JOINT GUIDE TO

ASEAN Model Contractual Clauses and EU Standard Contractual Clauses

Updated 31 January 2024

TABLE OF CONTENTS

FOREWORD

ASEAN stands at a critical juncture in the development and integration of its digital economy, which is estimated to contribute approximately USD 1 trillion in Gross Merchandise Value (GMV) by 2030. In order to harness the immense potential of the digital economy, it is imperative for ASEAN to propel the region's digital integration.

A key element in ASEAN's digital economy agenda is focused on the important role of data. Indeed, data is being generated and exchanged at an unprecedented pace, providing organisations, businesses and users with valuable insights and opportunities for innovation and growth. With the ever-increasing exchange of data, a sound and secure mechanism for cross-border data flow is essential to ensure data protection and security, as well as to build trust. This mechanism is also crucial to support global trade and promote innovation, which will position ASEAN as a future-ready region with a resilient economy and sustainable growth.

In this regard, the *ASEAN Framework on Digital Data Governance* was established to promote the free flow of data within ASEAN and to foster a dynamic data ecosystem that facilitates innovation and growth. At the same time, the *ASEAN Framework on Personal Data Protection* has outlined principles to guide the ASEAN Member States in developing their regulatory regime and strengthening personal data protection in the region.

The *Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses* is a concrete step to further reinforce ASEAN's efforts as well as reflects our shared commitment to enhancing data governance through the implementation of international best practices. This publication also serves as a valuable tool to assist businesses engaged in data transfers between ASEAN and the EU in navigating the data transfer landscape, streamlining data transfer processes, and improving business efficiency.

I am confident that the implementation of the Joint Guide will help empower ASEAN businesses, particularly micro, small and medium enterprises (MSMEs), to participate fully in the digital economy and contribute to the realisation of ASEAN's vision set out in the *ASEAN Digital Masterplan 2025* (ADM2025). I hope that readers and relevant stakeholders will find the information outlined in this publication useful, as we strive towards promoting the digital connectivity between ASEAN and the world, establishing an inclusive digital ecosystem in ASEAN, as well as transforming ASEAN into a leading digitally connected community and economic bloc powered by secure, transformative digital services, technologies, and ecosystems.

H.E. Dr Kao Kim Hourn
Secretary-General of ASEAN

FOREWORD

In December 2022, the EU and ASEAN celebrated 45 years of diplomatic relations at a commemorative Summit in Brussels. As evidenced by the Joint Leaders' Statement issued on that occasion[1], we have a strong partnership rooted in shared values, including with respect to the protection of personal data. In this digital era, where data can travel between jurisdictions with the click of a button, this includes a recognition of the importance of effective data protection rules as a key enabler of trust and a facilitator for safe cross-border data flows.

Against this background, both the EU and ASEAN have developed model contractual clauses – the ASEAN Model Contractual Clauses (MCCs) and EU Standard Contractual Clauses (SCCs) – as a voluntary tool that can be used by companies for cross-border data flows. Model clauses provide a ready-made, cost-effective solution to comply with applicable regulatory requirements, while ensuring that personal data benefit from a high level of protection when transferred internationally. In the EU, they are currently by far the most used instrument for international data transfers. Through their standardisation and pre-approval, they are particularly useful for SMEs, which often do not have the resources to engage in lengthy contractual negotiations.

Beyond the EU and ASEAN, the development of model clauses as a tool for transfers is gaining traction globally, with such clauses already being available in several jurisdiction and regions around the world – from those developed in Latin America by the Ibero-American Data Protection Network[2] to those adopted under the New Zealand's Privacy Act[3], just to name two examples. As also recognised by the G7, this convergence between transfer instruments provides new opportunities to facilitate free data flows with trust and foster interoperability.

Building on the commonalities between the EU SCCs and ASEAN MCCs, this Joint Guide provides a practical tool to businesses operating across our two regions with a view to facilitate compliance with applicable data protection requirements. This is certainly not the end of our joint work: we will now engage with stakeholders to operationalise this bridging of the two sets of clauses, by collecting best practices on their implementation and use.

All this confirms that, in the digital era, maintaining high data protection standards and facilitating international trade should and can go hand in hand. It also goes to show that, as the world's two most advanced regional integration organisations, the EU and ASEAN can together give a significant contribution to the development of much-needed international standards in this strategic area, to the benefit of their citizens and businesses alike.

Didier Reynders
European Commissioner for Justice

[1] https://www.consilium.europa.eu/media/60846/eu-asean-leaders-statement.pdf

[2] https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf

[3] https://www.privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/

FOREWORD

ASEAN and the EU have a strong, multi-faceted economic relationship. ASEAN is the EU's third largest trading partner; the EU is the second largest investor in ASEAN. In 2021, the volume of bilateral trade grew to an all-time high of €215.9 billion between the two regions. As our respective economies continue to digitally transform, we can expect data flows between ASEAN and the EU to increase and strengthen our bilateral economic relationship.

Singapore has worked closely with our ASEAN and EU partners to foster digital trust across geographical borders by promoting common baseline standards for data flows. This will allow businesses to share data in a trusted manner across borders more seamlessly. We are hence pleased to have developed this Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses, a collaboration between ASEAN and the European Commission Directorate-General for Justice and Consumers.

The Joint Guide builds on the ASEAN Framework on Digital Data Governance and the ASEAN Model Contractual Clauses, two foundational pillars developed to facilitate trust within ASEAN when businesses transfer data across borders. It will serve as a reference to help create common understanding between ASEAN and EU business partners and facilitate contractual negotiations between parties in relation to cross border data transfers. I look forward to the development of this reference guide into practical guidance for our companies. Singapore will continue to work closely with ASEAN Member States during our ASEAN Digital Ministers Meeting (ADGMIN) Chairmanship in 2024 to enhance our engagement with the EU and strengthen the digital linkages between our two economic blocs.

Josephine Teo
Minister for Communications and Information
Second Minister for Home Affairs
Minister-in-charge of Smart Nation and Cybersecurity
Republic of Singapore

INTRODUCTION

The ASEAN Model Contractual Clauses (ASEAN MCCs) and EU Standard Contractual Clauses (EU SCCs) are model data protection clauses ("clauses") that can be incorporated by data exporters and importers in their contractual arrangements as a basis to allow the transfer of personal data across borders. The clauses are a voluntary tool to ensure personal data continues to benefit from a high level of protection in cases of international transfers, and to ensure compliance with applicable legal requirements for international data transfers in this regard. This concerns requirements following the ASEAN Member States' legal frameworks and the General Data Protection Regulation (GDPR) for the ASEAN MCCs and EU SCCs respectively. The clauses reflect the core data protection requirements that follow the ASEAN Framework on Personal Data Protection (2016) and the GDPR, which are increasingly recognised internationally. Through their standardisation and pre-approval, model data protection clauses become "ready-made" and easy-to-implement tools. Both MCCs and SCCs contain certain optional clauses that can be used where applicable.

Under the GDPR, the EU SCCs can be used without the need to obtain prior authorisation for the data transfer, or an individual authorisation for the clauses used from a data protection authority.

The ASEAN MCCs are a baseline set of contractual clauses that can be used by data exporters and importers in all ASEAN Member States. The underlying aim of the ASEAN MCCs is to provide flexibility within the principles of the ASEAN Framework on Personal Data Protection. The MCCs may be amended to suit business needs so long as the amendment is consistent with the principles of the ASEAN Framework on Personal Data Protection. The respective contractual clauses can be viewed at the weblinks in the table below.

ASEAN MCCs	EU SCCs
https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf	https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

PURPOSE

This Joint Guide consists of two parts, namely the Reference Guide and the Implementation Guide.

The **Reference Guide** is a comparison highlighting the similarities and differences between the ASEAN Model Contractual Clauses (MCCs) and the EU Standard Contractual Clauses (SCCs). The Reference Guide was endorsed at the 3rd ASEAN Digital Ministers' Meeting (ADGMIN) in February 2023 and published in May 2023. The Reference Guide can be found on pages 8 to 45 of this document.

The **Implementation Guide** includes non-exhaustive examples of best practices companies can consider implementing to operationalise safeguards required under both sets of contractual clauses. The Implementation Guide can be found on pages 46 to 73 of this document.

The objective of the Joint Guide is to help companies operating across the ASEAN and EU regions, i.e., data exporters in those regions as well as any data importers, understand the similarities and differences between the respective contractual clauses, thereby facilitating compliance with ASEAN and EU data protection laws, as applicable.

The Joint Guide could serve as a useful resource for companies in the following data flow scenarios:

1. **Data flows from ASEAN to EU:** The parties may adopt the ASEAN MCCs for this scenario. The Joint Guide helps EU companies understand the similarities and differences between the ASEAN MCCs and the EU SCCs, and how to meet the requirements under the ASEAN MCCs. The Joint Guide also aims to help ASEAN companies understand and implement measures that go beyond what is needed under the ASEAN MCCs. This may help in streamlining processes and saving costs when companies expand their operations and business to the EU.

2. **Data flows from EU to ASEAN or data flows between EU and ASEAN:** As ASEAN companies may decide to put in place the EU SCCs to receive data from their EU business partners, this Joint Guide will help ASEAN companies, including those that are already using the ASEAN MCCs to:

   A. Identify areas/processes that they already have in place (and can be readily deployed to receive the data from EU); and

   B. Identify areas/processes that they might need to put in place, in addition to their existing policies and practices that are suited to the ASEAN MCC requirements.

3. **Data flows within the ASEAN region:** This Joint Guide aims to help companies trading within the ASEAN region to develop data governance policies and implement best practices that are aligned with the principles of the ASEAN Framework on Personal Data Protection. With the Joint Guide, this will not only help companies better navigate the regulatory landscape for data transfers with the EU, but also open future possibilities with other regions in the world.

The information in this document does not constitute legal advice and is provided for general informational purposes only.

PART 1: REFERENCE GUIDE

GENERAL

1 ENTERING INTO MCCS/SCCS

1.1 Choice of the appropriate module:

The ASEAN MCCs and EU SCCs adopt a "modular approach". Each set of clauses covers different modules which correspond to different transfer scenarios. The parties should choose the module that best applies to their situation and delete irrelevant modules.

Specific information on ASEAN MCCs	Specific information on EU SCCs
2 modules: ▶ **Module 1:** controller-to-processor transfers ▶ **Module 2:** controller-to-controller transfers See explanations in "ASEAN Model Contractual Clauses for Cross Border Data Flows" on p. 6 and Appendix A.	**4 modules:** ▶ **Module 1:** controller-to-controller transfers ▶ **Module 2:** controller-to-processor transfers ▶ **Module 3:** processor-to-processor transfers ▶ **Module 4:** processor-to-controller transfers See **Clause 1(c)-(d) (Purpose and scope), Clause 6 (Description of the transfer)** and the Appendix. See also further explanations provided in the Questions and Answers section of the SCCs[4].

1.2 Filling in and signing the annexes:

For both the ASEAN MCCs and the EU SCCs, the parties have to provide information on their specific transfers in an Appendix. This includes information on the data exporter and importer, the data transferred, the (categories of) individuals whose data is transferred, the purpose of the transfer, etc. (see Appendix A of the ASEAN MCCs and Annex I of the EU SCCs). In the EU SCCs, additional information (e.g., on the competent supervisory authority and applicable technical and organisational measures) should be provided. For both the ASEAN MCCs and the EU SCCs, the Appendix should be signed by the parties.

[4] *Available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en*

Specific information on ASEAN MCCs	Specific information on EU SCCs
In **Appendix A**, the parties have to provide information on the data exporter and importer, a description of data subjects and groups of data subjects as well as the purpose of processing. See also **Clause 9.1: Description of the Transfer.**	Detailed information on the transfer has to be provided in the **Appendix**, which consists of: ▶ Annex I, where information should be provided on the parties (A), as well as a description of the transfer (B), including categories of data subjects whose data is transferred, categories of data transferred, purposes of the processing, etc., and the competent supervisory authorities (C); ▶ Annex II, where the technical and organisational measures to ensure compliance (including data security) should be described; ▶ Annex III (only for transfers to processors), where authorised sub-processors should be listed. See also **Clause 6 (Description of the transfer).**

1.3 Relationship with other contractual commitments between the parties:

Both the ASEAN MCCs and the EU SCCs can be incorporated into a broader (commercial) contract and can be complemented with additional clauses. The parties may introduce certain changes to the MCCs (e.g., to comply with applicable data protection requirements), whereas the text of the SCCs may not be changed.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The parties may vary the Clauses as long as these amendments do not undermine the ASEAN Principles on Data Protection and are consistent with existing AMS Law (**Clause 8.1**).	The parties may include the SCCs into a broader commercial contract or add additional safeguards as long as they do not contradict the Clauses or prejudice the rights of individuals. The SCCs may not be altered, except to select a module or option and to complete the Appendix (**Clause 2**). One benefit of the SCCs is that they are standardised and pre-approved. As long as the parties do not change the text of the SCCs, they can be relied on as a transfer instrument without having to obtain authorisation from a national data protection authority.

