PAUL HASTINGS

Summary of Provisions in New Standard Contractual Clauses for Transfers of Personal Data to Third Parties

June 2021

Clause / Annex	Module	Description of Clause / Annex (see specific clause in SCCs for full provision)	Can a Data Subject invoke clause as a third party beneficiary?
1 (Purpose and Scope)	All	The purpose of the SCCs is to comply with the GDPR on the transfer of personal data to a third country. The data exporter and data importer agree to the SCCs and the SCCs apply with respect to the transfer specific in Annex I.B.	No
2 (Effect and invariability of the Clauses)	All	SCCs set out appropriate safeguards pursuant to Articles 46(1) and 46(2)(c) of the GDPR, provided they are not modified except to select the appropriate module(s) or to add/update information to the Appendix. Parties may incorporate SCCs into a wider contract.	No
3 (Third-party Beneficiaries)	All	Data subjects may invoke or enforce particular clauses under the SCCs against with the data exporter and/or data importer. See the fourth column of this table for further information.	No
4 (Interpretation)	All	Terms defined in the GDPR have the same meaning. SCCs shall be read in the light of the GDPR and shall not be interpreted in a way that conflicts with the GDPR.	Yes
5 (Hierarchy)	All	SCCs prevail over conflicting provisions of related agreements.	Yes
6 (Description of transfer(s))	All	Details of transfers are specified at Annex I.B.	No
7 (Docking clause)	All	With agreement from the existing parties, third parties can accede to the SCCs as either a data importer or data exporter by completing and signing the Appendix. This clause is optional – the parties can decide whether to include or not.	No
8 (Obligations of the parties)	All	The data exporter warrants it has used reasonable efforts to determine that the data importer is able to satisfy its obligations under the SCCs.	Yes
8.1 (Purpose limitation)	1	The data importer can only process the personal data for the purposes stated in Annex I.B, unless it satisfies one of the exemptions listed in this clause (e.g. obtained prior consent of data subject).	Yes
8.2 (Transparency)	1	• The data importer must inform the data subjects either directly or through the data exporter of certain information: its identity and contact details; the categories of personal data it will process; the right to obtain a copy of the SCCs; and details of any intended onward transfers. • This is subject to certain exceptions: the information has already been provided, possibly by the data exporter (e.g. in their privacy notice); or providing the information would be impossible or would involve disproportionate effort (this is subject to making the information publically available, e.g. in a privacy notice on a website). • The data subject can request a copy of the SCCs, including the relevant Appendix, and the parties must comply free of charge. The Appendix details can be redacted by the parties for confidentiality reasons but such redactions must be summarised if redaction would have an adverse effect on understanding the Appendix and reasons for the redactions must be provided.	Yes

