**Data Protection Agreement for Accredited Learning Providers**

*-for companies based outside the European Economic Area (EEA) or in a country without the UK/EU Adequacy Decision*

Please complete this questionnaire and complete the declaration before returning it to APM.

APM’s own Privacy Statement for reference purposes may be accessed [here](https://www.apm.org.uk/apm-privacy-statement/).

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Questionnaire** | ***Guidance examples*** | **Response (to be completed)** |
|  | **General** |
|  | Please provide the full name of your company/organisation  |  |  |
|  | (a) Is your company registered in the United Kingdom at Companies House? (b) If not, in which country is your company registered? |  | 1. Yes/No *(delete as appropriate)*
 |
|  | (a) Please list the different types of personal data which will be exchanged with APM and (b) the purpose for providing the data. | *e.g. (a) individual’s first name; surname; home address; date of birth etc (b) course application form; event management etc* | (a)(b) |
|  | (a) What is the postal address for the premises from which the data is processed? (b) Please confirm if your organisation owns these premises. |  | (a)(b) yes/no *(delete as appropriate)* |
|  | What is the name and telephone number of your company’s Information Security or Data Protection Manager?  |  | Name: Telephone no:  |
|  | (a) Is your company registered with the Information Commissioner’s Office? (b) If yes, what is your registration number?  |  | 1. Yes/no *(delete as appropriate)*
 |
|  | (a) Please list all sub-contractors you will use to process candidate data, and (b) the steps taken to ensure their compliance with data protection requirements. | *e.g. contractual clauses;**reviews of security controls; firewalls, anti-virus software; third party security suppliers; web services* | (a)(b) |
|  |  **Physical Security** |
|  | Describe the security measures in place to protect APM’s information on your premises, and how any electronic backups of data will be secured.  | *e.g. physical storage areas, security etc* |  |
|  | **Technical Controls** |
|  | What type of information security procedures does your company have for protecting its systems against the vulnerabilities of unauthorised or unlawful processing and against accidental loss or destruction of damage to data? Please provide details. | *e.g. limited/controlled user access to systems; password controls; server security; retention periods; staff and contractor data protection training* |  |
|  | **Operating System Security** |
|  | What security measures will be used to safeguard the data when in transit to APM? | *e.g. SFTP; password protection; encryption* |  |
|  | Please list all countries in which you will process data before forwarding to APM, and the country in which data will be processed when returned to you by APM (if different).  | *where information is held electronically - please confirm the country/territory where your server is located. Within EEA* |  |
|  | **Organisational Standards** |
|  | What practices does your company follow for disposing of sensitive written or printed material? | *e.g. confidential waste* |  |
|  | Does your company have procedures for reporting security incidents to your clients?  | *e.g. data protection policies/statements* |  |
|  | Is regular information security or data protection training mandatory for your staff? If so, how frequent  |  |  |
|  | **Human Resources Security** |
|  | Is your company registered with the ICO?Has your company self-reported or been reported for any information security incidents (theft, misuse, losses) to the Information Commissioner’s Office in the last 3 years? If so, please describe the incident(s) and the outcome.  |  |  |

**Declaration**

***I confirm that, as a company registered outside EEA (The European Economic Area) or in a country without UK/EU Adequacy Decisions, I accept the Standard Contractual Clauses (SCC), and I have completed Annex B of the SCC in Appendix A.***

***I confirm that the information I have provided on this questionnaire is true and accurate to the best of my ability.***

Company:

Signature:

Position:

Print name:

Date:

**Appendix A**

**Standard contractual clauses for international transfers from controller to controller**

|  |  |
| --- | --- |
| Definitions | For the purposes of the Clauses:‘personal data’, ‘special categories of data/sensitive data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘the Commissioner’ shall have the same meaning as in the UK GDPR  |
|  | ‘the data exporter’ shall mean the controller who transfers the personal data; |
|  | ‘the data importer’ shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018; |
|  | “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements. |
|  | The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses. |
| 1. Obligations of the data exporter |
| The data exporter warrants and undertakes that: |
| 1(a) | The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter. |
| 1(b) | It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses. |
|
| 1(c) | It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established. |
| 1(d) | It will respond to enquiries from data subjects and the Commissioner concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time. |
|
| 1(e) | It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause 3, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the Commissioner. However, the data exporter shall abide by a decision of the Commissioner regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the Commissioner where required. |
|
| 2. Obligations of the data importer |
| The data importer warrants and undertakes that: |
| 2(a) | It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected. |
|
| 2(b) | It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data. |
| 2(c)  | It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the Commissioner where required) if it becomes aware of any such laws. |
|
| 2(d) | It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses |
|
| 2(e) | It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the Commissioner concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause 1(e). |
|
| 2(f) | At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause 3 (which may include insurance coverage). |
| 2(g) | Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion. |
| 2(h) | It will process the personal data, at its option, in accordance with the data processing principles set forth in Annex A.  |
|
| 2(i) | It will not disclose or transfer the personal data to a third party data controller located outside the UK, unless it notifies the data exporter about the transfer andthe third party data controller processes the personal data in accordance with UK adequacy regulations finding that a third country provides adequate protection, orthe third-party data controller becomes a signatory to these clauses, or another data transfer agreement approved by the Commissioner, ordata subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, orwith regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer. |
|
| 3. Liability and third-party rights |
| 3(a) | Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third-party rights under these clauses. This does not affect the liability of the data exporter under the UK GDPR or the DPA 2018. |
|
| 3(b)  | The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses 1(b), 1(d), 1(e), 2(a), 2(c), 2(d), 2(e), 2(h), 2(i), 3(a), 5, 6(d) and 7 against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter’s country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts). |
|
| 4. Law applicable to the clauses |
|  | These clauses shall be governed by the law of the UK country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause 2(h), which shall apply only if so selected by the data importer under that clause. |
| 5. Resolution of disputes with data subjects or the Commissioner |
| 5(a)  | In the event of a dispute or claim brought by a data subject or the Commissioner concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion. |
|
| 5(b) | The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Commissioner. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes. |
|
| 5(c) | Each party shall abide by a decision of a competent court of the data exporter’s country of establishment or of the Commissioner which is final and against which no further appeal is possible. |
|
| 6. Termination |  |
| 6(a) | In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated. |
| 6(b) | In the event that:the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph 6(a);compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;a final decision against which no further appeal is possible of a competent court of the United Kingdom rules that there has been a breach of the clauses by the data importer or the data exporter; ora petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occursthen the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the Commissioner shall be informed where required. In cases covered by 6(i), 6(ii), or 6(iv) above the data importer may also terminate these clauses. |
| 6(c) | Either party may terminate these clauses if new UK adequacy regulations under Section 17A Data Protection Act 2018 are issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer. |
| 6(d) | The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred |
|
| 7. Variation of these clauses |
|  | The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the Commissioner where required. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding additional commercial clauses where required. |
| 8. Description of the transfer |
|  | The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause 1(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the Commissioner where required. Annex B may, in the alternative, be drafted to cover multiple transfers. |
| 9. Allocation of costs |
|  | Each party shall perform its obligations under these clauses at its own cost. |

|  |
| --- |
| Annex A |
| 1. | Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject. |
| 2. | Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed. |
| 3. | Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter. |
| 4. | Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller. |
| 5. | Rights of access, rectification, deletion and objection: data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the Commissioner has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the Commissioner. |
| 6. | Sensitive data: The data importer shall take such additional measures (eg relating to security) as are necessary to protect such sensitive data in accordance with its obligations under Clause 2. |
| 7. | Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes. |
| 8. | Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:(a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and;(ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.or(b) where otherwise provided by the law of the data exporter. |

|  |
| --- |
|  |
| Annex B (for Accredited Provider to complete) |
|  |
| Data subjects |  |
| The personal data transferred concern the following categories of data subjects: |
| Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes their staff.[ ]  Accredited Provider staff including volunteers, agents, temporary and casual workers[ ]  customers and clients (including their staff)[ ]  suppliers (including their staff)[ ]  members or supporters[ ]  shareholders[ ]  relatives, guardians and associates of the data subject[ ]  complainants, correspondents and enquirers;[ ]  experts and witnesses[ ]  advisers, consultants and other professional experts[ ]  patients[ ]  students and pupils [ ]  offenders and suspected offenders[ ]  other (please provide details of other categories of data subjects):       |
| Purposes of the transfer |
| The transfer is made for the following purposes: |
| Standard business purposes, which apply to most businesses and organisations:[ ]  Staff administration, including permanent and temporary staff, including appointment or removals, pay, discipline; superannuation, work management, and other personnel matters in relation to the data exporter’s staff.[ ]  Advertising, marketing and public relations of the data exporter’s own business or activity, goods or services.[ ]  Accounts and records, including * keeping accounts relating to the data exporter’s business or activity;
* deciding whether to accept any person or organisation as a customer;
* keeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter;
* keeping customer records
* records for making ﬁnancial or management forecasts; and
* other general record keeping and information management.