1.4 Changes to the contractual parties:

Specific information on ASEAN MCCs	Specific information on EU SCCs
Not addressed in the ASEAN MCCs.	The parties may agree to an optional "docking clause" (**Clause 7**), which enables entities that are not party to the SCCs to accede to the SCCs at any time, with the agreement of the existing parties. This provides additional flexibility in case of changes with respect to the entities participating in the processing arrangement throughout the life cycle of the contract (e.g., in case it becomes necessary to extend the processing chain by including a sub-processor).

2 INTERPRETING THE MCCS/SCCS

2.1 Key concepts:

The ASEAN MCCs and EU SCCs define the key concepts used in the clauses, such as "personal data", "processing", and "data breach". While the MCCs and SCCs are to be read and interpreted in accordance with applicable law, (i.e., AMS law and the GDPR respectively) there is a high degree of convergence between these definitions.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Clause 1 (Modules 1 and 2): Definitions follow standard industry definitions and are as follows: ▶ **Clause 1.2: "Data Breach"** – Any loss or unauthorised use, copying, modification, disclosure, or destruction of, or access to, Personal data transferred under this contract. ▶ **Clause 1.5 (Module 2), Clause 1.6 (Module 1): "Enforcement Authority"** – Any public authority empowered by applicable AMS Law to implement and enforce the applicable AMS Law.	**Clause 4 Interpretation:** Terms that are defined in the GDPR have the same meaning as in the GDPR. See e.g.: ▶ **Article 4 (12) GDPR: "Personal data breach"** – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. ▶ **Article 4 (21) GDPR: "Supervisory authority"** – An independent public authority which is established by a Member State pursuant to Article 51 [of the GDPR].

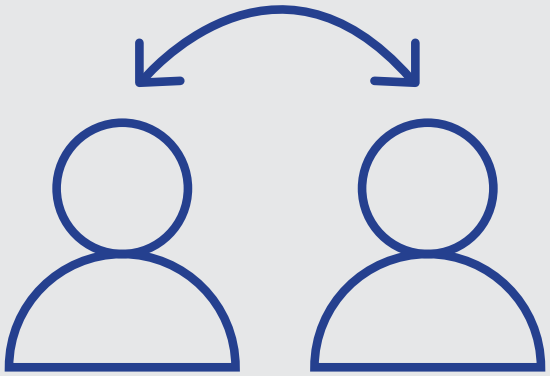
Specific information on ASEAN MCCs	Specific information on EU SCCs
▶ **Clause 1.6 (Module 2), Clause 1.7 (Module 1): "Personal data"** – Any information related to an identified or identifiable natural person ("data subject") transferred under this contract. ▶ **Clause 1.7 (Module 2), Clause 1.8 (Module 1): "Processing"**– Any operation or set of operations that are performed on Personal data or on sets of Personal data, whether or not by automated means, including, for example, collection, use and disclosure of Personal data. ▶ **Clause 1.1: "AMS Law"** – Any and all written laws of an ASEAN Member State relating to data protection (or are minimally relevant to the transfer of personal data) which the Data exporter or the Data importer (or both) are subject to. In case of a conflict between the MCCs and applicable AMS law, the latter will prevail (**Clause 5.2 for Module 2, Clause 4.2 for Module 1**).	▶ **Article 4(1) GDPR: "Personal data"** – Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. ▶ **Article 4(2) GDPR: "Processing"** – Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The SCCs should be read and interpreted in light of the GDPR and may not be interpreted in a way that conflicts with the GDPR (**Clause 4(b) and (c)**).

2.2 Choosing the law applicable to the contract:

For both the ASEAN MCCs and EU SCCs, the parties have to indicate which law will govern the application of the clauses. For the SCCs, the law chosen has to be that of an EU member country[5] and this choice is subject to specific conditions.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The parties may select the applicable law according to which the contract will be interpreted. Parties are advised to use the laws of one of the countries involved in the data transfer (**Clause 5.1 for Module 2, Clause 4.1 for Module 1**).	The parties have to choose the law of one of the EU countries that provides for third-party beneficiary rights as applicable law (**Clause 17**). If the data importer is a processor, this should, in principle, be the law of the country where the data exporter is established.

[5] *This refers to the 27 EU Member States, as well as countries associated to the EU through the EEA Agreement (Iceland, Liechtenstein and Norway).*



OBLIGATIONS FOR CONTROLLER-TO-CONTROLLER TRANSFERS

1 DATA PROTECTION SAFEGUARDS

Both the ASEAN MCCs and the EU SCCs contain contractual commitments by the parties to ensure core data protection principles, rights and obligations. This includes obligations for the data exporter[6] (acting as a controller) as well as the data importer[7] (also acting as a controller).

1.1 Lawfulness of the transfer:

Under both the ASEAN MCCs and the EU SCCs, the data exporter is responsible for ensuring that the data transfer takes place in compliance with applicable legal requirements.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Collection, use, disclosure or transfer of personal data must be in accordance with applicable AMS Law or with the consent of the data subject (**Clause 2.1**).	**Clause 2(b)** recalls that the data exporter has to comply with the GDPR, including Article 6 (legal basis), when transferring personal data based on the SCCs.

1.2 Specifying the purpose of the transfer and purpose limitation:

For both the ASEAN MCCs and the EU SCCs, the parties have to describe the purpose of the transfer and subsequent processing in an annex to the clauses. The data importer has to commit to the principle of processing the data only for those purposes, under a mandatory clause in the SCCs and an optional one in the MCCs.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Parties should specify the details of the transfer in the Appendix (see **Clause 9.1**). If the parties wish to limit the purposes of processing, they may choose to include an optional clause requiring the data importer to only process the personal data for the purposes described (**Clause 3.1**).	The parties should specify the purposes for which the data may be processed by the data importer in the Appendix (see **Clause 6**). The data importer may only process the data it receives under the SCCs for those purposes, except if (1) it obtains the individual's consent, (2) the processing is necessary to establish, exercise or defend legal claims (e.g., in judicial proceedings) or (3) this is necessary to protect the vital interests of an individual (**Clause 8.1**).

[6] *See Clause 1.3 of the MCCs, which defines "data exporter" as "the Party which transfers Personal data to the Data importer under this contract"; and Clause 1(b) of the SCCs, which defines the notion of "data exporter" as "the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data".*

[7] *See Clause 1.4 of the MCCs, which defines "data importer" as "the Party that receives Personal data from a Data exporter under this contract"; and Clause 1(b) of the SCCs, which defines the notion of "data importer" as "the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses".*

1.3 Data accuracy:

Under the ASEAN MCCs, the parties may agree to an optional clause whereby the data exporter has to ensure the accuracy of the data. The EU SCCs contain a mandatory clause committing both parties to do so.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 2.2: The data exporter must ensure that the data collected, used, disclosed and transferred is accurate and complete for the purposes of transfer. [*Note:* This clause should be inserted where accuracy of the personal data is relevant to the purposes of processing.]	Both the data exporter and the data importer have to ensure that the personal data is accurate and up to date. They also have to notify each other if they become aware of any inaccurate or outdated data and erase or rectify such data without delay (**Clause 8.3**).

1.4 Data minimisation:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The volume of data that is transferred is dependent on the commercial objective of the contract and thus left to the parties' negotiations. While the ASEAN MCCs do not contain specific clauses on data minimisation, the ASEAN Data Management Framework advises against overcollection or over-inclusion of data for processing on data as it may lead to the organisation incurring additional costs when implementing controls.	The data importer[8] has to ensure that the personal data it processes under the SCCs is adequate, relevant and limited to what is necessary in relation to the purpose of processing (**Clause 8.3**).

[8] *In addition, the data exporter has to ensure that the personal data it transfers is adequate, relevant and limited to what is necessary in relation to the purpose of the transfer, in accordance with Article 5(1)(c) of the GDPR.*

1.5 Storage limitation:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The period of retention is dependent on the commercial objective of the contract and thus left to the parties' negotiations. The same principles for data minimisation are relevant: the ASEAN Data Management Framework advises against over-inclusion on data as it may lead to the organisation incurring additional costs when implementing control. In addition, parties are also reminded of the retention principle in the ASEAN Framework on Data Protection, which states that an organisation should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes.	The data importer may not retain personal data for longer than is necessary for the purpose for which it is processed. It should put in place appropriate technical or organisational measures to ensure compliance with this clause, including erasure or anonymisation of personal data and all back-ups (**Clause 8.4**).

1.6 Security and confidentiality:

For both the ASEAN MCCs and the EU SCCs, the parties have to put in place appropriate measures to ensure security of the data, including protecting it against data breaches. Specific requirements are also included for the notification by the data importer of data breaches.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The parties should take appropriate steps to determine the level of risk of data breaches, consider the suitable security measures to manage this risk and agree on and implement appropriate controls and security standards (**Clauses 4.1 and 4.2**).	The parties have to agree on appropriate technical and organisational measures to ensure the security of personal data, which have to be specified in an annex to the SCCs (**Clause 8.5(a) and (b)**).

Specific information on ASEAN MCCs	Specific information on EU SCCs
Suitable security measures parties could consider taking include: ▶ Instituting a risk management framework to identify security threats to repositories or datasets containing personal data, assessing the risks involved and determining the controls to mitigate or minimise such risks; ▶ Periodically assessing the effectiveness of the risk mitigation controls; ▶ Requiring employees to be bound by confidentiality obligations in their employment agreements. The data importer has to put in place reasonable and appropriate technical, administrative, operational and physical measures to protect personal data against the risk of data breaches (**Clause 3.2**). These measures should be consistent with any applicable AMS law. When the data importer becomes aware of a potential or actual data breach, the data importer has to notify the data exporter. This should be done without undue delay or within the time period agreed on by both parties in the contract (**Clause 3.4**).	The data importer has to: ▶ Carry out regular checks to ensure that the measures continue to provide an appropriate level of security (**Clause 8.5(a) and (b)**); ▶ Ensure that persons authorised to process the personal data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality (**Clause 8.5(c)**). In case of a data breach, the data importer has to: ▶ Take appropriate measures to address and mitigate the possible adverse effects of the data breach (**Clause 8.5(d)**); ▶ Notify both the data exporter and the competent supervisory authority if the data breach is likely to result in a risk to the rights and freedoms of natural persons (**Clause 8.5(e)**); ▶ In cooperation with the data exporter, notify data subjects if the data breach is likely to result in a high risk to the rights and freedoms of natural persons, unless the data importer has taken measures to reduce such risk or it would require disproportionate efforts (**Clause 8.5(f)**); ▶ Document and record all facts relating to the data breach, including its effects and the remedial action undertaken (**Clause 8.5(g)**).

1.7 Sensitive data:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The ASEAN Data Protection Principles do not include a category of sensitive personal data. However, under the MCCs, the parties are required to take the risks involved in the data processing into account when determining and putting in place appropriate security measures (**Clauses 4.1 and 4.2**). In addition, the ASEAN Data Management Framework provides guidance on different levels of security measures that ought to be implemented for the protection of personal data of different levels of sensitivity. Parties are free to include additional protections within their contracts for the processing of personal data which they consider poses specific risks.	The data importer has to apply specific restrictions and/or additional safeguards, adapted to the specific nature of the data and the risks involved when the transfer involves sensitive data[9] (**Clause 8.6**). This can include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) or specific restrictions on disclosures.

1.8 Onward transfers:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The necessity for onward transfers is dependent on the commercial objective of the contract and thus left to the parties' negotiations. It is envisaged the ASEAN MCCs continue to be used for onward transfers. The principle applicable to transfers to another country or territory in the ASEAN Framework for Personal Data Protection is also relevant here. Before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with the principles in the framework.	The data importer may disclose personal data to a third party located outside the EU if the third party agrees to be bound by the SCCs or if one of the following conditions is met (**Clause 8.7**): ▶ The third party otherwise ensures appropriate data protection safeguards through one of the transfer tools available under the GDPR (e.g., binding corporate rules); ▶ The third party enters into an agreement with the data importer that ensures the same level of data protection as under the SCCs;

[9] *I.e., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed 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 offences.*

Specific information on ASEAN MCCs	Specific information on EU SCCs
	▶ The third party is located in a country that benefits from an adequacy decision adopted by the European Commission; ▶ The transfer is necessary to establish, exercise or defend legal claims (e.g., in the context of court proceedings); ▶ The transfer is necessary to protect the vital interests of an individual; ▶ The data importer obtains the explicit informed consent of the concerned individual.