Clause			Description	Included
8.3 (Accuracy and data minimisation)	1	• Parties must ensure the personal data is accurate and, where necessary, kept up to date. Any inaccurate personal data held by the importer should be deleted. • The data importer shall ensure the data is adequate, relevant and limited to what is necessary for the relevant purposes of processing.	Yes
8.4 (Storage limitation)	1	The data importer shall not retain the personal data for longer than is necessary for the purposes for which it is processed, and technical and organisations measures shall be implemented to ensure compliance with this.	Yes
8.5 (Security of processing)	1	• The data exporter (during transmission only) and the data importer shall each implement appropriate technical and organisation measures to ensure the security of the personal data against personal data breaches. Such measures must be agreed and documented Annex II. • The data importer shall ensure that the persons (e.g. employees) authorised to access the data are subject to confidentiality. • If the data importer suffers a personal data breach, it shall take appropriate measures to address it, including mitigating possible adverse effects. If such a breach is likely to result in a risk to the rights and freedoms of the individuals (i.e. satisfies the GDPR requirement for reporting the breach to authorities), the data importer must notify the data exporter and the competent supervisory authority (see Clause 13) without undue delay and provide certain details regarding the breach. If such a breach is likely to result in a <u>high</u> risk to the rights and freedoms of individuals (i.e. satisfies the GDPR requirement for reporting the breach to the affected individuals), the data importer must also notify the affected individuals without undue delay. The data exporter may be required to assist in such notification.	Yes, except for Cl 8.5(e)
8.6 (Sensitive data)	1	If the data importer processes any special category personal data processed, it shall implement specific restrictions and/or additional safeguards that are reflective of the nature of the personal data and the risks associated e.g. additional security measures.	Yes
8.7 (Onwards transfers)	1	The data importer can only transfer the personal to a third party located outside the EU (including in the same country as the importer) if the third party agrees to be bound by the SCCs or the transfer would otherwise be in accordance with certain of the transfer provisions of the GDPR (e.g. the third party was in a country deemed adequate or one of the derogations <u>listed</u> in the clause applies).	Yes
8.8 (Processing under authority of the data importer)	1	The data importer shall ensure that any person acting under its authority only processes the personal data based on its instructions (e.g. employees or processors).	Yes
8.9 (Documentation and compliance)	1	• Both parties must be able to demonstrate compliance with the applicable provisions of the SCCs. • The data importer shall maintain documentation of its processing activities which it can make available to the competent supervisory authority on request (see Clause 13).	Yes, except for Cl 8.9(b)
8.1 (Instructions)	2	The data importer shall only process the personal data on the documented instructions of the data exporter. The data importer must immediately inform the data exporter if it cannot comply with the instructions.	Yes, except for Cl 8.1(b)
8.2 (Purpose limitation)	2	The data importer can only process the data for the purposes stated in Annex I.B, unless it receives further instructions from the data exporter.	Yes
8.3 (Transparency)	2	The data subject can request a copy of the SCCs, including the Appendix related to the specific transfer, and the data exporter must comply free of charge. The Appendix details can be redacted for confidentiality reasons but such redactions must be summarised if redaction would have an adverse effect on understanding the Appendix and reasons for the redactions must be provided.	Yes
8.4 (Accuracy)	2	If the data importer becomes aware that the personal data is inaccurate, or is out of date, it must inform the data exporter without undue delay, and cooperate with the exporter to erase or rectify the personal data.	Yes

8.5 (Duration of processing and erasure or return of data)	2	• The data importer shall only process the personal data for the duration specified by the parties in Annex I.B at the end of which time, the data importer shall delete or return the personal data (based on the choice of the data exporter) and certify it has done so. • If the data importer is subject to local laws which do not permit this to happen, the data importer warrants it will continue to comply with the SCCs and will only process the personal data in order to comply with the relevant local laws.	Yes
8.6 (Security of processing)	2	• The data exporter (during transmission only) and the data importer shall each implement appropriate technical and organisation measures to ensure the security of the personal data against personal data breaches. The parties shall in particular consider encryption or pseudonymisation. In the case of pseudonymisation, the additional information for attributing to the personal data shall remain under the exclusive control of the data exporter (where possible). In complying with this obligation, the importer should at least comply with the measures specified in Annex II. • The data importer shall grant access only to those members of its personnel that are strictly necessary for the implementation, management and monitoring of the relevant contract, and shall ensure that the persons authorised to access the personal data are subject to confidentiality. • If the data importer suffers a personal data breach, it shall take appropriate measures to address it, including mitigating possible adverse effects. The data importer must notify the data exporter without undue delay and provide certain details regarding the breach. The data importer will cooperate with and assist the data exporter with regards the data exporter's compliance with the GDPR, e.g. notification to the supervisory authority.	Yes
8.7 (Sensitive data)	2	If the data importer processes any special category data processed, it shall implement specific restrictions and/or additional safeguards that are described in Annex I.B.	Yes
8.8 (Onward transfers)	2	The data importer is only permitted to disclose the personal data to a third party on the document instructions of the data exporter. In addition, the personal data can only be transferred to a third party located outside the EU (including in the same country as the importer) if the third party agrees to be bound by the SCCs or the transfer would otherwise be in accordance with certain of the transfer provisions of the GDPR (e.g. the third party was in a country deemed adequate or one of the derogations listed in the clause applied).	Yes
8.9 (Documentation and compliance)	2	• The data importer shall promptly and adequately deal with enquiries from the data exporter related to the processing. • Both parties must be able to demonstrate compliance with the applicable provisions of the SCCs. • The data importer shall maintain documentation of its processing activities. It shall also make available to the data exporter all documentation and information necessary to demonstrate its compliance with the SCCs and allow for and contribute to audits (including inspections of properties) of the processing activities at reasonable intervals of if there are indications of non-compliance. The audit may be undertaken by the data exporter or an independent auditor appointed by the data exporter. • Both parties must be able to make any of the information required by this clause available to the competent supervisory authority on request.	Yes, except for Cl 8.9(a), (c), (d) & (e)

