FUTURE OF PRIVACY FORUM

NOT-SO-STANDARD CLAUSES

Examining Three Regional Contractual Frameworks for International Data Transfers

MARCH 2023

AUTHORED BY

Lee Matheson

Senior Counsel, Global Privacy for the Future of Privacy Forum

EDITORS

Dr. Gabriela Zanfir-Fortuna

Sebastião Barros Vale

ACKNOWLEDGEMENTS

The author would like to thank Isabella Perera, Maria Badillo, Sebastião Barros Vale, and Dr. Gabriela Zanfir-Fortuna for their contributions to this report.

The Future of Privacy Forum (FPF) serves as a catalyst for privacy leadership and scholarship advancing responsible data practices in support of emerging technologies. FPF is based in Washington, DC, has offices in Brussels, Tel Aviv, Singapore and Nairobi, and includes an advisory board composed of leading figures from industry, law, and advocacy groups. The views herein do not necessarily reflect those of our supporters or our Advisory Board.

TABLE OF CONTENTS

INTRODUCTION

The flow of personal information across borders has been a thorny policy issue in the data protection and privacy sphere for decades. In recent years, it has seen a meteoric rise in prominence, moving beyond the orbit of privacy professionals and policy wonks and attracting attention from major international media outlets[1] and the highest levels of government.[2] This rise has been driven in part by substantially increased public scrutiny of international data flows after a number of high-profile cases and legal disputes, and in part by legal changes — the 2016 adoption of the EU's General Data Protection Regulation (GDPR)[3] chief among them.

The majority of international data transfers rely on relationships between or involving private and/or non-governmental entities. Whether discussing the operations of the world's social media and cloud computing tech titans, the considerations of a brand-new startup software developer, or the HR and payroll day-to-day of a large business, contracts are key to how organizations govern and monitor data transfers, particularly those that cross national borders. Because of the limitations imposed on international transfers by lawmakers and regulators, standardized contractual language has increasingly become a core tool in many businesses' compliance toolkit.

This language differs from the "standard boilerplate" common to many other commercial sectors operating in a global environment in that it has not emerged organically as a "best practice" but instead has been explicitly crafted by government authorities for use by the relevant entities processing personal information — and in some jurisdictions, has been officially recognized as a valid compliance mechanism under relevant law. The first efforts at producing this sort of officially standardized contractual text for data transfers predate even the EU's Data Protection Directive of 1995[4] and the clauses that followed it; studies of the contract clauses for use in the European Union and its predecessors date back to at least 1992, with formally recognized clauses adopted in 2001, 2004 and 2010.[5]

In the context of the EU-US relationship, both the 2013 Snowden leaks[6] and the 2018 Cambridge Analytica scandal[7] highlighted how far the reach of the vast, labyrinthine ecosystem for international transfers of personal information has grown. These developments, along with the 2016 adoption of the GDPR and the Court of Justice of the European Union (CJEU)'s landmark Schrems I and II cases[8], informed a 2021 update to the old decisions authorizing the Data Protection Directive-era Standard Contractual Clauses (SCCs) initially grandfathered into the GDPR.[9]

Additionally, increased scrutiny of international data transfers has not been limited to those between the United States and European Union. In Asia, the explosion of cross-border data transfers has prompted the Association of Southeast Asian Nations (ASEAN) to draft the Model Contractual Clauses (MCCs) to better enable transfers of data between its Member countries.[10] The Ibero-American Data Protection Network (RIPD) — a network of Data Protection Authorities from Latin America and other Spanish or Portuguese speaking countries[11] — has proposed a set of contractual clauses for its member governments' consideration along with guidelines for their implementation, for much the same reasons. Other individual national governments have also drafted or are in the process of drafting their own officially approved data transfer contract language — with the prominent recent examples of China and the United Kingdom. While these model clauses for data transfers will also be impactful, this Report will focus on regional, multilateral frameworks.

We will analyze, compare, and contrast the EU's Standard Contractual Clauses, the ASEAN Model Contract Clauses, and the Ibero-American Data Protection Network's Model International Transfer of Personal Data Agreement. They are intended to be used in three regions covering much of the world, showing that model contractual clauses could underpin a potential global regime to facilitate cross-border data transfers meeting the requirements of diverse data protection and privacy legal frameworks. We have chosen

these frameworks because of their recency, regional diversity, and potential applicability to multiple national jurisdictions. The Report sets out to identify the commonalities and points of divergence among these regional frameworks, with the purpose of laying out the path forward and potential barriers for a global regime that would allow international data transfers on the basis of standardized contracts.

The Report will first compare the source of the regional model clauses and the context in which they were adopted (Part I). It will then compare the significant obligations imposed by the different frameworks on the contracting parties, including how they handle onward transfers of personal information (Part II). The following sections will examine how the contracts address the application of individual rights to contemplated data transfers (Part III); the ability of national governments to access transferred personal data (Part IV); some relevant enforcement activity by data protection authorities (Part V); and lastly the extent to which parties may modify the text of the clauses (Part VI).

Another key contribution of the Report for both policymakers and practitioners is its Annexes, which include comparative charts of the summarized clauses of the three regional frameworks analyzed, organized under four themes: core provisions, such as liability and choice of forum (Annex I); the rights and obligations of exporters (Annex II); the rights and obligations of importers (Annex III); and a side-by-side comparison of the clauses authorized for enforcement by third-party beneficiaries (Annex IV).

PART I: LEGAL UNDERPINNINGS AND OVERVIEW

The legal authority underlying model contract frameworks for international transfers of personal information is not consistent across jurisdictions. Some jurisdictions explicitly recognize model frameworks at the national level — typically tied into the operation of national data protection laws, which often impose limits on entities' ability to transfer personal information abroad.[12] Some jurisdictions (generally those without data protection laws) do not explicitly limit transfers of personal information to other jurisdictions. Others rely on supranational rules and regulations like the EU's GDPR, which applies to all 27 EU Member States and includes standard clauses as an appropriate safeguard for the transfer of personal data abroad.

EU Standard Contractual Clauses

The GDPR authorizes transfers of personal data by a controller or processor ('exporter') to an entity in a third country or an international organization ('importer'), in the absence of an adequacy decision,[13] if the exporter "has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available."[14] Article 46(2) provides a list of options that meet the standard for including "appropriate safeguards" — and specifically offers "standard data protection clauses adopted by the Commission" as one such option.[15]

However, the operation of Chapter V of the GDPR (and the EU Commission decision authorizing the Clauses themselves) makes it clear that simply executing the Standard Contractual Clauses is not sufficient to make a transfer lawful — data controllers remain responsible for ensuring that "the level of protection for natural persons is not undermined"[16] and that "enforceable data subject rights and effective legal remedies for data subjects remain available."[17]

In litigation brought against the Irish Data Protection Commission seeking to compel the DPC to suspend transfers of personal data collected by Facebook Ireland to its American parent, Facebook Inc., the CJEU clarified the standard for transferring personal data out of the European Economic Area (EEA).[18] In 2015 (Schrems I) and 2020 (Schrems II) decisions, which invalidated two successive data transfer agreements between the EU and the United States, the CJEU held broadly that data subjects are entitled to "a level of protection essentially equivalent" to that provided by the GDPR when their personal data is transferred outside of the Union, and that controllers relying on the SCCs to transfer personal data may need to implement "supplementary measures" to ensure the legality of such transfers when sending data to non-adequate foreign jurisdictions.[19] The European Data Protection Board (EDPB) further clarified that such additional safeguards should be adjusted to the risks to the rights and freedoms of data subjects stemming from the "law or practice" of a transfer's destination country in the context of each specific transfer, as assessed by the exporter.[20]

On 4 June 2021, the EU Commission published Implementing Decision (EU) 2021/914, updating the standardized contractual language for data importers and exporters previously given a valid way to comply with the requirements set out in Chapter V of the GDPR.[21] The implementing decision replaced clauses adopted before both the GDPR and the CJEU's Schrems I and II rulings and included the contractual language covering four different relationships between parties: transfers from data controller to data controller ("M1"), data controller to data processor ("M2"), data processor to data processor ("M3"), and data processor to data controller ("M4").

Formulations "M3" and "M4" are unique to the EU SCCs; both the ASEAN and RIPD frameworks only contain modules for controller-to-controller and controller-to-processor data transfers.

ASEAN Model Contractual Clauses

The Association of Southeast Asian Nations approved a set of model contract clauses (MCCs) during its digital ministers' meeting on January 22, 2021.[22] These clauses were "designed to provide the appropriate safeguards" required by ASEAN Member State (AMS) national laws, as well as the principles articulated in the 2016 ASEAN Framework on Personal Data Protection, but the decision adopting their text does not apply directly to the national legal systems of ASEAN Member States in a binding manner. Similar to the EU SCCs, the MCCs exist for use by data importers and exporters on a voluntary basis; unlike the SCCs they are not grounded in explicit provisions of international or domestic law.

While there is no legal ASEAN equivalent to the EU's General Data Protection Regulation requiring ASEAN Member States to recognize the MCCs, several Member State data protection regulators have issued statements indicating that they will consider the use of the MCCs as positive indicators of compliance with the applicable provisions of Member State law.[23] The ASEAN Model Contractual clauses are designed to be "baseline in nature" and businesses using them are "advised to check if individual AMS have provided further guidance or templates." The supremacy of AMS national law in case of a conflict with the text of the MCCs is specified in the Clauses themselves, which make it clear that "[i]f there is any inconsistency between clauses in this contract and AMS Law, then the applicable AMS Law shall prevail."[24]

That the MCCs have been expressly drafted to operate in a setting where not all national jurisdictions may have a data protection law in place, and where no regionally-binding data protection obligations exist, is a critical difference from the EU SCCs. Similar to the framework proposed by the Ibero-American Data Protection Network discussed below, the MCCs are divided into two Modules: the first covers transfers between controllers and processors, and the second covers transfers between two controllers.

Ibero-American Data Protection Network Model Transfer Agreement

The Ibero-American Data Protection Network, an organization established in June 2003 to enable cooperation in the field of data protection among Spanish and Portuguese-speaking nations, promulgated a standardized set of contract clauses called the Model Agreement for the International Transfer of Personal Data for public comment in late 2021, along with an explanatory Implementation Guide, with final versions of both published in March 2023.[25]

Similar to the ASEAN MCCs, this Model Transfer Agreement (MTA) does not create a binding legal obligation for the Network's member states to recognize its validity; instead, it offers a view of how national data protection regulators and policymakers in Latin America are collectively approaching the issue of cross-border data transfer tools. The Ibero-American MTA is designed to assist regulators in creating tools that will enable entities processing personal data to meet the obligations of Article 36.1(c) of the Personal Data Protection Standards for the Ibero-American States, which permit transfers of data by parties that have signed "contractual clauses or any other legal instrument that offers [sufficient] guarantees … and that allows for the demonstration of the scope of processing personal data, the obligations and responsibilities assumed by the parties, and the rights of the [data subjects.]"[26]

Neither the RIPD's Data Protection Standards or the later-approved Model Transfer Agreement are directly binding on the RIPD's member governments, but rather are adopted to "promote and contribute to the strengthening and adoption of regulatory processes, through the elaboration of guidelines that serve as a parameter for future

regulations or for the revision of existing ones."[27] It is important to note that while the MTA modules are not a word-for-word reproduction of the EU SCCs, per the Implementation Guide they have been designed to "contain similar elements and principles in essence" to the EU's model framework, while also drawing on other sources.[28]

Similar to the ASEAN MCCs, the RIPD MTA includes two modular contract frameworks, published as an Annex to the Implementation Guide. Module 1 is designed for transfers between data controllers and Module 2 is designed for transfers between data controllers and data processors.[29]

PART II: KEY PARTY OBLIGATIONS

All three of the frameworks utilize a role-based approach applying different contractual language to parties with different relationships in the data transfer process. The different regional frameworks demonstrate an emerging international consensus on some core contractual concepts:

- All three are structured around "data exporters" who are responsible for moving personal data out of a given national jurisdiction, and "data importers" who receive personal data in a second jurisdiction.
- Each framework additionally characterizes exporters and importers as either "data controllers", who determine the collection, purposes, and means for processing personal data themselves, or "data processors", who receive and process personal data on behalf of and for purposes dictated by data controllers.[30]
- Stemming from this shared conceptual model, the three frameworks have a number of other features in common, though only the EU's SCCs explicitly include sets of clauses for other types of data transfer beyond controller-to-controller and controller-to-processor.

This section of the report discusses a number of areas where either convergence can be demonstrated, or substantial differences in approach should be highlighted.

Legality of Processing

Only one of the frameworks explicitly requires the exporting party to warrant the lawfulness of the initial collection of the personal data. Both Modules of the ASEAN MCCs include a non-optional stipulation that exporters must warrant that any data transferred was collected in compliance with the designated Applicable Law, or in the absence of such a law was collected

after notice was provided to the data subjects and consent for the processing obtained, if "reasonable and practicable" to do so.[31]

Neither the EU SCCs or the RIPD explicitly include the same stipulation, though the SCCs' recognition of applicability of the GDPR to covered transfers[32] necessarily imposes the "lawfulness" requirement of Articles 5 and 6 of the Regulation on any processing of such information,[33] and the MTAs necessitate that the contracting parties comply with the data protection law of the exporter's country.[34]

Accuracy

All three frameworks provide the option to the parties to make basic warranties as to the accuracy of transferred data, and additionally condition the parties' responsibilities concerning the accuracy of the transferred information based on their identified role within the data transfer. The SCCS and the MTAs require that when controllers transfer information to other controllers both parties "ensure data is accurate and up to date" and inform one another should either party discover transferred information is inaccurate or out of date, and further that controller-importers "take every reasonable step" to ensure the erasure or rectification of inaccurate transferred information.[35] Similarly, the SCCs and MTAs both require processor-importers to inform exporters when they become aware that transferred data is either "inaccurate or outdated" and cooperate with the exporter to rectify such quality issues.[36]

Both Modules of the ASEAN MCCs similarly offer a provision requiring that controller-exporters warrant transferred information is "accurate and complete" for the purposes of processing; the primary substantial difference between the frameworks is that the MCC provision is optionally included by the parties, rather than a fundamental part of the Clauses, and does not include a post-transfer obligation that importers notify exporters regarding inaccurate information.[37]

Transparency

While all three frameworks include transparency-based requirements, the degree and specificity of the disclosures required are different — substantially, in case of MCCs. The EU SCCs include the most thorough requirements, both in terms of what the parties must document and the degree to which the documentation must be shared outside of the contractual framework with both data subjects and relevant supervisory authorities.

All three frameworks require the memorialization of important information about a transfer in an appendix to the contract, but differ on the extent and specificity of information that must be provided in that appendix and circumstances under which it is accessible to third parties. All three frameworks' appendices require that the parties identify themselves in an appendix, and recognize the appendix "may contain confidential business information" and allow for some redaction when the information is released to third parties, but the appendices' contents are quite different.

