
ico.
Information Commissioner's Office

The standard contractual clauses for international transfers from controller to controller

		Non-legally binding guidance **This column does not form part of the standard contractual clauses, and is not legally binding on either party**
Parties		
Name of the data exporting organisation:	ACT (Administration) Limited and/or The Association of Corporate Treasurers	This is the sender of the restricted transfer of personal data (referred to as the exporter). Insert the full legal name: • If a sole trader, his/her full name. • If a company or limited liability partnership – as formally registered. • If a partnership as set out in the Partnership Deed. • If an unincorporated association, check the establishing document, as to who should enter into this contract.
Address and country of establishment	3rd Floor 150 Minories London EC3N 1LS Country: United Kingdom	This is the contact address for the exporter. It may be the registered address but does not need to be. You must include the country.
Telephone	0207 847 2555	This can be the exporter's general contact telephone number.
Fax		This can be the exporter's general contact fax number. Leave this blank if you do not have a fax.
Email	Contact: Ria Robinson Email: rrobinson@treasurers.org	This can be the exporter's general contact email address.

		Non-legally binding guidance
Other information needed to identify the organisation	ACT (Administration) Ltd: company registration number: 01713927 Association of Corporate Treasurers: RC000859 www.treasurers.org	For UK companies and limited liability partnerships it is helpful to include the following: A company/limited liability partnership (delete as appropriate) registered in England and Wales/Scotland/Northern Ireland (delete as appropriate). Company number: insert number. For companies outside the UK, if possible it is helpful to include the registration number and company of incorporation. A company number is useful as it can help identify a company even if it has changed its name and address.
	(the data **exporter**")	
	And	
Name of the data importing organisation:	The Sponsor	This is the receiver of the restricted transfer of personal data (referred to as the importer). Insert the full legal name: • If a sole trader, his/her full name. • If a company or limited liability partnership – as formally registered. • If a partnership as set out in Partnership Deed. • If an unincorporated association, check the establishing document, as to who should enter into this contract.
Address and Country of establishment	Country:	This is the contact address for the importer. It may be the registered address but does not need to be. You must include the country.

		Non-legally binding guidance
Telephone	Click here to enter text.	This can be the importer's general contact telephone number.
Fax	Click here to enter text.	This can be the importer's general contact fax number. Leave this blank if you do not have a fax.
Email	Click here to enter text.	This can be the importer's general contact email address.
Other information needed to identify the organisation		For UK companies and limited liability partnerships it is helpful to include the following: A company/limited liability partnership (delete as appropriate) registered in England and Wales/Scotland/Northern Ireland (delete as appropriate). Company number: insert number. For companies outside the UK, if possible it is helpful to include the registration number and country of incorporation. A company number is useful as it can help identify a company even if it has changed its name and address.
	(the data **importer**")	
Clause 1. Definitions	For the purposes of the Clauses: (a) '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	A brief overview of these definitions are: "Personal data" Information relating to an identified or identifiable natural person. "Special categories of data" Personal data which relates to an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics

		Non-legally binding guidance
		(where used for ID purposes), health, sex life, or sexual orientation. "Process/processing" In practice means anything which can be done to data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "Controller" A natural or legal person which decides the purposes and means of processing data "Processor" A natural or legal person which is responsible for processing personal data on behalf of a controller "Data subject" The individual that personal data relates to. "The Commissioner" The Information Commissioner, as the UK's independent data protection authority, which we refer to as the 'ICO'.
	(b) 'the data exporter' shall mean the controller who transfers the personal data;	This is the sender/exporter of the personal data, set out on page 1.
	(c) '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;	This is the receiver/importer of the personal data, set out on page 2. The definition clarifies that the importer should not be in a country covered by UK "adequacy regulations". These are UK regulations confirming that the legal

		Non-legally binding guidance
		framework in a country (or territory or sector) provides an adequate level of data protection for personal data. Currently, it includes all EEA countries and all countries (territories or sectors) covered by a European Commission "adequacy decision" You do not need to use the standard contractual clauses if the importer is covered by UK adequacy regulations.
	(d) "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 definition clarifies that these clauses are standalone, and that they do not incorporate the terms of any separate commercial agreement.
	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.	This explains that specific details relating to the restricted transfer are set out in Annex B and form part of the standard contractual clauses. (The parties are required to fill out Annex B and we provide guidance on this below).
I. Obligations of the data exporter	The data exporter warrants and undertakes that:	Section I sets out the general commitments which the exporter gives in relation to the data. These commitments are "warranties", which are promises given in a contract. If the exporter does not comply with a warranty, this may lead to a claim from the importer for damages. In addition, if the exporter does not comply with certain warranties, this may lead to a claim from data subjects. We have indicated below where a data subject can take such action in relation to a clause.
I(a)	The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.	The exporter of the data must make sure that it has complied with the UK GDPR and the DPA