8.1 (Instructions)	3	• The data exporter must inform the data importer that the data importer is a processor under the instructions of its controller(s). • The data importer shall only process the data on the documented instructions of the controller, as communicated by the data exporter, and any additional instructions from the data exporter (which must not conflict with instructions from the controller). • The data importer must immediately inform the data exporter if it is unable to follow any of the instructions. In such an instance, the data exporter must immediately notify the controller. • The data exporter warrants it has imposed the same data protection obligations on the data importer as between the controller and the data exporter.	Yes, except for Cl 8.1(a), (c) & (d)
8.2 (Purpose limitation)	3	The data importer can only process the personal data for the purposes stated in Annex I.B, unless it receives further instructions from controller (via the data exporter) or from the data exporter.	Yes
8.3 (Transparency)	3	The data subject can request a copy of the SCCs, including the Appendix related to the specific transfer, and the data exporter must comply free of charge. The Appendix details can be redacted for confidentiality reasons but such redactions must be summarised if redaction would have an adverse effect on understanding the Appendix and reasons for the redactions must be provided.	Yes
8.4 (Accuracy)	3	If the data importer becomes aware that the personal data is inaccurate, or is out of date, it must inform the data exporter without undue delay, and cooperate with the exporter to erase or rectify the personal data.	Yes
8.5 (Duration of processing and erasure or return of data)	3	• The data importer shall only process the personal data for the duration specified by the parties in Annex I.B at the end of which time, the data importer shall delete or return the personal data (based on the choice of the data exporter) and certify it has done so. • If the data importer is subject to local laws which do not permit this to happen, the data importer warrants it will continue to comply with the SCCs and will only process the personal data in order to comply with the relevant local laws.	Yes
8.6 (Security of processing)	3	• The data exporter (during transmission only) and the data importer shall each implement appropriate technical and organisation measures to ensure the security of the personal data against personal data breaches. The parties shall in particular consider encryption or pseudonymisation. In the case of pseudonymisation, the additional information for attributing to the personal data to a specific data subject shall remain under the exclusive control of the data exporter (where possible). In complying with this obligation, the importer should at least comply with the measures specified in Annex II. • The data importer shall grant access only to those members of its personnel that are strictly necessary for the implementation, management and monitoring of the relevant contract, and shall ensure that the persons authorised to access the personal data are subject to confidentiality. • If the data importer suffers a personal data breach, it shall take appropriate measures to address it, including mitigating possible adverse effects. The data importer must notify the data exporter, and where possible and feasible the controller too, without undue delay and provide certain details regarding the breach. The data importer will cooperate with and assist the data exporter with regards the data exporter's compliance with the GDPR, e.g. notification to the controller so the controller may, in turn, notify a supervisory authority or the data subjects.	Yes
8.7 (Sensitive data)	3	If the data importer processes any special category personal data processed, it shall implement specific restrictions and/or additional safeguards that are described in Annex I.B.	Yes
8.8 (Onward transfers)	3	The data importer is only permitted to disclose the personal data to a third party on the document instructions of the controller, as communicated by the data exporter. In addition, the personal data can only be transferred to a third party located outside the EU (including in the same country as the importer) if the third party agrees to be bound by the SCCs or the transfer would otherwise be in accordance with certain of the transfer provisions of the GDPR (e.g. the third party was in a country deemed adequate or one of the derogations listed in the clause applied).	Yes
8.9 (Documentation and compliance)	3	• The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller related to the processing. • Both parties must be able to demonstrate compliance with the applicable provisions of the SCCs. • The data importer shall maintain documentation of its processing activities. It shall also make available to the data exporter all documentation and information necessary to demonstrate its compliance with the SCCs (which the data exporter can provide to the controller) and allow for and contribute to audits (including inspections of properties) of the processing activities at reasonable intervals of if there are indications of non-compliance. The audit may be undertaken by the data exporter or an independent auditor appointed by the data exporter. • The controller may request the data exporter undertakes an audit. In such instances, the data exporter will make the results available to the controller. • Both parties must be able to make any of the information required by this clause available to the competent supervisory authority on request.	Yes, except for Cl 8.9(a), (c), (d), (e), (f) & (g)