The SCCs require the parties identify in detail, and exporters provide to the data subject on request and free of charge, appendices containing:

- The name, address, and contact individual, as well as the relevant activities of, the parties to the contract;
- The categories of data subjects whose data will be transferred, the categories of data to be transferred, any sensitive data to be transferred (along with applicable additional safeguards), the frequency of the transfers, the nature of the processing, the purposes of the transfer and ongoing processing, the retention period for transferred information (or the period used to determine such), and the applicable supervisory authority;
- The list of implemented technical and organizational measures to ensure security of the transferred information; and

- [For processors] the name, address, and contact person for any intended subprocessors, with a description of processing.[38]

Additionally, controller-importers are obligated to proactively inform data subjects (or make publicly available, if informing would be impossible or require disproportionate effort) of:

- The importer's identity and contact details, the categories of data processed, the right to obtain a copy of the Clauses; and
- whether there is any intention to transfer the data onward to additional third parties, unless data subjects already have the information or it has been provided by the exporter.[39]

Information may only be redacted to protect "business secrets or other confidential information" and if information is redacted, exporters must provide the reasons for the redaction on request.[40]

Similar to the SCCs, the RIPD MTA requires the parties prepare, and provide to the data subject on request and free of charge, a cover page and appendices containing:

- The name, address, and contact information for the parties to the contract, as well as the governing law and competent supervisory authority for the exporter;
- The categories of data subjects whose data will be transferred, the categories of data to be transferred, any sensitive data to be transferred (along with applicable additional safeguards), the frequency of the transfers, the nature of the processing, the purposes of the transfer and ongoing processing, the retention period for transferred information (or the period used to determine such);
- The list of implemented administrative, physical and technical measures implemented to ensure security of the transferred information; and
- [For processors] the name, address, and contact person for any intended subprocessors, with a description of processing.[41]

Additionally, MTA controller-importers are also obligated to proactively inform data subjects of:

- The importer's identity and contact details, the categories of data processed, the right to obtain a copy of the Clauses, and whether there is any intention to transfer the data onward to additional third parties.

Notably, unlike the SCCs, the MTA does not require the parties to identify contact individuals by name and title, only to provide "contact details," and does not require controller-importers to make information regarding transfers publicly available if providing it to data subjects is impossible or "requires disproportionate efforts."[42] Finally, when providing a copy of the MTA in response to a data subject request, parties are authorized to redact sections of the Agreement containing trade secrets or other confidential information, but are not obligated to provide data subjects with the reasons for those redactions.[43]

The ASEAN MCCs require, as a baseline, much less information be provided by the parties. Unless additional information is required by an applicable AMS law, under the MCCs parties must complete an appendix containing:

- The names of the parties;
- A description of the data subjects and "groups of data subjects";
- A description of the purposes of the data processing;
- [For controller-importers] a contact point authorized on behalf of the importer to respond to inquiries concerning personal data.[44]

The MCCs do not include a default obligation that parties provide data subjects with particular information or copies of the agreement on request, and also recognize that the descriptive appendix

may contain confidential business information not to be disclosed to third parties without either (for a processor-importer) instructions, or (for a controller-importer) the reasonable opportunity for the exporter to object.[45]

All three frameworks, however, firmly center transparency obligations on parties acting as controllers — and in the modules governing controller-processor transfers, restrict processors from responding to data subjects directly unless affirmatively authorized to do so by controllers.

Due Diligence and Record Keeping

Two places where the ASEAN MCCs diverge significantly in concept from the EU SCCs and RIPD MTA are the areas of pre-transfer due diligence and post-transfer record-keeping. The SCCs and MTA place an initial obligation on the data exporter to evaluate the data importer, before commencing a data transfer, and impose at least some obligations to keep records of the processing activity after the transfer has taken place.[46] Under the SCCs and the MTA exporters must assess importers and make reasonable efforts to determine whether they are capable of complying with the obligations imposed by applicable law and the contractual framework itself. By contrast, under the MCCs, there is no obligation for exporters to assess the ability of importers to comply with the Clauses or applicable AMS Law ahead of time; instead the obligation to warrant the ability to comply adheres to each party independently — regardless of whether the contemplated transfer is between controllers or controller-to-processor.[47]

Similarly, the three frameworks do not contain identical provisions regarding the maintenance of a record of processing related to the transferred information. The SCCs and the MTA both require controller-importers to maintain a record of processing for the data transferred "under [the importer's] responsibility" and, in the case of a data breach, document all relevant facts (including remedial measures) and maintain a record thereof.[48]

By contrast, the only reference to mandated record-keeping in the MCCs is an optional clause obligating processor-importers, upon reasonable request from an exporter, to "provide access to data processing facilities, data files, and documentation" for review or auditing purposes.[49] Any further record-keeping obligations would need to stem from applicable AMS legislation or other discretionary terms added by the parties.

Sensitive Data

There are significant differences between the frameworks on the question of "special category" or "sensitive" data. The MCCs do not address the concept at all — leaving it to the parties to modify any agreement that is subject to an AMS Law dealing with the concept accordingly. Both the SCCs and the MTA define "sensitive data," but there are substantial differences between how the two frameworks treat the issue.

The SCC provision covering sensitive data synthesizes the definition of "special category data" and the limitations on processing data relating to criminal convictions or offenses from Articles 9 and 10 of the GDPR,[50] and imposes an obligation to assess the additional risks posed by the processing of such information on the parties. Additionally, the SCCs explicitly impose an obligation on importer controllers to "apply specific restrictions and/or additional safeguards" adapted to the specific nature of the data and risks involved, suggesting example measures such as heightened access controls or pseudonymization as possible solutions.[51]

Unlike the SCCs, the MTA definition of sensitive personal data is not written as an exclusive list — instead, the MTA broadly defines the term as "personal data that refer to the intimate sphere of the Data Subject, the undue use of which may result in discrimination or create a serious risk thereof."[52] The framework gives a series of illustrative examples similar to the list provided in Article 9 of the GDPR, but notably does not

explicitly reference "data relating to criminal convictions or offenses," leaving an area of uncertainty that likely depends on the relevant national governing law to resolve. Additionally, the MTA includes an obligation for parties to "privilege the protection of [the] superior interests" of children or adolescents, "in accordance with the Convention on the Rights of the Child and other international instruments" for data transfers involving that type of personal data — but does not include a definition of "children" or "adolescents," terms often separately defined by other national laws.[53] The SCCs do not directly apply additional party responsibilities to the processing of children's personal data, and the GDPR only addresses the issue in the context of the "consent" lawful basis, providing a baseline that only children age 16 and older can provide valid consent (with Member States permitted to lower that age to a minimum of 13).[54]

Under both the SCCs and the MTA, the required risk assessment ties to the parties' collective transparency obligations, as the identification of specific special category data to be transferred and the associated additional security precautions taken are key parts of the required annexes describing the data transfer.[55]

Security Measures and Breach Notification Obligations

All three frameworks impose a security requirement on data importers and exporters that "reasonable and appropriate" technical and organizational measures be implemented to protect personal data from the possibility of unauthorized access, whether they are data controllers or data processors.[56] However, the SCCs and the MTA impose substantially greater requirements on the parties with regard to how security measures are selected and documented pre-transfer, and subsequently monitored after a transfer has taken place. The SCCs and the MTA require the parties to evaluate, when determining appropriate security measures:

- The state of the art;
- The costs of implementation;
- The nature of the personal data being transferred;
- The scope, context, and purposes of processing; and
- The risk to the rights and freedoms of/the potential consequences of a data breach for a data subject.

Under the MTA, importer-controllers are further required to evaluate any previously occurring data breaches.[57] Furthermore, under both the SCCs and MTA, the measures adopted as a result of these mandatory evaluations must be documented in a detailed annex.

Tied to security, the SCCs and the MTA identify an explicit obligation on importers to ensure that personnel authorized to process data are bound to an obligation of confidentiality, either by law or by contract.[58] Under the SCCs and the MTA, there is an additional obligation that importers carry out regular checks to ensure that the security measures adopted continue to provide adequate protection.[59]

The MCCs include a more general representation that importers have implemented measures that will protect the confidentiality, integrity and availability of personal data and (for controller-to-controller transfers) a representation that both parties have "taken appropriate steps to determine the level of potential risk of data breaches."[60]

All three frameworks explicitly define a breach of security to include loss or unauthorized use, copying, modification, disclosure, destruction of, or access to transferred personal information, whether accidentally or on purpose.[61]

All three frameworks also impose requirements on both controller-importers and processor-importers to notify exporters in the event of a breach of security; both the SCCs and the MTA also mandate

that relevant regulatory authorities be notified (the MTA notably requires controllers provide this notification "without any delay, but no later than 5 days.")[62] The SCCs and MCCs require the notification of an exporter by a processor-importer "without undue delay" (or, alternatively, within a reasonable time specified by the parties under the MCCs);[63] only the MTA explicitly requires that such notice be given within 72 hours of the discovery of a breach.[64] Only the MCCs do not necessitate the notification of an enforcement authority in the event of a breach as a matter of contract.

Finally, potential notification to affected individuals is handled quite differently by each framework. The MTA is by far the most stringent of the three — importer and exporter-controllers are obligated to notify data subjects "without any delay" and in any case "no later than 5 days" after becoming aware of any breach, and this obligation is not conditioned on an assessment of the risk posed by the breach to data subjects.[65] The MCCs do not address notification of individuals who are affected in a breach, leaving such obligations up to applicable AMS law to impose. The SCCs require, consistent with Article 34 of the GDPR, that in the case of a breach "likely to result in a high risk to the rights and freedoms of a data subject" a controller-importer provide notice "without undue delay" — and a processor-importer "cooperate and assist" its controller in making such notifications." In situations where individual notification would involve "disproportionate efforts" by an importer-controller, both the MTA and the SCCs permit notification of a breach via public communication.[66]

Onward Transfers

On the issue of onward transfers of personal information, the EU SCCs and the RIPD MTA are very similar — to be expected, given that the MTA's onward transfer provision is explicitly based on the SCC provision covering the same topic.[67] Both frameworks hew to the same broad expectation that any processor-importer will be bound to impose on any third-party transferee the same restrictions that the exporter has imposed on it; an expectation also reflecting in the ASEAN MCCs, which otherwise diverge substantially from the EU/RIPD model.[68]

The SCCs and MTA permit onward transfers in cases where the importer's jurisdiction has (if applicable) received an adequacy decision, if the importer has put in place otherwise adequate safeguards, if the transfer is necessary to establish, exercise, or defend a legal claim in a judicial, regulatory, or administrative proceeding, or if it is necessary to defend the vital interests of either the data subject or another natural person.[69] Finally, lacking another method under both frameworks controller-importers may also rely on the explicit consent of a data subject, assuming a discrete list of disclosures has been made.[70]

The MCCs diverge significantly from the other frameworks after the initial obligation for processor-importers to flow down applicable contractual obligations, however, imposing no restrictions at all on controller-importer onward transfers and minimal additional restrictions on such transfers by processors. The only additional onward transfer obligation imposed by the MCCs is a requirement that processor-importers notify exporters of further transfers in writing, leaving "reasonable opportunity for the Data Exporter to object."[71]

Sub-processor requirements

Sub-processor clauses are specific to the controller-processor transfer arrangement, and provide the rules for processor-importers to re-export data and engage other processors when carrying out the instructions of the original controller. All three frameworks impose some mandatory restrictions on the engagement of sub-processors by processors.

Under the SCCs and the MTA, exporters are given the option to authorize sub-processors in advance

on either a "specific" (where sub-processors must be individually approved ahead of engagement) or "general" (where the controller pre-approves a set list of sub-processors, and must be given an opportunity to reject additions or changes) approval basis, either option documented in a written annex to the agreement that includes significant information about the contemplated sub-processors.[72]

The only difference between the SCC and MTA implementations of this concept deals with timing — the SCCs allow the parties to specify the time period before which a processor must provide a controller with its proposed sub-processor information, while the MTA requires such information be submitted at minimum 15 business prior to engagement.

The MCCs, by contrast, impose only the general restrictions on onward transfers that apply to importer-processors: a requirement that processor-importers notify exporters of further transfers in writing, leaving "reasonable opportunity for the Data Exporter to object."[73]

"Optional Clauses"

One of the key distinctions between the different emerging frameworks appears to be the degree to which optional clauses within the role-based modules are considered.

The EU SCCs and ASEAN MCCs offer optional clauses that allow the parties to designate the agreement's governing national law — the SCCs' limited to the selection of an EU Member State that recognizes third-party beneficiary rights — while the MTA defaults to the national law of the exporter.[74] The EU SCCs and the RIPD MTA also offer the contracting parties optional language for controllers' governance of the use of sub-processors (discussed above).

The ASEAN MCCs in particular provide the parties with optional clauses on substantive contractual issues, such as the parties' warranties related to the accuracy and completeness of transferred data, or importer-processors' contractual obligations to provide access to processing facilities for auditing purposes or correct errors or omissions in transferred data.[75]

PART III: DATA SUBJECT AND THIRD-PARTY RIGHTS

Recognition of third-party beneficiary rights is a crucial area where noteworthy contrasts between the analyzed frameworks arise. The extent to which the model contract frameworks empower individuals to enforce specific rights and contractual obligations against the contracting parties is a key area of consideration. Although the RIPD MTA and the EU SCCs are similar in many ways (the MTAs seemingly having been drafted with the SCCs' structure and themes in mind) they are not purely identical. Under the SCCs, the Clauses may be generally enforced by third parties except for particular provisions that are exempted from such enforcement in each Module,[76] whereas the RIPD MTA makes all Clauses available for third party enforcement without imposing any exemptions.[77]

Contrary to the MTA and the EU SCCs, the ASEAN MCCs only deal with data subjects' requests in terms of assigning responsibility for their determination between the parties; any further outcome — including the rights that individuals have with regards to the processing of their personal data — relies on whatever applicable AMS Law governs the agreement, although the MCCs do offer an optional set of additional clauses for inclusion when the Parties have designated a jurisdiction with applicable law guaranteeing third party rights.[78]

EU SCCs: Broad possibilities for data subjects to enforce rights

The existence of data subject rights and their corresponding ability to enforce those rights as third-party beneficiaries is a core part of the functioning of the EU SCCs. Recital 12 of the underlying authorizing decision from the EU Commission indicates that "[w]ith some exceptions [relating to specific obligations between exporter and importer] data subjects should be able to invoke and enforce the [SCCs] as third-party beneficiaries."[79] Significant non-optional clauses in each of the four SCC Modules require that the parties warrant that data subjects will be able to enforce third party rights in the destination country of the relevant transfer.