2 DATA SUBJECT RIGHTS

2.1 Transparency:

Specific information on ASEAN MCCs	Specific information on EU SCCs
Data subject rights are dependent on domestic legislation. The ability to confer contractual rights under the ASEAN MCCs on data subjects when they are not a party to the agreement depends on the domestic contract laws of the ASEAN member state. Data subject rights are provided as optional clauses in the ASEAN MCCs.	**Clause 8.2(d)** recalls the transparency obligations of the data exporter under the GDPR (Articles 13 and 14), including to inform the individual about data transfers based on the SCCs. In addition, the data importer has an obligation to inform data subjects of its identity and contact details, the categories of personal data transferred, their right to obtain a copy of the clauses and intended onward transfers (**Clause 8.2**). This does not apply if the data subject already has the information, or providing the information would be impossible or require a disproportionate effort, although the information should in that case, to the extent possible, be made public.

Specific information on ASEAN MCCs	Specific information on EU SCCs
It is also good practice for data exporters to be transparent with data subjects when required to seek consent. Under the ASEAN MCCs, the data exporter is responsible for ensuring that, where there is no other legal basis for the collection, use, disclosure or transfer of the data, the data subject has been notified of and has given consent to the transfer of his/her personal data (**Clause 2.1**).	In turn, individuals have a right to obtain a copy of the SCCs. The parties may redact parts of the clauses if they contain confidential information (e.g., business secrets). In that case, the parties have to explain these redactions and provide the individual with a meaningful summary if it would otherwise not be possible to understand the content.

2.2 Point of contact:

For both the ASEAN MCCs and the EU SCCs, the data importer has to appoint and inform about a contact point for data subjects to submit their enquiries or complaints.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data importer shall provide an authorised contact point to the data exporter and/or data subjects for the purposes of responding to enquiries concerning personal data (**Clause 3.3**).	The data importer has to provide individuals with a contact point to handle their complaints (**Clause 11(a)**).

2.3 Rights of individuals:

While the ASEAN MCCs rely on the rights that are provided under the legal frameworks that apply to the data exporter and importer, under the EU SCCs, the parties additionally specifically agree that the data importer ensures certain rights for individuals that can be enforced against it.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 4.3: The data exporter and data importer shall each respond to enquiries from data subjects as regards to the processing of their personal data, including requests to access or correct such data.	The data importer has to deal with any inquiries or requests from data subjects without undue delay and at the latest within one month (**Clause 10(a)**).

Specific information on ASEAN MCCs	Specific information on EU SCCs
	The SCCs provide individuals with the following rights, which can be exercised against the data importer (**Clause 10(b)-(d)**): ▶ Right of access (including confirmation as to whether their personal data is being processed, a copy of the data relating to them as well as information on the processing and the right to lodge a complaint); ▶ Right to obtain rectification of inaccurate or incomplete data; ▶ Right of erasure of personal data processed in violation of any clauses ensuring third-party beneficiary rights; ▶ Right to object to the processing of data for direct marketing purposes (in which case the data importer must cease processing); ▶ Right not to be subject to fully automated decision-making, except under certain conditions and subject to specific safeguards. The data importer may refuse an individual's request if this is allowed under the laws of the country where the importer is located and the refusal is necessary and proportionate to protect important public interest objectives. In that case, the data importer must give reasons for any refusal and notify the data subject of the possibility to obtain (judicial) redress (**Clause 10(f) and (g)**).

2.4 Third-party beneficiary rights and redress:

Both the ASEAN MCCs and the EU SCCs grant contractual rights to third parties outside the contract for the safeguards for data subjects set out therein. The SCCs provide individuals with different avenues to obtain redress for non-compliance by the parties with those safeguards, while the MCCs offer an additional set of clauses that can be included by the parties where relevant legal frameworks require third-party rights to be built into the contract.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Additional terms for individual remedies: Data subjects can enforce the following rights, as long as the applicable law confers third party beneficiary rights (**Clause 1.1 of the Additional Terms**): ▶ **Against the data exporter:** Obligation to ensure the lawfulness of the transfer (**Clause 2.1**). ▶ **Against the data importer:** Obligation to provide a contact point for queries (**Clause 3.3**) and obligation to respond to requests from individuals (**Optional – Clause 4.3**). To the extent authorised by applicable AMS Law, data subjects may request compensation for breach of contract by the data importer and/or data exporter. Data exporters and data importers can state in the contract whether to bear such compensation in equal shares or allow the data subject to determine how to allocate his/her claim (**Clause 1.4 of the Additional Terms**). A data subject may be represented by another body if permitted by applicable law (**Clause 1.5 of the Additional Terms**).	Data subjects can enforce most clauses of the SCCs (except those that only regulate the relationship between the contractual parties, see **Clause 3**) against the parties. This includes the possibility to obtain compensation for any material or non-material damage (**Clause 12(b)**). When more than one party is responsible for the damage, all responsible parties will be jointly and severally liable (**Clause 12(c)**). In case of a dispute between a data subject and one of the parties concerning compliance with the clauses, that party must use its best efforts to resolve the issue amicably (**Clause 11(b)**). To obtain redress, data subjects can lodge a complaint with: ▶ The data importer (**Clause 11(a)**) and, if accepted by the data importer, an independent dispute resolution body; ▶ A supervisory authority of an EU country designated by the parties (**Clause 11(c)**); ▶ A court (either the competent courts in the jurisdiction that have been chosen by the parties in the SCCs, or the courts of the country where the individual resides) (**Clause 11(c) and Clause 18(c)**). An individual may be represented by a non-profit body (**Clause 11(d)**).

3 COMPLIANCE, DISPUTE RESOLUTION AND TERMINATION

3.1 Responsibility/accountability:

For both the ASEAN MCCs and the EU SCCs, the data importer assumes responsibility for processing the data in compliance with the contract.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 3.5: The data importer assumes responsibility for the protection, processing and maintenance of the personal data in its possession, in accordance with applicable AMS Law and the contract.	The data importer has to ensure that persons acting under its authority do not process data except on its instructions (**Clause 8.8**). Both parties must be able to demonstrate compliance with the SCCs (**Clause 8.9**). The data importer has to keep appropriate documentation and make it available to the competent supervisory authority upon request.

3.2 Ability to comply:

Both the ASEAN MCCs and the EU SCCs contain provisions on the ability of the parties to comply with their contractual commitments. The focus of the MCCs is on the legal capacity and authority of the parties to enter into and perform their contractual obligations, whereas the SCCs focus on local laws and practices in the country of the data importer that may prevent it from complying.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Both the data exporter and data importer confirm that they are able and authorised to enter into and perform their obligations under the contract (**Clause 7.1**).	**General:** The data exporter has to use reasonable efforts to determine that the data importer is able, through the implementation of technical and organisational measures, to satisfy its obligations under the SCCs (**Clause 8**).

Specific information on ASEAN MCCs	Specific information on EU SCCs
	Local laws and practices affecting compliance with the Clauses: The parties have to assess whether the laws and practices in the country of the data importer prevent it from complying with the SCCs (**Clause 14(a)**). Laws and practices that do not exceed what is necessary and proportionate in a democratic society to safeguard important public interest objectives are not considered to be in contradiction with the SCCs. The parties must document their assessment, which must be transfer specific (see **Clause 14(b)**) and made available to the competent supervisory authority upon request (**Clause 14(d)**). If, after having entered into the SCCs, the data importer has reason to believe that it can no longer comply with the SCCs because of local laws or practices, it has to notify the data exporter, who has to identify additional safeguards to be put in place by the parties to address the situation (**Clause 14(f)**). Where this is not possible, the transfer has to be suspended.

3.3 Supervision:

Both the ASEAN MCCs and the EU SCCs contain clauses relating to queries from relevant enforcement authorities. The ASEAN MCCs provide an optional clause for data exporters and data importers to cooperate with competent authorities, while the EU SCCs require data importers to submit to the jurisdiction of the relevant EU supervisory authority.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 4.3: Both the data exporter and data importer undertake to respond to queries from enforcement authorities regarding data processing in their respective jurisdictions.	The data importer has to submit to the jurisdiction of the competent EU supervisory authority, including by agreeing to cooperate in any procedures aimed at ensuring compliance with the SCCs (responding to enquiries, submitting to audits and complying with decisions), see **Clause 13(b)**.

3.4 Dispute resolution and liability between the parties:

Both the ASEAN MCCs and the EU SCCs contain clauses on avenues for dispute resolution. The ASEAN MCCs allow parties to identify an alternative dispute resolution method while the EU SCCs require disputes to be resolved in the courts of an EU country which parties have to specify. In addition, the EU SCCs make reference to the liability of the parties towards each other.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The parties have the option to identify a method for dispute resolution in the MCCs (**Optional – Clause 5.3**). As a practical rule of thumb, it would make sense for parties using the ASEAN MCCs to consider using dispute resolution venues within the region, particularly if data is being exported from an AMS.	The parties are liable for damages they cause one another due to a breach of the Clauses (**Clause 12(a)**). Any dispute arising from the SCCs has to be resolved by the courts of an EU country, to be specified in the SCCs (**Clause 18**).

3.5 Government access to data:

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 4.3: The data exporter and data importer shall each respond to enquiries from relevant enforcement authorities regarding the processing of personal data in their respective jurisdictions, including requests to access personal data.	**Notification:** If the data importer receives a request for access to data received under the SCCs from a public authority (or becomes aware of direct access to such data), it has to notify the data exporter and, where possible, the data subjects thereof (**Clause 15.1(a)**).

Specific information on ASEAN MCCs	Specific information on EU SCCs
	At the same time, the SCCs take into account that providing this information may not be possible, for legal or practical reasons. In particular, the data importer may be prohibited (by its national law) to inform about specific instances of government access. In this case, it should use its best efforts to obtain a waiver of such prohibition, with a view to communicating as much information as possible, as soon as possible (**Clause 15.1(b)**). In addition, it may be difficult in practice to contact the concerned individuals (e.g., because the data importer has no direct relationship with the individuals). In this respect, **Clause 15.1(a)** makes clear that the data importer may use the help of the data exporter (who may have a direct relationship with the individuals concerned). More generally, the data importer should provide the data exporter with aggregate information about access requests it has received at regular intervals (**Clause 15.1(c)**). This obligation only applies if the importer is allowed under its national law to provide such information. **Review of legality:** According to **Clause 15.2**, the data importer also has to review whether the requests it receives are lawful under the applicable domestic legal framework. If the importer determines that there are reasonable grounds to consider the request unlawful (e.g., if it is evident that the requesting authority has exceeded its powers), it should make use of the procedures available under its domestic law to challenge the request. If the data importer has challenged a request and considers that there are sufficient grounds to appeal the outcome of the procedure at first instance, such an appeal should be pursued. Finally, the data importer agrees to provide the public authority with only the minimum amount of information permissible when responding to a request for disclosure (**Clause 15.2(c)**).

3.6 Non-compliance and termination:

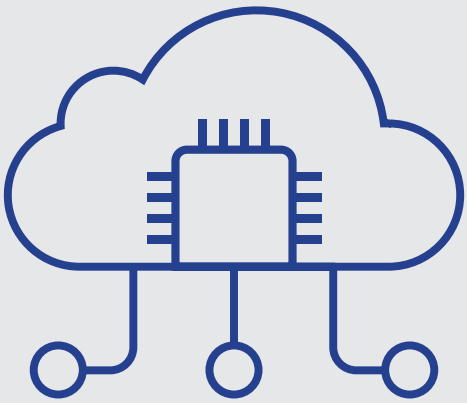
Both the ASEAN MCCs and the EU SCCs regulate the consequences of non-compliance with the clauses, including by providing for the possibility to terminate the contract in certain situations.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Clause 6: Either party may terminate the contract if: ▶ Compliance with the contract would put itself or the other party in breach of its obligations under the law of the country where it processes the data; ▶ The other party is in material breach of any obligation under the contract; ▶ There is a final decision of a competent court that there has been a breach of the contract by the party itself or the other party; ▶ The other party ceases its operations, announces its intent to do so, or transfers its assets to a non-affiliated entity.	The data importer has to inform the data exporter if it is unable to comply with the Clauses, for whatever reason (**Clause 16**). In case of non-compliance by the data importer, the data exporter must suspend the transfer of data. In addition, the data exporter has the possibility to terminate the contract if: ▶ The transfer has been suspended and compliance with the Clauses is not restored within a reasonable time and in any event within one month; ▶ The data importer is in substantial or persistent breach of the Clauses; ▶ The data importer fails to comply with a binding decision of a competent court or supervisory authority regarding compliance with the Clauses.