Other activities:[ ]  Accounting and auditing services[ ]  Administration of justice, including internal administration and management of courts of law, or tribunals and discharge of court business. [ ]  Administration of membership or supporter records.[ ]  Advertising, marketing and public relations for others, including public relations work, advertising and marketing, host mailings for other organisations, and list broking.[ ]  Assessment and collection of taxes, duties, levies and other revenue.[ ]  Beneﬁts, welfare, grants and loans administration.[ ]  Canvassing, seeking and maintaining political support amongst the electorate.[ ]  Constituency casework on behalf of individual constituents by elected representatives.[ ]  Consultancy and advisory services, including giving advice or rendering professional services, and the provision of services of an advisory, consultancy or intermediary nature.[ ]  Credit referencing, including the provision of information by credit reference agencies relating to the ﬁnancial status of individuals or organisations on behalf of other organisations.[ ]  Data analytics, including profiling.[ ]  Debt administration and factoring, including the tracing of consumer and commercial debtors and the collection on behalf of creditors, and the purchasing of consumer or trade debts from business, including rentals and instalment credit payments.[ ]  Education, including the provision of education or training as a primary function or as a business activity.[ ]  Financial services and advice including the provision of services as an intermediary in respect of any ﬁnancial transactions including mortgage and insurance broking.[ ]  Fundraising in support of the objectives of the data exporter.[ ]  Health administration and services, including the provision and administration of patient care.[ ]  Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.[ ]  Insurance administration including the administration of life, health, pensions, property, motor and other insurance business by an insurance firm, an insurance intermediary or consultant.[ ]  IT, digital, technology or telecom services, including use or provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software.[ ]  Journalism and media, including the processing of journalistic, literary or artistic material made or intended to be made available to the public or any section of the public.[ ]  Legal services, including advising and acting on behalf of clients.[ ]  Licensing and registration, including the administration of licensing or maintenance of ofﬁcial registers.[ ]  Not-for-proﬁt organisations’ activities, including:* establishing or maintaining membership of or support for a not-for-profit body or association, and
* providing or administering activities for individuals who are either members of the not-for-profit body or association or have regular contact with it.

[ ]  Pastoral care, including the administration of pastoral care by a vicar or other minister of religion.[ ]  Pensions administration, including the administration of funded pensions or superannuation schemes.[ ]  Procurement, including deciding whether to accept any person or organisation as a supplier, and the administration of contracts, performance measures and other records. [ ]  Private investigation, including the provision on a commercial basis of investigatory services according to instruction given by clients.[ ]  Property management, including the management and administration of land, property and residential property, and the estate management of other organisations. [ ]  Realising the objectives of a charitable organisation or voluntary body, including the provision of goods and services in order to realise the objectives of the charity or voluntary body.[ ]  Research in any ﬁeld, including market, health, lifestyle, scientiﬁc or technical research. [ ]  Security of people and property, including using CCTV systems for this purpose.[ ]  Trading/sharing in personal information, including the sale, hire, exchange or disclosure of personal information to third parties in return for goods/services/beneﬁts.[ ]  Other purposes: Provision of online examination, exam results and certification |
| Categories of data |  |
| The personal data transferred concern the following categories of data: |
| [ ]  Personal details, including any information that identiﬁes the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description.[ ]  Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving licence details.[ ]  Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject’s lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organisations.[ ]  Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualiﬁcations, skills, training records, professional expertise, student and pupil records.[ ]  Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, and security records.[ ]  Financial details, including information relating to the ﬁnancial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, beneﬁts, grants, insurance details, and pension information.[ ]  Goods or services provided and related information, including details of the goods or services supplied, licences issued, and contracts.[ ]  Personal data relating to criminal convictions and offences.[ ]  Other (please provide details of other categories of data)      **Recipients**The personal data transferred may be disclosed only to the following recipients or categories of recipients**.**The categories of recipients are: [ ]  Central government[ ]  Charitable and voluntary[ ]  Education and childcare[ ]  Finance, insurance and credit[ ]  General business[ ]  Health[ ]  IT, digital, technology and telecoms[ ]  Justice and policing[ ]  Land and property services[ ]  Legal and professional advisers[ ]  Local government[ ]  Marketing and research[ ]  Media[ ]  Membership association[ ]  Political[ ]  Regulators[ ]  Religious[ ]  Research[ ]  Retail and manufacture[ ]  Social care[ ]  Trade, employer associations, and professional bodies[ ]  Traders in personal data[ ]  Transport and leisure[ ]  Utilities and natural resources[x]  Other – Please add details: Accredited Training Provider |
| Sensitive data The personal data transferred concern the following categories of sensitive data. |
| Personal data which is on, which reveals, or which concerns: [ ]  racial or ethnic origin[ ]  political opinions[ ]  religious or philosophical beliefs[ ]  trade union membership[ ]  genetic data[ ]  biometric data (if used to identify a natural person)[ ]  health[ ]  sex life or sexual orientation[ ]  criminal convictions and offences[ ]  none of the above |
| Contact points for data protection enquiries |
| Data importer contact details:       |
| Data exporter contact details: data.protection@apm.org.uk |