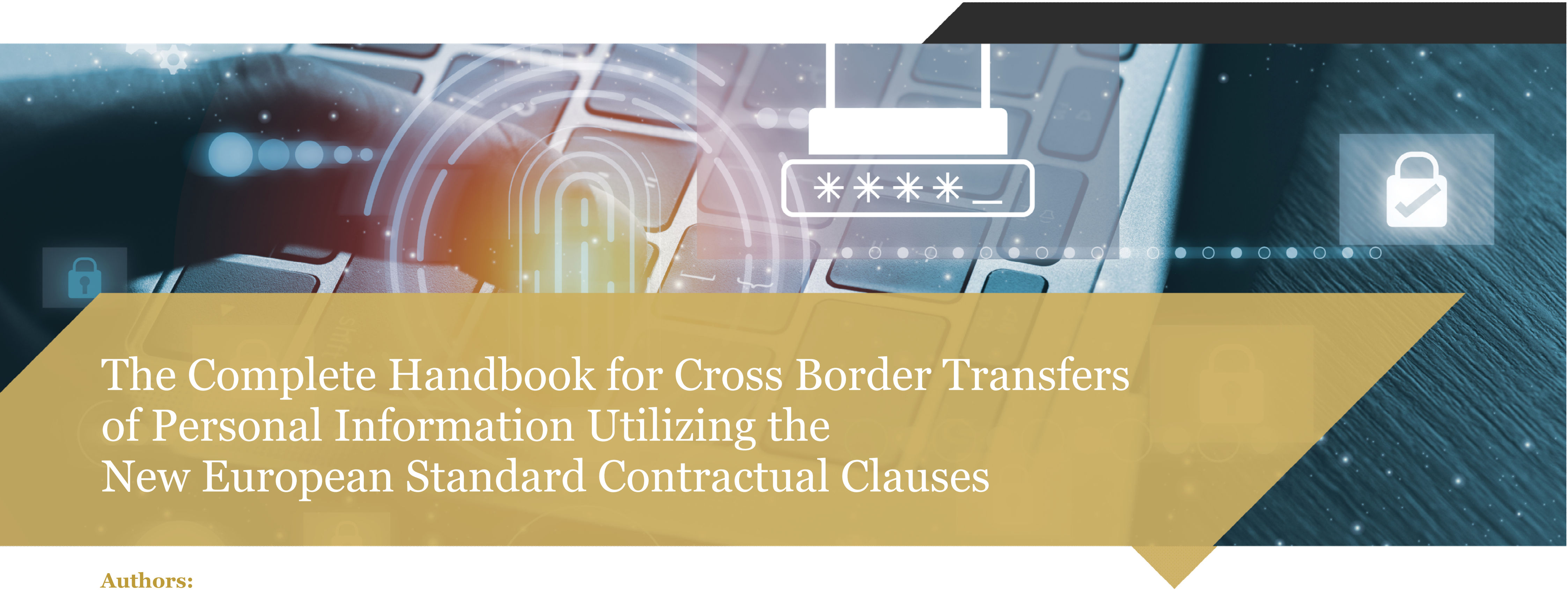
GT GreenbergTraurig

Greenberg Traurig, LLP | gtlaw.com



The Complete Handbook for Cross Border Transfers of Personal Information Utilizing the New European Standard Contractual Clauses

Authors:

David A. Zetoony
Co-Chair, U.S. Data, Privacy and Cybersecurity Practice
Greenberg Traurig, LLP
1144 15th Street, Suite 3300
Denver, CO 80202
T: +1 303.685.7425
zetoonyd@gtlaw.com

Carsten Kociok
Local Partner
Greenberg Traurig Germany, LLP
Budapester Str. 35
10787 Berlin, Germany
T: +49 30.700.171.119
Carsten.kociok@gtlaw.com

Andrea C. Maciejewski
Associate
Greenberg Traurig, LLP
1144 15th Street, Suite 3300
Denver, CO 80202
T: +1 303.685.7458
maciejewskia@gtlaw.com

About the Authors

David A. Zetoony

SHAREHOLDER

DAVID.ZETOONY@GTLAW.COM | LINKEDIN | DETAILED BIOGRAPHY

David Zetoony, Co-Chair of the firm's U.S. Data, Privacy and Cybersecurity Practice, focuses on helping businesses navigate data privacy and cyber security laws from a practical standpoint. David has helped hundreds of companies establish and maintain ongoing privacy and security programs, and he has defended corporate privacy and security practices in investigations initiated by the Federal Trade Commission, and other data privacy and security regulatory agencies around the world, as well as in class action litigation.

Carsten Kociok

LOCAL PARTNER

CARSTEN.KOCIOK@GTLAW.COM | LINKEDIN | TWITTER | DETAILED BIOGRAPHY

Carsten Kociok is a data privacy expert with a wide-ranging practice representing domestic and international clients on complex legal issues. He advises clients across all industries on a wide variety of complex matters, including international data transfers, data privacy compliance, litigation, cybersecurity and data breach response. Carsten is a recognized expert on the EU General Data Protection Regulation (GDPR) and other EU and German data privacy laws and a leading specialist in the field of financial technology laws.

Andrea C. Maciejewski

ASSOCIATE

MACIEJEWSKIA@GTLAW.COM | LINKEDIN | DETAILED BIOGRAPHY

Andrea C. Maciejewski designs and implements privacy and security programs for clients of all sizes – from Fortune 500s to start ups – and in all sectors, including digital entertainment, marketing, online education, retail, and consumer goods. Andrea helps companies navigate the intricacies of multi-jurisdictional compliance programs as well as compliance with sector-specific data privacy and security laws. Andrea offers clients practical legal counsel, striving to understand the underlying business model and provide strategies that manage costs and risks, while attempting to maintain the businesses operations.

Contents & Transfer Scenarios

1. Introduction

The General Data Protection Regulation is a comprehensive regulatory framework that imposes numerous requirements upon organizations that process personal data. One of the most complex aspects of the GDPR from a compliance standpoint are the restrictions that relate to the cross border transfer of personal data.

The GDPR contemplates several mechanisms by which personal data might be transferred from the European Economic Area ("EEA") to countries outside the EEA. These include the use of Standard Contractual Clauses, binding corporate rules, certification mechanisms, or codes of conduct. In practice, however, organizations have overwhelmingly favored the use of standard data protection clauses adopted by the European Commission also known as "Standard Contractual Clauses."

Although the first Standard Contractual Clauses were approved more than twenty years ago, there remains significant confusion regarding how the Standard Contractual Clauses should be applied to various data transfer scenarios. That confusion intensified in 2021 following the adoption of the latest Standard Contractual Clauses, and the creation of a sunset period for the three pre-existing versions. While an argument could be made that the new Standard Contractual Clauses are a significant improvement for both data subjects and organizations in that they anticipate a far greater number of transfer scenarios, they utilize an unfamiliar modular structure and contain new compliance obligations. The structure and format of the new clauses, combined with the myriad of different transfer scenarios to which the new Standard Contractual Clauses must be applied, can feel challenging to seasoned data privacy attorneys and overwhelming to transactional attorneys that are new to data privacy.

This handbook is intended to simplify the complexity and walk attorneys step-by-step through how the Standard Contractual Clauses might be applied in practice to more than forty transfer scenarios. Our hope is that it will be a useful resource to attorneys that have been working with the Standard Contractual Clauses for years as well as those that are wrestling with the clauses for the first time.
The authors would like to thank Veronica Mino, Senior Privacy Counsel at Frist Privacy GmbH, for her invaluable assistance reviewing and commenting on this handbook prior to finalization.

2. Notes on Citations and References

References to controllers. Controllers are referred to herein as **Company A**, **Company B**, and **Company C**. Unless otherwise noted, controllers are independent of each other and are not utilizing a joint controller relationship. Controllers designated with the same letter and a hyphenated number (e.g., **Company A-1** and **Company A-2**) indicate that the controllers are corporate affiliates under common ownership and control.

References to processors. Processors are generally referred to herein as **Company X**, **Company Y**, and **Company Z**. Processor designations that utilize the same letter and different hyphenated numbers (e.g., **Company Z-1** and **Company Z-2**) indicate that the processors are corporate affiliates under common ownership and control. If a controller and a processor are corporate affiliates, the affiliated relationship will be conveyed by using the letter of the controller and a sequential hyphenated number along with a controller/processor designation label (e.g., **Company A-1** (Controller) and **Company A-2** (Processor).

References to non-adequate countries. Countries that are outside of the European Economic Area and that have not been afforded an adequacy decision are referred to herein as **Countries Q, R**, and **S**. An up-to-date list of countries that have been afforded an adequacy decision can be found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en/.

References to transfers. References to "Transfer 1" and "Transfer 2" within a specific transfer scenario are not intended to necessarily indicate temporal relationships wherein data is first transferred pursuant to the description under Transfer 1 and is only then transferred pursuant to the description under Transfer 2. In some transfer scenarios data is transferred simultaneously, or in non-sequential order, and the descriptors of "Transfer 1" and "Transfer 2" are intended only to distinguish between different transfer-related documents.

Reference to "renvoi." Renvoi is used to refer to situations in which personal data is returned to the party that originally exported it.

Reference to "SCCs." SCCs refers to "Standard Contractual Clauses." As is discussed in Section 3, the European Commission approved three sets of SCCs between 2001 and 2014, and approved a new set of SCCs in 2021.[1] Where confusion may exist regarding which SCCs this handbook refers to, the term "old" SCCs is used to refer to the first three sets of SCCs, and the term "new" SCCs is used to refer to the most recent set of SCCs. Note that when the term "SCC" is used in this handbook without modification, it refers to the "new" SCCs.

References to "Cross-Border Transfers." The term "cross-border processing" is defined within the GDPR under Article 4(23) as referring to transfers of personal data between European Member States. Practitioners typically use the term "cross-border transfer" to refer to transfers between a Member State and a country that is *not* part of the European Economic Area. This Handbook adopts the latter practice of using the term cross-border transfer to refer to transfers between a Member State and a country that is not part of the European Economic Area.

3. Basic concepts and terminology

3.1 GDPR restriction on cross border transfers

The GDPR permits a company to transfer personal data outside of the EEA if (1) the company is transferring data to an entity that is within a country that has been recognized by the European Commission as ensuring an adequate level of protection, (2) the company and the data recipient have put in place a European Commission-approved mechanism (a "safeguard") that imposes many of the substantive provisions found within the GDPR, or (3) the data transfer is subject to an Art. 49 derogation.[2]

Note that while many of the transfers discussed in this handbook could be conducted pursuant to safeguards other than the SCCs (e.g., binding corporate rules, approved codes of conduct, or certification mechanisms), this handbook focuses only on transfers utilizing the SCCs.

3.2 The "old" Standard Contractual Clauses

The SCCs or "model clauses," are contractual agreements that have been pre-approved by the European Commission as sufficient to act as a safeguard. Historically, the European Commission approved three versions, or "sets," of Standard Contractual Clauses. Two sets – adopted in 2001 and in 2004 respectively – were designed to be used when a controller within the EEA transmitted personal data to a controller outside of the EEA.[3] A third set – adopted in 2010 – was designed to be used when a controller within the EEA transmitted personal data to a processor outside of the EEA.[4] These three sets are collectively referred to within this handbook as the "old" SCCs.

On 4 June 2021, the European Commission issued new SCCs. As part of its decision to implement new SCCs, the Commission repealed its prior approval of the old SCCs. The repeal effectively prohibited companies from using the old SCCs after 27 September 2021. It allowed companies that had entered into old SCCs prior to that date to continue to rely upon them until 27 December 2022. Note that when the term "SCC" is used in this handbook without modification, it refers to the "new" SCCs.

3.3 The "new" Standard Contractual Clauses

The new SCCs are comprised of four different "modules," which are intended to be used to account for the following types of transfers:

Module	Exporter	Importer
Module 1	Controller	Controller
Module 2	Controller	Processor
Module 3	Processor	Processor
Module 4	Processor	Controller

Despite the fact that the SCCs are designed to be used with relatively little customization (i.e., the material terms of the SCCs cannot be modified without jeopardizing their status as an approved safeguard), significant confusion exists as to when certain modules of the SCCs should be utilized, and what types of transfers are permitted. This handbook discusses how the SCCs apply to different transfer scenarios.

Note that the European Commission suggested in Recital 7 of its decision implementing the SCCs that an importer subject to the GDPR might not be able to utilize the new SCCs.[5] That position was reiterated by the European Commission in May of 2022.[6] Until the European Commission publishes further guidance or a new set of SCCs specifically designed to be used by importers subject to the Article 3(2) jurisdiction of the GDPR, this handbook suggests that *all* transfers subject to Chapter V of the GDPR use the new SCCs as a transfer mechanism.

3.4 Transfer Impact Assessments or TIAs

The term "Transfer Impact Assessment" or "TIA" is relatively new to the world of data privacy. Indeed, according to one widely used legal database the term was not referenced within any academic journals or secondary sources until 2021.[7] The term has come to refer to a written analysis, conducted by a controller or a processor, of the impact that a transfer of personal data to a country outside of the EEA may have on the protections afforded to the transferred data. TIAs focus specifically, although often not exclusively, on whether the laws of the country to which the data is being imported would permit government agencies to access the personal data.

The impetus to conduct a TIA comes from three legal authorities.

First, in the European Court of Justice's *Schrems II* decision, the ECJ stated that even when an organization uses a contractual mechanism provided for under the GDPR it is "above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."[8] While the ECJ decision did not mandate that the "verif[ication]" be documented and in writing, the concept of a written assessment to analyze the impacts of a transfer (i.e., a transfer impact assessment) can be used by parties to demonstrate that such verification occurred.

Second, approximately a year after the *Schrems II* decision, the European Data Protection Board finalized its recommendations on measures to supplement data transfer tools.[9] That document recommended that before transferring personal data outside of the EEA to a country that lacked an adequacy decision from the European Commission, a data exporter should "first assess, where appropriate in collaboration with the importer" whether there was "anything in the law and/or practices in force in the third country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR transfer tool you are relying on, in the context of your specific transfer."10 The EDPB further indicated that it considered the following to be necessary components of the assessment:

- An analysis of the legislation of the data importer's country.
- Whether public authorities of the third country may seek access to the data with or without the data importer's knowledge either via legislation, practice, or reported precedent.
- Whether public authorities of the third country may be able to access the data through the telecommunication providers or communication channels in light of legislation, legal powers, technical, financial, and human resources at their disposal and of reported precedent.

The EDPB stated that in its view companies should "document [the assessment] thoroughly."[11] It also noted that the assessment might be requested by "competent supervisory and/or judicial authorities."[12]

Third, the new SCCs contain a requirement within Clause 14 that for all transfers of personal information (regardless of whether they originate from, or are received by, a controller or a processor) the "Parties" must warrant that they have "no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer . . . prevent the data importer from fulfilling its obligations under these Clauses."[13] When providing such warranty, the Parties represent that they have taken specific factors into consideration (e.g., circumstances of the transfer, length of the processing chain, law and practices of the third country of destination). The data importer specifically warrants that it has "made its best efforts to provide the data exporter with the relevant information" to complete the assessment,[14] and the Parties jointly agree to "document the assessment . . . and make it available to the competent supervisory authority on request."[15]

From these three authorities the Transfer Impact Assessment emerged as a term-of-art to describe the process by which a data exporter and a data importer analyze the impact upon privacy or security when transmitting personal information from the EEA to a country outside of the EEA that has not been deemed adequate by the European Commission.

3.5 Information that must be included in a TIA

As discussed above, the impetus to conduct a TIA comes from three legal authorities: (1) the ECJ's recommendation in *Schrems II* that the parties to a transfer verify on a case-by-case basis whether the "law of the third country of destination ensures adequate protection of personal data transferred pursuant to the standard data protection clauses,"[16] (2) the EDPB's recommendations on measures to supplement data transfer tools, [17] and (3) Clause 14 of the new SCC, which requires the parties to warrant that they have analyzed certain factors about the destination country's laws.