The SCCs specifically obligate importer-controllers to, with the assistance of the data exporter, respond to data subject requests "without undue delay" and at minimum within one month of the receipt of a request.[80] Responses must be provided in an intelligible, easily accessible form, using clear and plain language.[81] Data subjects are specifically authorized to make several types of requests, including to:

- Confirm the processing of data about them and receive a copy of that data;
- Receive the transparency information guaranteed in Annex I of the agreement;
- Determine if personal data has been transferred onward, if so, for what purpose, and be informed of the categories of recipients;
- Receive information on the right to lodge a complaint with a supervisory authority;
- Rectify inaccurate or incomplete data, or erase data processed in violation of the Agreement;
- Withdraw consent for processing; and
- Opt out of direct marketing by the importer.[82]

In addition to the specifically listed requests in Article 10, the SCCs offer an expansive role for the enforcement of other contractual provisions by third party beneficiaries, with only a few provisions excepted from this right.[83] The exempt provisions largely deal with the parties' bilateral relationships with one another with regard to notifications, audits, or liability, or with the designated Supervisory Authority; only a few exempt provisions (such as Clause 6, which requires parties to describe the data transfer in an appendix) could theoretically impact a data subject.[84]

All primary data protection obligations imposed on the parties are enforceable by third parties, along with central clauses obligating the parties to evaluate the laws of the importer's jurisdiction, assess and respond to public authority access requests, and even suspend or terminate transfers in the event of a party's breach or inability to comply.[85]

Ibero-American Network MTA: Strong contractual protections for individuals, but contingent on the strength of national laws

Foundationally similar to the EU SCCs, the MTA is designed to "ensure that the level of protection of the personal data of the citizens of a country does not decrease or disappear when exported or transferred to another country or countries."[86] Functionally very similar to SCCs, the MTA has a minor difference in drafting design — Clause 3 provides blanket authorization for third parties to enforce the clauses against importers and exporters without any exceptions.[87]

The subject areas of the SCCs and MTA that permit third-party beneficiaries have substantial overlap — The MTA also specifically obligates importer-controllers to, with the assistance of the data exporter, respond to data subject requests "without undue delay" although the minimum specified timeframe is shorter at fifteen business days.[88] Data subjects are specifically authorized to make the same list of requests given above, with the minor variations:

- Data subjects may request the retention period (or criteria to determine it), and
- When opting out of direct marketing, data subjects may explicitly opt out of profiling "to the extent it is related to such activity."[89]

Given the expansive authorization for third party beneficiaries to generally enforce the provisions of both frameworks beyond the specific provisions for data subject rights, the relevant provisions of the SCCs that are enforceable by third-party beneficiary and their corresponding MTA provisions are laid out in Annex IV.

ASEAN MCCs: Parties determine applicable law, which can provide for data subject rights

The ASEAN MCCs are structured somewhat differently with regard to third party/data subject rights. Third-party beneficiary rights are not automatically included in either Module of the ASEAN MCCs; instead clauses governing such rights are incorporated as an extra, optional section of both Modules for use in cases where the applicable AMS Law recognizes and enables such claims by data subjects.

In such a case, the Parties designate the applicable AMS Law providing the individual rights, and the data subjects may enforce particular contractual provisions against either the exporter or importer.[90]

Automated Decision-Making (ADM)

Signaling the importance of personal data being accessed from different jurisdictions and potentially transferred to serve as a basis for automated-decision making, including profiling and other forms of algorithmic processing, both the EU SCCs and the RIPD MTA address the question of automated decision-making.[91] The SCCs prohibit importer-controllers from making decisions "solely based on the automated processing of the personal data transferred ... which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorized to do so under the laws of the country of destination."[92] Authorizing laws must provide "suitable measures to safeguard the data subject's rights and legitimate interests" and the importer must:

- Inform the data subject about the planned automated decision, envisaged consequences, and logic involved; and
- Implement suitable safeguards, at least permitting the data subject to context the decision, express his/her point of view, and obtain review by a human being.[93]

The MTA is drafted slightly differently and offers a more detailed definition of ADR than the SCCs. Initially, the MTA requires that "the Data Importer shall not make any Automated Individual Decision with respect to the transferred personal data," but defines an "Automated Individual Decision" as a decision "that produce[s] legal effects concerning the Data Subject, or that affect[s] him/her in a significant way, based solely on automated processing intended to assess, without human intervention, specific personal aspects, or to analyze or predict, specifically, his/her professional performance, economic situation, health status, sexual preferences, reliability or behavior."[94] The MTA similarly narrowly allows for such automated processing when based on the data subject's consent, or authorization under the laws of the data importer's country, so long as they "ensure appropriate safeguards for the rights of data subjects."[95] The MTA guarantees data subjects similar, but less granular rights regarding ADM as the SCCs — individuals are entitled to:

- An explanation about the decision made;
- Be heard and express his/her view and challenge the decision, and
- Obtain human intervention.

Adding a restriction not explicitly found under the SCCs, MTA importer-controllers are forbidden outright from using automated processing that "leads to discrimination against Data Subjects due to their racial or ethnic origins; religious, philosophical, and moral beliefs or convictions; trade union membership; political opinions; sexual life, preference, or orientation; or the Processing of health, genetic, or biometric data."[96]

The regulation of ADM (and data transfers for the purposes of ADM) is a rapidly changing field. Interestingly, the MTA's definition of "Automated Individual Decisions" is very similar to the language found in Recital 71 of the GDPR defining "profiling" in the context of that law's Article 22 restriction on automated decision-making, which also places extra limitations on ADM involving "special category" data.[97]

The ASEAN MCCs neither define ADM nor build particular restrictions on transfers for such a purpose into the framework — likely reflecting the significant diversity of the emerging field of potentially applicable AMS laws on the topic.

PART IV: RESPONDING TO GOVERNMENT REQUESTS

Perhaps the single most contentious issue within the broader cross-border data transfer policy space is the question of how data importers should deal with requests for access to data from public authorities, particularly for national security and law enforcement purposes. As we will see, the frameworks compared in this Report have different ways and levels of specificity in mandating due diligence and risk mitigating measures on this issue. This includes the degree to which data exporters are required to conduct analyses of destination countries' legal regimes — including the practical likelihood of public authorities' access requests — the representations that data importers are required to make about the national laws of their home countries, and obligations for the ongoing assessment of and transparency about the legal and practical conditions in a destination country.

EU SCCs: A thorough approach, combined with EDPB Recommendations

On this issue, the EU SCCs apply the same language to all Modules, as Clause 14 has no variation in application regardless of whether exporters and/or importers are controllers or processors. Contractual parties must perform initial due diligence on the laws and practices of the destination country, and not initiate the transfer of personal data if the laws and practices of the third country prevent the importer from complying with the SCCs.[98] Moreover, the importer must warrant "best efforts" made in assessing its local jurisdiction initially and on an ongoing basis, and notify the exporter in case it becomes unable to comply with the SCCs[99]. The written mandatory transfer impact assessment must be accessible to supervisory authority.

Clause 14(b) of the EU SCCs lists granular factors for consideration when evaluating a local jurisdiction. As mentioned in the EDPB Recommendations on Supplementary Measures, should the assessment reveal risks that personal transferred abroad could be accessed by foreign authorities in a manner which is not necessary and proportionate in a democratic society, the exporter should consider — in collaboration with the importer — if supplementary measures exist, which, when added to the safeguards contained in the SCCs, could ensure an equivalent level of data protection to the one in the EU. In principle, supplementary measures may have a contractual, technical or organizational nature and the EDPB Recommendations provide several examples of possibly effective ones, such as strong, well-implemented encryption; pseudonymisation that prevents re-identification without information that remains with the exporter; or contractual provisions reinforcing an exporter's ability audit an importer and mandating the implementation of tamper-proof access logs to enable those audits.[100]

In case of access by a public authority (or notice that an importer has become subject to law that will prevent it from fulfilling its obligations under the Clauses), the SCCs require exporters to either adopt additional technical and organizational measures preventing the incompatible access or, upon assessing such cannot be done, act to suspend a transfer.[101] Furthermore, importers are explicitly required to notify exporters and data subjects "promptly" of any legally binding requests (or direct access) by public authorities for transferred information, unless prohibited by law from doing so, and in such cases make "best efforts" to avoid the prohibition.[102] The SCCs also build in obligations for importers to regularly provide exporters with information about requests received, and to legally assess any such requests and pursue appeals of any that could reasonably be considered illegal under applicable domestic or international legal obligations.[103]

RIPD MTAs: Local law evaluation is required, but lacks specific guidance

The underlying purpose of the MTAs — that continuity in data protection be preserved for personal data transferred from one RIPD member country to another, and the data transfer "cannot become a scenario that reduces the level of protection on the data subject" — necessitates the evaluation of local laws in importer jurisdictions.[104] Both Modules of the MTA require the contracting parties to evaluate the laws and practices of the receiving jurisdiction and warrant that they are not incompatible with the representations made in the agreement.[105] Moreover, data importers must review any public authority request to use or disclose personal data not contemplated in the agreement and contest it if there are reasonable grounds to believe it is illegal, similar to the EU SCCs, as well as notify the exporter of such a request if permitted to do so.[106] Importers are similarly obligated to inform exporters of changes to applicable law that may affect compliance with the agreement.[107]

However, MTAs are not as detailed as the EU SCCs regarding the specific factors that must be considered during the evaluation of a jurisdiction, as parties are only required to use "reasonable efforts" to assess local law and practice and ensure they are not "beyond what is necessary and proportionate to a democratic society" or "reasonably expected to affect … the protections, rights, and safeguards afforded to Data Subjects under [the contract]."[108] The MTAs lack the specific set of granular assessment factors given in Clause 14 of the SCCs and the requirement that the Parties document such an assessment for future production. The MTAs also do not affirmatively require importers to regularly report to exporters about requests received and the outcome of any legal challenges to them. The MTA's Implementation Guide indicates that the government access provisions of the framework were based on New Zealand's Contractual Model Clause rather than explicitly modeled on the EU SCCs.[109]

ASEAN MCCs: Importer must notify exporter of government access requests, if possible

The ASEAN MCCs do not contain significant built-in limitations on parties' relationships with AMS governments with regards to access to transferred personal data. Importer processors are obligated to "promptly notify and consult" with exporters about "any investigation regarding the collection, use, transfer, disclosure, security, or disposal of the Personal Data transferred", but no language requiring analysis of local laws, or opposition and appeal of government access requests is included in either MCC Module.[110]

PART V: ENFORCEMENT

Enforcement is a key area of difference between the three contractual frameworks. As should probably be expected for contractual arrangements that by necessity touch multiple national jurisdictions, all three frameworks designate or select an applicable national law and the appropriate legal forum.

The EU SCCs and the RIPD MTA further require the designation of a particular regulatory authority for the oversight of compliance with the contractual obligations — the ASEAN MCCs do not presuppose that either of the contracting parties is necessarily subject to such an entity by requiring the designation of such a body.

The EU SCCs have robust, specific provisions requiring the parties to designate the relevant supervisory authorities, and to engage with them in a variety of contexts, such as when notifying data breaches. It is clear that Supervisory Authorities in the EU retain the competences and powers to enforce the GDPR's restrictions on international data transfers against the exporter and the importer, as long as the latter are subject to the GDPR. In fact, and particularly since the Schrems II ruling from the CJEU, EU Supervisory Authorities have increasingly used their corrective powers to order exporters to observe those restrictions, albeit with varying approaches and levels of tolerance for the existence of risks of foreign authorities' access to personal data that is transferred from the EU.[111]

By contrast, neither the ASEAN MCCs and the RIPD MTA make specific provisions for enforcement within the body of its contracts outside of limited provisions designating which national laws will apply to the contemplated transfer, as they will necessarily rely on national regulatory entities that exist outside of an institutional structure like the GDPR. Nonetheless, some enforcement activity relating to cross-border data transfer rules arising from national law-based restrictions has begun to emerge.[112]

As for disputes arising from non-compliance with the agreements and the choice of forum, again the SCCs and the MTA are more prescriptive compared to the MCCs, which merely include a clause offering an open-ended choice for the dispute resolution method, as an optional provision in the contract.[113] In contrast, the EU SCCs include a clause specifying that the parties agree disputes will be solved in an EU Member State Court they select — therefore in a Court of a jurisdiction relevant for the data exporter, and also that a data subject may bring proceedings against either party in the Member State where they reside.[114] Similarly, the MTA provides that disputes arising from the agreement shall be resolved by the courts in the data exporter's jurisdiction, and that the data subjects may bring action against a data exporter or a data importer either in the country of the data exporter, or in the country where the data subject resides.[115]

PART VI: WHAT MODIFICATIONS ARE PERMITTED?

One of the most important pieces of any standardized contractual tool is the degree of modification parties are permitted to make to the original language. All three frameworks substantially restrict the ability of the parties to modify the agreements. Such provisions are understandably foundational to the utility of such model contractual arrangements.

EU SCCs AND RIPD MTA: Parties are free to add additional, non-conflicting safeguards

The EU Commission decision implementing the Standard Contractual Clauses is relatively prescriptive on the question of whether the contractual language itself can be modified. In the event of conflict between the terms of the model clauses and a larger contractual arrangement, under the EU SCCs the model clauses must prevail.[116] The implementing decision states the data exporter and data importer are free to include the SCCs as part of a wider contract and to add other clauses or additional safeguards, provided that they do not contradict the SCCs "directly or indirectly," or "prejudice the fundamental rights or freedoms of data subjects," an obligation that is reflected in Clause 3 of the SCCs themselves.[117] However, entities using the EU SCCs are "encouraged to provide additional safeguards" in addition to those present in the adopted text, and in some instances, they may even be required to do so in the cases we mentioned in Part IV above.[118]

The RIPD's MTA uses similar language regarding modifications to the clauses. Both Modules of the MTA include a clause that the Clauses will only function to meet their purpose if they "are not modified in their essence with respect to the original model."[119] Beyond that, only "new definitions of terms, safeguards and guarantees" are permitted "when it is necessary to comply with the Applicable Law" and when making such modifications "does not imply a detriment to the protections granted by the model Clauses."[120] Notably, both SCCs and MTA require parties to consider whether any modified contractual text would, in addition to explicitly contradicting a provision in the original clauses, *imply* such a contradiction, or in some way affect the rights afforded in the clauses to a third party beneficiary.

ASEAN MCCs: Changes allowed in accordance with regional data protection frameworks

While similar, the language of the ASEAN MCCs is slightly more permissive of potential modification to the Model Clauses than the equivalent provisions in the SCCs or the RIPD Model Transfer Agreement. The explanatory text for the ASEAN Model Clauses endorsed at the 2nd ASEAN Digital Senior Officials Meeting indicates that parties may, "adopt or modify the MCCs in accordance with the principles set forth in the ASEAN Framework on Personal Data Protection (2016), or as required by AMS Law."[121] The MCC framework does not explicitly require parties to evaluate whether updated contractual language would affect the "fundamental rights and freedoms" of data subjects whose data is being transferred, reflecting that not all AMS domestic legal systems recognize an individually-enforceable rights-based model for personal data protection.

CONCLUSION

This complex comparative examination of the three regional contractual frameworks for cross-border data transfers — which cover vast and different geographies and more than 60 jurisdictions on three continents, shows that model contractual clauses are a candidate to potentially underpin a global regime to facilitate cross-border data transfers as one tool in the "transfers" toolbox.