8.1 (Instructions)	4	• The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller, and shall immediately inform the data importer if it is unable to comply with such instructions. • The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under the GDPR. • At the end of the provision of the processing, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify that the data exporter has done so, or return to the data importer the all personal data processed on its behalf and delete existing copies.	Yes, except for Cl 8.1 (b)
8.2 (Security of processing)	4	• The parties shall each implement appropriate technical and organisation measures to ensure the security of the personal data against personal data breaches. • The data exporter shall assist the data importer in ensuring appropriate security of the personal data. In case of a personal data breach concerning the personal data processed by the data exporter, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach. • The data exporter shall ensure that the persons (e.g. employees) authorised to access the personal data are subject to confidentiality.	Yes
8.3 (Documentation and Compliance)	4	• The parties shall be able to demonstrate compliance with the SCCs. • The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under the SCCs and all for and contribute to audits.	Yes, except for Cl 8.3(b)

9 (Use of sub-processors)	2	• Options:
		
		   1. <u>Specific authorisation</u>: The data importer can only sub-contract any of its processing if the data exporter provides its prior specific written authorisation. The data importer must submit a request for authorisation with a specific period of time (which the parties are permitted to agree in the SCCs). The list of sub-processers authorised is in Annex III, and the parties shall keep this list up to date.
		
		   2. <u>General written authorisation</u>: The data importer has the general authorisation of the data exporter for the engagement of sub-processors from an agreed list. The data importer must inform the data exporter in writing of any intended changes to the list with a specific period of time (which the parties are permitted to agree in the SCCs) in advance of engagement. During this time, the data exporter can object to the change.
		
		• The data importer must engage the sub-processor by way of a written contract that provides for the same data protection obligations as those binding the data importer under these SCCs. The SCCs note that this requirement may be satisfied by the sub-processor acceding to the SCCs under the appropriate module (in accordance with Clause 7).
		
		• At the data exporter's request, the data importer shall provide a cope of any such agreements with sub-processors. The data importer is permitted to redact confidential information.
		
		• The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations.
		
		• The data importer shall agree a third-party beneficiary clause with the sub-processor with the following meaning: in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent, the data exporter has the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.
			Yes, except for Cl 9(a), (c), (d) & (e)

9 (Use of sub-processors)	3	• Options:
		
		   1. <u>Specific authorisation</u>: The data importer can only sub-contract any of its processing if the controller (i.e. not the data exporter) provides its prior specific written authorisation. The data importer must submit a request for authorisation with a specific period of time (which the parties are permitted to agree in the SCCs) to the controller. If authorised, the data importer shall inform the data exporter. The list of sub-processers authorised is in Annex III, and the parties shall keep this list up to date.
		