Among the three sources, the new SCCs provide the most specific references as to what factors should be analyzed when conducting a TIA. These are viewed by many organizations as being necessary to a thorough TIA. In addition to those factors that are expressly required, the SCCs refer to other factors that "may be considered as part of an overall assessment." These are functionally viewed by many organizations as best practices, but potentially not strict requirements, along with additional factors noted in the EDPB's recommendation as being potentially "relevant." The following collects and lists all of the factors:

Laws and Practices of the Destination Country (required by Clause 14 of SCCs):

1. Laws requiring the disclosure of personal data by the importer to public authorities.[18]
2. Laws authorizing public authorities to access personal data held by the importer. [19]
3. Whether the above-referenced laws permit data subjects to obtain judicial redress against unlawful government access.[20]
4. Prior instances of requests (or the absence of such requests) for disclosures from public authorities to the importer.[21]
5. Reliable information on the existence or absence of requests for disclosure by public authorities "within the same [industry] sector."[22]
6. Case law impacting whether personal data by the importer must be disclosed to public authorities. [23]
7. Reports by independent oversight bodies discussing whether personal data (presumably within an industry sector) may be disclosed to public authorities.[24]
8. Whether the destination country has a comprehensive national data protection law.[25]
9. Whether the destination country has an independent data protection authority.[26]
10. Whether the destination country has adhered to international instruments providing for data protection safeguards.[27]

Circumstances of the transfer (required by Clause 14 of SCCs):

11. Length of the processing chain impacting the personal data.[28]
12. Number of actors that have access to personal data.[29]
13. Transmission channels used to send personal data.[30]
14. Intended onwards recipients of the personal data.[31]
15. Type of recipients of the personal data.[32]
16. Purpose of the processing.[33]
17. Categories and format of the transferred personal data.[34]
18. Economic sector in which the transfer occurs.[35]
19. Storage location of the data transferred.[36]

Supplemental measures to protect personal data (suggested by SCCs and/or EDPB)

20. Relevant contractual safeguards that may supplement the safeguards provided for in the SCCs.[37]
21. Relevant technical safeguards that may supplement the safeguards provided for in the SCCs.[38]
22. Relevant organizational safeguards that may supplement the safeguards provided for in the SCCs.[39]

3.6 Format to use when drafting a TIA

Neither the European Commission nor the European Data Protection Board mandate a format that must be used when conducting a TIA. In practice, the form, structure, length, and style of TIAs differ significantly between companies.

3.7 Law enforcement request policies

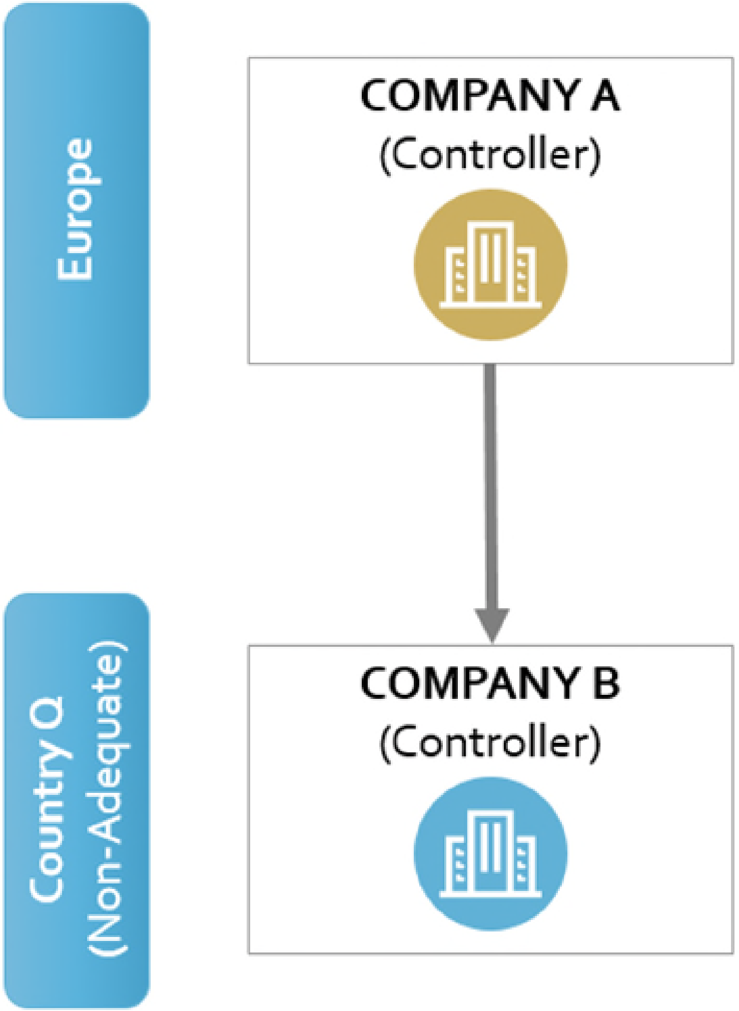
The concept of a law enforcement request policy is not new to the world of data privacy, although such policies often adopted titles that related to specific requests received in particular jurisdictions. For example, in the United States many companies maintained a policy or procedure for responding to subpoenas.

The new SCCs brought new focus and attention to law enforcement request policies. Specifically, Clause 15 requires that data importers contractually agree to notify data exporters in the event that the data importer receives a legally binding request from a public authority or becomes aware of direct access to personal data by a public authority. It further requires that a data importer take specific steps in the event that it is prohibited by the public authority from notifying the data exporter. Law enforcement request policies help ensure that data importers discharge their obligations under the new SCCs and can help demonstrate to exporters, and to regulators, that a data importer has processes, procedures, and policies in place to comply with the requirements of Clause 15.

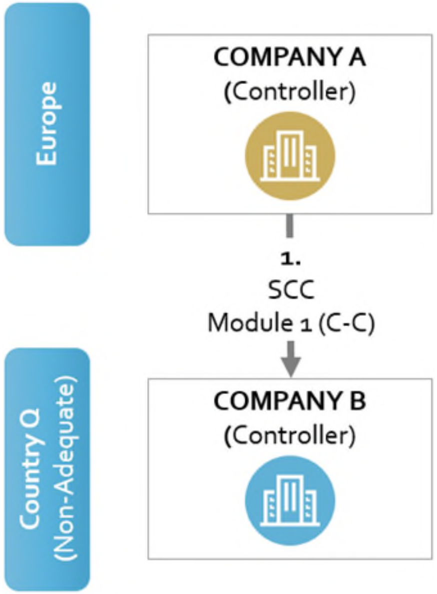
3.8 Format for drafting law enforcement request policies

As with TIAs, neither the European Commission nor the European Data Protection Board have mandated a format that must be used when creating a law enforcement request policy. In practice, the form, structure, length, and style of such policies differs significantly between companies.

4. Transfers from EEA Controllers to Non-EEA Controllers

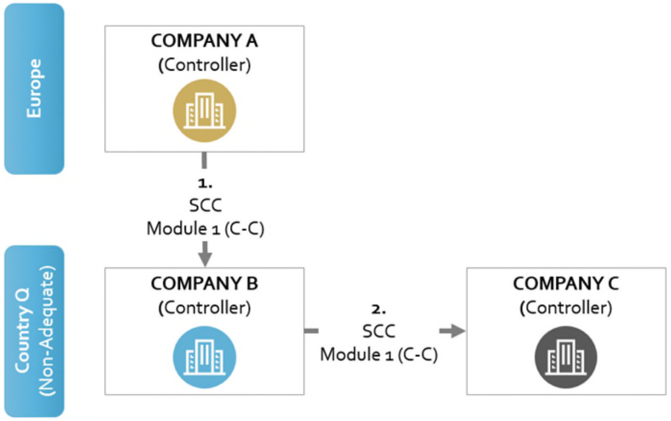


4.1 Controller A (EEA) → Controller B (Non-EEA)

Visual	Description and Implications
 Europe COMPANY A (Controller) 1. SCC Module 1 (C-C) Country Q (Non-Adequate) COMPANY B (Controller)	• Background. Company A in the EEA transfers personal data to Company B in Country Q. • Transfer 1: SCC Module 1. A cross-border transfer from Company A in the EEA to Company B in Country Q should utilize the SCC Module 1 which is designed for transfers from an EEA controller to a non-EEA controller. • Subsequent Onward Transfers from Company B. Note that if Company B makes any additional onward transfers the appropriate module of the SCCs would need to be used. • Transfer Impact Assessments. Clause 14 of the SCCs requires the parties (Company A and Company B) to document whether either party has reason to believe that the laws and practices of Country Q that apply to the personal data transferred prevent the data importer (i.e., Company B) from fulfilling its obligations under the SCCs. • Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company B) to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company B might consider creating a law enforcement request policy.

4.2 Controller A (EEA) → Controller B (Non-EEA) → Controller C (Non-EEA) (same country)

Visual



Europe

COMPANY A
(Controller)

1.
SCC
Module 1 (C-C)

Country Q
(Non-Adequate)

COMPANY B
(Controller)

2.
SCC
Module 1 (C-C)

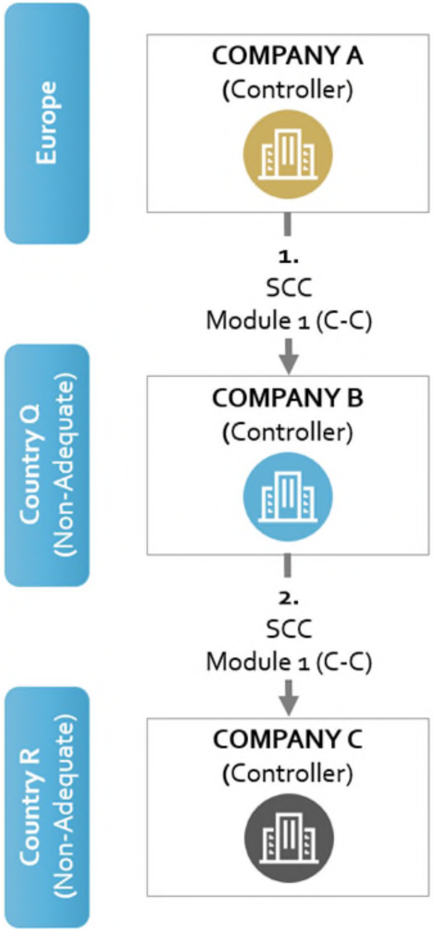
COMPANY C
(Controller)

Description and Implications

- Background. Company A in the EEA transfers personal data to Company B in Country Q. Company B then transfers the personal data to Company C in Country Q.
- Transfer 1: SCC Module 1. Initial cross-border transfer from the EEA to Country Q utilizes the SCC Module 1 designed for transfers from an EEA controller to a non-EEA controller (First SCC).
- Transfer 2: SCC Module 1. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions must also utilize the SCCs (appropriate module). According to Clause 8.7, transfers "in the same [non-EEA] country," should also utilize a safeguard mechanism such as the SCCs.[40] Note that the parties could decide to enter into a single SCC Module 1 with Company A, Company B, and Company C as signatories, or to enter into two separate SCC Module 1s with Company A and Company B signing one SCC Module 1 and Company B and Company C signing a separate SCC Module
- Subsequent Onward Transfers from Company C. Note that if Company C makes any additional onward transfers the appropriate module of the SCCs would also need to be used.
- Transfer Impact Assessments. Clause 14 of the SCCs requires all parties (Company A, Company B, and Company C) to document whether any party has reason to believe that the laws and practices of Country Q that apply to the personal data transferred prevent the data importers (i.e., Company B and Company C) from fulfilling their obligations under the SCCs. The TIA could take the form of a single document reviewed and approve by all parties, or separate documents that reflect the specific factors applicable to Company B and to Company C.
- Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importers (Company B and Company C) to take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company B and Company C might consider creating law enforcement request policies.

4.3 Controller A (EEA) → Controller B (Non-EEA) → Controller C (Non-EEA) (different countries)

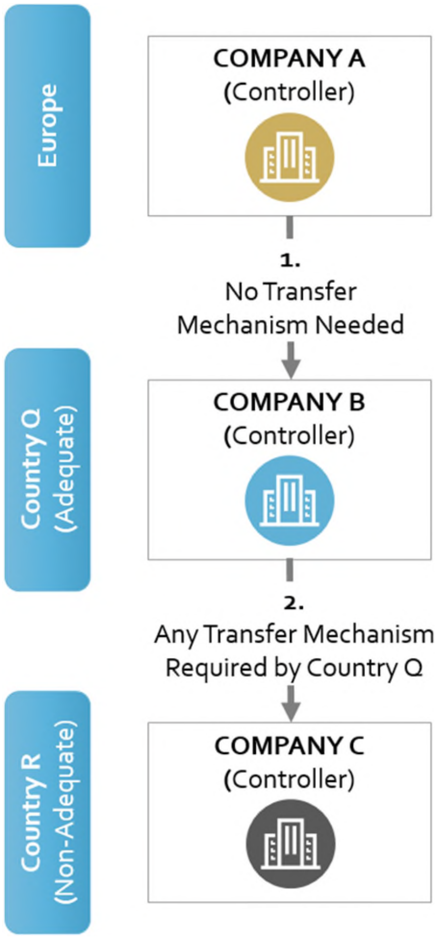
Visual	Description and Implications



- Background. Company A in the EEA transfers personal data to Company B in Country Q. Company B then transfers the personal data to Company C in Country R.
- Transfer 1: SCC Module 1. Initial cross-border transfer from the EEA to Country Q utilizes the SCC Module 1 designed for transfers from a controller to another non-EEA Controller (First SCC).
- Transfer 2: SCC Module 1. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions must also utilize the SCCs (appropriate module). As Company B and Company C are controllers, the appropriate module would be SCC Module 1. Note that the parties could decide to enter into a single SCC Module 1 that covers both Transfer 1 and Transfer 2.
- Subsequent Onward Transfers from Company C. Note that if Company C makes any additional onward transfers the appropriate module of the SCCs would also need to be used.
- Transfer Impact Assessment of Country Q. Clause 14 of the SCCs requires Company A and Company B to document whether either party has a reason to believe that the laws and practices of Country Q that apply to the personal data transferred prevent the data importer (i.e., Company B) from fulfilling its obligations under the SCC.
- Transfer Impact Assessment of Country R. Clause 14 of the SCCs requires Company B and Company C to document whether either party has reason to believe that the laws and practices of Country R prevent Company C from fulfilling its obligations under the SCCs.
- Law Enforcement Request Policies. Clause 15 of the SCCs requires that Company B and Company C take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company B and Company C might be expected to implement written law enforcement request policies.

4.4 Controller A (EEA) → Controller B (Non-EEA / Adequate) → Controller C (Non-EEA / Non-Adequate) (different countries)

Visual

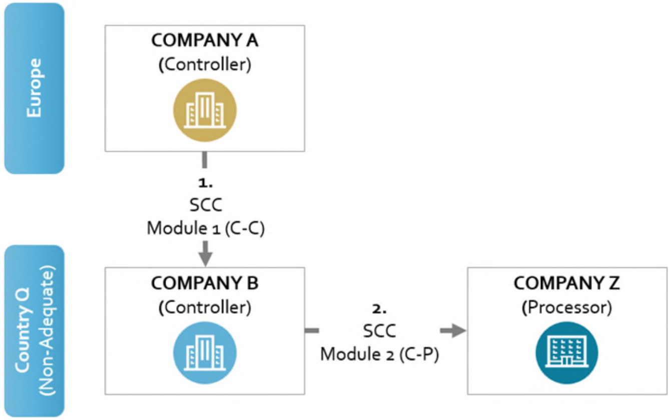


Description and Implications

- Background. Company A in the EEA transfers personal data to Company B in Country Q, which has been deemed an adequate country by the European Commission. Company B then transfers the personal data to Company C in Country R, which has not been deemed an adequate country by the European Commission.
- Transfer 1: No Mechanism Needed. The initial cross-border transfer from the EEA to Country Q does not require a transfer mechanism as the European Commission has determined that Country Q has adequate protections.
- Transfer 2: Any Transfer Mechanism Required by Country Q. To the extent that Company B is not subject to the GDPR, Company B is not required to identify a GDPR-compliant adequacy measure. Note, however, that Company B may be required to identify a safeguard that meets any cross-border transfer restriction imposed under the laws of Country Q. For example, if Company B is located in the United Kingdom, a country having been granted an adequacy decision, Company B might onward transfer the data by utilizing the ICO approved International Data Transfer Agreement.