First and foremost, the jurisdictions for which the three regional frameworks are relevant all recognize that contractual agreements based on standard or model clauses between data exporters and data importers can be valid options to protect their citizens' personal data when it is transferred abroad. Each operates based on similar legal concepts, is built on a similar structure, and includes provisions recognized as important across the board, such as:

- The adoption of similar role-based distinctions between Data Importers and Data Exporters along the controller-processor model that has largely come to define entities' responsibilities in the international data protection space;
- Transparency about personal data transferred and the purposes for its collection and processing, detailed in addenda attached to the agreements;
- The limitations imposed on importers' processing of transferred personal data;
- How to address requests from data subjects and appropriate limitations to impose on them;
- The need to set rules and limitations for onward transfers in line with the original contractual obligations and control the operations of subservient contract partners;
- The importance of maintaining the accuracy and currency of transferred personal data;
- Choice of law and choice of forum within the clauses governing any disputes that might arise, with a preference across the frameworks for the law of the exporter's jurisdiction;
- The recognition of exporters' auditing rights in controller to processor relationships;
- Detailing applicable recordkeeping obligations;
- Setting specific rules around responding to government requests for accessing personal data.

At a base level, the substantial number of similar areas among the regional frameworks we have evaluated points to a less fractured contractual environment for data transfers than might initially be anticipated. This provides policymakers with an impetus to work towards making these frameworks interoperable.

At the same time, our study also revealed several areas where the three frameworks operate differently, and will need to be bridged if interoperability is to be sought while building a global framework for standard contractual arrangements for cross-border data transfers:

- Though all three model clauses set out rules for two common types of relationships involving data transfers — controller to controller and controller to processor, the EU SCCs go a step further and recognize processor to processor and processor to controller relationships.
- How to deal with individuals acting as third-party beneficiaries in commercial arrangements involving their data, as the ASEAN MCCs are significantly less specific than the other two frameworks (see Annex IV). The significant range among the AMS governments in terms of national approaches to and expertise with data protection regulation is likely the main explanatory factor here.

- Specific obligations related to transferring sensitive data and related to automated decision-making are addressed in both SCCs and MTA, but are missing from the MCCs. It is likely that such topics will need to be addressed if these standard contractual frameworks seek to become interoperable.
- The degree of pre-transfer due diligence and post-transfer record-keeping that should be required — the SCCs and MTA are quite detailed compared to the MCCs. The former two frameworks place initial obligations on the data exporter to evaluate the data importer, and they also impose some obligations to keep records of the processing activity after the transfer has taken place. The MCCs refer to record keeping only in an optional clause focused on the auditing rights that data exporters have on the facilities, data files and documentation of importers.
- There are also differences in how government access to personal data transferred under model clauses is treated, as explained in Part IV. A common approach to this issue would be needed to ensure interoperability of the frameworks analyzed. For instance, reference to the principles agreed upon by the OECD for government access to personal data held by the private sector could serve as a reference point.

Overall, a path towards a global framework or at a minimum interoperable frameworks that allow international transfers of personal data on the basis of standard contracts is visible following the detailed comparison made in this study.

ANNEXES: MODEL CONTRACTUAL CLAUSES COMPARATIVE CHARTS

The following charts are designed to provide a side-by-side comparison of the EU Standard Contractual Clauses (SCCs), the Ibero-American Data Protection Network Model Transfer Agreement (MTA), and the ASEAN Model Contractual Clauses (MCCs). Except when necessary, the Clauses have been summarized rather than reproduced verbatim.

*The authors have relied on the published 2023 English-language translation of the Ibero-American Data Protection Network.

Annex I: Core Provisions

The "Core Provisions" chart is designed to track provisions that create principles-based obligations for both parties to a framework.

TRANSPARENCY OBLIGATIONS

EU Standard Contractual Clauses

M1: C2C
M2: C2P
M3: P2P
M4: P2C

The parties must create annexes with the following information, and be prepared to provide to the data subject on request:

M1/M2/M3/M4 Cl. 6: The detail(s) of the transfer, and in particular the categories of personal data that are transferred and the purpose(s) for the transfer, are specified in Annex I.B.

M1 Clause 8.2:
(a) The data importer must inform the DS either directly or through the exporter, of:

- Identity and contact details
- Categories of personal data processed
- the right to obtain a copy of the clauses
- Destination, purpose, and recipients of any planned onward transfer

(b) Except when the DS already has the information above, or providing it would be impossible or involve a disproportionate effort for the Importer, in which which case the information must be made publicly available
(c) the Clauses must be made available to the DS free of charge on request; redactions are permitted to protect business secrets or PI, but a meaningful summary must be included to enable the DS to understand its content or their rights; parties must also provide the reasons for redactions on request of DS.

M2/M3 Clause 8.3: On request, exporter shall make a copy of the Clauses, along with the appendix, available to the DS free of charge. Redactions are permitted to protect business secrets or PI, but a meaningful summary must be included to enable the DS to understand its content or their rights; parties must also provide the reasons for redactions on request of DS.

Annex I
Identity and contact details of the data exporter, DPO, and EU Representative (if applicable)
Identity and contact details of the data importer(s), including the contact for data protection

Description of the data transfer with

- Categories of data subjects
- Categories of personal data transferred
- Sensitive data, along with applied risks/safeguards
- Frequency of transfers
- Nature of data processing
- Purposes of the transfer
- Retention period of transferred data or criteria to determine that period
- Subject matter, nature, and duration of sub-processor transfers

Identity and contact details for competent supervisory authorities with responsibility for ensuring compliance by the data exporter.

Annex II
Technical and organizational measures to ensure security of data processing, described in specific terms, considering the nature, scope, context, and purpose of processing, and the risks to the rights and freedoms of natural persons.

The SCCs give a list of 18 example criteria that could be included in Annex II. Specific mention of pseudonymization and encryption of personal data.

- If used for sub-processor transfers, must include the specific measures taken by the sub-processor to provide assistance to the controller as well.

Annex III [if applicable]
A list of specifically authorized sub-processors, if applicable.

TRANSPARENCY OBLIGATIONS

Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 4:** The details and characteristics of the transfers and, in particular: » the categories of personal data that are transferred and » the purposes for which [the data] are transferred; are given in Annex B of this Agreement. **M1 Clause 6.3(a):** The data importer must inform data subjects, either directly or via the data exporter, of: » The data importer's identity and contact details; » The categories of personal data processed; » The purposes of processing personal data; » The right to request a copy of the Agreement free of charge; and » When onward transfers are intended, the recipient or category of recipient and the purpose of any such transfer. **M1 Clause 6.3(b):** The above provisions are not required if: The DS already has the information; or » It is impossible to communicate the information or if it involves disproportionate effort for the Importer. **M1 Clause 6.3(c):** Upon request, importer will make the Agreement available to the Owner. Importer may redact trade secrets or other confidential information. **M2 Clause 6.4(a):** The parties must make the Agreement available to the DS free of charge on request. Importer must 'proactively assume the responsibility' of informing the DS of its existence. The parties may redact trade secrets or other confidential information. **M1 Clause 6.6(b):** The parties have agreed to the administrative, physical and technical security measures listed in Annex C. **Annex B:** » Categories of DS whose personal data is transferred » Categories of personal data transferred » Sensitive data transferred, along with applied restrictions and/or safeguards » Frequency of transfers » Purpose of the transfer » Retention period, or criteria used to determine that period » Any sub-processors **Annex C:** Administrative, physical and technical measures to ensure security. Set out in detail; Annex provides non-exhaustive list of types of measures that might be discussed. **M2 Annex D:** A list of sub-processors, including for each: » Company Name » Address » Name, position, and contact details for a point of contact » Description of data processing, including a "well-defined' delimitation of the responsibilities if several sub-processors are authorized
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**ASEAN MCC Explanatory Text: "**Ensure that a process exists to respond to inquiries regarding the data, and that there is clear agreement between the parties as to who shall respond in a prompt fashion." **M2 Clause 3.3**: importer shall provide to the exporter and to DS a contact point who is authorized on behalf of the importer to respond to enquiries concerning the personal data being processed. **M1/M2 Cl. 9:** The details of the transfer and the personal data involved are specified in Appendix A. **Appendix A:** Requires parties to identify provide: » Name of the data exporter » Name of the data importer » Description of the data subjects and groups of data subjects » Description of the purposes for processing personal data

MODIFICATION OF CONTRACT TERMS

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3/M4 Clause 2:** The parties may add the Clauses to a wider contract, or include other clauses and/or safeguards, so long as they do not contradict, directly or indirectly, the SCCs or prejudice the rights and freedoms of data subjects."
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1/M2 Clause 2.1:** This agreement is based on model clauses and establishes adequate safeguards, including rights enforceable by Third Party beneficiaries, provided that the Clauses "are not modified in their essence compared to the original model, except to complete the title page and the annexes." This does not prevent the Parties from including model contractual clauses in a broader contract, nor does it prevent them from adding further clauses or safeguards, provided they do not directly or indirectly contradict these model contractual clauses or affect the rights of Data Subjects.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**ASEAN MCC Explanatory Text/M1 Clause 8.1**: "Parties may, by written agreement, adopt or modify the MCCs in accordance with the principles set forth in the ASEAN Framework on Personal Data Protection (2016) or as required by AMS Law." » Parties may additionally add other clauses as appropriate for business and commercial needs as long as they do not contradict the MCCs.

APPLICABILITY OF LOCAL LAW AND PRACTICES

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3/M4 Clause 14 (a-b):** Parties must warrant that they have "no reason to believe" laws and practices of the country of destination that will apply to the importer, including disclosure requirements, prevent the importer from fulfilling its obligations under the Clauses. Applicable law must "respect the essence of the fundamental rights and freedoms and not exceed what is necessary and proportionate to a democratic society to safeguard one of the objectives given in Article 23 [of the GDPR]. The required assessment must evaluate: » The specific circumstances of the transfer, including the parties, destinations, transmission channels, purpose/format of processing, economic sector of processing, and type of recipient; » The laws and practices of the recipient destination » Any relevant technical or organizational safeguards put in place to supplement the safeguards built into the Clauses **Clause 14(d):** The assessment must be documented and made available to the supervisory authority on request.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 11(a)/M2 Clause 12:** The Parties confirm that "reasonable efforts" have been made to identify if transferred data is covered by the local law or practice of the importer's jurisdiction that "goes beyond what is necessary and proportionate in a democratic society to safeguard important public interest objectives, and that may reasonably be expected to a ffect the protections, rights, and safeguards afforded to DS under this Agreement." Parties confirm they are not aware such a rule or practice exists.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

LIABILITY	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**Recital 14:** The Clauses should provide for liability between the parties/indemnification from data subjects. **M1/M2/M3/M4 Clause 12(a)**: Each party shall be held liable to the other Parties for any damages it causes by breach of the Clauses. If an exporter is held liable for damages caused by the data importer or a sub-processor, it is entitled to claim compensation from the importer related to the importer's responsibility for the damage. **M1/M4 Clause 12(b):** Each Party will be liable to the DS. The DS will be entitled to compensation for any material or non-material damages caused by any Party violating this Agreement's Third-Party Beneficiary Rights. **M1/M4 Clause 12(c)**: Parties are joint and severally liable. **M1/M4 Clause 12(d)**: Parties may claim back compensation for any assessed liability from other parties based on their responsibility for loss incurred. **M1/M4 Clause 12(e)**: importer cannot invoke the conduct of a processor or a subprocessor to avoid liability. **M2/M3 Clause 12(b):** Each Party will be liable to the DS. DS will be entitled to compensation for any material or non-material damages **caused by the importer or its Sub-processor** for violating this Agreement's Third-Party Beneficiary Rights. **M2/M3 Clause 12(c):** If data exporter is held liable for damages caused by the data importer (or its Sub-processor), it will be entitled to claim back from the data importer the compensation corresponding to the Importer's responsibility for the damage. **M2 Clause 12(d):** If more than one Party is responsible for any damage caused to the DS, all responsible Parties shall be jointly and severally liable. **M2 Clause 10(e):** If one Party is held liable, it shall be entitled to claim back from the other Party(s) the compensation corresponding to its responsibility for the damage. **M2 Clause 10(f):** Importer cannot invoke the conduct of a Sub-processor to avoid liability.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 9(a)/M2 Clause 10(a):** Each Party will be liable to the other Party(s) for any damages it causes the other Party(s) by any breach of this Agreement. **M1 Clause 9(b):** Each Party will be liable to the DS. DS will be entitled to compensation for any material or non-material damages **caused by any of the Parties** for violating this Agreement's Third-Party Beneficiary Rights. **M1 Clause 9(c)**: Parties are joint and severally liable. **M1 Clause 9(d)**: Parties may claim back compensation for any assessed liability from other parties based on their responsibility for loss incurred. **M2 Clause 10(b):** Each Party will be liable to the DS. The DS will be entitled to compensation for any material or non-material damages **caused by the data importer or its Sub-processor** for violating this Agreement's Third-Party Beneficiary Rights. **M2 Clause 10(c):** If the exporter is held liable for damages caused by the importer (or its Sub-processor), it will be entitled to claim back from the importer the compensation corresponding to the importer's responsibility for the damage. **M2 Clause 10(d):** If more than one Party is responsible for any damage caused to the DS, all responsible Parties shall be jointly and severally liable. **M2 Clause 10(e):** If one Party is held liable, it shall be entitled to claim back from the other Party(s) the compensation corresponding to its responsibility for the damage. **M2 Clause 10(f):** The Data Importer cannot invoke the conduct of a Sub-processor to avoid liability.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

ACCURACY OF INFORMATION

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 8.3(a): "**Each Party shall take reasonable steps to ensure the information is accurate." **M1 Clause 8.3(b):** Each party must inform the other if it becomes aware the personal data transferred or received is inaccurate. **M1 Clause 8.3(c):** the data importer shall ensure that the personal data is adequate, relevant, and limited to what is necessary in relation to the purpose of processing. **M2/M3 Clause 8.4:** If the data importer becomes aware that the personal data it has received has become inaccurate or outdated, it shall inform the exporter without delay.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C** **M2: C2P**	**M1 Clause 6.4 (a):** The Parties shall ensure that personal data is accurate and, where necessary, kept up to date. Importer shall take all reasonable steps to promptly delete or rectify any personal data that is inaccurate for the purposes for which it is being processed. **M1 Clause 6.4(b)/M2 Clause 6.5(a):** If one of the Parties becomes aware that the personal data transferred or received is inaccurate or outdated, it will inform the other party without undue delay. **M1 Clause 6.4(c):** Importer shall ensure that the personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is being processed. **M2 Clause 6.5(b):** The Importer shall cooperate with the exporter to erase or rectify the data.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1/M2 Clause 2.2 [Optional]:** "Any personal data that have been transferred under this contract is accurate and complete to the extent necessary for the purposes identified by the Data Exporter in order to comply with Clause 2.1."