		Non-legally binding guidance
		2018 (and any other UK laws which apply).
I(b)	It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.	The exporter must take steps to make sure that the receiver can comply with its obligations under the standard contractual clauses. In practice, the sender should carry out due diligence on the receiver. This might include asking questions about the receiver's data protection practices, reviewing its security measures and reviewing its privacy policy. Data subjects can take action directly against an exporter who does not comply with its obligations under this clause. The exporter will be responsible in this situation for showing that it has made reasonable efforts to determine that the receiver can comply with its obligations under the standard contractual clauses. Data subject enforcement against: Exporter
I(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.	The exporter must provide copies of relevant data protection laws of its country to the importer, if the importer requests them. For the UK exporter, the applicable data protection law will be the UK GDPR and the DPA 2018. The exporter is not required to provide legal advice to the importer.
I(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	The exporter must respond to enquiries from data subjects or the Commissioner about the processing of the data by the receiver. The exporter must

		Non-legally binding guidance
	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.	provide these responses within a reasonable time. However, the parties can decide that the importer will respond to enquiries instead of the exporter. But if the importer is not able to or is not willing to respond to the enquiry, the exporter must respond instead. Data subjects can take action directly against an exporter who does not comply with its obligations under this clause.
		Data subject enforcement against: Exporter
I(e)	It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, 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.	The exporter must provide a copy of the standard contractual clauses to data subjects who request them. The exporter can remove confidential information beforehand as long as it tells the data subjects in writing that it has done this, and why, and tells data subjects that they can complain to the ICO about the removal. The ICO has power to order the exporter to provide a full copy of the standard contractual clauses to data subjects. The exporter must also provide a copy (without any deletions) of the standard contractual clauses to the ICO, on its request. Data subjects can take action directly against an exporter who does not comply with its obligations under this clause.
		Data subject enforcement against:

		Non-legally binding guidance
	Exporter	
II. Obligations of the data importer	The data importer warrants and undertakes that:	Section II sets out the general commitments which the importer gives in relation to the data. These commitments are "warranties", which are promises given in a contract. If the importer does not comply with a warranty, this may lead to a claim from the exporter for damages. In addition, if the importer does not comply with certain obligations, this may lead to a claim from data subjects. The obligations in this section are intended to make sure that the importer, who is not subject to the UK GDPR, provides the same level of protection for the personal data as required under the UK GDPR.

		Non-legally binding guidance
II(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.	The importer must provide appropriate technical and organisational security measures to protect the personal data. When deciding what measures are appropriate, the importer should think about the type of data (eg how sensitive it is), the type of processing carried out (eg how intrusive it is) and the likely harm which could come to data subjects if the data were lost, stolen or accessed by an unauthorised person. The UK GDPR, the DPA 2018 or the standard contractual clauses themselves, do not specify any particular mandatory security requirements. It is for the parties to decide what is appropriate in any particular case. For more guidance on technical and organisation measures see the ICO Guide to the GDPR. Data subjects can take action directly against an importer who does not comply with its obligations under this clause. Data subject enforcement against: Importer (if the exporter fails to take action against the importer, when requested by the data subject)
II(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.	This clause applies where the importer allows any third-party to access the data. These third parties could be other controllers or processors. If the importer allows a third-party to access the data, it must ensure that these third parties: (i) maintain the confidentiality and security of the data; and (ii)

		Non-legally binding guidance
		only process the data according to the importer's instructions. In practice, it is good practice for these matters should be set out in a written agreement between the importer and the third-party. This clause does not apply if the importer is required by law to allow the third-party access to the personal data.
II(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.	This clause requires the importer to consider its own national laws, when entering into the standard contractual clauses. It should consider whether there are any which would have a substantial adverse effect on the guarantees given under the standard contractual clauses. If the importer later becomes aware of such a law, it must inform the exporter and the exporter must notify the ICO. Data subjects can take action directly against an importer who does not comply with its obligations under this clause.
		Data subject enforcement against: Importer (if the exporter fails to take action against the importer, when requested by the data subject)
II(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	The parties are required to fill in Annex B with various details, including the purposes for which the importer will process the data. The purpose of processing is something which must be agreed between the parties at the outset.