3.7 Survival clauses:

Both the ASEAN MCCs and the EU SCCs contain rules on the deletion or return of the data after termination of the contract and require the data importer to continue to ensure compliance with the clauses as long as the data has not been deleted or returned.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 3.6: Upon the termination or completion of the performance of the contract, the data exporter may either request the data importer to return the data in its possession to the exporter, or direct it to dispose of the data. The data importer will provide written confirmation that they have done as requested. **Optional – Clause 6.3:** Termination does not exempt from obligations to return or delete the data.	After termination of the clauses, all personal data transferred must, at the choice of the data exporter, be returned or deleted by the data importer. In case of deletion, the data importer must be able to demonstrate the deletion (**Clause 16(d)**). Prior to the return or deletion of the data, all the obligations of the Clauses continue to apply. In case of local laws applicable to the data importer that prohibit the return or deletion of the data, the data importer has to continue to ensure compliance with the Clauses and only process the data to the extent and for as long as required under such local laws.



OBLIGATIONS FOR CONTROLLER-TO-PROCESSOR TRANSFERS

1 DATA PROTECTION SAFEGUARDS

Both the ASEAN MCCs and the EU SCCs contain contractual commitments by the parties to ensure core essential data protection principles and obligations. This includes obligations for the data exporter[10] (acting as a controller) as well as the data importer[11] (acting as a processor).

1.1 Lawfulness of the transfer:

For both the ASEAN MCCs and EU SCCs, the data exporter is responsible for ensuring that the data transfer takes place in compliance with applicable legal requirements.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The collection, use, disclosure or transfer of personal data must be in accordance with applicable AMS Law or with the consent of the data subject (**Clause 2.1**).	**Clause 2(b)** recalls that the data exporter has to comply with the GDPR, including Article 6 (legal basis) when transferring personal data based on the SCCs.

1.2 Instructions:

For both the ASEAN MCCs and the EU SCCs, the data importer may only process the data received from the data exporter in accordance with the latter's instructions.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data importer shall process the personal data only in compliance with the data exporter's instructions (**Clause 3.1**).	The data importer may only process data in accordance with the data exporter's documented instructions. If the data importer becomes unable to respect those instructions, it has to inform the data exporter accordingly (**Clause 8.1**).

[10] *See Clause 1.3 of the MCCs, which defines "data exporter" as "the Party which transfers Personal data to the Data importer under this contract"; and Clause 1(b) of the SCCs, which defines the notion of "data exporter" as "the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data".*

[11] *See Clause 1.4 of the MCCs, which defines "data importer" as "the Party that receives Personal data from a Data exporter under this contract"; and Clause 1(b) of the SCCs, which defines the notion of "data importer" as "the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses".*

1.3 Specifying the purpose of the transfer and purpose limitation:

For both the ASEAN MCCs and the EU SCCs, the parties have to describe the purposes of the transfer and subsequent processing in an annex to the clauses. The data importer may process the data only for those purposes.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Parties should specify the details of the transfer in the Appendix to the contract (**Clause 9.1**). The data importer shall process the personal data only for the purposes described in Appendix A (**Clause 3.1**).	The parties should specify the purposes for which the data may be processed by the data importer in the Appendix (**Clause 6**). The data importer may only process the data it receives under the SCCs for those purposes, except upon further instructions from the data exporter (**Clause 8.2**).

1.4 Data accuracy:

Both the ASEAN MCCs and the EU SCCs contain clauses stipulating an obligation for the data exporter to ensure the accuracy of the data transferred and for the data importer to cooperate with the data exporter to ensure the accuracy of the data. However, these clauses are optional (subject to the needs of the contract) for the ASEAN MCCs.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 2.2: The data exporter must ensure that the data collected, used, disclosed and transferred is accurate and complete for the purposes of transfer. **Optional – Clause 3.7:** The data importer must correct any error or omission in the personal data reasonably requested by the data exporter within a mutually agreed upon time frame or within a time frame required by AMS law, whichever is shorter. [*Note:* These clauses should be included in the contract where the accuracy of the data is relevant to the required processing.]	In accordance with its obligations under the GDPR, the data exporter has to ensure that the data it transfers is accurate and up to date (see also **Clause 2(b)**). The data importer has to inform the data exporter without undue delay if any data it receives is inaccurate or outdated. The data importer must then cooperate with the data exporter to erase or rectify the data (**Clause 8.4**).

1.5 Storage limitation and return of the data:

For both the ASEAN MCCs and the EU SCCs, the data importer has to delete or return the data at the end of the processing. Under the SCCs, the parties also have to agree on the duration of the processing.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Upon completion of the processing, the data importer must follow the data exporter's instructions to return or delete the data (**Clause 3.8**). The ASEAN MCCs also contain an additional optional clause according to which the data importer would be required to confirm with the data exporter that it has ceased to retain the personal data.	The parties have to agree on the duration of the processing and include that information in an annex (**Clause 8.5**). At the end of the processing, the data importer has to delete (and confirm that it has done so) or return the data, depending on the choice of the data exporter.

1.6 Security and confidentiality:

For both the ASEAN MCCs and the EU SCCs, the parties have to put in place appropriate measures to ensure security of the data, including protecting it against data breaches. Both the ASEAN MCCs and the EU SCCs also include clauses on actions to be taken in case of a data breach by the data importer, including notifying the data exporter.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data exporter shall implement adequate technical and operational measures to ensure the security of the personal data during transmission to the data importer (**Clause 2.3**). The data importer is responsible for and must implement reasonable and appropriate technical, administrative, operational and physical measures to protect personal data, particularly against data breaches (**Clause 3.9**).	The parties have to agree on appropriate technical and organisational measures to be applied by the data importer to ensure the security of personal data, which have to be specified in an annex to the SCCs (**Clause 8.6(a)**). The data exporter has to ensure appropriate security during transmission of the data.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The ASEAN MCCs also provide for an optional clause according to which the data importer agrees to take reasonable steps to comply with adequate security standards prescribed by the data exporter (**Clause 3.4**). If there is a data breach affecting the data importer or any of its sub-processers, data importers have to notify the data exporter without undue delay or within a reasonable time period agreed between the parties (**Clause 3.10**).	The data importer has to: ▶ Carry out regular checks to ensure that the measures continue to provide an appropriate level of security (**Clause 8.6(a)**); ▶ Ensure that persons authorised to process the personal data have committed to confidentiality or are under appropriate statutory obligations of confidentiality (**Clause 8.6(b)**). In case of a data breach, the data importer has to: ▶ Take appropriate measures to address and mitigate the possible adverse effects of the data breach (**Clause 8.6(c)**); ▶ Notify the data exporter of the data breach (**Clause 8.6(c)**); ▶ Cooperate with and assist the data exporter to enable the exporter to comply with its obligations under the GDPR (**Clause 8.6(d)**).

1.7 Sensitive data:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The ASEAN Data Protection Principles do not include a category of sensitive personal data. However, under the MCCs, the data importer is required to take the risks involved in the data processing into account when determining and putting in place appropriate security measures (**Clause 3.9**). In addition, the ASEAN Data Management Framework provides guidance on different levels of security measures that ought to be implemented for the protection of personal data of different levels of sensitivity. Parties are free to include within their contracts additional protections for personal data to address specifically identified risks.	The data importer has to apply specific restrictions and/or additional safeguards, adapted to the specific nature of the data and the risks involved when the transfer involves sensitive data[12] (**Clause 8.7**). This can include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) or specific restrictions on disclosures.

1.8 Onward transfers:

For both the ASEAN MCCs and the EU SCCs, the data importer may only disclose personal data to a third party under certain conditions, such as ensuring that the third party is subject to the same or similar data protection obligations.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data importer must not disclose or transfer personal data to third parties, including sub-processors, unless it has informed the data exporter of this and provided reasonable opportunity for the data exporter to object (**Clause 3.2**). Disclosure to third parties may only occur if they are also subject to the same obligations as the processor (**Clause 3.3**).	The data importer may disclose personal data to a third party located outside the EU if the third party agrees to be bound by the SCCs, or otherwise only if one of the following conditions is met (**Clause 8.8**): ▶ The third party otherwise ensures appropriate data protection safeguards through one of the transfer tools available under the GDPR (e.g., binding corporate rules);

[12] *I.e., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed 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 offences.*

Specific information on ASEAN MCCs	Specific information on EU SCCs
	▶ The third party is in a country that benefits from an adequacy decision adopted by the European Commission; ▶ The transfer is necessary to establish, exercise or defend legal claims (e.g., in the context of court proceedings); ▶ The transfer is necessary to protect the vital interests of an individual.

1.9 Sub-processing:

For both the ASEAN MCCs and the EU SCCs, the data importer may only hire sub-processors with the agreement of the data exporter. It has to ensure that any sub-processor is subject to the same data protection obligations as the data importer. The data importer remains responsible for the actions of its sub-processors towards the data exporter.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data importer may only disclose or transfer personal data to sub-processors after it has notified the data exporter thereof and provided reasonable opportunity for the data exporter to object (**Clause 3.2**). Prior to any disclosure to sub-processors, the data importer shall ensure that the third party is subject to and bound by the same obligations (**Clause 3.3**).	The data importer may only hire a sub-processor with the authorisation of the data exporter (**Clause 9(a)**). This authorisation can be specific (for each sub-processor), or general (whereby the parties agree on a list of authorised sub-processors, which can be changed after giving the exporter the possibility to object). The data importer has to enter into written contracts with its sub-processors, ensuring that they are subject to the same data protection obligations as the data importer under the clauses (**Clause 9(b)**). The data importer has to provide the data exporter with a copy of its sub-processing agreements upon request, but may redact them to the extent necessary to protect business secrets or other confidential information (**Clause 9(c)**). The data importer is responsible to the data exporter for the performance of the sub-processor's obligations (**Clause 9(d)**). The data importer has to notify the data exporter in case a sub-processor fails to fulfil its obligations.

2 DATA SUBJECT RIGHTS

2.1 Transparency:

Specific information on ASEAN MCCs	Specific information on EU SCCs
Data subject rights are dependent on domestic legislation. The ability to confer contractual rights under the ASEAN MCCs on data subjects when they are not a party to the agreement depends on the domestic contract laws of the ASEAN member state. In the controller-processor arrangement, the data controller should remain primarily responsible to give effect to data subject rights under its domestic laws. It is also good practice for data exporters to be transparent with data subjects when required to seek consent. In particular, where there is no other legal basis for the collection, use, disclosure or transfer of the data, the data exporter is responsible for ensuring that the data subject has been notified of and has given consent to the transfer of his/her personal data, in accordance with applicable law (**Clause 2.1**).	**Clause 8.3** recalls the transparency obligations of the data exporter under the GDPR (Articles 13 and 14), including to inform the individual about data transfers based on the SCCs. Individuals have a right to obtain a copy of the SCCs from the data exporter (**Clause 8.3**). The exporter may redact parts of the clauses if they contain confidential information (e.g., business secrets). In that case, it has to explain these redactions and provide the individual with a meaningful summary if he/she would otherwise not be able to understand the content.

2.2 Point of contact:

For the ASEAN MCCs, data exporters are to handle inquiries from data subjects, unless the parties have agreed for the data importer to respond (and it is lawful for the importer to do so). For the EU SCCs, data importers are to provide a contact point for data subjects.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Although not specifically required, **Clause 2.4** provides that data exporters shall respond to inquiries from data subjects and law enforcement authorities. In order to facilitate such inquiries, it is a best practice for data exporters to provide a point of contact for individuals.	The data importer has to provide individuals with a contact point to handle their complaints (**Clause 11(a)**).

2.3 Rights of individuals:

For both the ASEAN MCCs and the EU SCCs, data exporters are in principle responsible for handling requests from individuals. However, the ASEAN MCCs allow data exporters and data importers to mutually agree to let data importers address such requests should they prefer this. Both the ASEAN MCCs and the EU SCCs require data importers to inform data exporters of any requests received from individuals, including requests to exercise their rights.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Clause 3.5: The data importer shall promptly communicate with and refer to the data exporter any enquiries and requests from data subjects relating to the personal data transferred by the data exporter, including requests to access or correct the data. **Clause 2.4:** The data exporter shall respond to enquiries from data subjects, including requests to access or correct personal data. However, data exporters and data importers can agree for the data importer to respond instead. Responses to such enquiries and requests shall be made within a reasonable time frame or within the time frame and in the manner, if any, required under the applicable AMS Law.	The data importer has to notify the data exporter of any request from an individual (**Clause 10**). The data importer should not reply to such requests unless authorised to do so by the data exporter, and has to assist the data exporter in handling the request. The parties have to set out in Annex II how they intend to cooperate to respond to data subject requests.