RECORDKEEPING

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 8.5(g): "**the data importer shall document all relevant facts relating to a data breach, including effects and any remedial measures taken." **M1 Clause 8.9(a):** "Each Party shall be able to demonstrate compliance with its obligations under these Clauses." **M2/M3 Clause 8.9(b):** "Each Party shall be able to demonstrate compliance with its obligations under these Clauses; and importer shall keep documentation of its ability to carry out processing for the Controller."
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.6(b)*:** The data importer shall document all relevant facts related to the personal data breach and keep a record thereof. **M1 Clause 6.10(a):** Parties must be able to demonstrate compliance with the obligations of the agreement. **M1 Clause 6.10(b)/M2 Clause 6.10(a):** The iata importer shall keep appropriate documentation of the processing activities carried out under its responsibility, which shall be made available upon request to the Data Exporter and, where appropriate, the Competent Supervisory Authority. *note that this is the second (b) under section 6.6
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**[Optional] M1 3.6:** On reasonable request from exporter, importer-processor shall provide access to processing facilities, files, and documentation for review and audit purposes, given [party-selected notice and timing.]

SECURITY	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 8.5/M2/M3 Clause 8.6/M4 Clause 8.2:** Importer, and exporter during the transfer, shall Implement and maintain appropriate technical and organizational security measures during transmission ... including consideration of encryption or pseudonymization. When determining security measures, the Parties shall account for: » The risk to the rights and freedoms of the DS, particularly due to the potential quantitative and qualitative value that the processed Personal Data could represent for a third party that is not authorized to possess it; » The state of the art; » The costs of Implementation; » The nature of the processed personal data, especially if it is Sensitive Personal Data; » The scope, context, and purposes of the processing; » The potential consequences of a data breach for the DS; » Previous data breaches that occurred in the processing. **M1 Clause 8.5(b); M2/M3 Clause 8.6(a):** the importer shall carry out regular checks to ensure the listed technical and organizational measures continue to provide an appropriate level of security. **M2/M3 Clause 8.6:** "...In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter."
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1/M2 Clause 6.6(a):** Importer, and exporter during the transfer, shall implement and maintain appropriate administrative, physical and technical measures to ensure the confidentiality, integrity, and availability of the personal data. When determining security measures, the Importer must consider: » The risk to the rights and freedoms of the DS, particularly due to the potential quantitative and qualitative value that the processed Personal Data could represent for a third party that is not authorized to possess it; » The state of the art; » The costs of Implementation; » The nature of the processed personal data, especially if it is Sensitive Personal Data; » The scope, context, and purposes of the processing; » The potential consequences of a data breach for the DS; » Previous data breaches that occurred in the processing.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 2.3:** "The Data Exporter shall implement adequate technical and operational measures to ensure the security of the Personal Data during transmission to the Data Importer." **M1 3.9/M2 3.2:** Importer shall have in place reasonable/appropriate technical, organizational and physical security measures. **M2 Clause 4.1:** Both Parties have taken appropriate steps to determine the level of potential risk of data breaches involved in transferring the relevant data and to consider suitable security measures that both parties must undertake; **M1 Clause 3.4 [optional]:** "The Data Importer agrees to take reasonable steps to implement measures ... that comply with adequate security standards prescribed by the Data Exporter." **M1 Clause 3.9/M2 Clause 3.2:** The Data Importer shall have in place reasonable and appropriate technical, administrative, operational and physical measures, consistent with AMS Law to protect the confidentiality, integrity, and availability of the PD. **M2 Clause 4.2:** Both Parties shall agree on an implement appropriate controls and adequate security standards that shall apply to the storage and Processing of personal data.

CHOICE OF LAW

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**Recital 12:** "while parties should be able to choose the law of one of the Member States as governing the standard contractual clauses, that law must allow for third-party beneficiary rights." **M1/M2/M3 Clause 13(a):** Identifies, based on the exporter's establishment/relationship to the EU, the competent supervisory authority. **(b):** Indicates that an importer will submit itself to the jurisdiction of the authority identified in (a). **M1/M2/M3 Clause 17:** The parties will select an EU Member State's law to apply that permits third party beneficiary rights. OR **M2/M3 Clause 17**: The Clauses shall be governed by the law of the EU Member State where the exporter is established, unless that state does not allow third party beneficiary rights in which case another Member State's law will be established.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 1.4(b): Governing Law** is the Personal Data Protection Law of the Data Exporter's jurisdiction. **M1 Clause 2.2(a):** This Agreement will be read and interpreted in accordance with the provisions of the Governing Law. **M1 Clause 2.2 (b):** Parties may add new terms when necessary to comply with the Governing Law and so long as this "does not negatively affect the protections granted by the model contractual clauses." **M1 Clause 2.2 (c):** This Agreement cannot be interpreted in a way that conflicts with the rights and obligations established in the Governing Law. **M1 Clause 13/ M2 Clause 14:** the Agreement shall be governed by [The exporter's jurisdiction]
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 4.1:** The parties designate an AMS jurisdiction law to govern the agreement. **M2 Clause 5.1:** The parties designate a national jurisdiction to govern the agreement. **M1/M2 Clause 4.2**: In the event of a conflict between AMS Law and these Clauses, AMS Law shall prevail.

CHOICE OF VENUE

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3 Clause 18:** The parties agree disputes will be solved in an EU Member State Court they select; A DS may bring proceedings against either Party in the MS where they have their primary residence; the Parties agree to submit to the jurisdiction of the designated courts.ç
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 14(a)/M2 Clause 15(a):** Any dispute arising from this Agreement shall be resolved by the courts of the Data Exporter's jurisdiction. **M1 Clause 14(b)/M2 Clause 15(b):** DS may also bring action against a Data Exporter and/or Data Importer, which may be initiated in the country of the Data Exporter or where the DS has habitual residence.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 4.3/M2 Clause 5.3 [Optional]:** Any dispute under the contract shall be resolved by [selected method].

SENSITIVE DATA

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 8.6:** Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offenses (hereinafter 'sensitive data') [definitions of taken from Articles 9 and 10 GDPR], importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved; this may include restricting personnel permitted to access the data, or additional security measures such as pseudonymization or additional restrictions with regard to further disclosure. **M2/M3 Clause 8:** Where the transfer involves [sensitive data] importer shall apply specific restrictions described in Annex I.B
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1/M2 Clause 1.4(b):** Sensitive personal data is personal data that refer to the intimate sphere of the Data Subject, the undue use of which may result in discrimination or create a serious risk thereof. In an illustrative way, PD that may reveal aspects such as racial or ethnic origin; beliefs or religious, philosophical and moral convictions; trade union memberships; political opinions; information regard health, sexual life, preference or orientation; genetic data; or biometric data aimed at identifying a natural person in an unequivocal matter shall be considered as sensitive. **M1 Clause 6.8:** Where the transfer involves sensitive data the Importer shall apply specific restrictions and additional safeguards based on the specific nature of the data and risks involved. These restrictions may include restricting personnel permitted to access PD; additional confidentiality agreements; or additional security measures; additional restrictions on Onward Transfers. Where the data involves children or adolescents, the Parties must "privilege the protection of their superior interests, in accordance with the Convention on the Rights of the Child and other international obligations. **M2 Clause 6.8:** Where the transfer involves Sensitive Personal Data, the Importer shall apply specific restrictions or safeguards described in Annex C. Where the data involves children or adolescents, the Parties must privilege the protection of their superior interests, in accordance with the Convention on the Rights of the Child and other international obligations.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

ACCESSION BY ADDITIONAL PARTIES

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3/M4 Clause 7**: "An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer..."
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1/M2 Clause 1.2(b):** This Agreement allows for the incorporation of additional importers and/or exporters as set out in Clause 5, using Annex A. **M1/M2 Clause 5(a):** The Parties accept that any entity that is not a Party to this agreement may, with the prior consent of all Parties involved, join at any time as a Data Exporter or Data Importer by signing Annex A and other Annexes if applicable. **M1/M2 Clause 5(c):** The joining Party shall not acquire rights and obligations under the Agreement prior to its adhesion.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

Annex II: Exporter Rights/Obligations

The "Exporter Rights/Obligations" chart is designed to track provisions that create obligations specific to Data Exporters.

LAWFULNESS OF PROCESSING	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3/M4 Clause 1:** General applicability of the GDPR, including Art. 5, to processing activity.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**N/A:** No affirmative requirement that exporters warrant lawfulness of data collection/transmission.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**MCC Explanatory Doc p.5; M1/M2 Clause 2.1:** "Lawful/Legal Basis for Collection, Use and Disclosure" – requires that an exporter warrant any data "is collected, used, disclosed, and transferred in accordance with applicable AMS law. In the absence of such law, DS have been notified and given consent to the purposes, where reasonable and practicable."

RESPONDING TO REQUESTS FROM INDIVIDUALS	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3 Clause 8.3**: On request from the data subject, the exporter shall provide the data subject a copy of the Clauses, including the descriptive Appendix as completed by the parties, free of charge. If necessary to protect business secrets or other confidential information, parties have the option to redact business secrets or confidential information. If redactions are made, the parties shall provide the DS the reasons for the redaction.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 7(a):** The Importer, with the assistance of the Exporter where necessary, must respond to DS requests free of charge within 15 business days, unless applicable law indicates a shorter time. **M2 Clause 8(a-c):** Importer shall promptly notify the exporter of requests from DS. The importer shall assist the exporter in fulfilling its obligations to respond to the requests. The Parties can set out the scope of the assistance required and the measures to be taken using Annex C. The data importer shall comply with the instructions from the data exporter.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 2.4**: The data exporter will respond to any requests from DS regarding the processing of personal data by importer, including requests to access or correct data, unless agreed otherwise by the parties and such delegation is permitted under AMS law. Responses must be made within "a resonable time frame" or alternatively, any time frame required by applicable AMS law.

RESPONDING TO REQUESTS FROM PUBLIC AUTHORITIES

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**[specific to EU processor • non-EU controller] Recital 16**: "Additional requirements to address any effects of the laws of the third country of destination on the controller's compliance with the clauses, in particular how to deal with binding requests from public authorities in the third country for disclosure of the transferred personal data, should apply where the Union processor combines the personal data received from the controller in the third country with personal data collected by the processor in the Union." **M3 Clause 15.1(a)(ii):** the data exporter shall forward any notice of government access to data from the data importer to the controller.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**N/A**
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 2.4**: The data exporter will respond to any requests from Enforcement Authorities regarding the processing of personal data by the data importer, including requests to access or correct data, unless agreed otherwise by the parties and such delegation is permitted under AMS law. Responses must be made within "a reasonable time frame" or alternatively, any time frame required by applicable AMS law.

DUE DILIGENCE

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3/M4 Clause 8**: "the data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through implementation of appropriate technical and organizational measures, to satisfy these clauses."
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.1(a)/M2 Clause 6.2(a):** The data exporter warrants that it has made reasonable efforts to determine that the importer is able to perform its obligations under this Agreement by applying appropriate "Administrative, Physical, and Technical Measures."
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

AUDIT AND ACCOUNTABILITY

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M2 Clause 8.9(d)**: the exporter may choose to conduct an audit itself or mandate an independent auditor. Audits may include inspections of the importer's premises or physical facilities and shall be carried out with reasonable notice where appropriate. **(e):** The Parties shall make audit results available to the SA on request. **M3 Clause 8.9(e):** If an audit of the importer is carried out on the controller's instructions, the results shall be made available to the controller. **(f):** the exporter may choose to conduct an audit itself or mandate an independent auditor. Audits may include inspections of premises or physical facilities and shall be carried out with reasonable notice where appropriate. **(g):** The Parties shall make audit results available to the SA on request.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.1(a)/M2 Clause 6.2(a):** The data exporter warrants that it has made reasonable efforts to determine that the importer is able to perform its obligations under this Agreement by applying appropriate "Administrative, Physical, and Technical Measures."
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	[**Optional**] **M1 Clause 3.6:** At the reasonable request of the exporter, the importer shall provide access to its data processing facilities, data files, and documentation by [notice and timing requirements selected by parties] for purposes of review and/or audit to verify compliance with the contract.

BREACH NOTIFICATIONS

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M2/M3 Clause 8.6(d)**: Acknowledgement of a controller-exporter's obligation to comply with GDPR's Article breach notification requirements under Articles 33 and 34, which require » notification of a breach "likely to result in a risk to the rights and freedoms of a natural person" to the supervisory authority within 72 hours » notification of a breach "likely to result in a high risk to the rights and freedoms of natural persons" to the data subject "without undue delay." **M4 Clause 8.4:** … in case of a personal data breach concerning the personal data processed by the data exporter under the Clauses, 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.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.6 "Personal Data Breach"*:** When any of the Parties becomes aware of a Personal Data Breach, it shall notify the other Party, the Competent Supervisory Authority, and the affected Data Subjects without any delay and at latest **within five days**. The notification must be in clear language and contain at least: » The nature of the incident » Affected Personal Data » Corrective actions taken so far » Recommendations, if any, to Data subjects to protect their interests; » How Data Subjects can obtain more information This notice can be delivered in a "phased" manner and does not need to be delivered at all if it involves disproportionate effort for the Data Importer. If no notice is given to Data Subjects, then the Data Importer must issue a public communication. *In the original document, this Clause is not numbered, but falls under Clause 6.6.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

RETENTION/SUSPENSION/TERMINATION

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3/M4 Clause 16(b):** If importer is in breach or cannot comply with the Clauses, the exporter will suspend transfers until compliance is regained or the contract is terminated. **(c):** the exporter is entitled to terminate the contract, as it applies to personal data transferred under the Clauses, if: » The exporter has suspended transfer due to non-compliance or breach and rectification has not occurred within a reasonable time, or within one month of suspension. » The importer is in persistent breach » The importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under the Clauses. **(d)** Personal data that has been transferred prior to the termination of the contract pursuant to the previous paragraph shall at the choice of exporter immediately be returned to exporter or deleted in its entirety. The same shall apply to any copies of the data. Importer shall certify the deletion of the data to exporter. Until the data is deleted or returned, importer shall continue to ensure compliance with this Agreement. In case of local laws applicable to importer that prohibit the return or deletion of the transferred personal data, importer warrants that it will continue to ensure compliance with this Agreement and will only process the data to the extent and for as long as required under that local law.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 12/M2 Clause 13(a-d):** Importer shall immediately notify exporter if it is unable to comply with any provision of this Agreement, for whatever reason. In the event that importer fails to comply with its obligations under this Agreement, exporter shall suspend the transfer of personal data to importer until compliance is again ensured or the contract is terminated. Exporter shall be entitled to terminate this Agreement when: » Exporter has suspended the transfer of personal data to importer pursuant to the previous paragraph and compliance with this Agreement is not restored within a reasonable period of time and within 30 business days following suspension; » Importer is in substantial or persistent breach of this Agreement; or » Importer fails to comply with a binding decision of a court or Competent Supervisory Authority regarding its obligations under this Agreement. In this case, it shall inform the Competent Supervisory Authority of its non-compliance. personal data that has been transferred prior to the termination of the contract pursuant to the previous paragraph shall at the choice of exporter immediately be returned to exporter or deleted in its entirety. The same shall apply to any copies of the data. Importer shall certify the deletion of the data to the exporter. Until the data is deleted or returned, importer shall continue to ensure compliance with this Agreement. In case of local laws applicable to importer that prohibit the return or deletion of the transferred personal data, the importer warrants that it will continue to ensure compliance with this Agreement and will only process the data to the extent and for as long as required under that local law.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1/M2 Clause 6.1.1/6.1.3/6.1.4:** Exporter may terminate the contract if: » Importer is in material breach of its obligations; » Transfer of personal data has been suspended longer than a designated time; » Compliance with the Contract by either Party would put that party in breach of the law that applies in the country where it is processing personal data; » Importer ceases operations voluntarily or involuntarily. » There has been a final decision from which no further appeal is possible that there has been a breach of the contract by either party. **M1/M2 Clause 6.1.1/6.1.3/6.1.4:** Exporter may terminate the contract if: » Importer is in material breach of its obligations; » Transfer of personal data has been suspended longer than a designated time; » Compliance with the Contract by either Party would put that party in breach of the law that applies in the country where it is processing personal data; » Importer ceases operations voluntarily or involuntarily. » There has been a final decision from which no further appeal is possible that there has been a breach of the contract by either party.