		Non-legally binding guidance
		The importer must only process the data for the purposes which the parties have set out in Annex B. The importer must not process the data for any other purpose. The importer must confirm it is able to give the warranties, and to fulfil its obligations, contained in the standard contractual clauses. Data subjects can take action directly against an importer who does not comply with its obligations under this clause.
		Data subject enforcement against: Importer (if the exporter fails to take action against the importer, when requested by the data subject)
II(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 I(e).	The importer must give the exporter a contact point in its organisation who is authorised to respond to enquiries about the importer's processing of the data. If the importer has a data protection officer, this person might be the appropriate contact point. The importer must cooperate in good faith with the exporter, data subjects and the ICO in relation to enquiries about its processing. The importer must also respond to these enquiries within a reasonable time. If the exporter is legally dissolved (i.e. it no longer exists) or if the parties have agreed, the importer must take on responsibility for providing copies of the standard contractual clauses to data subjects and the Commissioner on request.

		Non-legally binding guidance
		Data subject enforcement against: Importer (if the exporter fails to take action against the importer, when requested by the data subject)
II(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 III (which may include insurance coverage).	The importer must provide the exporter, upon request, with evidence to show it has the financial resources to meet any claims made against it by data subjects for breaches of the standard contractual clauses.
II(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.	The exporter (or a third-party auditor appointed by the exporter) is entitled to audit the importer's processing of the data and compliance with the standard contractual clauses. The exporter must give the importer reasonable notice and the audit must be carried out in normal business hours. The exporter must also make sure that it has obtained any consent it needs to carry out the audit from the relevant regulatory or supervisory authorities in the importer's country.

		Non-legally binding guidance
II(h)	It will process the personal data, at its option, in accordance with: (i) the UK GDPR and DPA 2018, or (ii) the relevant provisions[1] of any UK adequacy regulations pursuant to Section 17A Data Protection Act 2018 or Paras 4,5 & 6 Schedule 21 Data Protection Act 2018, where the data importer complies with the relevant provisions of such adequacy regulations and is based in a country to which such adequacy regulations pertains, but is not covered by such adequacy regulations for the purposes of the transfer(s) of the personal data[2], or (iii) the data processing principles set forth in Annex A.	The importer must choose and agree to apply one of the following data protection standards when processing the data. (i) **The data protection laws of the exporter's country** i.e. the UK GDPR and the DPA 2018. (ii) **UK adequacy regulations (which do not relate to the importer's business or sector) –** if there are adequacy regulations for the country in which the importer is based, but the adequacy regulations only applies to a particular sector – the importer may choose to apply the standards of those adequacy regulations. Currently this may apply only in Canada (where the adequacy regulations only apply to data protected by Canada's Personal Information protection and Electronic Documents Act). If the importer chooses option (ii), it may still need to comply with principle 5 of Annex A (see the guidance on Annex A for more details). (iii) **The processing principles in Annex A to the standard contractual clauses** (set out below). <u>This is the option most</u> frequently chosen by importers.
		Data subject enforcement: Importer (if the exporter fails to take action against the importer,

[1] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the adequacy regulations selected.

		Non-legally binding guidance
		when requested by the data subject)
	Data importer to indicate which option it selects: **(please click in the box next to the chosen option)** (i) ☐ the UK GDPR and DPA 2018, or (ii) ☐ the data processing principles set forth in Annex A.	→ **ACTION:** The importer must indicate whether it has chosen option (i), or (iii). It must also sign or initial this section. **In practice, the majority of importers (particularly small and medium sized businesses) find option (ii) the most straightforward to implement.** This is because all of the processing principles it needs to comply with are set out in Annex A and will not change during the contract period. This is not the case for option (i) . To use option (i), the importer would need keep up to date with the UK GDPR and the DPA 2018.
	Initials of data importer:	→ **ACTION: The importer should sign or initial where indicated.**
II(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 and (i) the third party data controller processes the personal data in accordance with UK adequacy regulations finding that a third country provides adequate protection, or (ii) the third-party data controller becomes a signatory to these clauses, or another data transfer agreement approved by the Commissioner, or (iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer,	This clause applies to disclosures/onward transfers by the importer of the data. If the importer wants to disclose/transfer the data to a third-party controller which is also outside the UK (including in the same country as the importer), it must notify the exporter. The importer must also ensure that one of the 3 options given in this clause applies. These are:

	the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or (iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.	**Non-legally binding guidance** Option 1: the third-party controller processes the data in accordance with UK adequacy regulations (i.e. UK adequacy regulations confirming that a particular country's laws provide an adequate level of protection for personal data). For more information on adequacy regulations, see the section on International Transfers in the ICO Guide to the GDPR. Option 2: the third-party controller signs the standard contractual clauses, or another data transfer agreement approved by the ICO. Option 3: the data subjects have been informed of the following: - the purpose of the transfer to the third-party receiver; - the categories of third-party receivers; - the fact that the countries where the data may go to may have different data protection standards, - and were given the chance to object and didn't. Option 4: if sensitive data (i.e. special categories of data) is being disclosed/transferred, the data subjects have unambiguously consented to the disclosure/transfer. Data subject enforcement against: Importer (if the exporter fails to take action against the importer, when requested by the data subject)

		Non-legally binding guidance
III Liability and third-party rights		Section III sets out which parties will be liable for breaches of the standard contractual clauses. It also sets out data subjects' rights to enforce compliance by the exporter and importer with the standard contractual clauses.
III(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.	This clause provides that each party must compensate the other for damage caused by any breach of the standard contractual clauses. This compensation is only for actual damage suffered by the other party. It does not include punitive damages (damages to punish the party for breaching the standard contractual clauses). The importer and the exporter must compensate data subjects for any damages each of them causes to the data subject by breaching those clauses which are enforceable by a data subject. This is a third-party right; data subjects are not party to the standard contractual clauses but are given the right to enforce certain clauses. These clauses are listed in clause III(b), below, and are highlighted in the relevant sections of this guidance.
		Data subject enforcement against: Exporter Importer (if the exporter fails to take action against the importer, when requested by the data subject)

		Non-legally binding guidance
III(b)	The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII 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).	Data subjects whose personal data is transferred can enforce compliance with those provisions listed, directly against the exporter or importer. If the data subject wants to bring a claim against the importer, they must first ask the exporter to take action against the importer. If the exporter does not take action within a month, the data subject may bring a claim against the importer. A data subject may also bring a claim against an exporter if the exporter did not use reasonable efforts to verify that the importer could comply with the standard contractual clauses. Data subjects may bring claims against either party in the courts of the exporter's country. Data subject enforcement against: Exporter Importer (if the exporter fails to take action against the importer, when requested by the data subject)
IV 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 II(h), which shall apply only if so selected by the data importer under that clause.	The standard contractual clauses are governed by the laws of the UK country in which the data exporter is based, i.e. England and Wales, Scotland or Northern Ireland. However, the UK GDPR will only apply to the importer if the importer selected option (i) in clause II(h).
V Resolution of disputes with data subjects		This clause sets out what the importer and exporter must do when dealing with claims and

		Non-legally binding guidance
or the Commissioner		disputes brought by data subjects or the ICO
V(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.	If a claim or dispute is brought against the exporter or the importer, or both, by a data subject or the ICO, the exporter or importer must inform one another. The exporter and importer must cooperate with each other to try to settle claims/disputes amicably and in good time.
		Data subject enforcement against: Exporter Importer (if the exporter fails to take action against the importer, when requested by the data subject)
V(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.	Data subjects and the Commissioner can require that the exporter and/or importer take part in any non-binding mediation procedure. Non-binding means that no one is bound by any decision or agreement reached. The importer and exporter may participate remotely in those mediation proceedings (for example, by telephone or video-link). The exporter and importer must also consider using other dispute resolution procedures outside of court processes – such as arbitration and binding mediation – which are designed for data protection disputes.
		Data subject enforcement against:

		Non-legally binding guidance
		Exporter Importer (if the exporter fails to take action against the importer, when requested by the data subject)
V(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.	In relation to disputes with data subjects or the ICO, the exporter and importer agree to comply with decisions made by a court in the United Kingdom or the ICO, at the point at which that decision is final and cannot be appealed.
		Data subject enforcement against: Exporter Importer (if the exporter fails to take action against the importer, when requested by the data subject)
VI Termination		Section VI sets out the circumstances in which the parties can terminate the standard contractual clauses and the effect of this termination.
VI(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.	The exporter can suspend the transfer of data to the importer on a temporary basis if the importer breaches its obligations under the standard contractual clauses. Transfers of data can be suspended until the importer corrects the breach or the contract terminated.
VI(b)	In the event that: (i) 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 (a);	This clause sets out the circumstances in which the exporter or importer can terminate the standard contractual clauses.