		   2. <u>General written authorisation</u>: The data importer has the general authorisation of the controller (i.e. not the data exporter) for the engagement of sub-processors from an agreed list. The data importer must inform the controller in writing of any intended changes to the list with a specific period of time (which the parties are permitted to agree in the SCCs) in advance of engagement. During this time, the controller can object to the change. The data importer shall inform the data exporter of the engagement of the sub-processors.
			Yes, except for Cl 9(a), (c), (d) & (e)

9 (Use of sub-processors) **Continued**	3	• The data importer must engage the sub-processor by way of a written contract that provides for the same data protection obligations as those binding the data importer under these SCCs. The SCCs note that this requirement may be satisfied by the sub-processor acceding to the SCCs under the appropriate module (in accordance with Clause 7). • At the controller's or the data exporter's request, the data importer shall provide a copy of any such agreements with sub-processors. The data importer is permitted to redact confidential information. • The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations. • The data importer shall agree a third-party beneficiary clause with the sub-processor with the following meaning: in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent, the data exporter has the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the data.	
10 (Data subject rights)	1	• Data importer (with assistance of the data exporter if relevant) shall deal with any enquiries or requests from data subjects related to their processing of their personal data or their rights under the SCCs within one month of receipt. This period can be extended by maximum of 2 months if necessary considering the complexity and number of requests. • Clause 10 creates contractual obligations of the rights granted under the GDPR e.g. right of access, erasure, rectification, or not be subject to a decision made solely on automated decision making. • If the requests from a data subject are excessive, in particular because of their repetitive character, the data importer may charge a reasonable free or refuse to act on the request. • The data importer may refuse a request if permitted under the laws of the country of destination and is necessary and proportionate in a democratic society. • If data importer intends to refuse a request, it must inform the data subject of the reasons and the possibility of making a complaint to the competent supervisory authority.	Yes
10 (Data subject rights)	2	• If data importer receives a request from a data subject, it must notify the data exporter promptly and must not respond to the request (unless authorised to do so by the data exporter). • The data importer shall assist the data exporter in fulfilling its obligations to respond to the request.	Yes
10 (Data subject rights)	3	• The data importer shall promptly notify the data exporter and, where appropriate, the controller, of any request received from a data subject and must not respond to the request (unless authorised to do so by the controller). • The data importer shall assist the controller (where appropriate in cooperation with the data exporter) in fulfilling its obligations to respond to the request.	Yes
10 (Data subject rights)	4	Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under the GDPR.	Yes
11 (Redress)	All	• The data importer shall inform data subjects in a transparent and easily accessible format of a contact point authorised to handle complaints. This could be through an individual notice or on its website. • <u>Optional provision</u>: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject.	Yes
11 (Redress)	1,2,3	• If there is a dispute between a party and a data subject, the party shall use its best efforts to resolve the issue amicably in a timely fashion. The parties shall keep each other informed of such disputes and, where appropriate, cooperate in resolving them. • Where a data subject invokes a third-party beneficial right the data importer shall accept the decision of the data subject to lodge a complaint with a supervisory authority in the Member States of his habitual residence or place of work, or the competent supervisory authority (if different) and to refer the dispute to the competent courts (see Clause 18). • The data importer shall abide by a decision that is binding under the applicable EU or Member State law.	Yes