DUE DILIGENCE	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1/M2/M3/M4 Clause 8**: "the data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through implementation of appropriate technical and organizational measures, to satisfy these clauses."
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.1(a)/M2 Clause 6.2(a):** The data exporter warrants that it has made reasonable efforts to determine that the importer is able to perform its obligations under this Agreement by applying appropriate "Administrative, Physical, and Technical Measures."
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

Annex III: Importer Rights/Obligations

The "Importer Rights/Obligations" chart is designed to track provisions that create obligations for Data Importers.

ONWARD TRANSFERS

EU Standard Contractual Clauses

M1: C2C
M2: C2P
M3: P2P
M4: P2C

Recital 11: "Onward transfers by the data importer to a third party in another country should only be acceded to by the importer if the third part accepts the SCCs."

M1 Clause 8.8
The Data Importer may only disclose the Personal Data to third parties located outside of the Exporter's jurisdiction if the third party agrees to be bound by this Agreement OR if:

i. The transfer is addressed to a country that has received a declaration of adequacy;
ii. The third party recipient provides "adequate safeguards" that comply with Chapter V GDPR;
iii. The third party enters a binding agreement with the Data Importer that "the same level of protection as the Clauses" and the Data Importer shares these safeguards with the Data Exporter;
iv. The onward transfer is required for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings;
v. The transfer is necessary to protect the vital interests of the Data Subject or another natural person; or
vi. Without the other conditions, the Importer has received the express consent of the Data Subject and has provided the Data Subject information regarding the purpose, identity of the recipient, and possible risks of the transfer, and informed the Data Exporter and, if the Exporter requests, has provided a copy of the information provided to the Data Subject.

M2/M3 Clause 8.8: The importer shall only disclose the personal data to a third party on instructions from the controller, as communicated by the exporter (if the controller is not the exporter).

The Data Importer may only disclose the Personal Data to third parties located outside of the Exporter's jurisdiction if the third party agrees to be bound by this Agreement OR if:

i. The transfer is addressed to a country that has received a declaration of adequacy;
ii. The third party recipient provides "adequate safeguards" that comply with Chapter V GDPR;
iii. The onward transfer is required for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings;
iv. The transfer is necessary to protect the vital interests of the Data Subject or another natural person; or

ONWARD TRANSFERS	
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.9(a):** The Data Importer may only disclose the Personal Data to third parties located outside of the Exporter's jurisdiction if the third party agrees to be bound by this Agreement OR if: i. The Governing Law includes adequacy and the transfer is addressed to a country that has received a declaration of adequacy; ii. The third party recipient provides "adequate safeguards" that comply with Governing Law; iii. The third party enters a binding agreement with the Data Importer that contains adequate safeguards, and the Data Importer shares these safeguards with the Data Exporter; iv. The onward transfer is required for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; v. The transfer is necessary to protect the vital interests of the Data Subject or another natural person; or vi. Without the other conditions, the Importer has received the express consent of the Data Subject and has provided the Data Subject information regarding the purpose, identity of the recipient, and possible risks of the transfer, and informed the Data Exporter and, if the Exporter requests, has provided a copy of the information provided to the Data Subject. **M2 Clause 6.9(a):** The Data Importer shall only disclose Personal Data to a third party on documented instructions from the Data Exporter, or if: i. The transfer is addressed to a country that has received a declaration of adequacy; ii. The third party recipient provides "adequate safeguards" that comply with Chapter V GDPR; iii. The onward transfer is required for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; iv. The transfer is necessary to protect the vital interests of the Data Subject or another natural person; or
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 3.2:** The Data Importer shall not further disclose or transfer the personal data it receives from the Data Exporter to another person, Enforcement Authority, or legal entity, including to Data Sub-Processors, unless it has notified the Data Exporter of such further disclosure or transfer in writing, and provided reasonable opportunity for the Data Exporter to object." **M1 Clause 3.3:** Importer agrees that prior to any disclosure to a sub-processor, it will ensure the sub-processor is bound to the same obligations it has to the exporter.

RESPONDING TO REQUESTS FROM PUBLIC AUTHORITIES	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**Recital 18**: "The standard contractual clauses should provide **specific safeguards** … **to address any effects of the laws of the third country of destination on the data importer's compliance with the clauses**, in particular how to deal with binding requests from public authorities in that country for disclosure of the transferred personal data." **M1/M2/M3/M4 Clause 15.1(a):** The importer will notify the exporter and where possible the DS promptly if: » it receives a legally binding request from a public authority, including judicial authorities. » it becomes aware of any direct access by public authorities to the data transferred pursuant to the Clauses. **(b):** If prohibited from notifying the data exporter about a request from a public authority, the data importer will use "best efforts" to obtain a waiver of the prohibition, to communicate as much as possible as fast as possible. The importer agrees to document its efforts to demonstrate them on the request of the exporter. **(c):** The data importer agrees to provide the data exporter with regular updates about the number and type of requests from public authorities it receives, if permitted by domestic law. **15.2 (a-b):** The data importer agrees to review the legality of government requests for disclosure; challenge requests if it believes on careful review there are grounds that a request may be unlawful, and pursue applicable any applicable appeals; importer also will document its legal assessment of such requests and make such documentation available to the data exporter.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 11(b)/M2 Clause 12(b):** The importer agrees to notify the exporter if it becomes subject to laws or practices beyond what is reasonable or necessary in a democratic society. **M1 Clause 11(d)/M2 Clause 12(c):** If a court or government agency requires the Importer to process the transferred data in a way not permitted by the Agreement, the Importer must: » Assess the legality of the request; » Challenge any requests it concludes there are reasonable grounds to believe are illegal under local law; » Where permitted under local law, promptly notify the Data Exporter it has received such a request. If not permitted to give such notice, make reasonable efforts to obtain a waiver of the prohibition.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 3.11:** "The Data Importer shall promptly notify and consult with the Data Exporter regarding any investigation regarding the collection, use, transfer, disclosure, security, or disposal of the Personal Data… unless otherwise prohibited under law."

AUDITS AND ACCOUNTABILITY	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**Recital 15:** "[the importer] must make available all information necessary to demonstrate compliance with the obligations set out in the clauses and to allow for AND CONTRIBUTE TO audits of its processing activities by the exporter." **Recital 17:** "the data importer should be required to keep appropriate documentation for the processing activities under its responsibility and to inform the data exporter promptly if it is unable to comply with the clauses, for whatever reason." ... "personal data that has been transferred prior to the termination of the contract, and any copies thereof, should at the choice of the exporter be returned to the exporter or destroyed in their entirety." **M1 Clause 8.9(a):** Each party shall be able to demonstrate compliance with its obligations under these clauses. **In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.** **M2 Clause 8.9(c):** The data importer shall make available to the exporter all information necessary to demonstrate compliance with the Clauses and at the exporter's request, allow for and contribute to audits of processing activities at reasonable intervals or if there is indication of noncompliance. **(e):** The Parties shall make audit results available to the SA on request. **M3 Clause 8.9(c):** The data importer shall make all information necessary to demonstrate compliance available to the exporter, which shall provide it to the controller. **(d):** The data importer shall allow for and contribute to audits by the data exporter; at reasonable intervals or if there is indication of noncompliance. **(e):** If an audit of the importer is carried out on the controller's instructions, the results shall be made available to the controller. **(f):** the exporter may choose to conduct an audit itself or mandate an independent auditor. Audits may include inspections of premises or physical facilities and shall be carried out with reasonable notice where appropriate. **(g):** The Parties shall make audit results available to the SA on request.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1: N/A** **M2 Clause 6.10(c):** The data importer shall make available to the exporter all information necessary to demonstrate compliance with the Clauses and at the exporter's request, allow for and contribute to audits of processing activities at reasonable intervals or if there is indication of noncompliance.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 3.6 [Optional]:** At the reasonable request of the Data Exporter, the importer shall provide access to its processing facilities, files, and documentation, for the purposes of auditing or to verify compliance with the obligations of the MCCs. **M2:** N/A

AUTOMATED DECISION-MAKING	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 10(d):** The data importer shall not make decisions solely based on automated processing that would produce legal or similarly significant effects without the express consent of the data subject. The data importer will where necessary ensure the data subject is informed of any envisaged automated decision-making, the logic involved, and the potential consequences, and implement suitable safeguards that at least: » Enable the DS to contest the decision » Enable the DS to obtain review by a human being
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 7.2(a-b):** The Data Importer will not make an Automated Individual Decision with respect to the transferred Personal Data unless: » The decision is authorized by the law of the Importer's country, or » It is based on the express consent of the Data Subject **M1 Clause 7.2(c):** If an Automated Individual Decision is made, the Data Subject has the right to: » An explanation about the decision made; » Express their point of view and challenge the decision; and » Obtain human intervention. **M1 Clause 7.2(d):** The Controller may not carry out automated Personal Data Processing that leads to discrimination against Data Subjects due to their: » Racial or ethnic origins; » Religious, philosophical, and moral beliefs or convictions; » Trade union membership; » Political opinions; » Sexual life, preference or orientation; or » The Processing of health, genetic or biometric data.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

EXPORTER/IMPORTER RELATIONSHIP	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**Recital 16:** "The SCCs require the processor to inform the controller if it is unable to follow its instructions, including if the controllers' instructions infringe EU data protection law." **M2 Clause 8.1:** The importer shall process data only pursuant to the instructions of the exporter. **M2 Clause 8.9(a):** The importer shall respond promptly to enquiries from the exporter about the processing. (c): The importer shall make information necessary to demonstrate compliance **M3 Clause 8.1:** An importer processor receiving information from an exporter processor must be informed that the exporter is a processor, and receive the exporter's instructions from the controller. Additional instructions from the exporter may not conflict with those from the controller. **M2/M3 Clause 8.9:** "The importer shall promptly and adequately deal with requests from the exporter or the controller (where the exporter is not the controller) that relate to processing under the clauses." **M3 Clause 11**: in the event of a dispute between a DS and one of the Parties, the party will attempt to resolve the dispute quickly and fairly. Importer and Exporter shall keep one another informed about any such disputes. **M1/M2/M3/M4 Clause 14(e):** The data importer will notify the exporter (and controller, if different) if after agreeing to the Clauses, it has reason to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the Clauses.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M2 Clause 6.1:** The Data Importer shall carry out Personal Data processing activities without any decision-making power over the scope and content thereof, and instead limit its actions to the terms and instructions established by the Data Exporter. **M2 Clause 6.7(b):** The Data Importer shall ensure that the persons authorized to process the Personal Data maintain and respect the confidentiality thereof, which is an obligation that shall continue to apply **even after the end of its contractual relationship with the Data Exporter.**
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1/[optional M2] Clause 3.1:** The Importer shall process the data only in accordance with the Exporter's instructions and for the purposes given in Appendix A. **M1 Clause 3.7 [Optional]**: The importer shall correct any error or omission in the PD reasonably requested by the Data Exporter, within the shorter of the designated timeframe or the timeframe imposed by AMS Law.

RESPONDING TO REQUESTS FROM INDIVIDUALS

EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**Recital 16:** "The parties should be required to assist one another with any requests from data subjects based in local law OR based on the GDPR." **M1 Clause 10(a):** The data importer shall be responsible for dealing with requests from individuals data subjects without undue delay and at the latest within 30 days of the receipt of a request. Complex requests may be extended for up to 60 days. Responses must be intelligible, easily accessible, and use clear and plain language. **M2/M3 Clause 10(a)**: the importer shall inform the exporter of any request received, and shall not respond unless authorized to do so by the exporter. **M1 Clause 10(b):** The data importer shall on request from a data subject provide: » whether processing of the DS's information is happening. » a copy of the information and a copy of the information in Annex I [the purposes of processing] » If the data is further transferred, information about the recipient or categories of recipients » information on the purposes of any onward transfer » information on the right to lodge a complaint with a supervisory authority **M1 Clause 10(c)**: The data importer will cease direct marketing if requested by the DS. **M1 Clause 10(e-g):** An importer may refuse a data subject request if: » The requests are excessive/repetitive » Refusal is allowed under the laws of the importer's country, and the laws are necessary and proportionate to a democratic society and protect principles given in GDPR Article 23. » If a request is refused, the importer must inform the DS of the reasons for doing so and of the DS right to lodge a complaint/seek judicial review.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 7(a):** The Importer, with the assistance of the Exporter where necessary, must respond to Data Subject requests free of charge within 15 business days, unless applicable law indicates a shorter time. **M1 Clause 7(b):** The Importer will take appropriate measures to facilitate such requests. Any information provided to Data Subjects shall be in an intelligible and easily accessible form, using clear and plain language. **M2 Clause 8(a-c):** The Data Importer shall promptly notify the Data Exporter of any request it has received from a Data Subject. It shall not respond to such a request itself unless it has been authorized to do so by the Data Exporter. The Data Importer shall assist the Data Exporter in fulfilling its obligations to respond to Data Subjects' requests in the exercise of their rights under the Governing Law. In this regard, the Parties shall set out in Annex C the appropriate Administrative, Physical and Technical Measures, taking into account the nature of the Processing, by which they ensure the assistance to the Data Exporter, as well as the scope and the extent of the assistance required.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 3.5**: The data importer shall promptly communicate any requests from DS about personal data to the data exporter. **M2 Clause 3.3**: The importer shall provide to the exporter and the DS a contract point who is authorized on behalf of the importer to respond to enquiries concerning personal data. [**Optional**] **M2 4.3**: The data exporter and the data importer shall each respond to enquiries from relevnt DS or enforcement authorities regarding processing of personal data in their respective jurisdictions, including requests for access or correction.