4.5 Controller A (EEA) → Controller B (Non-EEA) → Processor Z (Non-EEA) (same country)

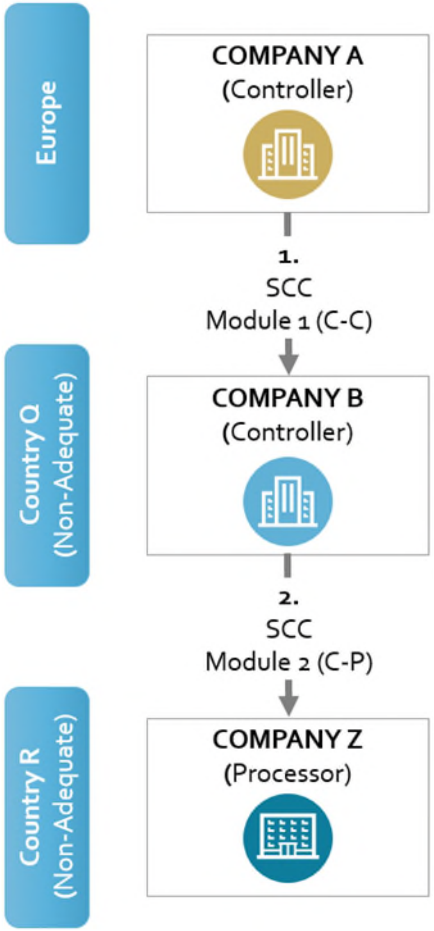
Visual



Description and Implications

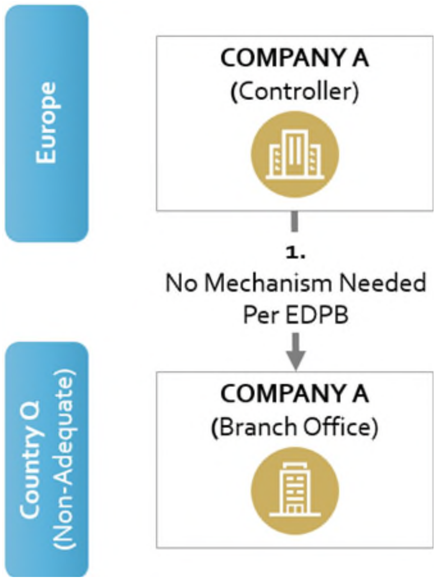
- Background. Company A in the EEA transfers personal data to Company B in Country Q. Company B then transfers the personal data to its processor, Company Z, in Country Q.
- Transfer 1: SCC Module 1. Initial cross-border transfer from the EEA to Country Q utilizes the SCC Module 1 designed for transfers from a controller to a non-EEA controller (First SCC).
- Transfer 2: SCC Module 2. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions must also utilize the SCCs (appropriate module). In this case the appropriate module would be Module 2, for transfers from controllers to processors. The fact that Company B and Company Z are located in the same country does not obviate the need to utilize the SCCs as the SCCs provide that an onward transfer "in the same [non-EEA] country," should still utilize a safeguard mechanism such as the SCCs.[41]
- Subsequent Onward Transfers from Company Z. If Company Z makes any additional onward transfers to sub-processors Company Z should utilize Module 3 of the SCCs. If Company Z were to transfer the data back to Company B, Company Z should utilize Module 4.
- Transfer Impact Assessments. Clause 14 of the SCCs requires (Company A, Company B, and Company Z) to document whether any party has reason to believe that the laws and practices of Country Q prevent Company B or Company Z from fulfilling their obligations under the SCCs. In practice, Company A and Company B might create one TIA, and Company B and Company Z might create a second TIA.
- Law Enforcement Request Policy. Clause 15 of the SCCs requires that Company B and Company Z take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company B and Company Z might consider creating written law enforcement request policies.

4.6 Controller A (EEA) → Controller B (Non-EEA) → Processor Z (Non-EEA) (different countries)

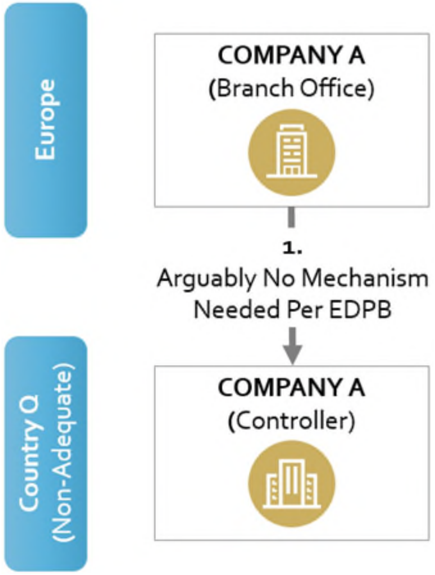
Visual	Description and Implications
	See below

- Background. Company A in the EEA transfers personal data to Company B in Country Q. Company B then transfers the personal data to its processor, Company Z, in Country R.
- Transfer 1: SCC Module 1. Initial cross-border transfer from the EEA to Country Q utilizes the SCC Module 1 designed for transfers from a controller to a non-EEA controller (First SCC).
- Transfer 2: SCC Module 2. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions must also utilize the SCCs (appropriate module). As a result, Company B's transfer of data to Company Z should utilize SCCs. Because Company B is a controller and Company Z is a processor, the parties should utilize SCC Module 2 (Second SCC).
- Subsequent Onward Transfers from Company Z. Note that if Company Z makes any additional onward transfers to sub-processors Company Z should utilize Module 3 of the SCCs. If Company Z were to transfer the data back to Company B, Company Z should utilize Module 4 of the SCCs.
- Country Q Transfer Impact Assessment. Clause 14 of the First SCC requires Company A and Company B to document whether either party has reason to believe that the laws and practices of Country Q prevent Company B from fulfilling its obligations under the SCCs.
- Country R Transfer Impact Assessment. Clause 14 of the Second SCC requires Company B and Company Z to conduct a transfer impact assessment to document whether either party has reason to believe that the laws and practices of Country R prevent Company Z from fulfilling its obligations under the SCCs. Note that as a practical matter this TIA might be shared with Company A upon request, or during an audit.
- Law Enforcement Request Policy. Clause 15 of the First SCC and the Second SCC require that Company B and Company Z take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company B and Company Z might consider creating written law enforcement request policies.

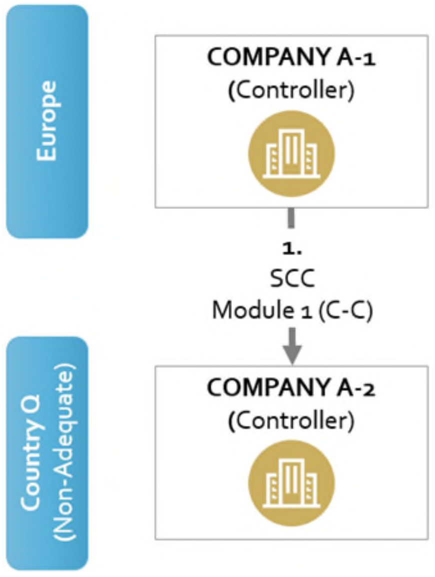
4.7 Controller A (EEA) → Branch Office Controller A (Non-EEA)

Visual	Description and Implications
 Europe COMPANY A (Controller) 1. No Mechanism Needed Per EDPB Country Q (Non-Adequate) COMPANY A (Branch Office)	- Background. Company A is a European entity that has a branch office (which is not a separate legal entity) in Country Q. Data is being directly sent from Company A in the EEA to the branch office. - Transfer 1. The EDPB has suggested that Company A's branch office is not considered a controller or a processor (separate and apart from Company A itself) and, as a result, no cross-border transfer mechanism is needed (as data has not been transferred from a controller/processor to a different controller/processor in a non-adequate country).[42] Under that reasoning no SCCs may be needed. - Transfer Impact Assessment. A formal transfer impact assessment is not required by contract if a SCC has not been signed. Nonetheless, the EDPB has suggested that a controller is "accountable for [its] processing activities" which includes assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[43] As a result, Company A might consider conducting a TIA to analyze the various risks that may result from the transmission of data to a branch office in Country Q. - Law enforcement request policy. If no SCCs are signed, Company A would not be directly subject to Clause 15 of the SCCs that requires specific steps in the event that a company receives a request from a public authority for access to personal data. Nonetheless, the EDPB has suggested that controllers are "accountable for [their] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[44] As a result, Company A might consider creating a law enforcement request policy to mitigate risks surrounding law enforcement requests from Country Q.

4.8 Branch Office Controller A (EEA) → Controller A (Non-EEA)

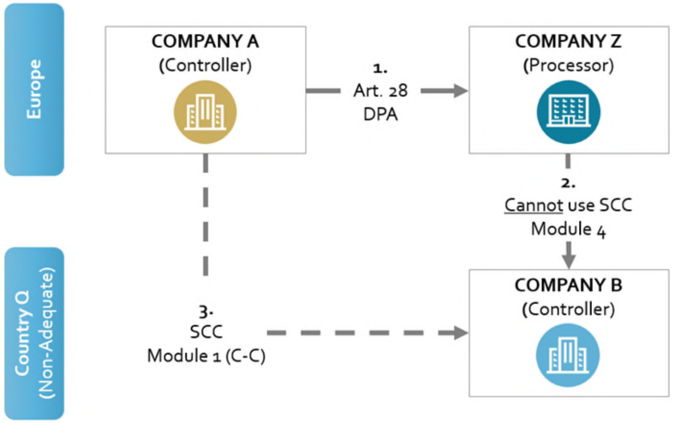
Visual	Description and Implications
 Europe COMPANY A (Branch Office) 1. Arguably No Mechanism Needed Per EDPB Country Q (Non-Adequate) COMPANY A (Controller)	• Background. Company A is headquartered in Country Q but has a branch office (not a separate legal entity) that is located in the EEA. Data is being sent from Company A's branch office to Company A. • Transfer 1. Note that this transfer scenario has not been specifically addressed by European supervisory authorities. It is possible that the supervisory authorities would suggest the use of SCC Module 1 in order to ensure that the personal data collected by Company A's branch office continues to receive the protections of the GDPR when it is transferred to Country Q. That said, the EDPB has suggested that Company A's branch office is not considered a separate controller or processor (separate and apart from Company A itself) and, as a result, no cross-border transfer mechanism might be needed as data has not been transferred from a controller/processor to a different controller/processor in a non-adequate country.[45] Under that reasoning no SCC may be needed. Furthermore, agreeing to SCCs might be counter-factual in the sense that it implies the existence of two separate controllers with different purposes for collecting personal data. • Transfer Impact Assessment. A formal transfer impact assessment may not be required by contract if the parties did not enter into a SCC. Nonetheless, the EDPB has suggested that a controller is "accountable for [its] processing activities" which includes assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[46] As a result, Company A might consider conducting a TIA to analyze various risks that may result from the transmission of data from the branch office in Europe to Company A in Country Q. • Law enforcement request policy. If no SCCs are signed, Company A would not be directly subject to Clause 15 of the SCCs that requires specific steps in the event that a company receives a request from a public authority for access to personal data. Nonetheless, the EDPB has suggested that controllers are "accountable for [their] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[47] As a result, Company A might consider creating a law enforcement request policy to mitigate risks surrounding law enforcement requests from Country Q.

4.9 Controller A-1 (EEA) → Controller A-2 (Non-EEA)

Visual	Description and Implications
 Europe COMPANY A-1 (Controller) 1. SCC Module 1 (C-C) COMPANY A-2 (Controller) Country Q (Non-Adequate)	• Background. Company A-1 and Company A-2 are corporate affiliates that are under common ownership or control, but are separate legal entities. Company A-1 in the EEA transfers personal data to Company A-2 in Country Q. • Transfer 1: SCC Module 1. A cross-border transfer from Company A-1 in the EEA to Company A-2 in Country Q should utilize the SCC Module 1 which is designed for transfers from an EEA controller to a non-EEA controller. • Subsequent Onward Transfers from Company A-2. Note that if Company A-2 makes any additional onward transfers, the appropriate module of the SCCs would need to be used. • Transfer Impact Assessments. Clause 14 of the SCCs requires both parties (Company A-1 and Company A-2) to document whether either has reason to believe that the laws and practices of Country Q prevent the data importer (i.e., Company A-2) from fulfilling its obligations under the SCCs. • Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company A-2) to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company A-2 might consider creating a law enforcement request policy.

4.10 Controller A (EEA) → Processor Z (EEA) → Controller B (Non-EEA)

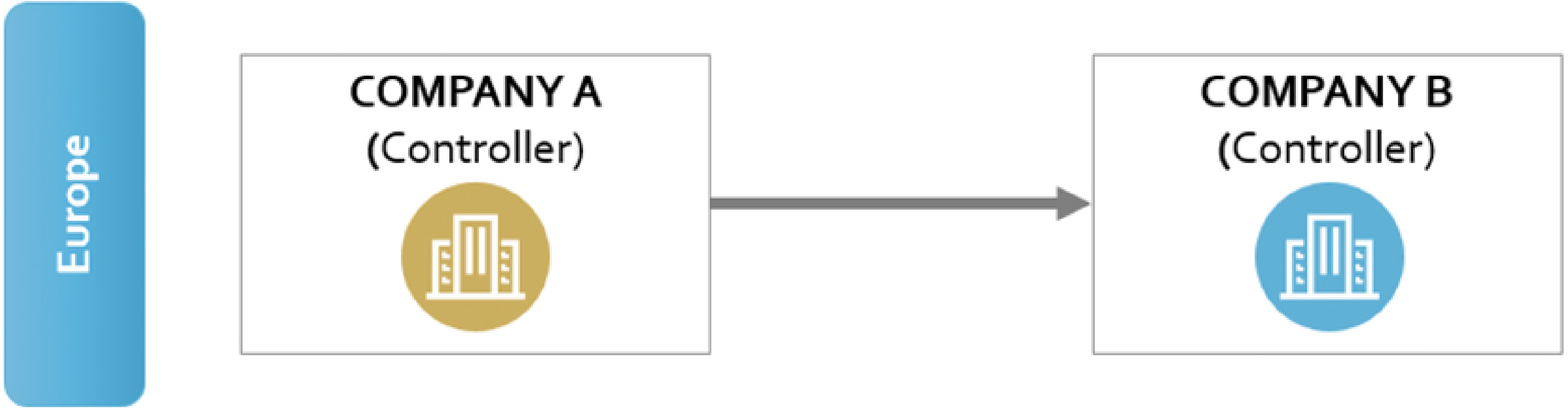
Visual



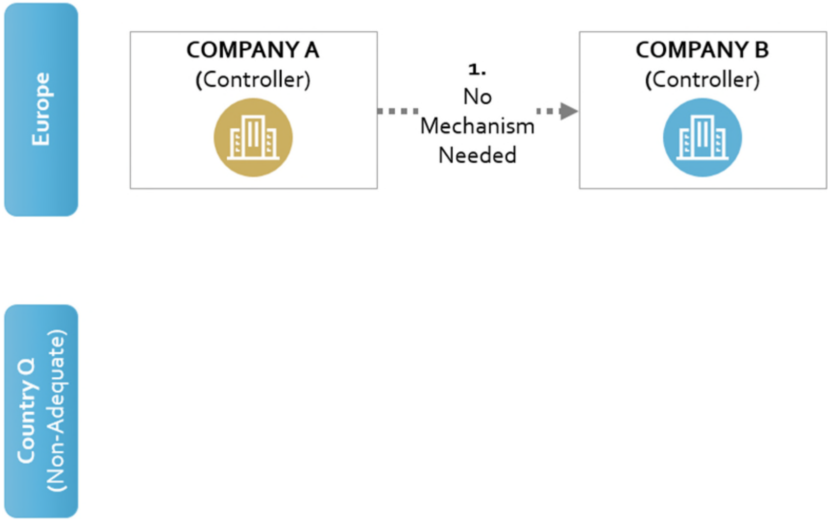
Description and Implications

- Background. Company A transmits personal data to its processor Company Z, and then instructs its processor to onward transfer the personal data to Company B – a separate controller.
- Transfer 1: Art. 28 DPA. As personal data has not left the EEA, an adequacy measure is not required. The parties should enter into an agreement that complies with Article 28 of the GDPR as Company Z is acting as a processor to Company A.
- Transfer 2: No mechanism available. Although the SCC Module 4 is designed for transfers from processors to controllers, it cannot be used in this situation as Clause 8.1(a) of that SCCs states that the data exporter (Company Z) must be acting on the instructions of the data importer (Company B). In this scenario, the data exporter is acting on the instructions of Company A (which is not the data importer). As a result, Company Z could not utilize the SCC Module 4.
- Transfer 3: SCC Module 1. Although the data is being triangulated through Company Z, the only available contractual mechanism is for Company A to enter into a SCC Module 1 with Company B. Note that the SCC Module 1 might contain within its Annex 2 a description and explanation of its use of Company Z as a processor.
- Transfer Impact Assessments. Clause 14 of the SCCs requires Company A and Company B to document whether either party has reason to believe that the laws and practices of Country Q prevent the data importer (i.e., Company B) from fulfilling its obligations under the SCCs.
- Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company B) to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company B might consider creating a law enforcement request policy.

5. Transfers from EEA Controllers to EEA Controllers

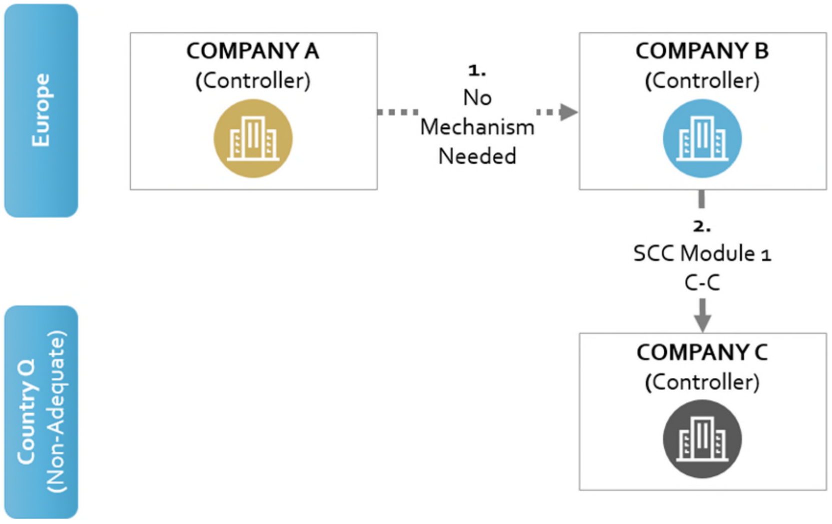


5.1 Controller A (EEA) → Controller B (EEA)

Visual	Description and Implications
 Europe COMPANY A (Controller) 1. No Mechanism Needed COMPANY B (Controller) Country Q (Non-Adequate)	- Background. Company A in the EEA transfers personal data to Company B in the EEA. - Transfer 1: No Mechanism Needed. The GDPR does not require a safeguard mechanism for data that is transferred from a controller in the EEA to another controller in the EEA.