12 (Liability)	1&4	• Each party shall be liable to the other parties for any damages it causes to the other parties by breaching the SCCs.	Yes, except for Module 1 Cl 12(a) & (d)
		• Each party shall be liable to each data subject for any material or non-material damages that the party causes by breaching one of the third party beneficiary clauses. In such instances, the data subject is entitled to compensation.	
		• Where more than one party is responsible for data subject damage, such parties shall be jointly and severally liable. The data subject is entitled to bring an action in court against of these parties. If one party is held liable in this instance, it shall be entitled to claim back from the other party any part of the compensation they were responsible for.	
		• The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.	
12 (Liability)	2&3	• Each party shall be liable to the other parties for any damages it causes to the other parties by breaching the SCCs.	Yes, except for Cl 12(a), (d) and (f)
		• The data importer shall be liable to each data subject for any material or non-material damages that the data importer (or its sub-processor) causes by breaching one of the third party beneficiary clauses. In such instances, the data subject is entitled to compensation.	
		• Notwithstanding data importer liability, the data exporter shall be liable to each data subject for any material or non-material damages that the data exporter or data importer (or its sub-processor) causes by breaching one of the third party beneficiary clauses. In such instances, the data subject is entitled to compensation. If the data exporter is held liable for damages caused by data importer, it shall be entitled to claim back such damages.	
		• Liability under this clause is without prejudice to any liability under the GDPR, including if the data exporter is processor acting on behalf of a controller.	
		• Where more than one party is responsible for data subject damage, such parties shall be jointly and severally liable. The data subject is entitled to bring an action in court against of these parties. If one party is held liable in this instance, it shall be entitled to claim back from the other party any part of the compensation they were responsible for.	
		• The data importer may not invoke the conduct of a sub-processor to avoid its own liability.	
13 (Supervision)	1,2,3	• 3 options determined by fact:	No
		o <u>The data exporter is established in a Member State</u>: The supervisory authority with responsibility for ensuring the data exporter's compliance with the GDPR as regards the transfer is the competent supervisory authority and should be named in Annex I.C.	
		o <u>The data exporter is not established in a Member State but within scope of GDPR pursuant to Article 3(2) and has an EU representative</u>: The supervisory authority where the EU representative is established is the competent supervisory authority and should be named in Annex I.C.	
		o <u>The data exporter is not established in a Member State but within the scope of the GDPR pursuant to Article 3(2) but does not have an EU representative</u>: The supervisory authority of one of the Member States in which data subjects whose personal data is transferred under the SCCs is the competent supervisory authority and should be named in Annex I.C.	
		• The data importer agrees to submit to the jurisdiction of and cooperate with the competent supervisory authority including responding to enquiries, submitting to audits etc.	
14 (Local laws and practices affecting compliance with the Clauses)	All	Note, only applies to module 4 where the EU processor combines the personal data received from a third country-controller with personal data collected by the processor in the EU	Yes
		• Parties warrant they have no reason to believe the laws and practices in the third country prevent the data importer from fulfilling its obligations under the SCCs, including any requirements to disclose the personal data to public authorities.	
		• In providing the warranty, the parties have taken account of the following elements:	
		o The specific circumstances of the transfer;	
		o The laws and practices of the third country relevant in light of the transfer;	
		o Any relevant contractual, technical or organisational safeguards in place to supplement the SCCs.	