2.4 Third-party beneficiary rights and redress:

Both the ASEAN MCCs and the EU SCCs grant contractual rights to third parties outside the contract, with respect to certain safeguards set out therein. The EU SCCs provide individuals with different avenues to obtain redress for non-compliance by the parties with those safeguards. The ASEAN MCCs offer an additional set of clauses that can be included by the parties where relevant legal frameworks require third-party rights to be built into the contract.

Specific information on ASEAN MCCs

Optional – Additional terms for individual remedies: Data subjects can enforce the following rights, as long as the applicable law confers third party beneficiary rights (**Clause 1.1 of the Additional Terms**):

- **Against the data exporter: Clause 2.1** (obligation to ensure the lawfulness of the transfer) and **Clause 2.4** (obligation to respond to enquiries);
- **Against the data importer: Clause 3.5**: obligation to refer requests from individuals to the data exporter.

Individuals can also enforce the abovementioned clauses against sub-processors when both the data exporter and data importer have ceased operations, ceased to exist, or transferred all or substantially all of their assets to a non-associated entity that has assumed the legal obligations of the data exporter (**Clause 1.4 of the Additional Terms**).

Optional – Clause 4.3: any dispute under the contract shall be resolved via a method selected by both the data exporter and data importer.

To the extent authorised by applicable AMS Law, data subjects may obtain compensation for breaches of the MCCs by the data importer and/or data exporter (**Clause 1.5 of the Additional Terms**).

A data subject may be represented by another body if this is permitted by applicable law (**Clause 1.6 of the Additional Terms**).

Specific information on EU SCCs

Data subjects can enforce most clauses of the SCCs (except those that only regulate the relationship between the contractual parties, see **Clause 3**) against the parties. This includes the possibility to obtain compensation for any material or non-material damage by the data importer, either from the data exporter (**Clause 12(c)**) or the data importer (**Clause 12(b)**). When more than one party is responsible for the damage, all responsible parties will be jointly and severally liable (**Clause 12(e)**).

In case of a dispute between a data subject and one of the parties concerning compliance with the clauses, the party must use its best efforts to resolve the issue amicably (**Clause 11(b)**).

To obtain redress, data subjects can lodge a complaint with:

- The data importer (**Clause 11(a)**) and, if accepted by the data importer, an independent dispute resolution body;
- A supervisory authority (**Clause 11(c)**);
- A court (either the competent courts in the jurisdiction that has been chosen by the parties, or the courts of the country where the individual resides (**Clause 11(c) and Clause 18(c)**).

An individual may be represented by a non-profit body (**Clause 11(d)**).

3 COMPLIANCE, DISPUTE RESOLUTION AND TERMINATION

3.1 Compliance by the importer and audits:

Both the ASEAN MCCs and the EU SCCs require the data importer to cooperate with and provide relevant information to the data exporter with respect to compliance with its obligations under the contract (e.g., through audits).

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 3.6: At the reasonable request of the data exporter, the data importer must provide access to documents, data files and facilities for audit.	Both parties must be able to demonstrate compliance with the SCCs (**Clause 8.9**). The data importer has to keep appropriate documentation and make it available to the competent supervisory authority upon request. In addition, the data importer has to: ▶ Deal with enquiries from the data exporter concerning the transferred data (**Clause 8.9(a)**); ▶ Make all information necessary to demonstrate compliance with the clauses available to the data exporter at the exporter's request (**Clause 8.9(c)**); ▶ Allow for audits (which can be carried out by the data exporter or by an independent auditor), at reasonable intervals or in case of indications of non-compliance (**Clause 8.9(c) and (d)**).

3.2 Ability to comply:

The ASEAN MCCs and EU SCCs contain provisions on the ability of the parties to comply with their contractual commitments. The focus of the MCCs is on the legal capacity and authority of the parties to enter into and perform their contractual obligations, whereas the SCCs focus on local laws and practices in the country of the data importer that may prevent it from complying.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Both the data exporter and data importer confirm that they are able and authorised to enter into and perform their obligations under the contract (**Clause 7.1**).	**General:** The data exporter has to use reasonable efforts to determine that the data importer is able, through the implementation of technical and organisational measures, to satisfy its obligations under the SCCs (**Clause 8**). **Local laws and practices affecting compliance with the Clauses:** The parties have to assess whether the laws and practices in the country of the data importer prevent it from complying with the SCCs (**Clause 14(a)**). Laws and practices that do not exceed what is necessary and proportionate in a democratic society to safeguard important public interest objectives are not considered to be in contradiction with the SCCs. The parties must document their assessment, which must be transfer specific (see **Clause 14(b)**) and make it available to the competent supervisory authority upon request (**Clause 14(d)**). If, after having entered into the SCCs, the data importer has reason to believe that it can no longer comply with the SCCs because of local laws or practices, it has to notify the data exporter, who has to identify additional safeguards to be put in place by the parties to address the situation (**Clause 14(f)**).

3.3 Supervision:

Both the ASEAN MCCs and EU SCCs contain clauses relating to queries from relevant enforcement authorities. The ASEAN MCCs require the data importer to cooperate with competent authorities if authorised to do so by the data exporter, while the EU SCCs require data importers to submit to the jurisdiction of the relevant EU supervisory authority.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data exporter must respond to enquiries from enforcement authorities on the processing by the data importer (**Clause 2.4**). The data importer may respond to such enquiries if authorised to do so by the data exporter (**Clause 3.12**).	The data importer has to submit to the jurisdiction of the competent EU supervisory authority, including by agreeing to cooperate in any procedures aimed at ensuring compliance with the SCCs by responding to enquiries, submitting to audits and complying with decisions (**Clause 13(b)**).

3.4 Dispute resolution and liability between the parties:

Both the ASEAN MCCs and the EU SCCs contain clauses on avenues for dispute resolution. The ASEAN MCCs allow parties to identify an alternative dispute resolution method, while the EU SCCs require disputes to be resolved in the courts of an EU country, which parties have to specify. In addition, the EU SCCs make reference to the mutual liability of parties.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The parties have the option to identify a method for dispute resolution in the MCCs (optional **Clause 4.3**). As a practical rule of thumb, parties using the ASEAN MCCs should consider using dispute resolution venues within the region, particularly if data is being exported from an AMS. [*Note:* As they provide a baseline set of clauses and can be amended, the ASEAN MCCs do not address the issue of indemnification, which can be commercially negotiated by parties and included in the contract if preferred. This can also be something determined by the applicable law.]	The parties are liable for damages they cause one another due to a breach of the Clauses (**Clause 12(a)**). Any dispute arising from the SCCs has to be resolved by the courts of an EU country, to be specified by the parties in the SCCs (**Clause 18**).

3.5 Government access to data:

Both the ASEAN MCCs and the EU SCCs require data importers to alert data exporters about investigations regarding personal data that have been transferred to them, unless prohibited by law. The EU SCCs provide further detailed obligations on data importers actions vis-à-vis such requests.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data importer has to promptly inform and consult with the data exporter regarding any investigation regarding the transferred personal data, unless prohibited under law (**Clause 3.11**).	**Notification:** If the data importer receives a request for access to data received under the SCCs from a public authority (or becomes aware of direct access to such data), it has to notify the data exporter and, where possible, the data subjects thereof (**Clause 15.1(a)**). At the same time, the SCCs take into account that providing this information may not be possible for legal or practical reasons. In particular, the data importer may be prohibited (by its national law) to inform about specific instances of government access. In this case, it should use its best efforts to obtain a waiver of such prohibition, with a view to communicating as much information as possible, as soon as possible (**Clause 15.1(b)**). In addition, it may be difficult in practice to contact the concerned individuals (e.g., because the data importer has no direct relationship with the individuals). In this respect, **Clause 15.1(a)** makes clear that the data importer may use the help of the data exporter (who may have a direct relationship with the individuals concerned). More generally, the data importer should provide the data exporter with aggregate information about access requests it has received at regular intervals (**Clause 15.1(c)**). This obligation again only applies if the data importer is allowed under its national law to provide such information.

Specific information on ASEAN MCCs	Specific information on EU SCCs
	Review of legality: According to **Clause 15.2**, the data importer also has to review whether the requests it receives are lawful under the applicable domestic legal framework. If the importer determines that there are reasonable grounds to consider the request unlawful (e.g., if it is evident that the requesting authority has exceeded its powers), it should make use of the procedures available under its domestic law to challenge the request. If the data importer has challenged a request and considers that there are sufficient grounds to appeal the outcome of the procedure at first instance, such appeals should be pursued. Finally, the data importer agrees to provide the public authority only with the minimum amount of information permissible when responding to a request for disclosure (**Clause 15.2(c)**).

3.6 Non-compliance and termination:

Both the ASEAN MCCs and the EU SCCs allow for the temporary suspension of data transfers in case of non-compliance with the clauses, and set out the situations where the contract may be terminated.

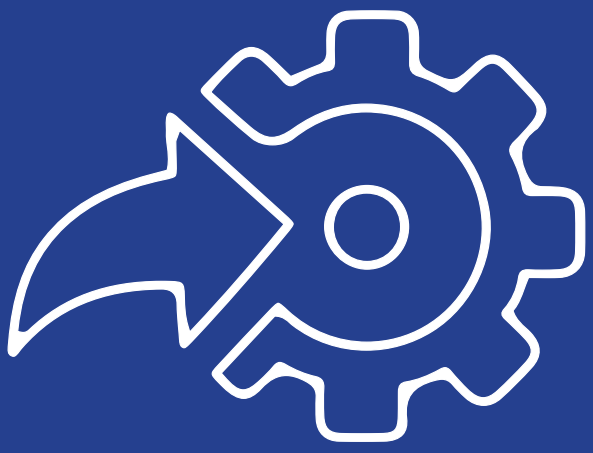
Specific information on ASEAN MCCs	Specific information on EU SCCs
In the event that the data importer is in breach of its obligations, the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the processing is terminated (**Clause 5.1**).	The data importer has to inform the data exporter if it is unable to comply with the Clauses, for whatever reason (**Clause 16**). In case of non-compliance by the data importer, the data exporter must suspend the transfer of data.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Either party may terminate the contract if (**Clause 6**): ▶ The data exporter suspended the transfer despite a breach being repaired or processing having been terminated pursuant to **Clause 5.1**; ▶ Continued compliance with the contract would be illegal under the law of the country where the data is processed; ▶ The other party is in material breach of any obligation under the contract; ▶ There is a final decision of a competent court that there has been a breach of the contract by the party itself or the other party; ▶ The other party ceases its operations, announces its intent to do so, or transfers its assets to a non-affiliated entity.	In addition, the data exporter has the possibility to terminate the contract if: ▶ The transfer has been suspended and compliance with the Clauses is not restored within a reasonable time and in any event within one month; ▶ The data importer is in substantial or persistent breach of the Clauses; ▶ The data importer fails to comply with a binding decision of a competent court or supervisory authority regarding compliance with the Clauses.

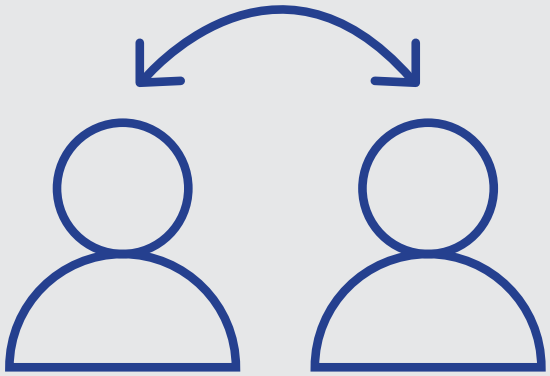
3.7 Survival clauses:

The ASEAN MCCs and EU SCCs contain rules on the deletion or return of the data after termination of the contract and require the data importer to continue to ensure compliance with the clauses as long as the data has not been deleted or returned.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Upon termination of the contract, the data exporter may either request the data importer to return the data in its possession, or direct the data importer to dispose of the data. The data importer must provide written confirmation to the data exporter that it has acted as requested (**Clause 3.8**). Termination of the contract does not exempt parties from their obligations regarding the return or deletion of the personal data transferred (**Clause 6.3**).	After termination of the clauses, all personal data transferred must, at the choice of the data exporter, be returned or deleted by the data importer. In case of deletion, the data importer must be able to demonstrate the deletion (**Clause 16(d)**). Prior to the return or deletion of the data, all the obligations of the Clauses continue to apply. In case of local laws applicable to the data importer that prohibit the return or deletion of the data, the data importer has to continue to ensure compliance with the Clauses and only process the data to the extent and for as long as required under such local laws.