5.2 Controller A (EEA) → Controller B (EEA) → Controller C (Non-EEA)

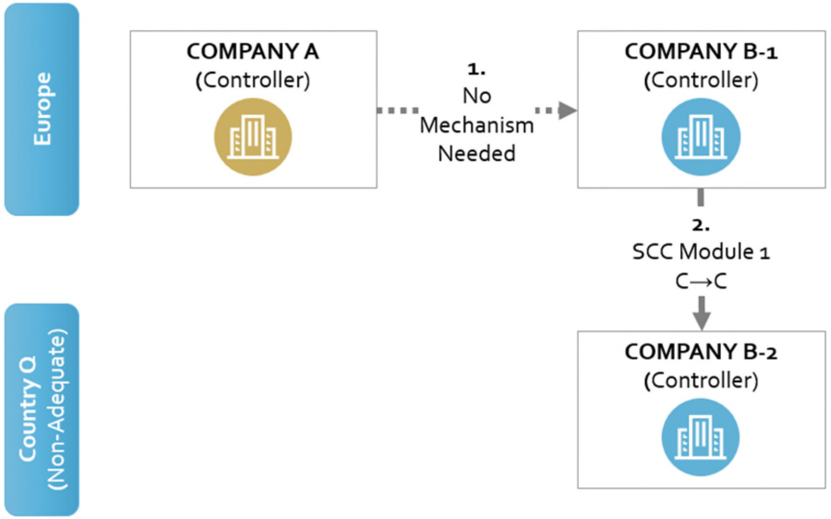
Visual



Description and Implications

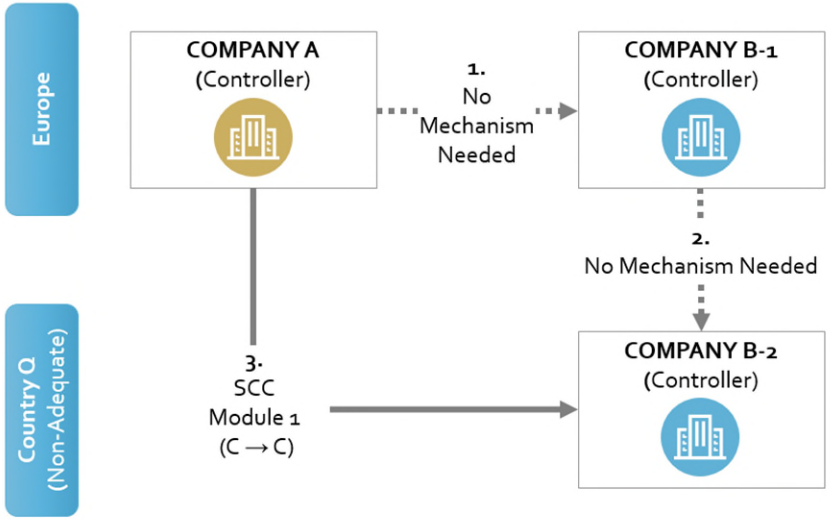
- Background. Company A in the EEA transfers personal data to Company B in the EEA. Company B then transfers the personal data to Company C in Country Q.
- Transfer 1: No Mechanism Needed. The GDPR does not require a safeguard mechanism for data that is transferred from a controller in the EEA to another controller in the EEA.
- Transfer 2: SCC Module 1. A cross-border transfer from Company B in the EEA to Company C in Country Q should utilize the SCC Module 1 which is designed for transfers from an EEA controller to a non-EEA controller.
- Subsequent Onward Transfers from Company C. Note that if Company C makes any additional onward transfers, the appropriate module of the SCCs would need to be used.
- Transfer Impact Assessments. Clause 14 of the SCCs requires Company B and Company C to document whether either party has reason to believe that the laws and practices of Country Q prevent the data importer (i.e., Company C) from fulfilling its obligations under the SCCs.
- Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company C) to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company C might consider creating a law enforcement request policy.

5.3 Controller A (EEA) → Controller B-1 (EEA) → Controller B-2 (Non-EEA)

Visual	Description and Implications
 Europe Country Q (Non-Adequate) COMPANY A (Controller) 1. No Mechanism Needed COMPANY B-1 (Controller) 2. SCC Module 1 C→C COMPANY B-2 (Controller)	● Background. Company B-1 and Company B-2 are corporate affiliates that are under common ownership or control, but are separate legal entities. Company A in the EEA transfers personal data to Company B-1 in the EEA. Company B-1 then transfers the personal data to Company B-2 in Country Q. ● Transfer 1: No mechanism needed. The GDPR does not require a safeguard mechanism for data that is transferred from a controller in the EEA to another controller in the EEA. ● Transfer 2: SCC Module 1. Although Company B-1 and Company B-2 may be under common ownership or control, as separate legal entities they are required to put into place a safeguard when transferring data from the EEA to a non-adequate jurisdiction.[48] ● Transfer Impact Assessments. Clause 14 of the SCCs requires that Company B-1 and Company B-2 document whether either party has reason to believe that the laws and practices of Country Q would prevent Company B-2 from fulfilling its obligations under the SCCs. ● Law Enforcement Request Policy. Clause 15 of the SCCs requires Company B-2 to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company B-2 might consider creating a law enforcement request policy.

5.4 Controller A (EEA) → Controller B-1 (EEA) → Controller B-2 (Non-EEA) (data directly sent from original to final controller)

Visual



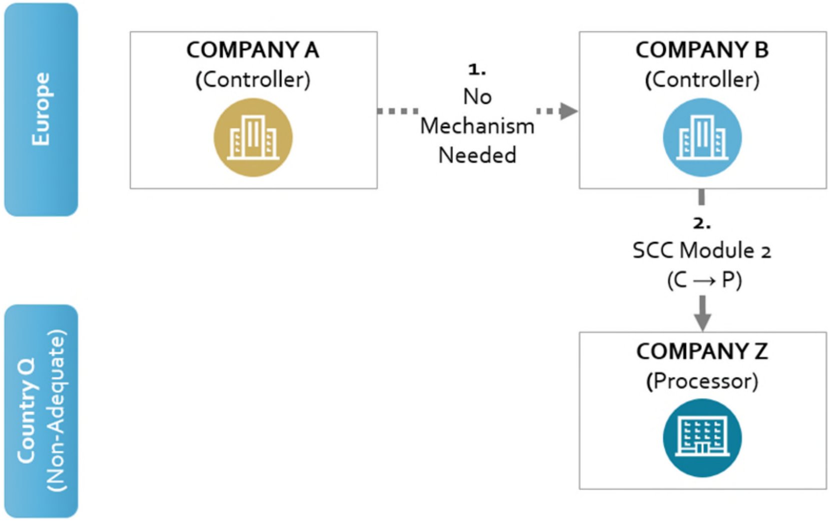
Description and Implications

- Background. Company B-1 and Company B-2 are corporate affiliates that are under common ownership or control, but are separate legal entities. While data is directly sent from Controller A in the EEA to Controller B-2 in Country Q, Controller A has contracted only with Controller B-1 in the EEA. The solid line indicates the data flow; the dashed line indicates the contractual relationship.
- Transfer 1: No Mechanism Needed. The GDPR does not require a safeguard mechanism for data that is transferred from a controller in the EEA to another controller in the EEA. In the visual depiction while data is not being physically transferred from Company A to Company B-1, Company B-1 might be classified as a "controller" to the extent that it helps determine the purpose and means of processing of the data while it is in the possession of Company B-2. Because Company B-1 is considered the controller of the data, a cross-border transfer mechanism is not needed between Company A and Company B-1, as both companies are controllers located in the EEA.
- Transfer 2: No Mechanism Needed. Although Company B-1 and Company B-2 may be under common ownership or control, as separate legal entities they are required to put into place a safeguard when transferring data from the EEA to a non-adequate jurisdiction.[49] In this case, because no physical data is being transferred from Company B-1 to Company B-2, an argument could be made that a cross-border transfer mechanism might not be needed between the two entities.
- Transfer 3: SCC Module 1. The GDPR requires that "any transfer of personal data" has an adequate safeguard.[50] As data is being physically transmitted by Company A to Company B-2, an argument could be made that a SCC Module

Visual	Description and Implications
	1 should be in place between those two entities, even if Company A transmitted the data pursuant to a separate contract with Company B-1. • Transfer Impact Assessments. Clause 14 of the SCCs requires that Company A and Company B-2 document whether either party has reason to believe that the laws and practices of Country Q would prevent Company B-2 from fulfilling its obligations under the SCCs. • Law Enforcement Request Policy. Clause 15 of the SCCs requires Company B-2 to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company B-2 might consider creating a law enforcement request policy.

5.5 Controller A (EEA) → Controller B (EEA) → Processor Z (Non-EEA)

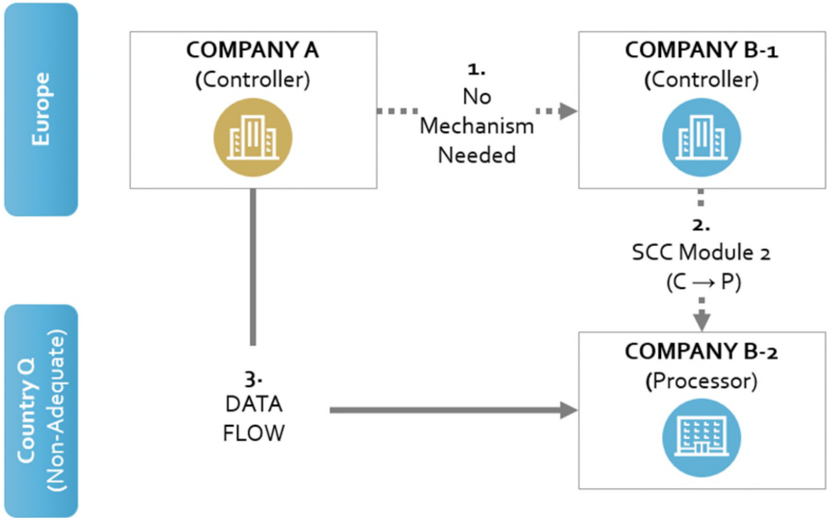
Visual	Description and Implications



- Background. Company A in the EEA transfers personal data to Company B in the EEA. Company B then transfers the personal data to its processor, Company Z, in Country Q.
- Transfer 1. No mechanism needed. The GDPR does not require a safeguard mechanism for data that is transferred from a controller in the EEA to another controller in the EEA.
- Transfer 2. SCC Module 2. The transfer from Company B to Company Z should utilize the SCC Module 2 designed for transfers from controllers in the EEA to processors that are located outside of the EEA.
- Transfer Impact Assessments. Clause 14 of the SCCs requires that Company B and Company Z create a transfer impact assessment about the laws of Country Q to determine if they prevent Company Z from fulfilling its obligations under the SCCs.
- Law enforcement request policy. Clause 15 of the SCCs requires Company Z to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company Z might consider creating a law enforcement request policy for handling requests from public authorities.

5.6 Controller A (EEA) → Controller B-1 (EEA) → Processor B-2 (Non-EEA) (data directly sent to processor)

Visual



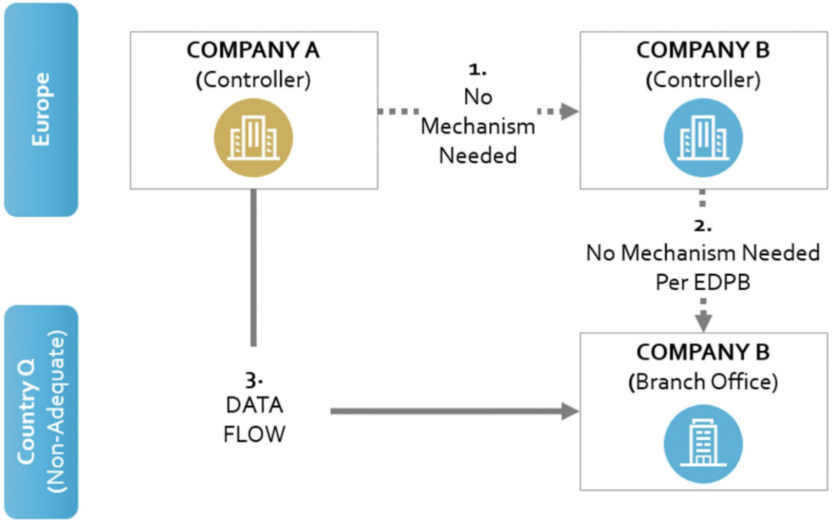
Description and Implications

- <u>Background</u>. Company B-1 and Company B-2 are corporate affiliates that are under common ownership or control, but are separate legal entities. Company B-2 is the processor of Company B-1. While data is being directly sent from Company A in the EEA to Company B-2, Company B-2 is not acting as the processor of Company A; instead Company B-1 is utilizing Company B-2 as its processor and has directed Company A to directly transmit information to Company B-2. The solid line indicates the data flow; the dashed line indicates the contractual relationships.
- <u>Transfer 1. No Mechanism Needed</u>. The GDPR does not require a safeguard mechanism for data that is transferred from a controller in the EEA to another controller in the EEA. In the visual depiction while data is not being physically transferred from Company A to Company B-1, Company B-1 is classified as a "controller" of such personal data because it determines the purpose and means of processing of the data while the data is in the possession of Company B-2.
- <u>Transfer 2. SCC Module 2</u>. Although Company B-1 and Company B-2 may be under common ownership or control, as separate legal entities they are required to put into place a safeguard when transferring data from the EEA to Country Q.[51] While data has not physically been sent from Company B-1 to Company B-2, it has been sent at the direction of Company B-1. As a result, the parties should utilize SCC Module 2. The appendix to that SCC might provide information regarding how the data will be transferred to Company B-2, including the method by which the transmission will take place.
- <u>Transfer 3 (actual data flow)</u>. A separate SCC is not needed (and may be inappropriate) between Company A and Company B-2. While the GDPR requires that "any transfer of personal data" has an adequate safeguard, in this situation the transfer of data from Company A to Company B-2 is

Visual	Description and Implications
	arguably being done at the direction and under the control of Company B-1.[52] Furthermore, if Company B-2 is not functioning as the processor of Company A (i.e., it is not taking instructions from Company A) the use of a SCC Module 2 would be inappropriate as it would incorrectly classify Company B-2 as Company A's processor, and would assign to Company B-2 processor-oriented obligations that Company B-2 cannot fulfil. ● Transfer Impact Assessments. Clause 14 of the SCCs requires that Company B-1 and Company B-2 document their analysis as to whether the laws of Country Q prevent Company B-2 from fulfilling its obligations under the SCCs. ● Law enforcement request policy. Clause 15 of the SCCs requires Company B-2 to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company B-2 might consider creating a law enforcement request policy for handling requests from public authorities.