14 (Local laws and practices affecting compliance with the Clauses)	All	• The data importer warrants it has made its best efforts to provide the data exporter with relevant information with respect to the assessment described in this Clause 14. • The parties must document the assessment described in this Clause 14 and make it available to the competent supervisory authority on request. • The data importer will promptly notify the data exporter if has reason to believe that it is or has become subject to laws or practices that are not in line with this Clause 14. For module 3, the data exporter shall forward the notification to the controller. • If the data exporter receives such a notification, or has another reason to believe the data importer cannot comply with its obligations under the SCCs, it will promptly identify measures to be adopted by the data importer to address the situation. For module 3, the data exporter should consult controller if necessary. The data exporter shall suspend the transfer if there are no appropriate safeguards or if instructed by the competent supervisory to do so (or, if module 3, the controller may also instruct). In such instance, the data exporter will be entitled to terminate the contract insofar as it relates to the SCCs.	Yes
15.1 (Notification)	All	Note, only applies to module 4 where the EU processor combines the personal data received from a third country-controller with personal data collected by the processor in the EU • The data importer will notify the data exporter and, where possible, the data subject if it receives a legally binding request from a public authority under its local laws for disclosure of personal data transferred to it or if it becomes aware of any direct access by public authorities to personal data transferred to it in accordance with its locals laws. For module 3, the data exporter will forward the notification to the controller. • If the data importer is prohibited by law from notifying the data exporter and/or the data subjects, the data importer shall use its best efforts to obtain a waiver of the prohibition and shall document such efforts. • If permitted under local laws, the data importer will keep the data exporter up to date with all information related to the requests received. • The data importer will preserve all information pursuant to this Clause 15.1 and make it available to the competent supervisory authority if requested.	Yes, except for Cl 15.1(c), (d) & (e)
15.2 (Review of legality and data minimisation)	All	Note, only applies to module 4 where the EU processor combines the personal data received from a third country-controller with personal data collected by the processor in the EU • The data importer will review the legality of the request for disclosure and will challenge the request if it concludes there are reasonable grounds to consider the request unlawful. The data importer shall also appeal if possible/necessary. It shall disclose the personal data requested until required to do so under applicable procedural rules. • The data importer will document its legal assessment and any challenge made. If permitted by law, it shall also provide such documentation to the data exporter. If module 3, the data exporter will make this available to the controller. • The data importer shall only provide minimum amount of information possible when responding to a request for disclosure.	Yes

16 (Non-compliance with the Clauses and termination)	All	• The data importer shall inform the data exporter if it is unable to comply with the SCCs.
		
		• If the data importer is in breach or unable to comply with SCCs, the data exporter shall suspend transfer until the data importer is in compliance or until the contract is terminated.
		
		• The data exporter may terminate the contract, insofar as it relates to processing of personal data under the SCCs, where:
		
		    ○ The data importer is in breach or unable to comply and is not in compliance within one month;
		
		    ○ The data importer is in substantial or persistent breach of SCCs; or
		
		    ○ The data importer fails to comply with a binding decision regarding obligation under the SCCs.
		
		• If the contract is terminated per the above, the data exporter must inform the supervisory authority and, if module 3, the controller also.
		
		• SCCs can be revoked where the EC adopts new SCCs or GDPR becomes part of the legal framework for the third country.
			Yes, except for Cl 16(e)

16 (Non-compliance with the Clauses and termination)	1,2,3	If the contract has been terminated per Clause 16, the data exporter may choose to have the personal data immediately returned or deleted. The data importer must certify deletion and comply with SCCs until the personal data has been either returned or deleted.	Yes
16 (Non-compliance with the Clauses and termination)	4	If the contract has been terminated per Clause 16, data collected by the data exporter in the EU that has been transferred prior to termination must be immediately deleted.	Yes

17 (Governing law)	1,2,3	• Parties agree that SCCs shall be governed by either of the following options:
		
		    o <u>Option for modules 1, 2, or 3</u>: The law of one of the EU Member States that the parties can select, provided such law allows for third-party beneficiary rights; or
		
		    o <u>Option for modules 2 or 3</u>: The law of the EU Member State in which the data exporter is established provided that such law does allows for third-party beneficiary rights. If it does not, the parties shall select another EU Member State.
			Yes

17 (Governing law)	4	Parties agree that SCCs shall be governed by the law of a country allowing for third-party beneficiary rights, not limited to EU Member States, and shall specify such country in the SCCs.	Yes
18 (Choice of forum and jurisdiction)	1,2,3	Any dispute arising from the SCCs shall be resolved by the courts of an EU Member State which the parties must select. Data subject may bring proceedings in the Member State that they reside.	Yes, except for Cl 18(a) & (b)
18 (Choice of forum and jurisdiction)	4	Parties specify the applicable jurisdiction, not limited to EU Member States.	No
Annex I.A (List of parties)	All	Parties state the details of the data exporter(s) and the data importer(s), including whether they are acting as controller or processor.	
Annex I.B (Description of transfer)	All	Parties state the categories of data subjects, personal data, frequency of transfer, nature and purpose of processing, period of personal data retention and transfers to (sub)processors.	
Annex I.C (Competent supervisory authority)	1,2,3	Parties identify the relevant supervisory authority.	
Annex II (Technical and organisational measures including technical and organisational measures to ensure the security of the data)	1,2,3	Parties state the technical and organisational measures in place to ensure the security of the personal data.	
Annex III (List of sub-processors)	2,3	Parties list the applicable sub-processors.	