DATA PROCESSING PURPOSE LIMITATION	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 8.1:** The data importer shall process the personal data only for the specific purposes(s) of the transfer, as set out in Annex I B. It may only process for another purpose: (i) where it has obtained the data subject's prior consent; (ii) where it is necessary for the establishment, exercise or defense of legal claims in the context of specific proceedings; (iii) where necessary to protect the vital interests of the data subject or another natural person." **M2 Clause 8.1-8.2**: The importer shall process data only on the instructions of the exporter, as set forth in the applicable Annex.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.2(a)/M2 Clause 6.3:** Importer will not process the personal data subject to this Agreement for purposes other than those set out in Annex B, **unless otherwise instructed by the Data Exporter.** **M1 Clause 6.2(b):** The Importer may only process personal data for other purposes: » With the prior consent of the DS; » When necessary for the establishment, exercise, or defense of legal claims within the framework of specific administrative, regulatory, or judicial procedures; or » When necessary to protect the vital interests of the DS or of another natural person.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1/[optional M2] Clause 3.1:** The Importer shall process the data only in accordance with the Exporter's instructions and for the purposes given in Appendix A.

RETENTION/SUSPENSION/TERMINATION	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 8.4:** The data importer shall retain information for no longer than necessary for the purposes of processing. **M2/M3 Clause 8.5:** the importer shall return or delete transferred information after the specified duration, at the instruction of the exporter. **M1/M2/M3/M4 Clause 16(a):** Importer shall inform exporter if it is unable to comply with the Clauses for any reason.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.5(a):** Importer will not retain Personal Data longer than is necessary for the purposes for which it is processed. **M1 Clause 6.5(b)**: Importer will establish appropriate administrative, physical, and technical methods to ensure compliance with this obligation, including deletion or anonymization of data and backup copies at the end of processing.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**M1 Clause 3.8:** Upon termination of the agreement or completion of processing, importer shall either return the personal data to exporter or cease to retain it, at the election of exporter. **M1 Clause 6.1.1/6.2.1-6.2.4:** Importer may terminate the contract if: » Exporter is in material breach of its obligations; » Transfer of personal data has been suspended longer than a designated time; » Compliance with the Contract by either Party would put that party in breach of the law that applies in the country where it is processing personal data; » Importer ceases operations voluntarily or involuntarily. » There is a final decision from which no further appeal is possible that there has been a breach of the contract by either party

CONFIDENTIALITY	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 8.5(c):** Persons authorized to process data have committed to confidentiality or are subject to such a legal requirement. **M2/M3 Clause 8.6(b):** The importer shall grant access only to personnel strictly necessary for the implementation of the contract.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1/M2 Clause 6.7(a-b):** Importer will ensure persons processing personal data under its authority are bound by a duty of confidentiality, and that duty continues beyond the end of the relationship with exporter.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**N/A**

BREACH NOTIFICATIONS	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M1 Clause 8.5(e):** Without undue delay, importer shall notify exporter and Supervisory Authority of breach likely to result in risk to rights and freedoms of DS. **M1 Clause 8.5(f):** In the event of a breach likely to result in a high risk to the rights and freedoms of affected individuals, the importer will notify the individuals, unless: » The importer has taken measures to significantly reduce the risk OR » Notification would involve disproportionate effort If either applies, a public communication or similar shall be issued. **M1 Clause 8.5(d):** The importer shall take appropriate measures to address any breach **M2 Clause 8.6(c-d):** The importer shall notify the exporter **without undue delay** after learning of a breach; describe the nature of the breach; response to the breach and mitigation efforts; and cooperate with the exporter to enable it to meet its obligations. **M3 Clause 8.6(c):** the importer shall notify the controller of a breach as well as the exporter where appropriate and feasible

BREACH NOTIFICATIONS	
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M1 Clause 6.6 "Personal Data Breach" (a*:** In the event of a breach of personal data processed by importer, importer will take appropriate steps to address the breach and to mitigate any potential negative effects. **(c)** When any of the Parties becomes aware of a Personal Data Breach, it shall notify the other Party, the Competent Supervisory Authority, and the affected Data Subjects **within five days**. The notification must be in clear language and contain at least: » The nature of the incident » Affected Personal Data » Corrective actions taken so far » Recommendations, if any, to Data subjects to protect their interests; » How Data Subjects can obtain more information This notice can be delivered in a "phased" manner and does not need to be delivered at all if it involves disproportionate effort for importer. If no notice is given to DS, then importer must issue a public communication. **M2 Clause 6.6(c):** The data importer shall notify the exporter within 72 hours of becoming aware of the breach. The notification must include a description (including the categories of personal data and number of DS affected, if possible), likely consequences, and measures taken or proposals to address the breach and mitigate its effects. *In the original document, this Clause is not numbered, but falls under Clause 6.6.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**Obligations of ASEAN MCCs, p5**: "The Data Importer shall notify the relevant authorities and Data Exporter without undue delay or within a reasonable time specified by the parties if it becomes aware of [a breach of security.]" **M1 Clause 3.10**: If Importer becomes aware that a data breach has occurred affecting data in its possession or control, or under the control of an importer who received the data as part of an onward transfer, it shall notify the Exporter » without undue delay or » within a reasonable time specified by the Parties. **M2 Clause 3.4**: If importer becomes aware that a data breach has occurred affecting data in its possession or control, or under the control of an importer who received the data as part of an onward transfer, it shall notify the exporter » without undue delay or » within a reasonable time specified by the Parties.

USE OF SUB-PROCESSORS	
EU Standard Contractual Clauses **M1: C2C** **M2: C2P** **M3: P2P** **M4: P2C**	**M2/M3 Clause 9(a):** The data importer shall not sub-contract any of its processing activities to a sub-processor without prior specific written authorization from the data exporter, or if the exporter is not the controller, the data controller; a list of authorized parties will be maintained in the annex. **OR** the data importer has general authorization to engage sub-processor(s) from a previously-agreed-upon list. The data importer must inform the data exporter/controller of any changes to the authorized list. **M2/M3 Clause 9(b-c):** any sub-processor engaged by the data importer must be bound by a written agreement that includes the same data protections as bind the importer, including third-party beneficiary rights for data subjects. The importer must provide a copy of this agreement to the exporter or the controller on request. The importer is responsible for the sub-processor's compliance with the Clauses and must inform the exporter of any failure to comply. **M2 Clause 9(e)**: The data importer must include a clause in the sub-processor agreement giving the data exporter the right to terminate said agreement in the event that the data importer becomes insolvent, bankrupt, or legally ceases to exist.
Ibero-American Data Protection Network Model Transfer Agreement **M1: C2C M2: C2P**	**M2 Clause 7.1 Option 1:** Importer can only sub-contract processing activities with exporter's written authorization, which must be solicited at least 15 business days in advance. **M2 Clause 7.1 Option 2:** Importer has a general authorization to engage sub-processors from a pre-approved list; importer will inform exporter of any changes to the list at least 15 business days in advance. **M2 Clause 7.2(a):** Importer will require any sub-processor to engage in a written agreement that establishes "in essence" the same obligations imposed on importer by this agreement, specifically with rights of third party beneficiaries. importer will ensure the sub-processor complies with the obligations. **M2 Clause 7.2(b):** Importer will provide exporter at exporter's request a copy of the Sub-processor Agreement; importer may protect confidential information such as personal data before sharing the copy. **M2 Clause 7.2(c):** Importer will remain fully responsible to the exporter for the performance of the Sub-processor's obligations under its agreement with importer. Importer shall notify exporter of any failure by the Sub-processor to fulfill its obligations under the Agreement.
ASEAN Model Contractual Clauses **M1: C2P M2: C2C**	**Obligations of ASEAN MCCs, p5:** "Data Importers are encouraged to conduct due diligence on [third party importers] to ensure that they also meet the obligations imposed under these MCCs." **M1 Clause 3.2:** Importer shall not further disclose or transfer the personal data it receives from exporter to another person, Enforcement Authority, or legal entity, including to sub-processors, unless it has notified exporter of such further disclosure or transfer in writing, and provided reasonable opportunity for exporter to object." **M1 Clause 3.3:** Importer agrees that prior to any disclosure to a sub-processor, it will ensure the sub-processor is bound to the same obligations it has to the exporter.

Annex IV: Individual/Third Party Rights Guarantees

The following table aligns the clauses authorized for enforcement of third party rights under the EU Standard Contractual Clauses (Clause 3) with their equivalents in the RIPD MTAs and the ASEAN MCCs, assuming the use of the optional MCC provision recognizing third-party beneficiary rights. The clauses highlighted in green may only be enforced as a third party beneficiary against a data importer that is a processor.

EU SCCs	RIPD MTA	ASEAN MCCs (Optional)
Interpretation of Clauses (Clause 4)	Hierarchy of the clause with governing law (Clause 2.2)	
Hierarchy of Clauses re: other agreements (Clause 5)	Hierarchy of Clauses with other agreements (Clause 2.3)	
Purpose limitation (Clause M1 8.1/M2 8.2) **except** M2 Clause 8.1(b) – obligation to inform exporter if it cannot follow instructions M3 Clause 8.1(a), (c), (d) – obligation for exporter to inform importer it is a processor; obligation for importer to inform exporter it cannot follow instructions; exporter warranty that it has imposed the same restrictions on importer that it is subject to.	Purpose Principle (Clause 6.2)	
Transparency (Clause 8.2)	Transparency (M1 Clause 6.3/M2 Clause 6.4)	
Accuracy and Data Minimization (Clause 8.3)	Accuracy & Data Minimization (M1 Clause 6.4/M2 Clause 6.5)	
Storage Limitation (Clause 8.4)	Storage Limitation (Clause 6.5)	

EU SCCs	RIPD MTA	ASEAN MCCs (Optional)
Security of Processing (Clause 8.5) **except** M1 8.5(e) – notification of breach to data exporter/supervisory authority	Principle of Data Security (Clause 6.6)	
Sensitive Data (Clause 8.6)	Processing Sensitive Data (Clause 6.8)	
Onward Transfers (Clause 8.7)	Onward Transfers (Clause 6.9)	
Processing under the authority of the importer (Clause 8.8)	Processing under authority of Importer and Principle of Confidentiality (Clause 6.7)	
Demonstration and Compliance (Clause 8.9) **except** M1 8.9(b) – obligation to make documentation of compliance available to SA on request M2/M3 8.9(a), (c),(d),(e) – obligation for importer to respond to exporter inquiries; make compliance information available to exporter; allow and assist with audits; obligation of Parties to make that information available to SA on request	Principle of Accountability (M1 Clause 6.1/M2 Clause 6.2) Documentation and Compliance (Clause 6.10)	The Data Exporter will respond to enquiries from Enforcement Authorities as required by AMS Law, unless the parties have agreed the Data Importer will respond and the delegation is permitted under AMS Law (M1 Clause 2.4)
Sub-processors (obligation for processor to engage sub-processor w/written contract containing the same binding requirements as these clauses.) M2/M3 Clause 9(b): **except** M2 9(a): option to select either specific or general written authorization for sub-processors	Sub-processors – all requirements (M2 Clause 7)	

EU SCCs	RIPD MTA	ASEAN MCCs (Optional)
Data Subject Rights (Clause 10)	Rights of the [Data Subject] (M1 Clause 7/M2 Clause 8)	The Data Exporter will responds to enquiries from DS as required by AMS; unless Parties have agreed the Importer will respond. (M1 Clause 2.4)
Redress (Clause 11)	Redress (M1 Clause 8/M2 Clause 9)	Importer shall provide Exporter and DS a contact point authorized to respond to enquiries (M2 Clause 3.3) Importer shall promptly refer and provide to Exporter any requests from DS (M1 Clause 3.5)
Liability (Clause 12) **Except** M1 Clause 12(a), (d) – Ability of Parties to recover from one another M2/M3 Clause 12(a), (d), (f) – Ability of Parties to recover from one another	Civil Liability (M1 Clause 9/M2 Clause 10)	To the extent authorized by AMS Law, DS may obtain compensation for breaches of this Agreement; if applicable law is silent on allocation liability may be at discretion of DS or split equally between parties (M1 App'x 1.5, M2 App'x 1.4)
Local Laws and Practices Affecting Compliance (Clause 14)	Local Laws and Practices Affecting Compliance (M1 Clause 11/M2 Clause 12)	
Obligations of Importer for Access by Public Authorities (Clause 15) **Except** Clauses 15.1(c), (d), (e) – obligations to regularly provide data exporter (and supervisory authority on request) as much information as possible about public authority requests.	Supervision by the Competent Supervisory Authority (M1 Clause 10/M2 Clause 11)	
Clause 16: Non-compliance with Clauses and Termination	Non Compliance with the Clauses and Termination (M1 Clause 12/M2 Clause 13)	

EU SCCs	RIPD MTA	ASEAN MCCs (Optional)
Governing Law (Clause 17)	Governing Law (M1 Clause 13/M2 Clause 14)	Compliance w/Law Representation that PD processed and transferred to Importer in accordance with applicable AMS Law, or if without such law, DS notified and consented. (M1 Clause 2.1)
Choice of Forum and Jurisdiction (Clause 18) **Except** clauses selecting the applicable national jurisdiction.	Choice of Forum and Jurisdiction (M1 Clause 14/M2 Clause 15)	

ENDNOTES

1 See, e.g. Satariano, Adam, "EU Court Strikes Down Trans-Atlantic Data Transfer Pact," *The New York Times*, (July 16, 2020), available at https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html, Scott, Mark, "Data Transfer Pact Between U.S. and Europe is Ruled Invalid," *The New York Times*, (Oct. 6, 2020) available at: https://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html; Fioretti, Julia, "Schrems: the law student who brought down a transatlantic data pact," *Reuters*, (Oct. 6, 2015), available at https://www.reuters.com/article/us-eu-ireland-privacy-schrems-idINKCN0S02NY20151006.

2 Statement from U.S. Secretary of Commerce Gina Raimondo on Enhancing Safeguards for United States Signals Intelligence Activities Executive Order, United States Dept. of Commerce (October 7, 2022), available at https://www.commerce.gov/news/press-releases/2022/10/statement-us-secretary-commerce-gina-raimondo-enhancing-safeguards; Luca Bertuzzi, "EU-US data transfer framework: European privacy authorities put forth caveats," EURACTIV (Feb. 28, 2023), available at https://www.euractiv.com/section/data-privacy/news/eu-us-data-transfer-framework-european-privacy-authorities-put-forth-caveats/.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1678374811217 (hereafter cited as "Regulation (EU) 2016/679 (GDPR)").

4 Directive 95/46/CE of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

5 'Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum', study made jointly by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce, Strasbourg, 2 November 1992; Commission Decision of 15 June 2001, 2001/497/EC, on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, available at: https://op.europa.eu/en/publication-detail/-/publication/47b75fff-a11d-48bf-9636-483a80f9564d/language-en; Commission Decision of 27 December 2004, 2004/915/EC, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer for personal data to third countries, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF; Commission Decision of 5 February 2010, 2010/87/EU, on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

6 Macaskill, Ewen & Dance, Gabriel, "NSA Files: Decoded; What the revelations mean for you, *The Guardian*, (November 1, 2013), available at: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/3; *see also* "Snowden Revelations" available at https://www.lawfareblog.com/snowden-revelations (comprehensive list of leaked documents).