		Non-legally binding guidance
	(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import; (iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses; (iv) 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; or (v) a 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 occurs then 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 (i), (ii), or (iv) above the data importer may also terminate these clauses.	Circumstances in which the importer and exporter can terminate • ~~Where~~ the transfer has been temporarily suspended for longer than one month under clause VI(a), above. • Where the importer would be in breach of its own national legal or regulatory obligations if it complied with the standard contractual clauses. • Where a court in the United Kingdom or the ICO has ruled that either the importer or exporter has breached the standard contractual clauses. This must be a final decision, which cannot be appealed. Circumstances in which only the exporter can terminate • ~~Where the importer~~ has substantially or persistently breached any of its obligations under the standard contractual clauses. • Where the importer becomes insolvent, goes into administration or liquidation, is being wound up, or any equivalent event in any country is underway.
VI(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.	Either the exporter or the importer may also terminate the standard contractual clauses if new UK adequacy regulations under Section 17A Data Protection Act 2018 are issued. (This is because if the country, territory or sector is considered adequate then "appropriate safeguards", such as the standard contractual clauses, would no longer be required to transfer the data).

		Non-legally binding guidance
VI(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	Even if the standard contractual clauses are terminated, both parties must continue to comply with the clauses for as long as the importer processes the data (even if it is only storing it). Data subject enforcement against: Exporter Importer (if the exporter fails to take action against the importer, when requested by the data subject)
VII 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.	The parties must not amend the standard contractual clauses, although: - they must fill in Annex B and select the relevant option in clause II(h)). - they may make changes which are only to make the Clauses make sense in a UK context (as permitted by Paragraph 7(3) & (4) of Schedule 21 DPA 2018). - they may add commercial clauses, which don't contradict the standard contractual clauses. Data subject enforcement against: Exporter Importer (if the exporter fails to take action against the importer, when requested by the data subject)
VIII 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	The parties must fill in Annex B of the standard contractual clauses with the details of the transfer.

		Non-legally binding guidance
	to a competent regulatory or government agency, or as required under clause I(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.	This clause acknowledges that some of the information which the parties may include in Annex B may be confidential and would not therefore be disclosed to third parties (such as data subjects). It also states that Annex B may be drafted to cover multiple transfers. It says that the parties may add additional annexes to the standard contractual clauses, if they later wish to make additional transfers with different details.
Additional commercial clauses	The parties are able to add additional commercial clauses. When including additional commercial clauses, the parties should ensure that these clauses do not in any way: • overlap with or contradict the standard contractual clauses; • reduce the level of protection which the data importer is required to provide for the personal data; or • reduce the rights of data subjects, or make it any more difficult for them to exercise their rights. If you are unsure whether you can add a particular additional clause or not, you should consider adding it to your main controller – processor agreement, and including a clause in that agreement which says that if there is any conflict between a provision of that agreement and a provision of the standard contractual clauses, the provision in the standard contractual clauses will prevail.	You may add in any additional commercial clauses to the standard contractual clauses. You do not need to add any of these clauses in order to comply with the UK GDPR rules on transfers. When including additional commercial clauses, the parties should ensure that these clauses do not in any way: - overlap with or contradict the standard contractual clauses; - reduce the level of protection which the data importer is required to provide for the personal data; or - reduce the rights of data subjects, or make it any more difficult for them to exercise their rights. We would not recommend including in the standard contractual clauses those terms required under the UK GDPR for a controller- processor contract.

		Non-legally binding guidance In nearly all cases it is better to have those in a separate agreement.
Indemnification	Please click the box if you wish to include the following optional clause: ☐ **Include** Indemnification between the data exporter and data importer: The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the "indemnified party(ies)") promptly notifying the other party(ies) (the "indemnifying party(ies)") of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.".	The standard contractual clauses contain this indemnification clause as an example of an additional clause which you could include. This example is optional – you do not need to include it, and you can choose to add other additional commercial clauses instead of, or in addition to, this example. You can also amend this example. The clause is a mutual indemnity: - the importer indemnifies the exporter; and - the exporter indemnifies the importer; if either of them is in breach of the standard contractual clauses. In this context, an "indemnity" means that the party in breach has to fully compensate the other for its losses which arise from its breach. This may be more than just a standard claim for breach of contract, where damages can be claimed. This clause provides a route for an innocent party to claim back from the other any compensation it has had to pay to a data subject under the standard contractual clauses, arising from a breach by that other party. This example indemnity is wider than that, and provides additional compensation for any breach of the standard contractual clauses.