5.7 Controller A (EEA) → Controller B (EEA) → Branch Office Controller B (Non-EEA)

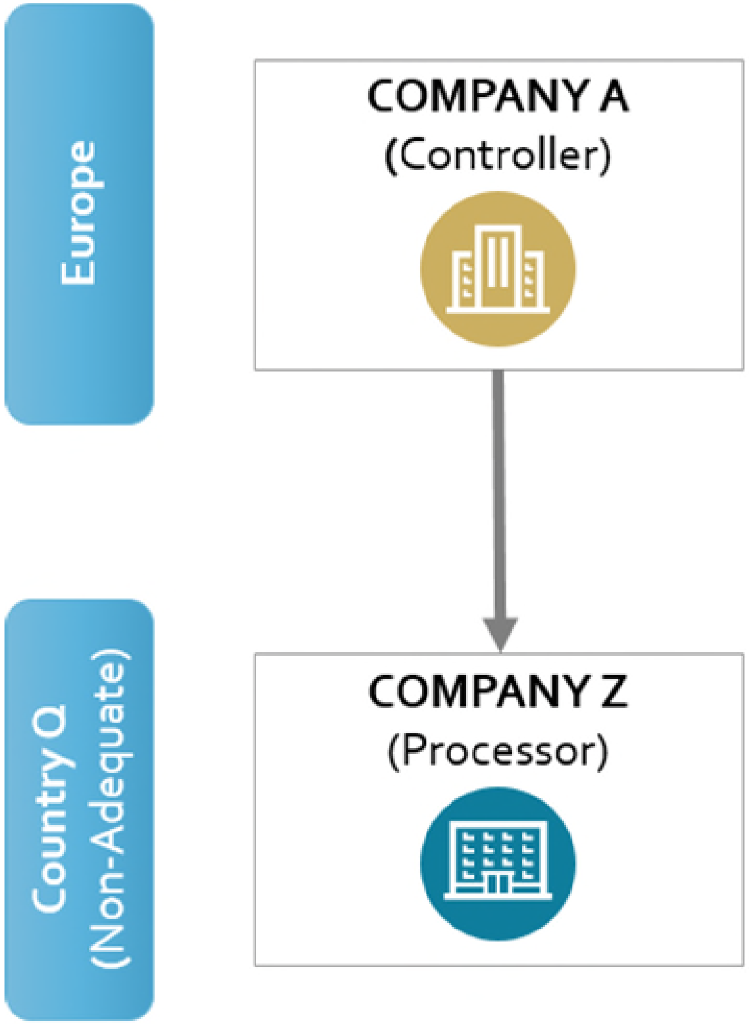
Visual	Description and Implications



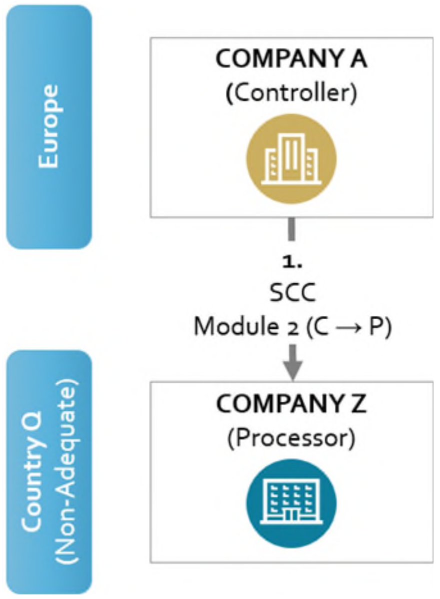
- Background. Company B is a European entity that has a branch office (which is not a separate legal entity) in Country Q. While data is being directly sent from Company A in Europe to Company B's branch office in Country Q, the contract is between Company A and Company B. The EDPB has suggested that Company B's branch office is not considered a controller or a processor (separate and apart from Company B itself).[53] Note, however, that the EDPB has not directly addressed a situation in which an entity sends personal information to an unincorporated office outside of the EEA. The solid line indicates the data flow; the dashed line indicates the contractual relationships.
- Transfer 1 and 3. The EDPB has not directly addressed this situation, as a result there are two possible interpretations of how to approach compliance.
  - Option 1. While data is being directly transmitted from Company A to Company B's branch office in Country Q, based upon the EDPB's guidance discussed above, an argument could be made that the branch office is not considered a separate controller or processor as compared to Company B in the EEA. As a result, the data has not been transmitted to a controller that is located in Country Q. Note that Company B (including Company B's branch office) would be directly subject to the GDPR and thus the data received should be subject to all GDPR requirements even in the absence of a SCC.
  - Option 2. An argument could also be made that because data is being transmitted from one controller (Controller A) to a second controller's agents who are physically located outside of the EEA, the parties could enter into the SCC Module 1 wherein Company B would sign as the "data importer" listing Country Q as a country in which processing will occur.
- Transfer 2. The EDPB has suggested that Company B's branch office is not considered a controller or a processor (separate and apart from Company B itself), and, as a result, a cross border data transfer from one

Visual	Description and Implications
	controller/processor is not occurring to another controller/processor.[54] As a result, no SCC may be needed. ● Transfer Impact Assessments. A formal transfer impact assessment is not required by contract if neither Company A nor Company B sign SCCs (i.e., if the parties follow option 1). Nonetheless, the EDPB has suggested that controllers (Company A and Company B) are "accountable for [their] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[55] As a result, Company A and/or Company B might consider conducting a TIA to analyze various risks that may result from the transmission of data (with respect to Company A) and/or the retention of data in a third country (with respect to Company B). If the parties follow option 2 and enter into the SCC Module 1, Clause 14 of the SCCs would require that Company A and Company B document a transfer impact assessment of the laws of Country Q to determine if they prevent Company B from fulfilling its obligations under the SCCs. ● Law enforcement request policy. If SCCs are signed (option 2), Clause 15 of the SCCs would require Company B to take specific steps in the event that it receives a request from a public authority for access to personal data. If no SCCs are signed (option 1), neither Company A nor Company B would be directly subject to Clause 15 of the SCCs. Nonetheless, the EDPB has suggested that controllers (Company A and Company B) are "accountable for [their] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[56] As a result, under both option 1 and under option 2 Company B might consider creating a law enforcement request policy to mitigate risks surrounding law enforcement requests from Country Q.

6. Transfers from EEA Controllers to Non-EEA Processors

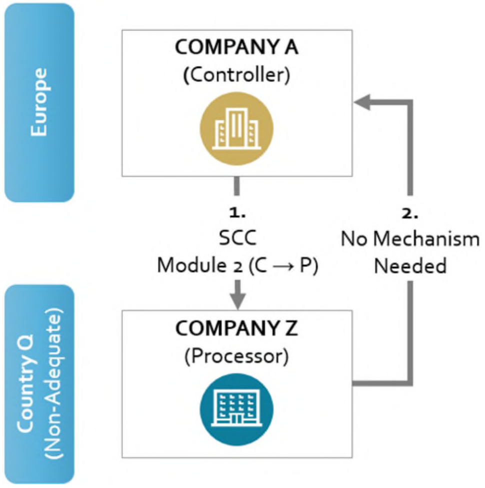


6.1 Controller A (EEA)→ Processor Z (Non-EEA)

Visual	Description and Implications
 Europe COMPANY A (Controller) 1. SCC Module 2 (C → P) COMPANY Z (Processor) Country Q (Non-Adequate)	• Background. Company A transmits personal data to a processor (Company Z) that is located in a country that has not been granted an adequacy decision by the European Commission. • Transfer 1: SCC Module 2. The cross-border transfer of personal data from the EEA to Country Q should utilize the SCC Module 2 designed for transfers from a controller to a non-EEA processor. • Transfer Impact Assessments. Clause 14 of the SCCs requires both parties (Company A and Company Z) to determine whether either party has reason to believe that the laws and practices of Country Q prevent Company Z from fulfilling its obligations under the SCCs. • Law enforcement request policy. Clause 15 of the SCCs requires the data importer (Company Z) to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company Z might consider creating a written law enforcement request policy.

6.2 Controller A (EEA)→ Processor Z (Non-EEA) → Controller A (EEA) (Renvoi)

Visual

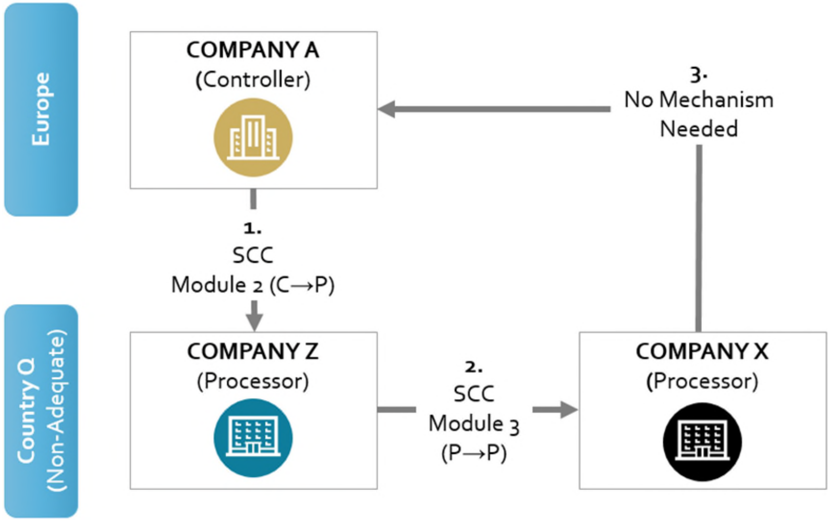


Description and Implications

- Background. Company A transmits personal data to a processor (Company Z) that is located in a country that has not been granted an adequacy decision by the European Commission. After processing the personal data Company Z returns it (Renvoi) to the original controller.
- Transfer 1: SCC Module 2. The initial cross-border transfer from the EEA to Country Q should utilize the SCC Module 2 designed for transfers from a controller to a non-EEA processor.
- Transfer 2: No Mechanism. The GDPR does not require a company that transmits data from a non-adequate country to the EEA to utilize a safeguard mechanism. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.
- Transfer Impact Assessments. Clause 14 of the SCCs requires all parties (Company A and Company Z) to document whether any has a reason to believe that the laws and practices of Country Q prevent Company Z from fulfilling its obligations under the SCCs.
- Law enforcement request policy. Clause 15 of the SCCs requires the data importer (Company Z) to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company Z might consider creating a written law enforcement request policy.

6.3 Controller A (EEA) → Processor Z (Non-EEA) → Processor X (Non-EEA) → Controller A (EEA) (Renvoi)

Visual



Description and Implications

- Background. Company A transmits personal data to a processor (Company Z) that is located in a country that has not been granted an adequacy decision by the European Commission. Company Z, in turn, onward transfers the personal data to another processor (Company X) also located in Country Q. After processing the personal data Company X returns it (Renvoi) to the original controller.
- Transfer 1: SCC Module 2. The initial cross-border transfer from the EEA to Country Q should utilize the SCC Module 2 designed for transfers from a controller to a non-EEA processor (First SCC).
- Transfer 2: SCC Module 3. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions must also utilize the SCCs. The SCCs further specify that transfers to another company "in the same [non-EEA] country," should also utilize a safeguard mechanism such as the SCCs".[57] Company Z and Company X should utilize the SCC Module 3 designed for transfers from a processor to a non-EEA processor (Second SCC).
  - Note that the parties could alternatively decide to enter into a single SCC between Company A, Company Z, and Company X that integrates a Module 2 SCC (as to Company A and Company Z) and a Module 2 SCC (as to Company A and X).
  - Note that Clause 9 of the First SCC would require Company Z to obtain authorization from Company A to utilize Company X.
- Transfer 3: No Mechanism. The GDPR does not require a company that transmits data from a non-adequate country to the EEA to utilize a safeguard mechanism. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.

Visual	Description and Implications
	● Transfer Impact Assessments. Clause 14 of the SCCs requires all parties (Company A, Company Z, and Company X) to document whether any party has reason to believe that the laws and practices of Country Q prevent Company Z and/or Company X from fulfilling their obligations under the SCCs. ● Law enforcement request policy. Clause 15 of the SCCs requires the data importers (Company Z and Company X) to take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company Z and Company X might consider creating a written law enforcement request policy.

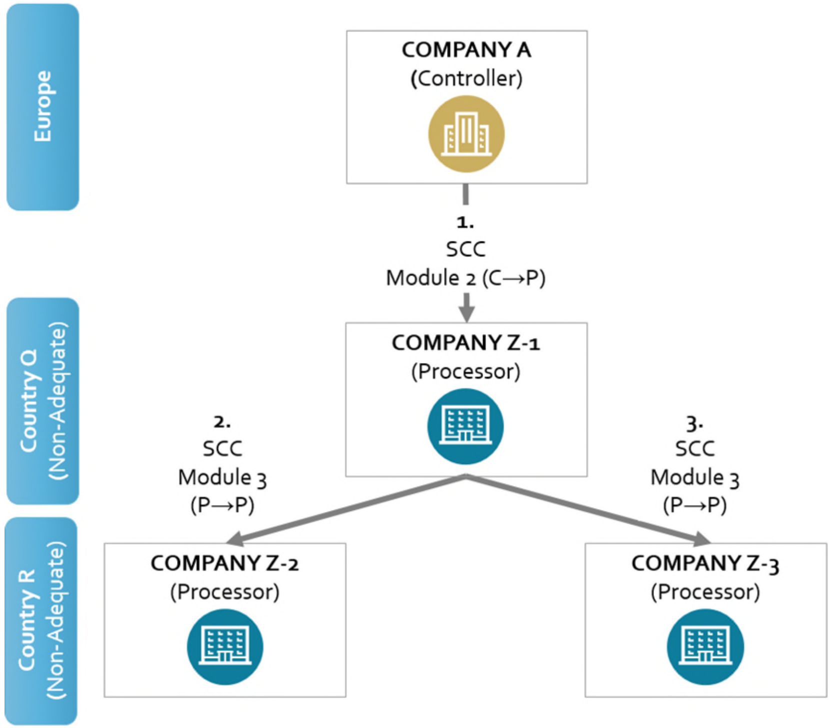
6.4 Controller A (EEA)→ Processor Z-1 (Non-EEA), Processor Z-2 (Non-EEA), Processor Z-3 (Non-EEA).

Background. Company A in the EEA retains Company Z-1 in Country Q to process personal data. Country Q has not been granted an adequacy decision by the European Commision. Company Z-1 intends to transmit the personal data to corporate affiliates in other countries throughout the world that have also not been granted adequacy decisions by the European Commission (i.e., Company Z-2 and Company Z-3 in Country R). There are two general strategies for how the transfer could be structure.

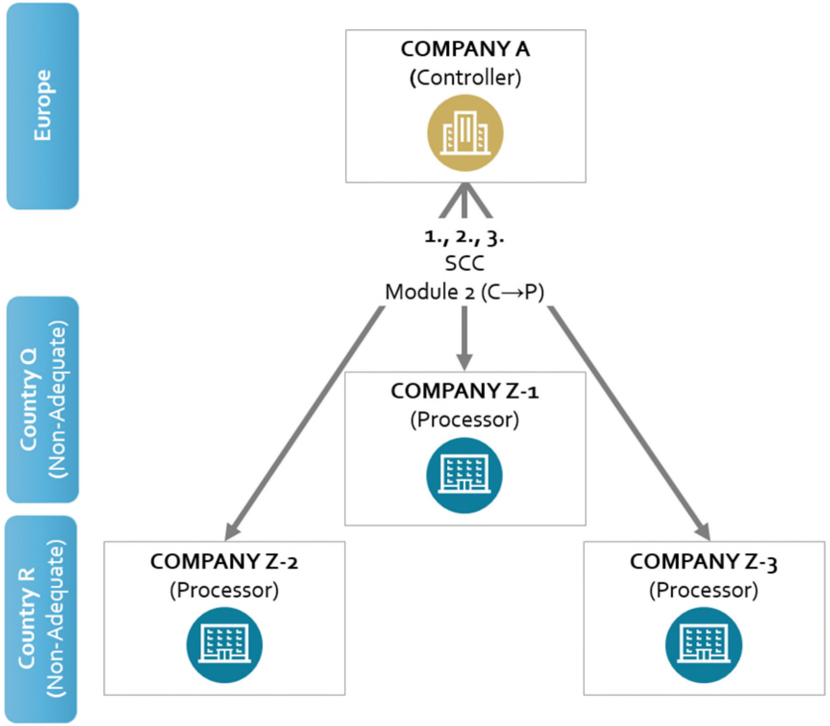
Visual

Description and Implications

Option 1

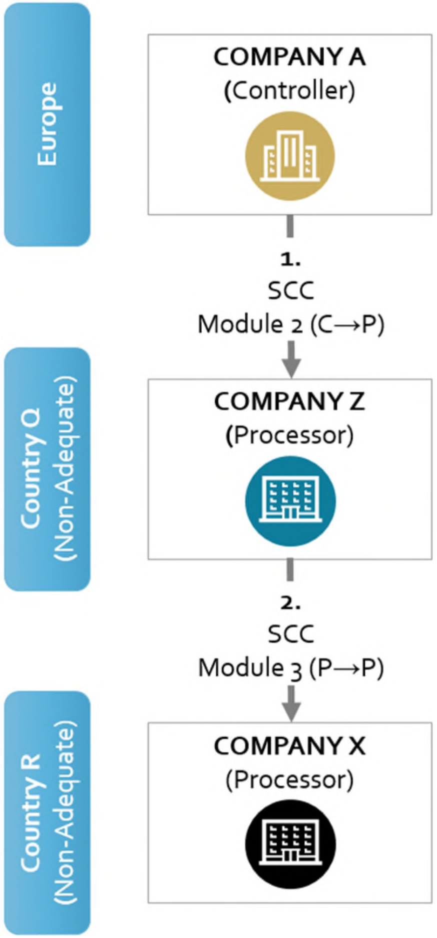


- Transfer 1: SCC Module 2. The initial cross-border transfer from the EEA to Country Q could utilize the SCC Module 2 designed for transfers from a controller to a non-EEA processor (First SCC).
- Transfers 2 and 3: SCC Module 3. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions should also utilize the SCCs (appropriate module). While these could take the form of two separate documents, they might also take the form of a single intragroup agreement that incorporates the SCC Module 3 (Second SCCs).
- Country Q Transfer Impact Assessment. Clause 14 of the First SCC requires Company A and Company Z-1 to document whether either party has reason to believe that the laws and practices of Country Q prevent Company Z-1 from fulfilling its obligations under the SCCs.
- Country R Transfer Impact Assessment. Clause 14 of the Second SCCs requires Companies Z-1, Z-2, and Z-3 to create a transfer impact assessment of the laws in which Companies Z-2 and Z-3 operate (e.g., Country R). It is unclear whether Company A must participate in this process, or should conduct its own transfer impact assessment (with the participation of Company Z-1) that assesses any impact of transfers to Country R.
- Law enforcement request policy. Clause 15 of the SCCs requires the data importers (Companies Z-1, Z-2, and Z-3) to take specific steps in the event

Visual	Description and Implications
	that they receive a request from a public authority for access to personal data. As a result, Company Z-1, Z-2, and Z-3 might consider creating a written law enforcement request policy.
Option 2	
 Europe COMPANY A (Controller) 1., 2., 3. SCC Module 2 (C→P) Country Q (Non-Adequate) COMPANY Z-1 (Processor) Country R (Non-Adequate) COMPANY Z-2 (Processor) COMPANY Z-3 (Processor)	• Transfers 1, 2, and 3: SCC Module 2. The parties could enter into a single SCC Module 2 designed for transfers from a controller to a non-EEA processor, which would list Company Z-1, Company Z-2, and Company Z-3 each as separate data importers (First SCC) • Transfer Impact Assessments. Clause 14 of the First SCC would require Company A to document a transfer impact assessment with each of the data importers (Company Z-1, Z-2, and Z-3) with regard to their respective countries to determine whether Company A, or whether each of the respective importers, has a reason to believe that the laws of their respective jurisdictions (i.e., Country Q and Country R) would prevent them from fulfilling their obligations under the First SCC. • Law enforcement request policy. Clause 15 of the First SCC requires the data importers (Companies Z-1, Z-2, and Z-3) to take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company Z-1, Z-2, and Z-3 might consider creating a written law enforcement request policy.