PART 2: IMPLEMENTATION GUIDE



OBLIGATIONS FOR CONTROLLER-TO-CONTROLLER TRANSFERS

A Specifying the purpose of the transfer and purpose limitation:

For both the ASEAN MCCs and the EU SCCs, the parties have to describe the purpose of the transfer and subsequent processing in an annex to the clauses. The data importer has to commit to the principle of processing the data only for those purposes, under a mandatory clause in the SCCs and an optional one in the MCCs.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Parties should specify the details of the transfer in the Appendix (see **Clause 9.1**). If the parties wish to limit the purposes of processing, they may choose to include an optional clause requiring the data importer to only process the personal data for the purposes described (**Clause 3.1**).	The parties should specify the purposes for which the data may be processed by the data importer in the Appendix (see **Clause 6**). The data importer may only process the data it receives under the SCCs for those purposes, except if (1) it obtains the individual's consent, (2) the processing is necessary to establish, exercise or defend legal claims (e.g., in judicial proceedings) or (3) this is necessary to protect the vital interests of an individual (**Clause 8.1**).

Examples of how safeguards required under the clauses can be operationalised

- Documenting how the transferred personal data is handled e.g., using data inventory maps to specify the purposes, frequency of collection, use and disclosure of personal data, and keeping records of who has access to the personal data.
- Where the personal data is to be further processed or used for purposes that deviate from what was agreed upon (i.e., secondary use), documenting the data importer's assessment on whether consent had been obtained, or whether it could rely on other legal bases for the use of the personal data.
- If consent is relied on as a legal basis, to maintain policies/procedures for requirements on obtaining valid consent and keeping a record of consent obtained.

B Data accuracy:

Under the ASEAN MCCs, the parties may agree to an optional clause whereby the data exporter has to ensure the accuracy of the data. The EU SCCs contain a mandatory clause committing both parties to do so.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 2.2: The data exporter must ensure that the data collected, used, disclosed and transferred is accurate and complete for the purposes of transfer. [*Note:* This clause should be inserted where accuracy of the personal data is relevant to the purposes of processing.]	Both the data exporter and the data importer have to ensure that the personal data is accurate and up to date. They also have to notify each other if they become aware of any inaccurate or outdated data and erase or rectify such data without delay (**Clause 8.3**).

Examples of how safeguards required under the clauses can be operationalised

- **For data exporters:** having a mechanism in place to ensure the data importer is updated on any data inaccuracy, including automating the process for notifying data importers (e.g., transmitting a notification and/or updated data set to the data importer whenever the relevant data is being corrected/updated).
- **For data importers:** putting a process in place to ensure it can rectify and correct any data inaccuracy within the agreed time period. Documenting any correction and updating in a data inventory map where possible, and having a process (including, for instance, a specific contact point) to inform the data exporter of any corrections/updates made.
- **For both data exporters and importers:** e.g., maintaining policies/procedures to ensure data quality, including procedures to ensure data is accurate and kept up-to-date, identifying personal data that they often use or rely on, and where feasible, periodically remind individuals (or users) to update for accuracy and completeness.

C Data minimisation:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The volume of data that is transferred is dependent on the commercial objective of the contract and thus left to the parties' negotiations. While the ASEAN MCCs do not contain specific clauses on data minimisation, the ASEAN Data Management Framework advises against overcollection or over-inclusion of data for processing on data as it may lead to the organisation incurring additional costs when implementing controls.	The data importer[13] has to ensure that the personal data it processes under the SCCs is adequate, relevant and limited to what is necessary in relation to the purpose of processing (**Clause 8.3**).

Examples of how safeguards required under the clauses can be operationalised

- Evaluating each personal data set and only transferring and/or processing data that is directly relevant to the purposes of the processing. Having a process in place to ensure that staff is aware of the need for such evaluations through appropriate guidance, training, etc.
- Documenting the internal assessment and providing external justification as to its assessment of what is necessary in relation to the purpose for their use of personal data, and why it would not be possible to achieve the intended purposes if there is an absence/lack of such data.

[13] *In addition, the data exporter has to ensure that the personal data it transfers is adequate, relevant and limited to what is necessary in relation to the purpose of the transfer, in accordance with Article 5(1)(c) of the GDPR.*

D Storage limitation:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The period of retention is dependent on the commercial objective of the contract and thus left to the parties' negotiations. The same principles for data minimisation are relevant: the ASEAN Data Management Framework advises against over-inclusion on data as it may lead to the organisation incurring additional costs when implementing control. In addition, parties are also reminded of the retention principle in the ASEAN Framework on Data Protection, which states that an organisation should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes.	The data importer may not retain personal data for longer than is necessary for the purpose for which it is processed. It should put in place appropriate technical or organisational measures to ensure compliance with this clause, including erasure or anonymisation of personal data and all back-ups (**Clause 8.4**).

Examples of how safeguards required under the clauses can be operationalised

- Putting in place a data retention policy for the types of personal data handled.
- Reviewing personal data held on a regular basis to determine if the relevant data is still needed. As good practice, organisations may consider involving/tasking a data protection or compliance officer within the organisation to carry out such transfer/context-specific reviews.
- Mapping out the subsequent actions required based on business needs (e.g., delete after a specific retention timeframe, anonymise the data for future processing) and designing IT system features to accommodate the varying requirements.

E Security and confidentiality:

For both the ASEAN MCCs and the EU SCCs, the parties have to put in place appropriate measures to ensure security of the data, including protecting it against data breaches. Specific requirements are also included for the notification by the data importer of data breaches.

Specific information on ASEAN MCCs

The parties should take appropriate steps to determine the level of risk of data breaches, consider the suitable security measures to manage this risk and agree on and implement appropriate controls and security standards (**Clauses 4.1 and 4.2**).

Suitable security measures parties could consider taking include:

- Instituting a risk management framework to identify security threats to repositories or datasets containing personal data, assessing the risks involved and determining the controls to mitigate or minimise such risks;
- Periodically assessing the effectiveness of the risk mitigation controls;
- Requiring employees to be bound by confidentiality obligations in their employment agreements.

The data importer has to put in place reasonable and appropriate technical, administrative, operational and physical measures to protect personal data against the risk of data breaches (**Clause 3.2**). These measures should be consistent with any applicable AMS law.

When the data importer becomes aware of a potential or actual data breach, the data importer has to notify the data exporter. This should be done without undue delay or within the time period agreed on by both parties in the contract (**Clause 3.4**).

Specific information on EU SCCs

The parties have to agree on appropriate technical and organisational measures to ensure the security of personal data, which have to be specified in an annex to the SCCs (**Clause 8.5(a) and (b)**).

The data importer has to:

- Carry out regular checks to ensure that the measures continue to provide an appropriate level of security (**Clause 8.5(a) and (b)**);
- Ensure that persons authorised to process the personal data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality (**Clause 8.5(c)**).

In case of a data breach, the data importer has to:

- Take appropriate measures to address and mitigate the possible adverse effects of the data breach (**Clause 8.5(d)**);
- Notify both the data exporter and the competent supervisory authority if the data breach is likely to result in a risk to the rights and freedoms of natural persons (**Clause 8.5(e)**);
- In cooperation with the data exporter, notify data subjects if the data breach is likely to result in a high risk to the rights and freedoms of natural persons, unless the data importer has taken measures to reduce such risk or it would require disproportionate efforts (**Clause 8.5(f)**);
- Document and record all facts relating to the data breach, including its effects and the remedial action undertaken (**Clause 8.5(g)**).

Examples of how safeguards required under the clauses can be operationalised

Security measures

- Having a process in place (including, where necessary, carrying out data protection impact assessments) to identify data protection risks and security threats so as to determine appropriate mitigation/prevention/security measures. For instance, include establishing data inventory maps and data flow diagrams to classify risk levels throughout the data life cycle.
- Given the evolving nature of security threats, putting a process in place for the data importer and exporter to periodically (or on a need-to basis, e.g., whenever there are new security threats) review/update the agreed security measures and data protection/management processes to be applied in relation to the transferred data.
- Anonymisation[14]/pseudonymisation and encryption of personal data (e.g., encryption of data in transit, or at rest).
- Privacy-enhancing technologies (PETs) that enable the processing of data, analyses and sharing of insights without actually sharing the raw personal data.
- Ensuring the confidentiality, integrity and accessibility of data processing systems, services and processes to regularly monitor and evaluate the effectiveness of the security measures in place.
- Measures for user identification and authorisation in the provision of access to data (e.g. defining user access control privileges, regularly reviewing user accounts), measures to harden Internet-facing websites and computing systems that offer web services to users, measures to secure computer networks used in the transmission of data, measures to secure databases that contain personal data, measures to ensure physical security of locations at which the data is stored and processed (e.g., CCTV monitoring, requiring access cards to enter location where data is stored), and measures for ensuring events logging.
- Periodically audit configurations and security controls to ensure compliance with the organisation's security policies (e.g., cloud configurations).

Data breach management

- Putting policies/procedures in place for breach notification and reporting to regulators when such notification is required under privacy and data protection laws.
- Putting in place a data breach management and response plan in place (e.g. with a strategy for containing, assessing and managing data breaches, including having contingency plans and running regular breach simulation exercises).
- Detailing the assessment of the breach, for instance, regarding the cause of the data breach, number of affected individuals, types of personal data involved, affected systems, servers' data, etc., and whether any remediation actions have been taken to reduce harm to affected individuals. Developing guidance, training and templates to assist staff with such documentation.
- Taking immediate containment actions, such as isolating the compromised system from the Internet or network by disconnecting all affected systems, re-routing or filtering network traffic, and closing particular ports or mail servers. Recording details of the data breach and post-breach responses in an incident record log.

[14] *Some jurisdictions may use the terms "anonymisation" and "pseudonymisation" interchangeably. In this guide, anonymisation refers to the conversion of personal data into data that cannot be used to identify an individual in an irreversible manner, while pseudonymisation refers specifically to the replacement of identifying data with made-up values. Some jurisdictions may use the terms "anonymisation" and "pseudonymisation" interchangeably. Depending on the countries the data exporter and importer are operating in, some data protection laws do not apply to anonymised data (e.g., Singapore's Personal Data Protection Act, the General Data Protection Regulation).*

F Sensitive data:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The ASEAN Data Protection Principles do not include a category of sensitive personal data. However, under the MCCs, the parties are required to take the risks involved in the data processing into account when determining and putting in place appropriate security measures (**Clauses 4.1 and 4.2**). In addition, the ASEAN Data Management Framework provides guidance on different levels of security measures that ought to be implemented for the protection of personal data of different levels of sensitivity. Parties are free to include additional protections within their contracts for the processing of personal data which they consider poses specific risks.	The data importer has to apply specific restrictions and/or additional safeguards, adapted to the specific nature of the data and the risks involved when the transfer involves sensitive data[15] (**Clause 8.6**). This can include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) or specific restrictions on disclosures.

Examples of how safeguards required under the clauses can be operationalised

- Including a "sensitive data" label or category, and specifying the additional security measures or safeguards for such data, for instance, by separating the data from other datasets, limiting access to specifically authorised employees, providing additional training to personnel authorised to process the data, additional security measures, etc.

[15] *I.e., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed 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 offences.*

G Onward transfers:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The necessity for onward transfers is dependent on the commercial objective of the contract and thus left to the parties' negotiations. It is envisaged the ASEAN MCCs continue to be used for onward transfers. The principle applicable to transfers to another country or territory in the ASEAN Framework for Personal Data Protection is also relevant here. Before transferring personal data to another country or territory, the organisation should either obtain the consent of the individual for the overseas transfer or take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with the principles in the framework.	The data importer may disclose personal data to a third party located outside the EU if the third party agrees to be bound by the SCCs or if one of the following conditions is met (**Clause 8.7**): ▶ The third party otherwise ensures appropriate data protection safeguards through one of the transfer tools available under the GDPR (e.g., binding corporate rules); ▶ The third party enters into an agreement with the data importer that ensures the same level of data protection as under the SCCs; ▶ The third party is located in a country that benefits from an adequacy decision adopted by the European Commission; ▶ The transfer is necessary to establish, exercise or defend legal claims (e.g., in the context of court proceedings); ▶ The transfer is necessary to protect the vital interests of an individual; ▶ The data importer obtains the explicit informed consent of the concerned individual.