		Non-legally binding guidance
		Indemnities are often dealt with in the main agreement between the parties.
Dispute resolution	Please click the box if you wish to include the following optional clause: ☐ **Include** Dispute resolution between the data exporter and data importer (the parties may of course substitute any other alternative dispute resolution or jurisdictional clause): In the event of a dispute between the data importer and the data exporter concerning any alleged breach of any provision of these clauses, such dispute shall be finally settled under the rules of arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules. The place of arbitration shall be (insert location, which can be the country of either the importer or exporter or a neutral location: The number of arbitrators shall be (insert number of arbitrators):	The standard contractual clauses contain this as an example of an optional additional clause. It sets out what will happen if there is a dispute between the importer and the exporter in relation to the standard contractual clauses. If the parties are unable to resolve the dispute between themselves, they will settle the dispute using the arbitration rules of the International Chamber of Commerce. The exporter and importer need to agree where the arbitration will take place. It could be the country of either the exporter or importer or a neutral location. The exporter and importer also need to decide on the number of arbitrators. Arbitration can be just as expensive as using the courts. It can be helpful for international disputes. So, before you include this clause you should consider taking appropriate professional advice
Allocation of costs	Please click the box if you wish to include the following optional clause: ☐ **Include** Each party shall perform its obligations under these clauses at its own cost.	The standard contractual clauses contain this as an example of an optional additional clause. It explains that each party is responsible for its own costs of complying with the standard contractual clauses.
Extra termination clause	Please click the box if you wish to include the following optional clause: ☐ **Include** Extra termination clause:	The standard contractual clauses contain this as an example of an optional additional clause. It sets out requirements on the importer to return the personal data to the exporter or destroy it (if the exporter asks it to), if the

		Non-legally binding guidance
	In the event of termination of these clauses, the data importer must return all personal data and all copies of the personal data subject to these clauses to the data exporter forthwith or, at the data exporter's choice, will destroy all copies of the same and certify to the data exporter that it has done so, unless the data importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The data importer agrees that, if so requested by the data exporter, it will allow the data exporter, or an inspection agent selected by the data exporter and not reasonably objected to by the data importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours." Please click the box if you wish to include the following optional clause: ☐ **Include** The Clauses take priority over any other agreement between the parties, whether entered into before or after the date the Clauses are entered into. Unless the Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Clauses are entered into, will amend the terms or the effects of the Clauses, or limit any liability under the Clauses, and no term of any such other agreement should be read or interpreted as having that effect.	standard contractual clauses are terminated. This clause is provided by the ICO, as it may be helpful to you. Please review it carefully and only include it if you think it is appropriate for your circumstances. The intended effect of the clause is to make sure that you and the other party do not inadvertently amend the standard contractual clauses or limit your liability. If you did, then you would risk not being able to rely on the standard contractual clauses for compliance with the UK GDPR rules on restricted transfers. The clause allows you the freedom to amend the standard contractual clauses, but only if you expressly refer to them. If you are going to amend the standard contractual clauses, we would always recommend you seek professional legal advice. Any amendment runs the risk that the standard contractual
Priority of standard contractual clauses		

	Non-legally binding guidance clauses will not comply with the UK GDPR rules on restricted transfers.
On behalf of the data exporter: Name (written out in full): *Ria Robinson.* Position: *Director of Membership and Governance* Address: *The ACT (Administration) Ltd, 69 Leadenhall Street, EC3A 2BG, UK* Other information necessary in order for the contract to be binding (if any): *Click here to enter text.* Signature:	→ **ACTION**: The exporter should fill in this section with the: • Full name of the person signing. This must be a person who is authorised to enter into contracts on behalf of the exporter. • Their position. • Their business addresses. And sign where indicated.
On behalf of the data importer: Name (written out in full): *The Sponsor for ACTAC – name .* Position: *Click here to enter text.* Address: Other information necessary in order for the contract to be binding (if any): Signature:	→ **ACTION**: The importer should fill in this section with the: • Full name of the person signing. This must be a person who is authorised to enter into contracts on behalf of the importer. • Their position. • Their business addresses. And sign where indicated.
Date of the Standard Contractual Clauses:	Do not date the standard contractual clauses until both the exporter and importer have signed. It can be the date of the last signature, or a later date if that is agreed by the exporter and importer.