6.5 Controller A (EEA)→ Processor Z (Non-EEA) → Processor X (Non-EEA) (different countries)

Visual


Europe

COMPANY A
(Controller)

1.
SCC
Module 2 (C→P)

Country Q
(Non-Adequate)

COMPANY Z
(Processor)

2.
SCC
Module 3 (P→P)

Country R
(Non-Adequate)

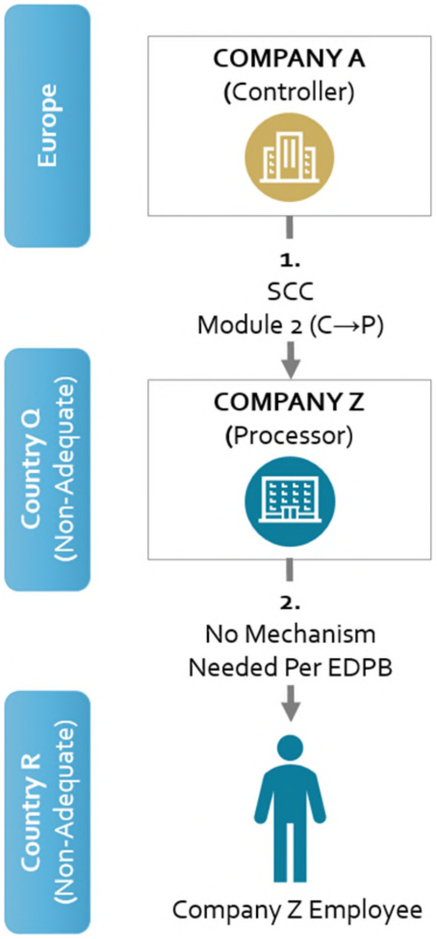
COMPANY X
(Processor)

Description and Implications

- Background. Company A transmits personal data to a processor (Company Z) that is located in Country Q. Country Q has not been granted an adequacy decision by the European Commission. Company Z, in turn, onward transfers the personal data to another processor (Company X) located in Country R. Country R also has not been granted an adequacy decision by the European Commission.
- Transfer 1: SCC Module 2. The cross-border transfer of personal data from the EEA to Country Q should utilize the SCC Module 2 designed for transfers from a controller to a non-EEA processor (First SCC).
- Transfer 2: SCC Module 3. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions must also utilize the SCCs. Company Z and Company X should utilize the SCC Module 3 designed for transfers from a processor to a non-EEA processor (Second SCC).
  - Note that the parties could alternatively decide to enter into a single SCC between Company A, Company Z, and Company X that integrates a Module 2 SCC (as to Company A and Company Z) and a Module 2 SCC (as to Company A and X).
  - Note that Clause 9 of the First SCC would require Company Z to obtain authorization from Company A to utilize Company X.
- Transfer Impact Assessments. Clause 14 of the SCCs requires all parties (Company A, Company Z, and Company X) to document whether any party has reason to believe that the laws and practices of Country Q or Country R prevent Company Z and/or Company X from fulfilling their obligations under the SCCs.
- Law enforcement request policy. Clause 15 of the SCCs requires the data importers (Company Z and Company X) to take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company Z and Company X might consider creating a written law enforcement request policy.

6.6 Controller A (EEA) → Processor Z (Non-EEA) → Employee of Processor Z (Non-EEA) (remote worker) (different country)

Visual

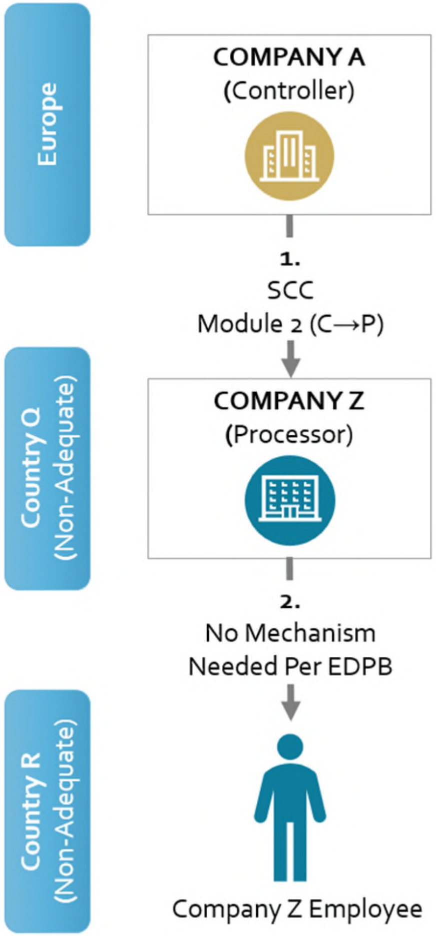


Description and Implications

- Background. Company A is an EEA controller that utilizes Company Z, which is a processor that is based in Country Q. Company Z does not have a legal presence in Country R, but does have an employee that works remotely from Country R (e.g., a remote worker). Neither Country Q, nor Country R, have been granted adequacy decisions by the European Commission.
- Transfer 1: SCC Module 2. The cross-border transfer of personal data from the EEA to Country Q should utilize the SCC Module 2 designed for transfers from a controller to a non-EEA processor.
- Transfer 2: No Mechanism Needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[58] While the EDPB provided, as an example, the use-case whereby an employee travels for work to India where he or she remotely accesses personal data from the EEA, this rationale presumably also applies to other remote-work situations such as where an employee resides in a non-EEA country, or where the remote employee downloads personal data (as opposed to remotely accessing such data). While the example provided by the EDPB involved a European company sending data to an employee outside of the EEA, the rationale utilized by the EDPB presumably applies where a company located in Country Q sends data to an employee located in Country R.
- Transfer Impact Assessments. Clause 14 of the SCCs requires both parties (Company A and Company Z) to document whether either party has reason to believe that the laws and practices of Country Q prevent Company Z from fulfilling its obligations under the SCCs. Clause 14 might also be interpreted as requiring that the companies consider any additional countries to which data might be transferred (e.g., Country R).
- Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company Z) to take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company Z might consider creating a written law enforcement request policy.

6.7 Controller A (EEA) → Processor Z (Non-EEA) → Employee of Processor Z (Non-EEA) (on vacation)

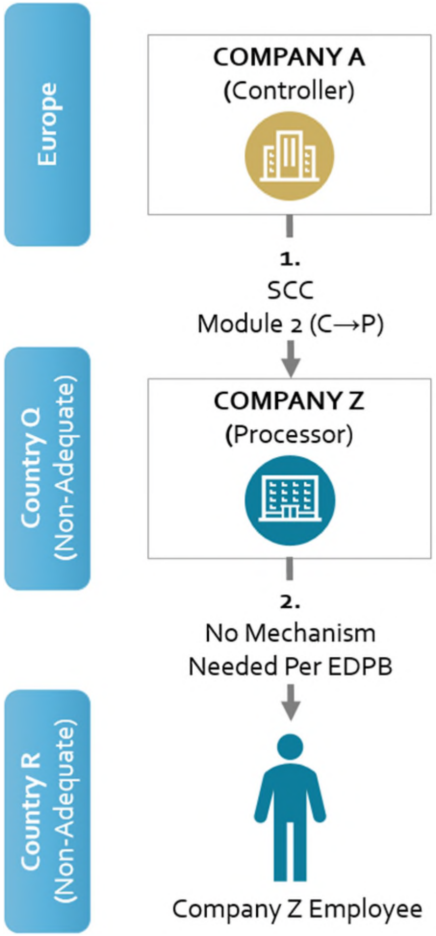
Visual



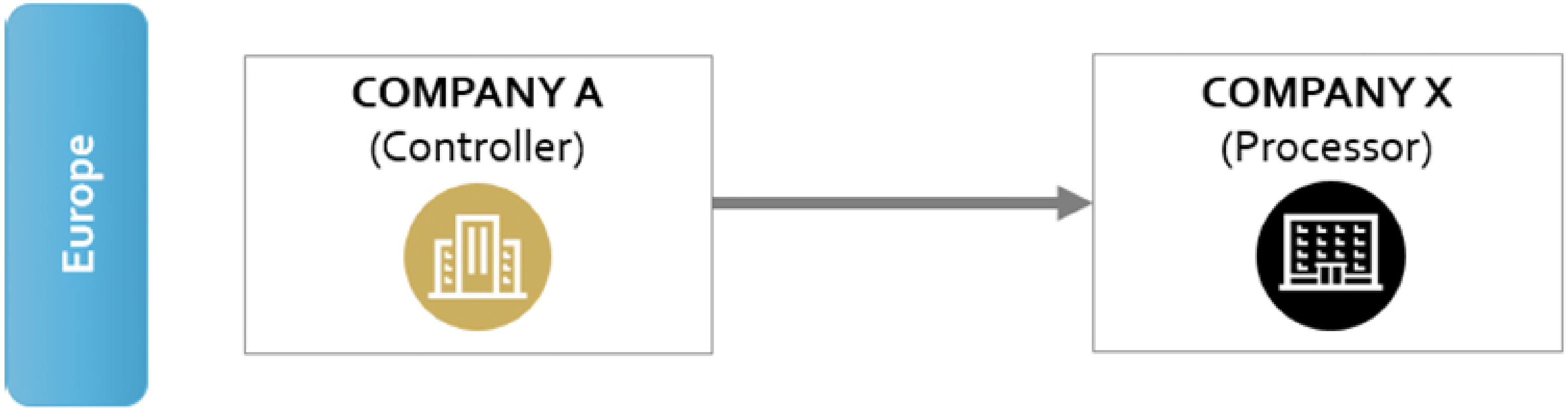
Description and Implications

- Background. Company A is an EEA controller that utilizes Company Z, which is a processor that is based in Country Q. Company Z does not have a legal presence in Country R, but does have an employee that is on a personal vacation in Country R and receives personal information while on vacation. Neither Country Q, nor Country R, have been granted adequacy decisions by the European Commission.
- Transfer 1: SCC Module 2. The cross-border transfer of personal data from the EEA to Country Q should utilize the SCC Module 2 designed for transfers from a controller to a non-EEA processor.
- Transfer 2: No Mechanism Needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[59] While the EDPB provided, as an example, the use-case whereby an employee travels for work to India where he or she remotely accesses personal data from the EEA, this rationale presumably also applies to other remote-work situations such as where an employee goes on a personal vacation in a non-EEA country, or where the remote employee downloads personal data (as opposed to remotely accessing such data). Although the example provided by the EDPB also involved a European company sending data to an employee outside of the EEA, the rationale utilized by the EDPB presumably applies where a company located in Country Q sends data to an employee located in Country R.
- Transfer Impact Assessments. Clause 14 of the SCCs requires both parties (Company A and Company Z) to document whether either party has reason to believe that the laws and practices of Country Q prevent Company Z from fulfilling its obligations under the SCCs. Clause 14 might also be interpreted as requiring that the companies consider any additional countries to which data might be transferred (e.g., Country R).
- Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company Z) to take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company Z might consider creating a written law enforcement request policy.

6.8 Controller A (EEA) → Processor Z (EEA) → Employee of Processor Z (Non-EEA) (on business trip)

Visual	Description and Implications
 Europe COMPANY A (Controller) 1. SCC Module 2 (C→P) Country Q (Non-Adequate) COMPANY Z (Processor) 2. No Mechanism Needed Per EDPB Country R (Non-Adequate) Company Z Employee	- Background. Company A is an EEA controller that utilizes Company Z, which is a processor that is based in Country Q. Company Z does not have a legal presence in Country R, but does have an employee that is on a business trip in Country R and receives personal information while on that trip. Neither Country Q, nor Country R, have been granted adequacy decisions by the European Commission. - Transfer 1: SCC Module 2. The cross-border transfer of personal data from the EEA to Country Q should utilize the SCC Module 2 designed for transfers from a controller to a non-EEA processor. - Transfer 2: No Mechanism Needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[60] The EDPB provided, as an example, the use-case whereby an employee travels for work to India where he or she remotely accesses personal data from the EEA. While the example provided by the EDPB involved a European company sending data to an employee outside of the EEA, the rationale utilized by the EDPB presumably applies where a company located in Country Q sends data to an employee located in Country R. - Transfer Impact Assessments. Clause 14 of the SCCs requires both parties (Company A and Company Z) to document whether either party has reason to believe that the laws and practices of Country Q prevent Company Z from fulfilling its obligations under the SCCs. Clause 14 might also be interpreted as requiring that the companies consider any additional countries to which data might be transferred (e.g., Country R). - Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company Z) to take specific steps in the event that they receive a request from a public authority for access to personal data. As a result, Company Z might consider creating a written law enforcement request policy.

7. Transfers from EEA Controllers to EEA Processors



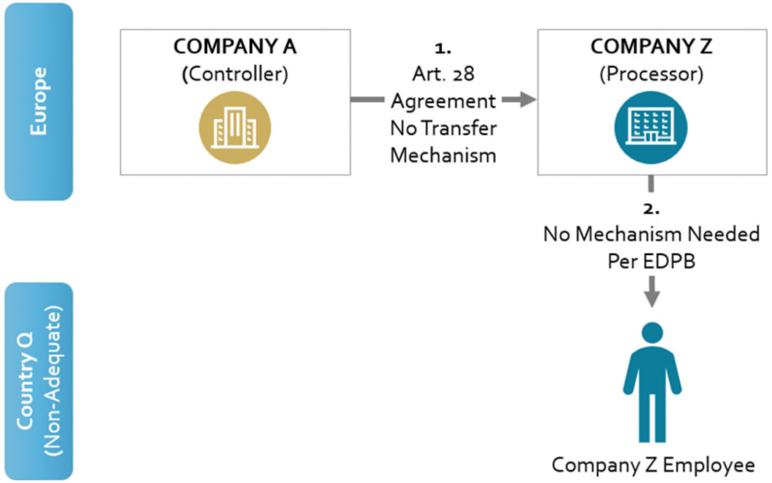
7.1 Controller A (EEA) → Processor Z (EEA) → Employee of Processor Z (Non-EEA) (remote worker)

Background. Company A is an EEA controller that utilizes Company Z, which is an EEA-based processor. Company Z does not have a legal presence in Country Q, but does have an employee that works remotely from Country Q (e.g., a remote worker).