Examples of how safeguards required under the clauses can be operationalised

- Having a process in place to assess the necessity and legality, data transfer mechanism to be used for the onward transfer, whether the third party in the third country will be subject to similar data protection obligations (e.g., via contract), and details of the transfer (e.g., how long the data will be retained by the third party, how it will be used, whether it is a one-off transfer).
- Keeping documentation on assessments regarding the need for onward transfers, applicable transfer mechanisms relied on and purposes for which such transfers take place.
- Documenting the onward transfers assessment (e.g., data protection impact assessment) and keeping the assessment up to date.

H Transparency:

Specific information on ASEAN MCCs	Specific information on EU SCCs
Data subject rights are dependent on domestic legislation. The ability to confer contractual rights under the ASEAN MCCs on data subjects when they are not a party to the agreement depends on the domestic contract laws of the ASEAN member state. Data subject rights are provided as optional clauses in the ASEAN MCCs. It is also good practice for data exporters to be transparent with data subjects when required to seek consent. Under the ASEAN MCCs, the data exporter is responsible for ensuring that, where there is no other legal basis for the collection, use, disclosure or transfer of the data, the data subject has been notified of and has given consent to the transfer of his/her personal data (**Clause 2.1**).	**Clause 8.2(d)** recalls the transparency obligations of the data exporter under the GDPR (Articles 13 and 14), including to inform the individual about data transfers based on the SCCs. In addition, the data importer has an obligation to inform data subjects of its identity and contact details, the categories of personal data transferred, their right to obtain a copy of the clauses and intended onward transfers (**Clause 8.2**). This does not apply if the data subject already has the information, or providing the information would be impossible or require a disproportionate effort, although the information should in that case, to the extent possible, be made public. In turn, individuals have a right to obtain a copy of the SCCs. The parties may redact parts of the clauses if they contain confidential information (e.g., business secrets). In that case, the parties have to explain these redactions and provide the individual with a meaningful summary if it would otherwise not be possible to understand the content.

Examples of how safeguards required under the clauses can be operationalised

- Having a redacted copy of each data transfer agreement to be provided upon individuals' request for information, as well as a summary of relevant elements in case requested by the individual.
- As a good practice, companies may also choose to make a copy of their agreement available on their website, with the necessary redactions (e.g., to remove business secrets).

I Rights of individuals:

While the ASEAN MCCs rely on the rights that are provided under the legal frameworks that apply to the data exporter and importer, under the EU SCCs, the parties additionally specifically agree that the data importer ensures certain rights for individuals that can be enforced against it.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 4.3: The data exporter and data importer shall each respond to enquiries from data subjects as regards to the processing of their personal data, including requests to access or correct such data.	The data importer has to deal with any inquiries or requests from data subjects without undue delay and at the latest within one month (**Clause 10(a)**). The SCCs provide individuals with the following rights, which can be exercised against the data importer (**Clause 10(b)-(d)**): ▶ Right of access (including confirmation as to whether their personal data is being processed, a copy of the data relating to them as well as information on the processing and the right to lodge a complaint); ▶ Right to obtain rectification of inaccurate or incomplete data; ▶ Right of erasure of personal data processed in violation of any clauses ensuring third-party beneficiary rights; ▶ Right to object to the processing of data for direct marketing purposes (in which case the data importer must cease processing); ▶ Right not to be subject to fully automated decision-making, except under certain conditions and subject to specific safeguards. The data importer may refuse an individual's request if this is allowed under the laws of the country where the importer is located and the refusal is necessary and proportionate to protect important public interest objectives. In that case, the data importer must give reasons for any refusal and notify the data subject of the possibility to obtain (judicial) redress (**Clause 10(f) and (g)**).

Examples of how safeguards required under the clauses can be operationalised

- Establishing an internal policy on handling requests, specifying e.g., through which channels requests should be submitted, what information is required from the applicant, how the individual's identity will be verified, setting a timeframe for responding to requests, how exceptions should be assessed and applied, and keeping records of the requests.
- Data protection laws in ASEAN may not provide for all the rights indicated in the EU SCCs. Organisations receiving personal data on the basis of the SCCs therefore need to ensure the necessary processes are in place to enable EU individuals to exercise those rights.

J Responsibility/accountability:

For both the ASEAN MCCs and the EU SCCs, the data importer assumes responsibility for processing the data in compliance with the contract.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 3.5: The data importer assumes responsibility for the protection, processing and maintenance of the personal data in its possession, in accordance with applicable AMS Law and the contract.	The data importer has to ensure that persons acting under its authority do not process data except on its instructions (**Clause 8.8**). Both parties must be able to demonstrate compliance with the SCCs (**Clause 8.9**). The data importer has to keep appropriate documentation and make it available to the competent supervisory authority upon request.

Examples of how safeguards required under the clauses can be operationalised

- Implementing a data protection management programme, ensuring that data processing activities and policies are properly documented (e.g., by documenting and regularly reviewing/updating risk assessment frameworks, data inventory mapping, complaints handling frameworks, breach notification policies).
- Having policies in place to ensure monitoring, auditing and ensuring compliance with the documented policies.

K Ability to comply:

Specific information on ASEAN MCCs	Specific information on EU SCCs
	Local laws and practices affecting compliance with the Clauses: The parties have to assess whether the laws and practices in the country of the data importer prevent it from complying with the SCCs (**Clause 14(a)**). Laws and practices that do not exceed what is necessary and proportionate in a democratic society to safeguard important public interest objectives are not considered to be in contradiction with the SCCs. The parties must document their assessment, which must be transfer specific (see **Clause 14(b)**) and made available to the competent supervisory authority upon request (**Clause 14(d)**). If, after having entered into the SCCs, the data importer has reason to believe that it can no longer comply with the SCCs because of local laws or practices, it has to notify the data exporter, who has to identify additional safeguards to be put in place by the parties to address the situation (**Clause 14(f)**). Where this is not possible, the transfer has to be suspended.

Examples of how safeguards required under the clauses can be operationalised

- With regard to the requirement under the EU SCCs to carry out an assessment of the laws and practices of the country of the data importer prior to entering into the clauses, further guidance is available in the answer to question 40 in the Commission's Q&A (https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en) and in the guidance cited there.

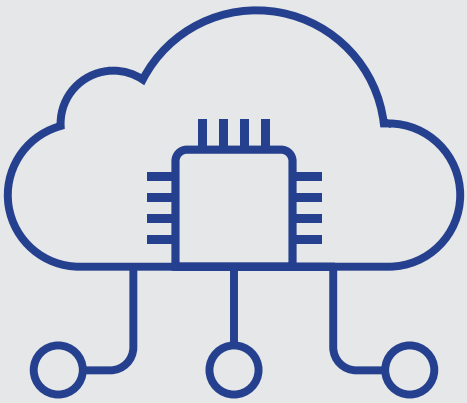
L Government access to data:

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 4.3: The data exporter and data importer shall each respond to enquiries from relevant enforcement authorities regarding the processing of personal data in their respective jurisdictions, including requests to access personal data.	**Notification:** If the data importer receives a request for access to data received under the SCCs from a public authority (or becomes aware of direct access to such data), it has to notify the data exporter and, where possible, the data subjects thereof (**Clause 15.1(a)**). At the same time, the SCCs take into account that providing this information may not be possible, for legal or practical reasons. In particular, the data importer may be prohibited (by its national law) to inform about specific instances of government access. In this case, it should use its best efforts to obtain a waiver of such prohibition, with a view to communicating as much information as possible, as soon as possible (**Clause 15.1(b)**). In addition, it may be difficult in practice to contact the concerned individuals (e.g., because the data importer has no direct relationship with the individuals). In this respect, **Clause 15.1(a)** makes clear that the data importer may use the help of the data exporter (who may have a direct relationship with the individuals concerned). More generally, the data importer should provide the data exporter with aggregate information about access requests it has received at regular intervals (**Clause 15.1(c)**). This obligation only applies if the importer is allowed under its national law to provide such information.

Specific information on ASEAN MCCs	Specific information on EU SCCs
	Review of legality: According to **Clause 15.2**, the data importer also has to review whether the requests it receives are lawful under the applicable domestic legal framework. If the importer determines that there are reasonable grounds to consider the request unlawful (e.g., if it is evident that the requesting authority has exceeded its powers), it should make use of the procedures available under its domestic law to challenge the request. If the data importer has challenged a request and considers that there are sufficient grounds to appeal the outcome of the procedure at first instance, such an appeal should be pursued. Finally, the data importer agrees to provide the public authority with only the minimum amount of information permissible when responding to a request for disclosure (**Clause 15.2(c)**).

Examples of how safeguards required under the clauses can be operationalised

- Having a policy/process in place to review requests received regarding the data covered (and whether it resides within the organisation) and the legality of requests, including, where necessary, through seeking legal advice.
- As good practice and for transparency, data importers may consider publishing the number of government data disclosures made on a periodic basis without specifying the details of each disclosure (e.g., data requestor, purpose of access, data disclosed).



OBLIGATIONS FOR CONTROLLER-TO-PROCESSOR TRANSFERS

A Specifying the purpose of the transfer and purpose limitation:

For both the ASEAN MCCs and the EU SCCs, the parties have to describe the purposes of the transfer and subsequent processing in an annex to the clauses. The data importer may process the data only for those purposes.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Parties should specify the details of the transfer in the Appendix to the contract (**Clause 9.1**). The data importer shall process the personal data only for the purposes described in Appendix A (**Clause 3.1**).	The parties should specify the purposes for which the data may be processed by the data importer in the Appendix (**Clause 6**). The data importer may only process the data it receives under the SCCs for those purposes, except upon further instructions from the data exporter (**Clause 8.2**).

Examples of how safeguards required under the clauses can be operationalised

- **For data exporters and importers:** maintaining a transfer register that contains information included in the Annexes of MCCs/SCCs (e.g., purposes for which specific types/categories of data have been transferred, and to who, for how long, whether the data will be returned to the exporter).
- **For data importers:** documenting how the transferred personal data is handled (e.g., using data inventory maps to specify the purposes, frequency of collection, use and disclosure of the personal data, keeping records of who has access to the personal data).

B Data accuracy:

Both the ASEAN MCCs and the EU SCCs contain clauses stipulating an obligation for the data exporter to ensure the accuracy of the data transferred and for the data importer to cooperate with the data exporter to ensure the accuracy of the data. However, these clauses are optional (subject to the needs of the contract) for the ASEAN MCCs.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Optional – Clause 2.2: The data exporter must ensure that the data collected, used, disclosed and transferred is accurate and complete for the purposes of transfer. **Optional – Clause 3.7:** The data importer must correct any error or omission in the personal data reasonably requested by the data exporter within a mutually agreed upon time frame or within a time frame required by AMS law, whichever is shorter. [*Note:* These clauses should be included in the contract where the accuracy of the data is relevant to the required processing.]	In accordance with its obligations under the GDPR, the data exporter has to ensure that the data it transfers is accurate and up to date (see also **Clause 2(b)**). The data importer has to inform the data exporter without undue delay if any data it receives is inaccurate or outdated. The data importer must then cooperate with the data exporter to erase or rectify the data (**Clause 8.4**).

Examples of how safeguards required under the clauses can be operationalised

- **For data exporters:** having a mechanism in place to ensure that the data importer is updated on any data inaccuracy, including automating the process to notify data importers (e.g., transmitting a notification and/or updated data set to the data importer whenever the relevant data is being corrected/updated).
- **For data importers:** putting in place a process to ensure that it can rectify or correct any data inaccuracy within the agreed time frame. Documenting any corrections and updating a data inventory map where possible and having a process (including, for instance, a specific contact point) to inform the data exporter of any corrections and/or updates made.
- **For both data exporters and importers:** e.g., maintaining policies and procedures to ensure data quality, including procedures to ensure data is accurate and kept up-to-date, identifying personal data that they often use or rely on, and where feasible, periodically remind individuals (or users) to update for accuracy and completeness.
- In the case where individuals (or users) have control and direct access to correcting their personal data (e.g., user profile updates), such actions taken by individuals may form the basis of triggering notifications to update the data exporter and/or importer (depending on which party has direct access/control over the front-end system).

C Storage limitation and return of the data:

For both the ASEAN MCCs and the EU SCCs, the data importer has to delete or return the data at the end of the processing. Under the SCCs, the parties also have to agree on the duration of the processing.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Upon completion of the processing, the data importer must follow the data exporter's instructions to return or delete the data (**Clause 3.8**). The ASEAN MCCs also contain an additional optional clause according to which the data importer would be required to confirm with the data exporter that it has ceased to retain the personal data.	The parties have to agree on the duration of the processing and include that information in an annex (**Clause 8.5**). At the end of the processing, the data importer has to delete (and confirm that it has done so) or return the data, depending on the choice of the data exporter.