		Non-legally binding guidance
Annex A		Annex A sets out the data processing principles which the importer must comply with if it selects this option in clause II(h) above.
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.	The importer can only use, disclose and make onward transfers of the data for the purposes listed in Annex B, or for other purposes which have been agreed to by the data subject after the standard contractual clauses have been entered into. This principle broadly aligns with Article 5(1)(b) of the UK GDPR which sets out the principle of purpose limitation. It requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In practice, the parties must be clear on how the importer intends to use the data, and this should be recorded in appropriate detail in Annex B. If the importer later wishes to use the data for a different purpose, this will only be possible if the data subject agrees to this different purpose.
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.	The importer should ensure that the data is accurate and kept up to date, and that the personal data transferred to it is adequate, relevant and not excessive in relation to the purpose for which it is processed. This principle broadly aligns with Article 5(1)(c) of the UK GDPR

		Non-legally binding guidance
		which sets out the principle of data minimisation. It requires that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. In practice, the importer should only request from the exporter, and the exporter should only transfer data to the importer which is necessary for the importer's purpose. Data should not be transferred "just in case" it may be useful in future.
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.	The importer must provide data subjects with information about how their data will be processed. The importer is not required to do this if the information has already been provided to the data subject by the exporter. This principle broadly ties in with part of Article 5(1)(a) of the UK GDPR. This requires data to be processed fairly, lawfully and in a transparent manner in relation to the data subject. What is "necessary to ensure fair processing" is a matter of interpretation. A court may look to the UK GDPR to assess what is considered appropriate information to be provided in relation to the use of the personal data by the importer. It may be prudent to look at the list of requirements in Art 14 of UK GDPR as a starting point. The key elements being: - the identity and contact details of the importer (and where there is one, the importer's representative and data protection officer); - the purposes of the processing; - the categories of personal data concerned;

		Non-legally binding guidance - recipients or categories of recipients of the personal data from the importer; - the period for which the personal data is to be held by the importer, or the criteria used to decide that period; - the existence of the data subject's rights of access, rectification, deletion and objection (as set out below); - the right to complain to the ICO; and - the existence of automated decision making, meaningful information about the logic involved in that, and the significance and envisaged consequences of such processing.
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.	The importer must provide appropriate technical and organisational security measures for the personal data which is being transferred. This principle broadly aligns with the integrity and confidentiality principle in Article 5(1)(f) of the UK GPDR. This requires personal data to be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. For more guidance on technical and organisation measures see the ICO's Guide to the GDPR. Neither the UK GDPR nor the standard contractual clauses set out any mandatory security measures. It is for the importer to decide what is appropriate. In doing so, the importer should think about the type of data (eg how confidential or sensitive it is), the type of processing

		Non-legally binding guidance
		carried out (eg how intrusive it is) and the likely harm which could come to data subjects if the data were lost, stolen or accessed by an unauthorised person.
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.	The importer must provide data subjects with rights of access, rectification, deletion and objection. Rights of access Broadly speaking, "rights of access" means the right of the data subject to be given access to their personal data which is being processed, and often to receive a copy. The standard contractual clauses are not intended to grant rights of access which go beyond those in the law of the data exporter's country. For a UK exporter, rights of access are governed by the UK GDPR and DPA 2018. An importer who receives data from the UK should therefore look at the rights of access and various exemptions in the UK GDPR and the DPA 2018 when assessing how to respond to a request. The ICO's guidance on data subject rights can be found in its Guide to GDPR. This principle sets out circumstances in which the importer does not need to provide the data subject with rights of access. The importer does not have to provide the right of access if a request is "manifestly abusive". This includes where the data subject has made a large number of requests or has made repetitive or systematic requests.

		Non-legally binding guidance
		The importer can also refuse access if it would be likely to seriously harm the interests of the importer (or other organisations dealing with the importer), and these interests are not overridden by those of the data subject. If the importer is planning to refuse access on this basis, then it must obtain the approval of the ICO. The principle also provides that a data subject does not have to be told the sources of the personal data if this is not possible with a reasonable level of effort, or if it would violate the rights of another person. Rectification and deletion Data subjects have the right to have the importer rectify, amend or delete their personal data if it is inaccurate or if the importer has processed it in breach of the principles in Annex A. The importer can request further information from the data subject if it has a very good reason to believe that the request may not be legitimate. This may include requesting confirmation of the data subject's identity, eg by asking for a copy of a passport or national identity document. If a data subject makes a request to have their data rectified, amended or deleted, the importer must tell any third parties to whom it has disclosed the data of such request, unless this involves disproportionate effort. Right to object A data subject has the right to object to the processing of his/her data if there are