Visual

Description and Implications

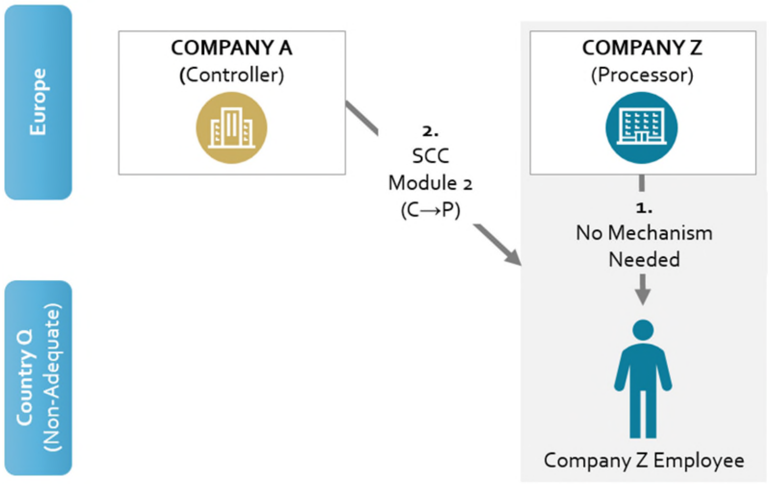
Option 1



- Transfer 1: No Mechanism Needed. The GDPR does not require a cross-border transfer mechanism for data that is transferred from a company in the EEA to another company in the EEA. Note that Company Z would be directly subject to the GDPR, and, as a result, data received would be subject to all GDPR requirements that apply to processors even in the absence of a SCC. Further note that while a cross-border transfer mechanism is not needed, the GDPR requires that a written contract be entered into between Company A and Company Z that complies with the requirements of Article 28 of the GDPR.
- Transfer 2: No Mechanism Needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[61] While the EDPB provided, as an example, the use-case whereby an employee travels for work to India where he or she remotely accesses personal data from the EEA, this rationale presumably also applies to other remote-work situations such as where an employee resides in a non-EEA country, or where the remote employee downloads personal data (as opposed to remotely accessing such data).
- Transfer Impact Assessments. A formal transfer impact assessment is not required by contract if neither Company A nor Company Z signed SCCs. Nonetheless, the EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country

Visual	Description and Implications
	although there is no ‘transfer’ situation.”[62] As a result, Company A and/or Company Z might consider conducting a TIA to analyze various risks that may result from the transmission of data to an employee in Country Q. • Law Enforcement Request Policy. If no SCCs are signed, neither Company A nor Company Z would be directly subject to Clause 15 of the SCCs that requires specific steps in the event that a company receives a request from a public authority for access to personal data. Nonetheless, the EDPB has suggested that a controller (Company A) is “accountable for [their] processing activities” which include assessing risks “to conduct or proceed with a specific processing operation in a third country although there is no ‘transfer’ situation.”[63] As a result, Company A might expect that Company Z create a law enforcement request policy to mitigate risks surrounding law enforcement requests that Company Z might receive from Country Q. • Visibility regarding cross-border transfer. While Article 28(3)(a) requires processors to process personal data only on documented instructions from a controller, including with regard to transfers of personal data to a third country, based upon the EDPB’s guidance there is ambiguity about whether this provision would govern the ability of Company Z to permit its employees to work outside of the EEA (i.e., the EDPB suggests that Company Z may not be transferring personal information outside the EEA when it permits an employee to work outside of the EEA). In order to fully understand the countries in which their information will be processed, Company A might consider requiring Company B to disclose the physical locations in which all employees processing personal data will be located either through a provision in the party’s agreement or as part of due diligence (e.g., a data privacy or data security questionnaire).

Visual	Description and Implications
Option 2	



Europe

Country Q (Non-Adequate)

COMPANY A (Controller)

COMPANY Z (Processor)

2. SCC Module 2 (C→P)

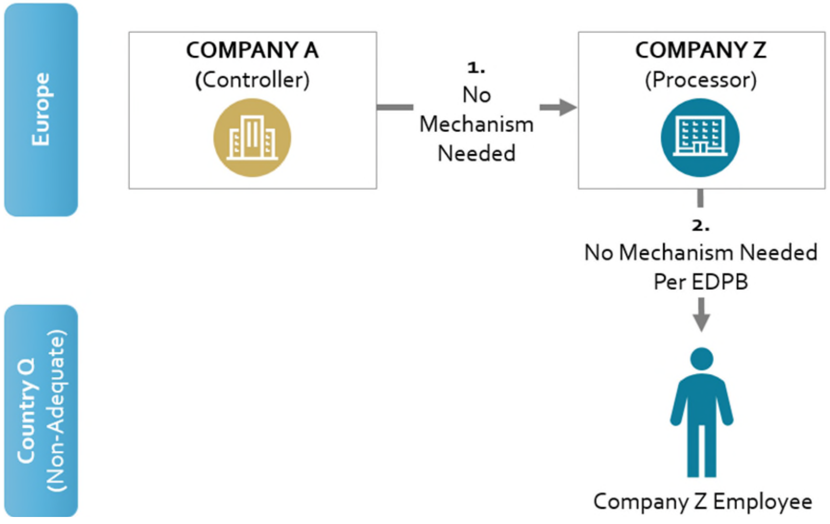
1. No Mechanism Needed

Company Z Employee

- Transfer 1: No Mechanism Needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA, the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[64] While the EDPB provided, as an example, the use-case whereby an employee travels for work to India where he remotely accesses personal data from the EEA, the EDPB has not indicated whether its rationale would apply to other remote-work situations such as transfers to an employee that resides in a non-EEA country, or situations where a remote employee downloads personal data (as opposed to remotely accesses such data).
- Transfer 2: SCC Module 2. The parties could enter into a SCC Module 2 designed for transfers from a controller to a non-EEA processor, which would list Company Z as a processor that is importing data into Country Q (via its employee in that country).
- Transfer Impact Assessments. Clause 14 of the SCCs would require the parties to document whether Company A or Company Z has reason to believe that the laws of Country Q would prevent Company Z from fulfilling its obligations under the SCC.
- Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company Z) to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company Z might consider creating a written law enforcement request policy.

7.2 Controller A (EEA) → Processor Z (EEA) → Employee of Processor Z (Non-EEA) (on vacation)

Visual



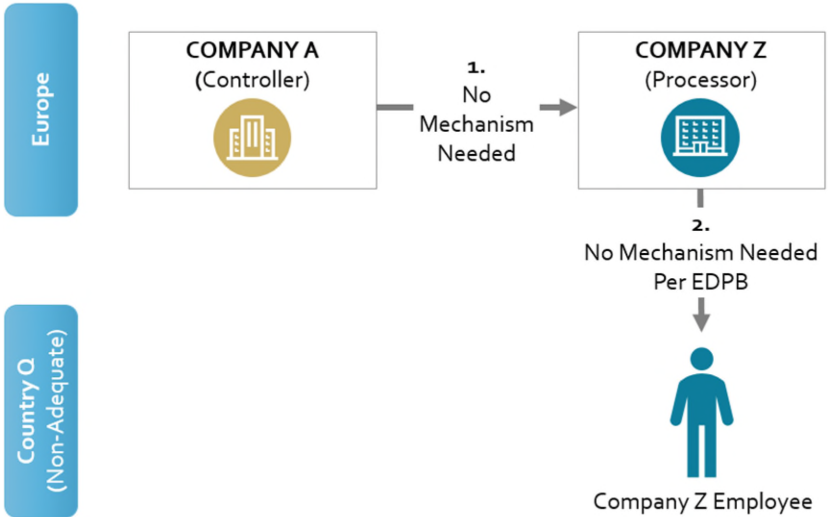
Description and Implications

- Background. Company A is an EEA controller that utilizes Company Z, an EEA processor. Company Z does not have a legal presence in Country Q, but does have an employee that is working from Country Q while on vacation (e.g., a travelling employee).
- Transfer 1: No Mechanism Needed. The GDPR does not require a cross-border transfer mechanism for data that is transferred from a company in the EEA to another company in the EEA. Note that Company Z would be directly subject to the GDPR, and, as a result, data received would be subject to all GDPR requirements that apply to processors even in the absence of a SCC. Further note that while a cross-border transfer mechanism is not needed, the GDPR requires that a written contract be entered between Company A and Company Z that complies with the requirements of Article 28 of the GDPR.
- Transfer 2: No Mechanism Needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA, the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[65] While the EDPB provided, as an example, the use-case of an employee traveling for work to India who remotely accesses personal data from the EEA, the EDPB has not indicated that its rationale would differ for other remote-work situations such as when an employee is travelling for personal reasons or when a remote employee downloads personal data (as opposed to remotely accesses such data).
- Transfer Impact Assessments. A formal transfer impact assessment is not required by contract if neither Company A nor Company Z signed SCCs. Nonetheless, the EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country

Visual	Description and Implications
	although there is no ‘transfer’ situation.”[66] As a result, Company A and/or Company Z might consider conducting a TIA to analyze various risks that may result from the transmission of data to an employee in Country Q. The EDPB further suggests that, in the event Company A’s and/or Company Z’s analysis determines that the risk associated with such transmission is too high, Company A and/or Company Z may conclude that the employee should not bring their laptop or access company systems while travelling to Country Q.[67] • Law Enforcement Request Policy. If no SCCs are signed, neither Company A nor Company Z would be directly subject to Clause 15 of the SCCs that requires specific steps in the event that a company receives a request from a public authority for access to personal data. Nonetheless, the EDPB has suggested that a controller (Company A) is “accountable for [their] processing activities” which include assessing risks “to conduct or proceed with a specific processing operation in a third country although there is no ‘transfer’ situation.”[68] As a result, Company A might expect that Company Z create a law enforcement request policy to mitigate risks surrounding law enforcement requests that Company Z might receive from Country Q.

7.3 Controller A (EEA) → Processor Z (EEA) → Employee of Processor Z (Non-EEA) (on business trip)

Visual



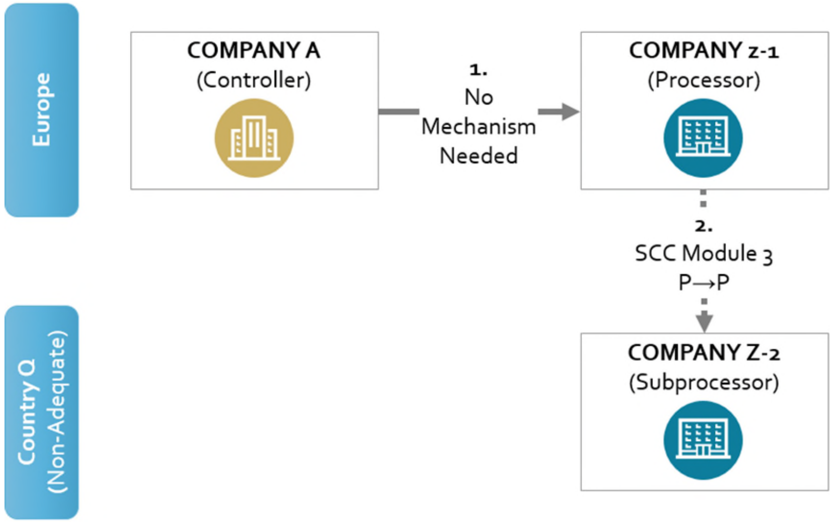
Description and Implications

- Background. Company A is an EEA controller that utilizes Company Z, an EEA processor. Company Z does not have a legal presence in Country Q, but has instructed an employee to work from Country Q while on a business trip.
- Transfer 1: No Mechanism Needed. The GDPR does not require a cross-border transfer mechanism for data that is transferred from a company in the EEA to another company in the EEA. Note that Company Z would be directly subject to the GDPR, and, as a result, data received would be subject to all GDPR requirements that apply to processors even in the absence of a SCC. Further note that while a cross-border transfer mechanism is not needed, the GDPR requires that a written contract be entered between Company A and Company Z that complies with the requirements of Article 28 of the GDPR.
- Transfer 2: No Mechanism Needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA, the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[69] The EDPB provided, as an example, the use-case where an employee travels for work to India where she remotely accesses personal data from the EEA. Note that the EDPB has not indicated that its rationale would not apply to other remote-work situations such as where the remote employee downloads personal data (as opposed to remotely accesses such data).
- Transfer Impact Assessments. A formal transfer impact assessment is not required by contract if neither Company A nor Company Z signed SCCs. Nonetheless, the EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country

Visual	Description and Implications
	although there is no ‘transfer’ situation.”[70] As a result, Company A and/or Company Z might consider conducting a TIA to analyze various risks that may result from the transmission of data to an employee in Country Q. The EDPB further suggests that, in the event Company A’s and/or Company Z’s analysis determines that the risk associated with such transmission is too high, Company A and/or Company Z may conclude that the processing should not be allowed to occur in Country Q.[71] ● Law Enforcement Request Policy. If no SCCs are signed, neither Company A nor Company Z would be directly subject to Clause 15 of the SCCs that requires specific steps in the event that a company receives a request from a public authority for access to personal data. Nonetheless, the EDPB has suggested that a controller (Company A) is “accountable for [their] processing activities” which include assessing risks “to conduct or proceed with a specific processing operation in a third country although there is no ‘transfer’ situation.”[72] As a result, Company A might expect that Company Z create a law enforcement request policy to mitigate risks surrounding law enforcement requests that Company Z might receive from Country Q.

7.4 Controller A (EEA) → Processor Z-1 (EEA) → Affiliated Subprocessor Z-2 (Non-EEA)

Visual



Europe

COMPANY A
(Controller)

1.
No
Mechanism
Needed

COMPANY z-1
(Processor)

2.
SCC Module 3
P→P

Country Q
(Non-Adequate)

COMPANY Z-2
(Subprocessor)

Description and Implications

- Background. Company A is an EEA controller that utilizes Company Z-1, an EEA processor. Company Z-1 and Company Z-2 are corporate affiliates that are under common ownership or control, but are separate legal entities. Personal data is being sent from Controller A in the EEA to Processor Z-1 in the EEA; Processor Z-1 onward transfers the personal data to Processor Z-2 (its sub-processor) in Country Q. Company A has contracted only with Processor Z-1 in the EEA; Company A has not contracted with Processor Z-2.
- Transfer 1: No Mechanism Needed. The GDPR does not require a cross-border transfer mechanism for data that is transferred from a company in the EEA to another company in the EEA. That said, the GDPR requires that an Article 28 data processing agreement (DPA) be completed between Company A and Company Z-1. Note that under the GDPR, Company Z-1 is not permitted to transfer personal data outside of the EEA without the authorization of Company A.[73] As a result, the DPA should, at a minimum, include a general authorization to transfer personal data outside of the EEA; it might also identify the specific country in which Company Z-2 is located (i.e., Country Q).
- Transfer 2: SCC Module 3. Although Company Z-1 and Company Z-2 may be under common ownership and control, as separate legal entities they are required to put into place a safeguard when transferring personal data from the EEA to Country Q.[74] In this case, because both entities are processors, SCC Module 3 should be selected. Note that in practice the SCC Module 3 might be integrated into an intragroup data transfer agreement that attempts to address the cross-border transfer restrictions imposed by all countries in which affiliates of Company Z operate.
- Transfer Impact Assessments. Clause 14 of the SCCs requires that Company Z-1 and Company Z-2 document whether either party has reason to believe

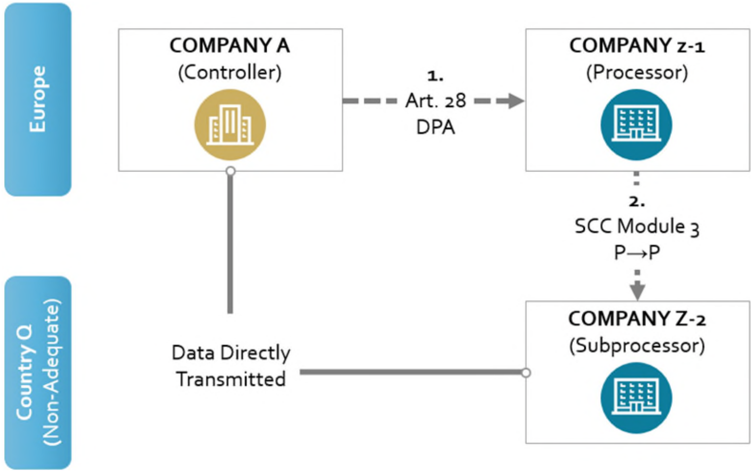
Visual	Description and Implications
	that the laws and practices of Country Q prevent Company Z-2 from fulfilling its obligations under the SCCs. Note that the Article 28 DPA entered into between Company A and Company Z-1 must require that Company Z-1 "make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article."[75] As a result, Controller A may argue that they have a right to receive a copy of the TIA as part of an audit or assessment of Company Z-1. • Law Enforcement Request Policy. Clause 15 of the SCCs requires Company Z-2 to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company Z-2 might consider creating a law enforcement request policy.

7.5 Controller A (EEA) → Processor Z-1 (EEA) → Affiliated Processor Z-2 (Non-EEA) (data directly sent to Non-EEA Processor)

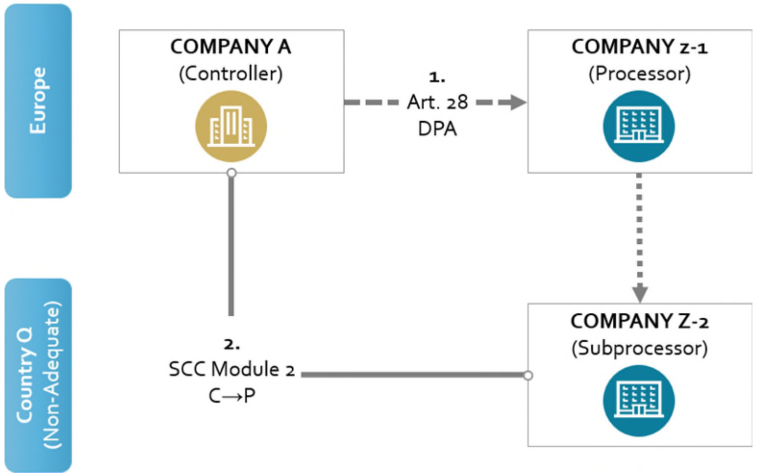
Background. Company Z-1 and Company Z-2 are corporate affiliates that are under common ownership or control, but are separate legal entities. Data is being directly sent from Controller A in the EEA to Processor Z-2 in a non-adequate jurisdiction. Company A has contracted only with Processor Z-1 in the EEA. The solid line indicates the data flow; the dashed line indicates the contractual relationships.