Examples of how safeguards required under the clauses can be operationalised

- Putting in place processes to ensure that the agreed retention periods are adhered to (e.g., keeping track of the "deletion date" in a data inventory or transfer register).
- Having processes in place to ensure that the data is being deleted or returned by then (e.g., obtaining written confirmation from importer that the data is no longer retained).

D Security and confidentiality:

For both the ASEAN MCCs and the EU SCCs, the parties have to put in place appropriate measures to ensure security of the data, including protecting it against data breaches. Both the ASEAN MCCs and the EU SCCs also include clauses on actions to be taken in case of a data breach by the data importer, including notifying the data exporter.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data exporter shall implement adequate technical and operational measures to ensure the security of the personal data during transmission to the data importer (**Clause 2.3**). The data importer is responsible for and must implement reasonable and appropriate technical, administrative, operational and physical measures to protect personal data, particularly against data breaches (**Clause 3.9**). The ASEAN MCCs also provide for an optional clause according to which the data importer agrees to take reasonable steps to comply with adequate security standards prescribed by the data exporter (**Clause 3.4**). If there is a data breach affecting the data importer or any of its sub-processers, data importers have to notify the data exporter without undue delay or within a reasonable time period agreed between the parties (**Clause 3.10**).	The parties have to agree on appropriate technical and organisational measures to be applied by the data importer to ensure the security of personal data, which have to be specified in an annex to the SCCs (**Clause 8.6(a)**). The data exporter has to ensure appropriate security during transmission of the data. The data importer has to: ▶ Carry out regular checks to ensure that the measures continue to provide an appropriate level of security (**Clause 8.6(a)**); ▶ Ensure that persons authorised to process the personal data have committed to confidentiality or are under appropriate statutory obligations of confidentiality (**Clause 8.6(b)**). In case of a data breach, the data importer has to: ▶ Take appropriate measures to address and mitigate the possible adverse effects of the data breach (**Clause 8.6(c)**); ▶ Notify the data exporter of the data breach (**Clause 8.6(c)**); ▶ Cooperate with and assist the data exporter to enable the exporter to comply with its obligations under the GDPR (**Clause 8.6(d)**).

Examples of how safeguards required under the clauses can be operationalised

Security measures

- Having a process in place (including, where necessary, carrying out data protection impact assessments) to identify data protection risks and security threats to determine appropriate mitigation/prevention/security measures. This can, for instance, include establishing data inventory maps and data flow diagrams to classify risk levels throughout the life cycle of the data.
- Given the evolving nature of security threats, putting a process in place for the data importer and exporter to together periodically (or on a need-to basis, e.g., whenever there are new security threats) review/update the agreed security measures and data protection/management processes to be applied in relation to the transferred data.
- Anonymisation[16]/pseudonymisation and encryption of personal data (e.g., encryption of data in transit, or at rest).
- Privacy-enhancing technologies (PETs) that enable the processing of data, analyses and sharing of insights without actually sharing the raw personal data.
- Ensuring the confidentiality, integrity and accessibility of data processing systems and services, processes to regularly monitor and evaluate the effectiveness of the security measures in place.
- Measures for user identification and authorisation in the provision of access to data (e.g., defining user access control privileges, regularly reviewing user accounts), measures to harden Internet-facing websites and computing systems that offer web services to users, measures to secure computer networks used in the transmission of data, measures to secure databases that contain personal data, measures to ensure physical security of locations at which the data is stored and processed (e.g., CCTV monitoring, requiring access cards to enter location where data is stored), and measures for ensuring events logging.

Data breach management

- Putting in place policies/procedures for breach notification and reporting to regulators when such notification is required under privacy and data protection laws.
- Putting in place a data breach management and response plan (e.g., with a strategy for containing, assessing and managing data breaches, including having contingency plans and running regular breach simulation exercises).
- Detailing the assessment of the breach, for instance, with regard to the cause of the data breach, number of affected individuals, types of personal data involved, affected systems, servers data, and whether any remediation actions were taken to reduce harm to affected individuals. Developing guidance, training and templates to assist staff with such documentation.
- Taking immediate containment actions, such as isolating the compromised system from the Internet or network by disconnecting all affected systems, re-routing or filtering network traffic, and closing particular ports or mail servers. Recording details of the data breach and post-breach responses in an incident record log.

[16] Some jurisdictions may use the terms "anonymisation" and "pseudonymisation" interchangeably. In this guide, anonymisation refers to the conversion of personal data into data that cannot be used to identify an individual in an irreversible manner, while pseudonymisation refers specifically to the replacement of identifying data with made-up values. Depending on the countries the data exporter and importer are operating in, some data protection laws do not apply to anonymised data (e.g., Singapore's Personal Data Protection Act, the General Data Protection Regulation).

E Sensitive data:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The ASEAN Data Protection Principles do not include a category of sensitive personal data. However, under the MCCs, the data importer is required to take the risks involved in the data processing into account when determining and putting in place appropriate security measures (**Clause 3.9**). In addition, the ASEAN Data Management Framework provides guidance on different levels of security measures that ought to be implemented for the protection of personal data of different levels of sensitivity. Parties are free to include within their contracts additional protections for personal data to address specifically identified risks.	The data importer has to apply specific restrictions and/or additional safeguards, adapted to the specific nature of the data and the risks involved when the transfer involves sensitive data[12] (**Clause 8.7**). This can include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) or specific restrictions on disclosures.

Examples of how safeguards required under the clauses can be operationalised

- Including a "sensitive data" label or category, and specifying the additional security measures or safeguards for such data, for instance, separating the data from other datasets, limiting access to specifically authorised employees, providing additional training to personnel authorised to process the data, additional security measures, etc.

F Sub-processing:

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data importer may only disclose or transfer personal data to sub-processors after it has notified the data exporter thereof and provided reasonable opportunity for the data exporter to object (**Clause 3.2**). Prior to any disclosure to sub-processors, the data importer shall ensure that the third party is subject to and bound by the same obligations (**Clause 3.3**).	The data importer may only hire a sub-processor with the authorisation of the data exporter (**Clause 9(a)**). This authorisation can be specific (for each sub-processor), or general (whereby the parties agree on a list of authorised sub-processors, which can be changed after giving the exporter the possibility to object). The data importer has to enter into written contracts with its sub-processors, ensuring that they are subject to the same data protection obligations as the data importer under the clauses (**Clause 9(b)**). The data importer has to provide the data exporter with a copy of its sub-processing agreements upon request, but may redact them to the extent necessary to protect business secrets or other confidential information (**Clause 9(c)**). The data importer is responsible to the data exporter for the performance of the sub-processor's obligations (**Clause 9(d)**). The data importer has to notify the data exporter in case a sub-processor fails to fulfil its obligations.

Examples of how safeguards required under the clauses can be operationalised

- **For data importers:** documenting its selection process for sub-processor, and how it maps to the data exporter's criteria/requirements for engaging any sub-processor.
- **For the general authorisation approach:** having a mechanism in place, including allocating responsibility to a dedicated actor, to for instance, ensure the necessary information flows to the data exporter, develop templates to consult the data exporter and provide training and guidance material to staff on the relevant criteria for selecting sub-processors and the process/timeframe to involve the data exporter.

G Transparency:

Specific information on ASEAN MCCs	Specific information on EU SCCs
Data subject rights are dependent on domestic legislation. The ability to confer contractual rights under the ASEAN MCCs on data subjects when they are not a party to the agreement depends on the domestic contract laws of the ASEAN member state. In the controller-processor arrangement, the data controller should remain primarily responsible to give effect to data subject rights under its domestic laws. It is also good practice for data exporters to be transparent with data subjects when required to seek consent. In particular, where there is no other legal basis for the collection, use, disclosure or transfer of the data, the data exporter is responsible for ensuring that the data subject has been notified of and has given consent to the transfer of his/her personal data, in accordance with applicable law (**Clause 2.1**).	**Clause 8.3** recalls the transparency obligations of the data exporter under the GDPR (Articles 13 and 14), including to inform the individual about data transfers based on the SCCs. Individuals have a right to obtain a copy of the SCCs from the data exporter (**Clause 8.3**). The exporter may redact parts of the clauses if they contain confidential information (e.g., business secrets). In that case, it has to explain these redactions and provide the individual with a meaningful summary if he/she would otherwise not be able to understand the content.

Examples of how safeguards required under the clauses can be operationalised

- Having a redacted copy of each data transfer agreement to be provided upon individuals' request for information, as well as a summary of relevant elements in case requested by the individual.
- As a good practice, companies may also choose to make a copy of their agreement available on their website, with the necessary redactions (e.g., to remove business secrets).

H Rights of individuals:

For both the ASEAN MCCs and the EU SCCs, data exporters are in principle responsible for handling requests from individuals. However, the ASEAN MCCs allow data exporters and data importers to mutually agree to let data importers address such requests should they prefer this. Both the ASEAN MCCs and the EU SCCs require data importers to inform data exporters of any requests received from individuals, including requests to exercise their rights.

Specific information on ASEAN MCCs	Specific information on EU SCCs
Clause 3.5: The data importer shall promptly communicate with and refer to the data exporter any enquiries and requests from data subjects relating to the personal data transferred by the data exporter, including requests to access or correct the data. **Clause 2.4:** The data exporter shall respond to enquiries from data subjects, including requests to access or correct personal data. However, data exporters and data importers can agree for the data importer to respond instead. Responses to such enquiries and requests shall be made within a reasonable time frame or within the time frame and in the manner, if any, required under the applicable AMS Law.	The data importer has to notify the data exporter of any request from an individual (**Clause 10**). The data importer should not reply to such requests unless authorised to do so by the data exporter, and has to assist the data exporter in handling the request. The parties have to set out in Annex II how they intend to cooperate to respond to data subject requests.

Examples of how safeguards required under the clauses can be operationalised

- Establishing an internal policy on handling requests, specifying e.g., through which channels requests should be submitted, the required information from the applicant, how the individual's identity will be verified, setting a timeframe for responding to requests, how exceptions should be assessed and applied, and keeping records of the requests.
- Having agreed processes in place that determine how the exporter and importer will cooperate in case of requests from individuals (e.g., the timeframe to inform each other about requests, who will handle the request and respond to the individual).

I Government access to data:

Both the ASEAN MCCs and the EU SCCs require data importers to alert data exporters about investigations regarding personal data that have been transferred to them, unless prohibited by law. The EU SCCs provide further detailed obligations on data importers actions vis-à-vis such requests.

Specific information on ASEAN MCCs	Specific information on EU SCCs
The data importer has to promptly inform and consult with the data exporter regarding any investigation regarding the transferred personal data, unless prohibited under law (**Clause 3.11**).	**Notification:** If the data importer receives a request for access to data received under the SCCs from a public authority (or becomes aware of direct access to such data), it has to notify the data exporter and, where possible, the data subjects thereof (**Clause 15.1(a)**). At the same time, the SCCs take into account that providing this information may not be possible for legal or practical reasons. In particular, the data importer may be prohibited (by its national law) to inform about specific instances of government access. In this case, it should use its best efforts to obtain a waiver of such prohibition, with a view to communicating as much information as possible, as soon as possible (**Clause 15.1(b)**). In addition, it may be difficult in practice to contact the concerned individuals (e.g., because the data importer has no direct relationship with the individuals). In this respect, **Clause 15.1(a)** makes clear that the data importer may use the help of the data exporter (who may have a direct relationship with the individuals concerned). More generally, the data importer should provide the data exporter with aggregate information about access requests it has received at regular intervals (**Clause 15.1(c)**). This obligation again only applies if the data importer is allowed under its national law to provide such information.

Specific information on ASEAN MCCs	Specific information on EU SCCs
	Review of legality: According to **Clause 15.2**, the data importer also has to review whether the requests it receives are lawful under the applicable domestic legal framework. If the importer determines that there are reasonable grounds to consider the request unlawful (e.g., if it is evident that the requesting authority has exceeded its powers), it should make use of the procedures available under its domestic law to challenge the request. If the data importer has challenged a request and considers that there are sufficient grounds to appeal the outcome of the procedure at first instance, such appeals should be pursued. Finally, the data importer agrees to provide the public authority only with the minimum amount of information permissible when responding to a request for disclosure (**Clause 15.2(c)**).

Examples of how safeguards required under the clauses can be operationalised

- Having a policy/process in place to review requests received, both concerning the data covered (and whether it resides within the organisation) and the legality of requests, including, where necessary, seeking legal advice. To the extent possible under domestic law, have a process in place to ensure information exchange and cooperation between the data importer and exporter in this context.
- As good practice and for transparency, data importers may consider publishing the number of government data disclosures made on a periodic basis without specifying the details of each disclosure (e.g., data requestor, purpose of access, data disclosed).