		Non-legally binding guidance
		compelling legitimate grounds in a particular situation. If the importer wants to continue processing the data, it must show that the grounds are not compelling. If the importer does not stop processing, following an objection by the data subject, the data subject can raise this with the ICO.
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 II.	The importer must provide additional protection, including by security measures, to protect "sensitive data". Due to the way the definitions operate, sensitive data is equivalent to "special categories of data" in the UK GDPR and are listed in the Definitions section above. In practice, importers should ensure that enhanced security measures are in place for this data. These could include stricter access controls on a need to know basis, pseudonymisation and/or limited retention periods.
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.	The importer must provide procedures allowing data subjects to opt out, at any time, of the use of their data for direct marketing purposes (if it is used for that purpose). This principle aligns with data subjects' right under Article 21(3) of the UK GDPR. This provides that if a data subject objects to its data being used for direct marketing purposes, then the data controller must stop using the data for that purpose.
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	This principle restricts the ability of the importer to make automated decisions. Automated decisions are decisions which are

		Non-legally binding guidance
	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.	- made by the importer/exporter which: - produce legal effects on a data subject or significantly affect them; - are based solely on automated processing of personal data; and - are intended to evaluate certain personal aspects relating to them, eg performance at work, creditworthiness, reliability, conduct etc. Automated decisions could therefore include decisions such as automatic refusals of an online credit application or e-recruiting practices without any human intervention. Automated decisions can only be made if: - they are made by the importer in entering into or performing a contract with the data subject, and the data subject is given the chance to discuss the results and make representations; or - the law in the country of the data exporter permits particular automated decisions. In the UK this would be under the UK GDPR and DPA 2018. For more information on this, please see our Guide to the UK GDPR.

		Non-legally binding guidance
# Annex B		
		→ **ACTION**: This Annex must be appropriately completed for the standard contractual clauses to be an appropriate safeguard and allow restricted transfers of personal data under the UK GDPR. Instructions for using the checklists: To help you completing this Annex, we have provided optional checklists. These are just suggestions. You do not need to use the checklists at all. You can amend the contents of any category, as you consider best reflects the international transfer of personal data, including to add specific details. If you do not fit into any of these types, you may add your own description at the end of the checklist.
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. ☐ 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		→ **ACTION:** The parties should list the categories of data subject. Instructions: Think about who the personal data being transferred is about, and click in the box next to all of the categories of data subjects which are included in the personal data being transferred. You may make appropriate amendments or add specific details to any of the categories or click the "other" box and add your own categories at the end.

		Non-legally binding guidance
☐ 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.		→ **ACTION:** The parties should list the purposes for which the transfer of data is made Instructions: Think about the personal data being transferred and why the data exporter and data importer are making the transfer. Click in the box next to all of the purposes which apply. You may make appropriate amendments or add specific details to any of the purposes or click the "other" box and add your own purposes at the end.

	Non-legally binding guidance
☐ 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	

	Non-legally binding guidance
• 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 (please provide details):	
Categories of data — *The personal data transferred concern the following categories of data.*	
☐ Personal details 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.	→ **ACTION:** The parties should list the categories of personal data being transferred. Instructions: Think about <u>what</u> the personal data being transferred is about and click the box next to all of the categories of personal data which are being transferred You may make appropriate amendments or add specific details to any of the categories

		Non-legally binding guidance
☐ 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)		or click "other" and add your own categories at the end.
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		→ **ACTION:** The parties should list the recipients or categories of recipients to whom the importer may forward or disclose the data. These may be processors (eg service providers) or other controllers (eg legal advisers or regulatory bodies). Instructions: Think about <u>what</u> types of business or organisation the data importer might need to pass on the transferred personal data to. Click in the box next to all the types of recipient which apply. You may make appropriate amendments or add specific details to any of the categories or click the "other" box and add your own categories at the end.

		Non-legally binding guidance
☐ 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 ☐ Other – Please add details:		
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		→ **ACTION:** Include a list of any of the categories of sensitive data which are being transferred: For completeness, and to ensure the clauses work under the GDPR, we have included the new special categories of data added by the GDPR and criminal convictions and offences data. _____ Instructions: Think about the set of personal data being transferred and click the box next to any which are included.
Contact points for data protection enquiries	*Contact points for data protection enquiries*	→ **ACTION:** The exporter and the importer should provide a contact point for data protection enquiries.

	Non-legally binding guidance
Data importer contact details:	If the parties have data protection officers, these people may be the appropriate contact points. You do not need to name individuals if you do not consider that to be appropriate. This can simply be a job title or team, and a generic email. For example: SCC Data Protection Officer: dataprotectionenquiries@sccs.com
Data exporter contact details:	