7 Rosenberg, Matthew, et al. "How Trump Consultants Exploited the Facebook Data of Millions," *The New York Times*, (March 17, 2018), available at https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

8 Court of Justice of the European Union, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650 ("Schrems I"); Court of Justice of the European Union, Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, ECLI:EU:C:2020:559 ("Schrems II").

9 Regulation (EU) 2016/679 (GDPR), Article 45(9). The newly adopted SCCs are relevant for the Member States of the EU: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden; as well as the Member States of the European Economic Area: Iceland, Liechtenstein and Norway.

10 ASEAN Member Countries: Brunei, Cambodia, Indonesia, Lao, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam.

11 Member Countries of the Red Iberoamericana de Protección de Datos: Andorra, Argentina, Brazil, Chile, Colombia, Costa Rica, Cabo Verde, Dominican Republic, Ecuador, Spain, Guatemala, Honduras, Mexico, Nicaragua, Panama, Peru, Portugal, Paraguay, El Salvador, Uruguay, Sao Tome and Principe.

12 *See, e.g.* NPC Advisory No. 2021-02, Guidance for the use of the ASEAN Model Contract Clauses and ASEAN Data Management Framework, Section 5(A)(2), (June 28, 2021), available at *https://www.privacy.gov.ph/wp-content/uploads/2021/06/Advisory-ASEAN-MCC-DMF_FINAL-signed.pdf* (recognizing that "ASEAN MCCs may also be used by companies or organizations to fulfill…obligations under Section 21 of the DPA").

13 Regulation (EU) 2016/679 (GDPR) Articles 45-46.

14 Regulation (EU) 2016/679 (GDPR) Article 46(1).

15 Id. at Article 46(2).

16 Id. at Article 44(1).

17 Id. at Article 46(1).

18 The EEA comprises the 27 Member States of the European Union, Liechtenstein, Norway, and Iceland.

19 Court of Justice of the European Union, Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems ("Schrems II"), para. 133.

20 European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, November 10, 2020, available at https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

21 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (hereafter cited as Commission Implementing Decision (EU) 2021/914), available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

22 ASEAN Model Contractual Clauses for Cross Border Data Flows, January 22, 2021, available at https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pd.

23 Guidance for the Use of ASEAN Model Contractual Clauses for Cross Border Data Flows in Singapore, Personal Data Protection Commission of Singapore, (January 22, 221), available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/Singapore-Guidance-for-Use-of-ASEAN-MCCs---010921.pdf; Guidance for the Use of the ASEAN Model Contract Clauses and ASEAN Data Management Framework, Republic of the Philippines National Privacy Commission, (June 28, 2021), available at https://www.privacy.gov.ph/wp-content/uploads/2021/06/Advisory-ASEAN-MCC-DMF_FINAL-signed.pdf.

24 ASEAN Model Contractual Clauses For Cross Border Data Flows 2021, Module 1 Cl. 4.2, Module 2 Cl. 5.2 (January 22, 2021).

25 *See* Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, March 2023, available at https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf; Red Iberoamericana de Protección de Datos, Implementation Guide On Model Contract Clauses for International Personal Data Transfers (IPDT), March 2023, available at https://www.redipd.org/sites/default/files/2023-02/guia-implementacion-clausulas-contractuales-modelo-tidp-en.pdf.

26 Standards for Personal Data Protection for Ibero-American States, Art. 36.1(c), (June 20, 2017), available at https://www.redipd.org/sites/default/files/2022-04/standars-for-personal-data.pdf.

27 Id., at 3.

28 Red Iberoamericana de Protección de Datos, Implementation Guide On Model Contract Clauses for International Personal Data Transfers (IPDT), March 2023.

29 Id.

30 *See* Commission Implementing Decision (EU) 2021/914; Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, March 2023; ASEAN Model Contractual Clauses for Cross Border Data Flows, January 22, 2021.

31 ASEAN Model Contractual Clauses for Cross Border Data Flows, Cl. 2.1, January 22, 2021.

32 Commission Implementing Decision (EU) 2021/914, Art. 1.

33 Regulation (EU) 2016/679 (GDPR) Article 6(1)(a).

34 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 2.2(a), March 2023, available at

35 Commission Implementing Decision (EU) 2021/914, Module 1, Cl. 8.3(a), (b); Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 6.4, March 2023.

36 Commission Implementing Decision (EU) 2021/914, Module 2, Cl. 8.4(a); Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 6.5, March 2023.

37 ASEAN Model Contractual Clauses for Cross Border Data Flows, Cl. 2.2 January 22, 2021.

38 Commission Implementing Decision (EU) 2021/914, Annexes I, II and III.

39 Commission Implementing Decision (EU) 2021/914, Module One, Cl. 8.2.

40 Id.

41 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, March 2023, Module 1 Annexes A, B, C, available at https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf

42 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, March 2023, Module 1, Cl. 6.3(b) available at https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf

43 Id. at Cl. 6.3(c).

44 ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 2 Cl. 3.3, App'x A, (January 22, 2021).

45 Id. Cl. 9.1.

46 Commission Implementing Decision (EU) 2021/914, Module 1, Cl. 8; Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 6.1, March 2023.

47 ASEAN Model Contractual Clauses for Cross Border Data Flows, Cl. 7.1 (January 22, 2021).

48 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 6.6(b), 6.10(b), March 2023.

49 ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 1 Cl. 3.6, (January 22, 2021).

50 *See* Commission Implementing Decision (EU) 2021/914, Module 1, Cl. 8.3(a); Regulation (EU) 2016/679 (GDPR) Articles 9(1), 10.

51 Commission Implementing Decision (EU) 2021/914, Module 1, Cl. 8.3(a); Regulation (EU) 2016/679 (GDPR) Articles 9(1), 10.

52 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 1.4, March 2023

53 Id. at Cl. 1.4, 6.8.

54 Regulation (EU) 2016/679 (GDPR) Article 8(1).

55 See Commission Implementing Decision (EU) 2021/914, Annex I.B; Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Annex C, March 2023.

56 ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 1 Cl. 3.9, Module 2 Cl. 3.2, (January 22, 2021).

57 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 1, Cl. 6.6(a), March 2023; Commission Implementing Decision (EU) 2021/914, Module 1 Cl. 8.5(a), Module 2 Cl 8.6(a).

58 See Commission Implementing Decision (EU) 2021/914, Module 1 Cl. 8.5(c), Module 2/3 Cl. 8.6(b); Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 1, Cl. 6.7(b), March 2023

59 Commission Implementing Decision (EU) 2021/914, Cl. 8.5(b); Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 6.6(c), March 2023.

60 ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 1 Cl. 3.9, Module 2 Cl. 3.2, 4.1, 4.2 (January 22, 2021).

61 Commission Implementing Decision (EU) 2021/914, Cl. 8.5(a); ASEAN Model Contractual Clauses for Cross Border Data Flows, pp. 10, 17, January 22, 2021; Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 6.6(c), March 2023.

62 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 1, Cl. 6.6(c), March 2023.

63 Commission Implementing Decision (EU) 2021/914, Module 2/3 Cl. 8.5(a) 8.6(c).

64 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 2, Cl. 6.6(c), March 2023.

65 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 1, Cl. 6.6(c), March 2023.

66 Commission Implementing Decision (EU) 2021/914, Cl. 8.5(f); Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 1, Cl. 6.6(f), March 2023.

67 Red Iberoamericana de Protección de Datos, Implementation Guide On Model Contract Clauses for International Personal Data Transfers (IPDT), p. 19, March 2023.

68 ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 1 Cl. 3.3, (January 22, 2021).

69 Commission Implementing Decision (EU) 2021/914, Module 1, Cl. 8.7, Module 2, Cl. 8.8; Red Iberoamericana de Protección de Datos, Implementation Guide On Model Contract Clauses for International Personal Data Transfers (IPDT), Module 1 & 2 Cl. 6.9, March 2023.

70 Commission Implementing Decision (EU) 2021/914, Module 1, Cl. 8.7(vi); Red Iberoamericana de Protección de Datos, Implementation Guide On Model Contract Clauses for International Personal Data Transfers (IPDT), Module 1, Cl. 6.9(vi), March 2023.

71 ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 1 Cl. 3.2 (January 22, 2021).

72 Commission Implementing Decision (EU) 2021/914, Module 2/3, Cl. 9; Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 2 Cl. 7.1, March 2023.

73 ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 1, Cl. 3.2 (January 22, 2021).

74 Commission Implementing Decision (EU) 2021/914, Cl. 17; ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 1, Cl. 4.1, Module 2 Cl. 5.1, (January 22, 2021); Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 1 Cl. 13, Module 2 Cl. 14, March 2023.

75 ASEAN Model Contractual Clauses for Cross Border Data Flows, Module 1, Cl. 2.2, 3.6, 3.7 (January 22, 2021).

76 Commission Implementing Decision (EU) 2021/914, Cl. 3.

77 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Cl. 3, March 2023.

78 ASEAN Model Contractual Clauses for Cross Border Data Flows, Additional Terms for Individual Remedies, January 22, 2021.

79 Id, Recital 12.

80 Commission Implementing Decision (EU) 2021/914, Module 1, Cl. 10(a).

81 Id.

82 Id. at C. 10(b).

83 Id. at Cl. 3(a).

84 Id.

85 Id. at Cl. 3(a), 8, 10, 14, 15, 16.

86 Red Iberoamericana de Protección de Datos, Implementation Guide On Model Contract Clauses for International Personal Data Transfers (IPDT), p. 13, March 2023.

87 Red Iberoamericana de Protección de Datos, Annex, Model Contractual Clauses, Cl. 3, March 2023.

88 Id. at Module 1, Cl. 7, March 2023.

89 Id. at Module 1, Cl. 7.1(c)(i), (iv), March 2023.

90 ASEAN Model Contractual Clauses For Cross Border Data Flows 2021, Additional Terms for Individuals Remedies, pp. 13, 20 (January 28, 2021).

91 Commission Implementing Decision (EU) 2021/914, Module 1, Cl. 8.3(a)

92 Id. at Module 1, Cl. 10(d).

93 Id.

94 Red Iberoamericana de Protección de Datos, Annex, Model Contractual Clauses, Module 1, Cl. 1.4, 7.2, March 2023.

95 Id.

96 Id.

97 Regulation (EU) 2016/679 (GDPR), Rec. 71; Art. 22.

98 Commission Implementing Decision (EU) 2021/914, Recital 19, Cl. 14.

99 Id. at Recitals 20-22.

100 European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, at pp. 22-4 (November 10, 2020).

101 Commission Implementing Decision (EU) 2021/914, Cl. 14(f), 15.1.

102 Id. at Art. 15.1(b).

103 Id. at Art. 15.2(a).

104 Red Iberoamericana de Protección de Datos, Implementation Guide On Model Contract Clauses for International Personal Data Transfers (IPDT), at pp. 14, 31 March 2023.

105 Red Iberoamericana de Protección de Datos, Model Contractual Clauses, Annex 1, Cl. 3, March 2023.

106 Id. at Annex 1 Cl. 11(d), Annex 2 Cl. 12(c).

107 Id. at Annex 1 Cl. 11(b), Cl. 12(b).

108 Id. at Annex 1 Cl. 11, Annex 2 Cl. 12.

109 Red Iberoamericana de Protección de Datos, Implementation Guide On Model Contract Clauses for International Personal Data Transfers (IPDT), at p. 19, March 2023.

110 ASEAN Model Contractual Clauses For Cross Border Data Flows 2021, p. 17, available at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

111 Illustrative of the stringent approach taken by some DPAs, see this analysis of the Austrian DPA and the EDPS decisions in cases concerning the use of Google Analytics cookies by websites in the EU and the subsequent transfers of personal data outside of the EU resulting from it — G. Zanfir-Fortuna, *Understanding why the first pieces fell in the transatlantic transfers domino*, available at https://fpf.org/blog/understanding-why-the-first-pieces-fell-in-the-transatlantic-transfers-domino/.

112 For example, in October 2022, Singapore's Personal Data Protection Commission (PDPC) issued directions to Supernova Pte Ltd. ("SNPL") to remedy its failure to impose PDPA-comparable protection for data transferred abroad via a legally binding contract or set of corporate rules on its local payment services provider, Shopify Commerce Singapore Ltd ("Shopify SG") and its foreign parent ("Shopify"). The PDPC's investigation of a data breach of Shopify Inc. that affected Singaporean citizens' personal data determined that because Shopify Inc. was processing transferred personal data for its own purposes, and not solely on behalf of its merchant customers (like SNPL), its local affiliate Shopify SG was acting as a data controller, and was subject to the relevant restrictions in the PDPA, and both Shopify SG and its Singaporean client SNPL had failed to ensure that appropriate data protections were in place as required by law. Accordingly, the Commission specifically directed SNPL and Shopify SG to impose processes compliant with the Transfer Limitation Obligation applied by section 26 of Singapore's Personal Data Protection Act (PDPA). The PDPA requires any organization that transfers personal data outside of Singapore to take appropriate steps to ensure that the recipient of the data is bound by legally enforceable obligations to provide the transferred data a comparable standard of protection to the PDPA. Both SNPL and Shopify SG were responsible for the transfer of personal data out of Singapore and thus required to ensure via contract that the non-Singaporean recipient of their was appropriately bound; the PDPC indicated that the existing Shopify agreement did not satisfy the PDPA and that ASEAN Model Contractual Clauses may be adapted to meet those requirements. *See* PDPC Decision *In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and (1) Supernova Pte Ltd and (2) Shopify Commerce Singapore Pte Ltd*, Case No. DP-2103-B8147/DP-2206-B9935, available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/GD_Supernova-Pte-Ltd_06102022.pdf.

113 ASEAN Model Contractual Clauses For Cross Border Data Flows 2021, Module 1 Cl. 4.3 and Module 2 Cl. 5.3.

114 Commission Implementing Decision (EU) 2021/914 M1/M2/M3 Cl. 18.

115 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, M1 Cl. 14(a) and (b)/M2 Cl. 15(a) and (b), March 2023.

116 Commission Implementing Decision (EU) 2021/914, Annex I, Cl. 5.

117 Id. at Recital 3, Annex I, Cl. 3.

118 Id.

119 Red Iberoamericana de Protección de Datos, Annex 1 — Model Contractual Clauses, Module 1, Cl. 2.1, 2.2, March 2023.

120 Id.

121 ASEAN Model Contractual Clauses For Cross Border Data Flows, at p. 4, (January 28, 2021).

The Future of Privacy Forum (FPF) is a global non-profit organization that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data use, identify the risks, and develop appropriate protections. FPF has offices in Washington D.C., Brussels, Singapore, and Tel Aviv.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | INFO@FPF.ORG