responsible for all physical data centre security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform patrols of the data centre regularly.

Datacentre Access Procedures. The data centre facility maintains formal access procedures for allowing physical access to the data centre. The data centre is housed in facilities that require electronic card key and biometric access, with alarms that are linked to the on-site security operation. All entrants to the data centre are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centre.

On-site Datacentre Security Devices. The co-location facilities employ an electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. The fire doors at the data centre are alarmed. CCTV cameras are in operation both inside and outside the data centre. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data centre building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment.

2.2. Access Control.

Infrastructure Security Personnel. PCL has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. PCL has policies for the ongoing monitoring of PCL's security infrastructure, the review of the Services, and for responding to security incidents.

Access Control and Privilege Management. Client's administrators and end users must authenticate themselves via a central authentication system or via an integrated system in order to use the Services. Each application checks credentials to allow the display of data to an authorized End User or authorised Administrator.

Internal Data Access Processes and Policies – Access Policy. PCL's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process Personal Data. PCL aims to design its systems to only allow authorised persons to access data they are authorized to access. PCL requires the use of unique user IDs and strong passwords to minimize the potential for unauthorized account use. The granting or modification of access rights is based on:

- the authorised personnel's job responsibilities;
- job duty requirements necessary to perform authorised tasks;
- and a need-to-know basis.

Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at

least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength.

3.Data.

3.1. Data Storage, Isolation & Authentication.

PCL stores data in a multi-tenant environment on dedicated servers. PCL logically separates Client's data, including data from different end users, from each other, and data for an authenticated end user will not be displayed to another end user.

3.2. Decommissioned Disks and Disk Erase Policy.

Certain disks containing data may experience performance issues, errors or hardware failure that will lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes for reuse or destruction. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed.

4.Personnel Security.

PCL personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. PCL conducts reasonably appropriate backgrounds checks and in accordance with law and statutory regulations.

Personnel acknowledge receipt of, and compliance with, PCL's policies. Personnel are provided with security training.