Our Locations

The Americas

Atlanta
1170 Peachtree Street, N.E.
Suite 100
Atlanta, GA 30309
t: +1.404.815.2400
f: +1.404.815.2424

Century City
1999 Avenue of the Stars
Los Angeles, CA, 90067
t: +1.310.620.5700
f: +1.310.620.5899

Chicago
71 South Wacker Drive
Forty-Fifth Floor
Chicago, IL 60606
t: +1.312.499.6000
f: +1.312.499.6100

Houston
600 Travis Street
Fifty-Eighth Floor
Houston, TX 77002
t: +1.713.860.7300
f: +1.713.353.3100

Los Angeles
515 South Flower Street
Twenty-Fifth Floor
Los Angeles, CA 90071
t: +1.213.683.6000
f: +1.213.627.0705

New York
200 Park Avenue
New York, NY 10166
t: +1.212.318.6000
f: +1.212.319.4090

Orange County
695 Town Center Drive
Seventeenth Floor
Costa Mesa, CA 92626
t: +1.714.668.6200
f: +1.714.979.1921

Palo Alto
1117 S. California Avenue
Palo Alto, CA 94304
t: +1.650.320.1800
f: +1.650.320.1900

San Diego
4747 Executive Drive
Twelfth Floor
San Diego, CA 92121
t: +1.858.458.3000
f: +1.858.458.3005

San Francisco
101 California Street
Forty-Eighth Floor
San Francisco, CA 94111
t: +1.415.856.7000
f: +1.415.856.7100

São Paulo
Av. Presidente Juscelino
Kubitschek, 2041
Torre D, 21º andar
Sao Paulo, SP
04543-011
Brazil
t: +55.11.4765.3000
f: +55.11.4765.3050

Washington, D.C.
2050 M Street NW
Washington, DC, 20036
t: +1.202.551.1700
f: +1.202.551.1705

Asia

Beijing
Suite 2601, 26/F
Yintai Center Office Tower
2 Jianguomenwai Avenue
Chaoyang District
t: +86.10.8567.5300
f: +86.10.8567.5400

Hong Kong
21-22/F Bank of China Tower
1 Garden Road
Hong Kong
t: +852.2867.1288
f: +852.2523.2119

Seoul
33/F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu,
Seoul, 04539, Korea
t: +82.2.6321.3800
f: +82.2.6321.3900

Shanghai
43/F, Jing An Kerry Center
Tower II
1539 Nanjing West Road
Shanghai, 200040 PRC
t: +86.21.6103.2900
f: +86.21.6103.2990

Tokyo
Ark Hills Sengokuyama Mori
Tower
40th Floor, 1-9-10 Roppongi
Minato-ku Tokyo 106-0032
Japan
t: +81.3.6229.6100
f: +81.3.6229.7100

Europe

Brussels
Avenue Louise 222
1050 Brussels
Belgium
t: +32.2.641.7460
f: +32.2.641.7461

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt am Main
Germany
t: +49.69.907485.0
f: +49.69.907485.499

London
100 Bishopsgate
London EC2N 4AG
United Kingdom
t: +44.20.3023.5100
f: +44.20.3023.5109

Paris
32, rue de Monceau
75008 Paris
France
t: +33.1.42.99.04.50
f: +33.1.45.63.91.49