Visual | **Description and Implications**

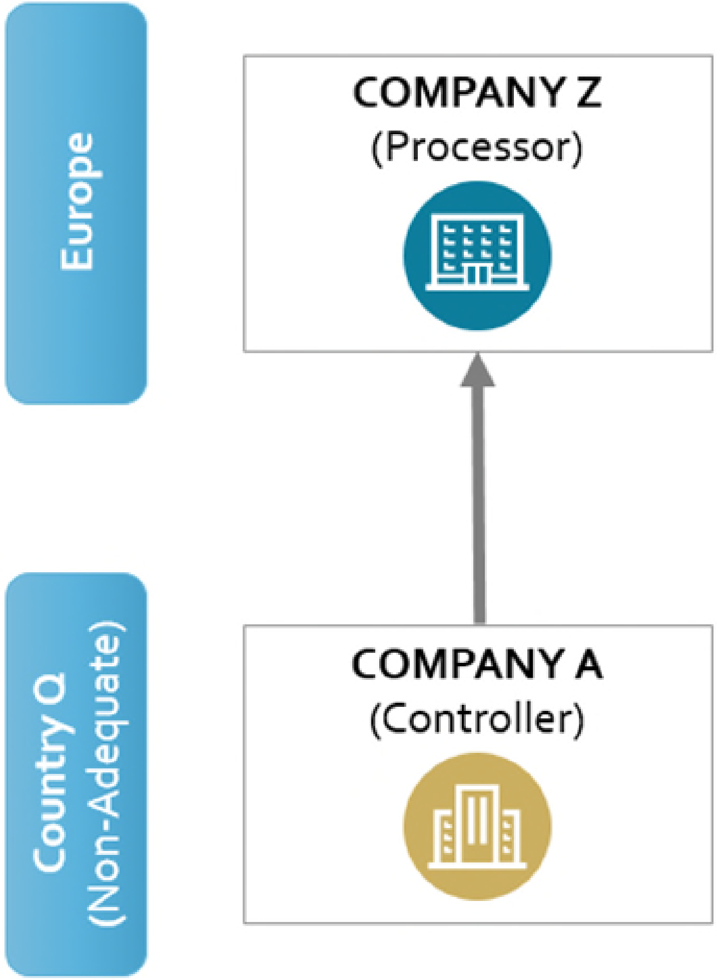
Option 1



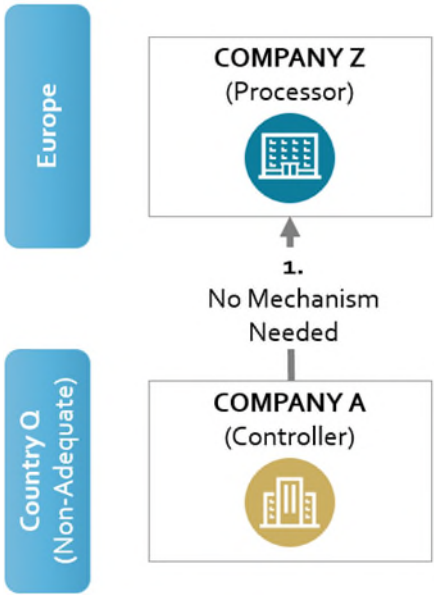
- Transfer 1: Article 28 DPA. The GDPR requires that an Article 28 data processing agreement (DPA) be completed between Company A and Company Z-1. Note that under the GDPR, Company Z-1 is not permitted to transfer personal data outside of the EEA without the authorization of Company A.[76] If Company Z-1 intends to subcontract the processing of personal data (including the receipt of personal data from Company A), the DPA should at a minimum include a general authorization to transfer information outside of the EEA; it might also identify the specific country in which Company Z-2 is located (i.e., the US).
- Transfer 2: SCC Module 3. Although Company Z-1 is not physically exporting or importing personal data, if the contractual relationship between Company A and Company Z-1 makes Company Z-1 responsible for the processing activities (including the selection of Company Z-2 as a sub-processor), Company Z-1 may consider utilizing SCC Module 3 with Company Z-2.
- Transfer Impact Assessments. Clause 14 of the SCCs requires that Company Z-1 and Company Z-2 document whether either party has reason to believe that the laws and practices of Country Q prevent Company Z-2 from fulfilling its obligations under the SCCs.
- Law enforcement request policy. Clause 15 of the SCCs requires Company Z-2 to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company Z-2 might consider creating a law enforcement request policy.

Visual	Description and Implications
Option 2	
 Europe COMPANY A (Controller) 1. Art. 28 DPA COMPANY z-1 (Processor) Country Q (Non-Adequate) 2. SCC Module 2 C→P COMPANY Z-2 (Subprocessor)	• Transfer 1: Article 28 DPA. The GDPR requires that an Article 28 data processing agreement (DPA) be completed between Company A and Company Z-1. Note that under the GDPR, Company Z-1 is not permitted to transfer personal data outside of the EEA without the authorization of Company A.[77] If Company Z-1 intends to subcontract the processing of personal data (including the receipt of personal data from Company A), the DPA should at a minimum include a general authorization to transfer information outside of the EEA; it might also identify the specific country in which Company Z-2 is located (i.e., the US). • Transfer 2: SCC Module 2. The European Commission has defined the "data exporter" as being the "controller or processors transferring the personal data to a third country."[78] As Company A is physically transmitting personal data to Company Z-2 an argument could be made that Company A should enter into a cross-border transfer mechanism directly with Company Z-2. In this case, SCC Module 2 could be utilized. • Transfer Impact Assessments. Clause 14 of the SCCs requires that Company A and Company Z-2 to create a transfer impact assessment to determine whether either party has reason to believe that the laws and practices of Country Q prevent Company Z-2 from fulfilling its obligations under the SCCs. • Law enforcement request policy. Clause 15 of the SCCs requires Company Z-2 to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company Z-2 might consider creating a law enforcement request policy.

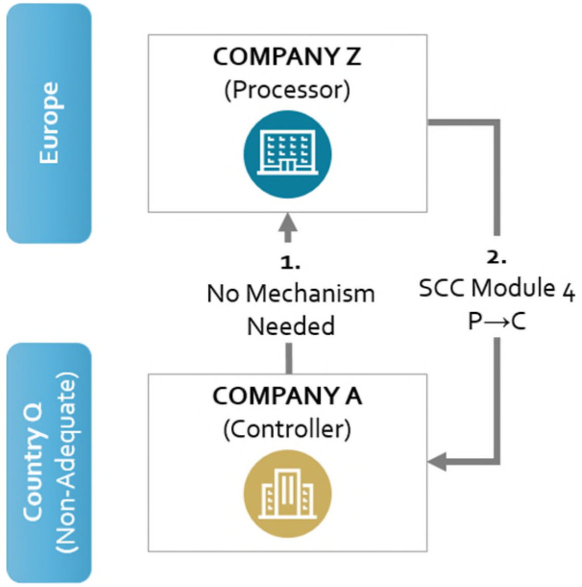
8. Transfers from Non-EEA Controllers to EEA processors



8.1 Controller A (Non-EEA) → Processor Z (EEA) → Controller A (Non-EEA) (Basic Renvoi)

Visual	Description and Implications
 Europe COMPANY Z (Processor) 1. No Mechanism Needed Country Q (Non-Adequate) COMPANY A (Controller)	- Background. Company A, located in Country Q, transfers personal data to its processor, Company Z, located in the EEA. - Transfer 1: No mechanism needed. Company A is not required under the GDPR to put safeguards in place to transfer information to a processor that is located in the EEA. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.

8.2 Controller A (Non-EEA) → Processor Z (EEA) → Controller A (Non-EEA) (Basic Renvoi)

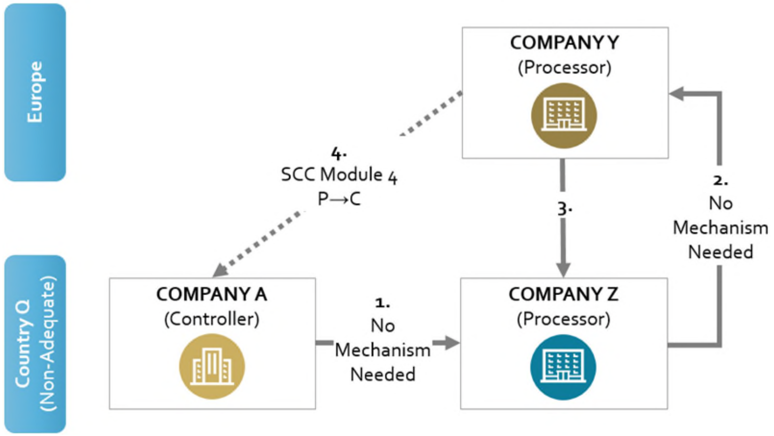
Visual	Description and Implications
 Europe COMPANY Z (Processor) 1. No Mechanism Needed 2. SCC Module 4 P→C Country Q (Non-Adequate) COMPANY A (Controller)	• Background. Company A, located in Country Q, transfers personal data to its processor, Company Z, located in the EEA. Company Z onward transfers the personal data back to Company A. • Transfer 1: No mechanism needed. Company A is not required under the GDPR to put safeguards in place to transfer information to a processor that is located in the EEA. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed. • Transfer 2: SCC Module 4. Article 46 of the GDPR requires that a processor that transfers personal data outside of the EEA to a non-adequate country must utilize a safeguard. The EDPB has confirmed that this requirement applies when an EEA processor (Company Z) sends data to a controller (Company A).[79] Company Z and Company A should utilize the SCC Module 4. • Transfer Impact Assessments. Clause 14 of SCC Module 4 does not typically require Company Z or Company A to conduct a transfer impact assessment ("TIA") of the laws of Country Q. Note, however, that a TIA would be required if Company Z combined the personal data that it received from a separate company (Company Y) with its own personal data (e.g., did a data enhancement or a data append), and transmitted the combined data to Company A. • Law enforcement request policy. Clause 15 of SCC Module 4 does not typically require that Company A take specific steps in the event that it receives a request from a public authority for access to personal data. Note, however, that a law enforcement policy might be warranted if Company Z combined the personal data that it received from a separate company (Company Y) with its own personal data (e.g., did a data enhancement or a data append), and transmitted the combined data to Company A.

8.3 Controller A (Non-EEA) → Processor Z (Non-EEA) → Sub-processor Y (EEA) → Processor Z (Non-EEA)

Background: Company A, located in Country Q, transfers personal data to its processor, Company Z, also located in Country Q. Company Z onward transfers the personal data to its sub-processor, Company Y, located in the EEA. Company Y then onward transfers the personal data back to Company Z. Note for purposes of this example Company A is assumed not to be subject to Article 3(2) of the GDPR.

Visual	Description and Implications

Option 1



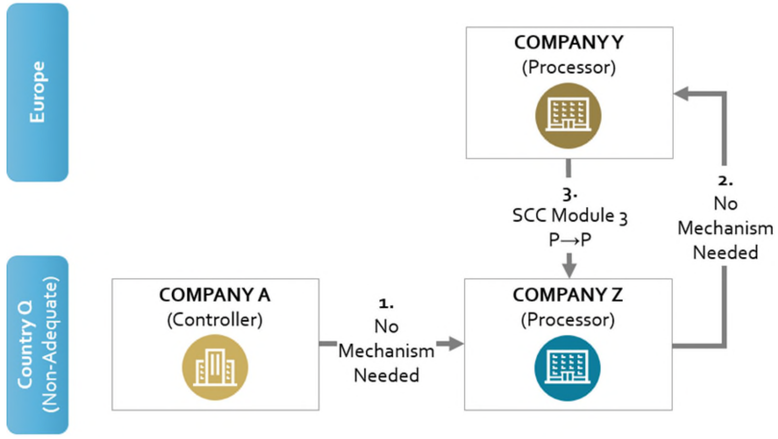
- Transfer 1: No mechanism needed. Company A is not required under the GDPR to put safeguards in place to transfer information to a processor that is also located in Country Q.
- Transfer 2: No mechanism needed. Company Z is not required under the GDPR to put in place a transfer mechanism when it transmits (exports) personal data to the EEA. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.
- Transfer 3: SCC Module 4. Article 46 of the GDPR requires that a processor that transfers data outside of the EEA to a non-adequate country must utilize a safeguard. The EDPB has confirmed that this requirement applies when an EEA processor (Company Y) sends data to another processor (Company Z).[80] While SCC Module 3 is designed for transfers from a processor to another processor note that SCC Module 3 assumes that the data importer is a sub-processor of the data exporter. For example, Article 8.1(b) states that the importer (in this case Company Z) must process the data only upon the instructions of the controller (in this case Company A) as communicated by the exporter (in this case Company Y). To the extent that Company Y is the sub-processor of Company Z (i.e., it receives instructions from Company Z, and does not provide instructions to Company Z), the parties might consider having Company Y execute SCC Module 4 with Company A, as SCC Module 4 might best approximate the relative positions of the parties. Note that in the diagram the solid line depicts the data transfer; the dashed line depicts the proposed contractual relationships.

Visual

Description and Implications

- Subsequent Onward Transfers by Company Z. Note that if Company Z sends data back to Company A, it is not required to put a transfer mechanism in place.
- Transfer Impact Assessments. Clause 14 of SCC Module 4 generally does not require Company A conduct a TIA, unless Company Y combined the personal data received from Company Z with personal data collected in the EEA.
- Law enforcement request policy. Clause 15 of SCC Module 4 does not require that Company A take specific steps in the event that it receives a request from a public authority for access to personal data, unless Company Y combined personal data received from Company Z with personal data collected in the EEA.

Option 2

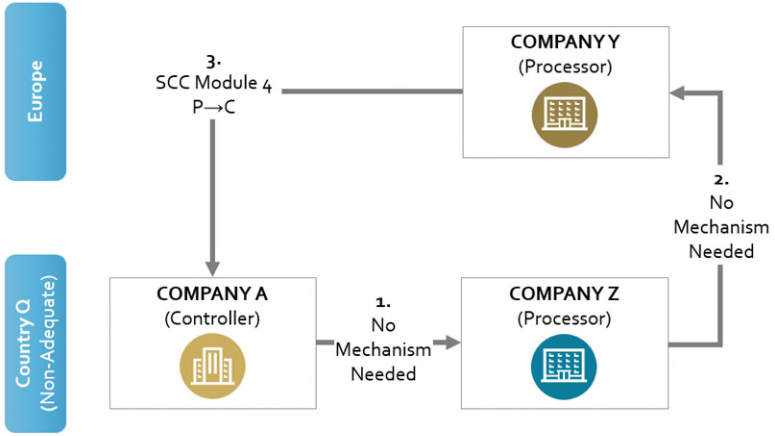


- Transfer 1: No mechanism needed. Company A is not required under the GDPR to put safeguards in place to transfer information to a processor that is also located in Country Q.
- Transfer 2: No mechanism needed. Company Z is not required under the GDPR to put in place a transfer mechanism when it transmits (exports) personal data to the EEA. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.
- Transfer 3: SCC Module 3. Article 46 of the GDPR requires that a processor that transfers data outside of the EEA to a non-adequate country must utilize a safeguard. The EDPB has confirmed that this requirement applies when an EEA processor (Company Y) sends data to another processor (Company Z).[81] While SCC Module 3 is designed for transfers from a processor to another processor note that SCC Module 3 assumes that the data importer is a sub-processor of the data exporter. For example, Article 8.1(b) states that the importer (in this case Company Z) must process the data only upon the instructions of the controller (in this case Company A) and the exporter (in this case Company Y). The parties

Visual	Description and Implications
	should consider whether such provisions are counter-factual to the relationships of the relative processors. ● Subsequent Onward Transfers by Company Z. Note that if Company Z sends data back to Company A, it is not required to put a transfer mechanism in place. If, however, Company Z were to onward transfer personal data to another sub-processor in a non-adequate jurisdiction (e.g., Company X located in the U.S.), it would be required pursuant to SCC Module 3 Clauses 8.8 and 9(b) to ask Company X to agree to SCC Module 3. ● Transfer Impact Assessments. Clause 14 of SCC Module 3 requires Company Y and Company Z to conduct a TIA to determine whether either party has reason to believe that the laws and practices of Country Q prevent Company Z from fulfilling its obligations under the SCCs. ● Law enforcement request policy. Clause 15 of SCC Module 3 requires that Company Z take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company Z might be expected to implement a written law enforcement request policy.

8.4 Controller A (Non-EEA) → Processor Z (Non-EEA) (same country) → Sub-processor Y (EEA) → Controller A (Non-EEA)

Visual	Description and Implications



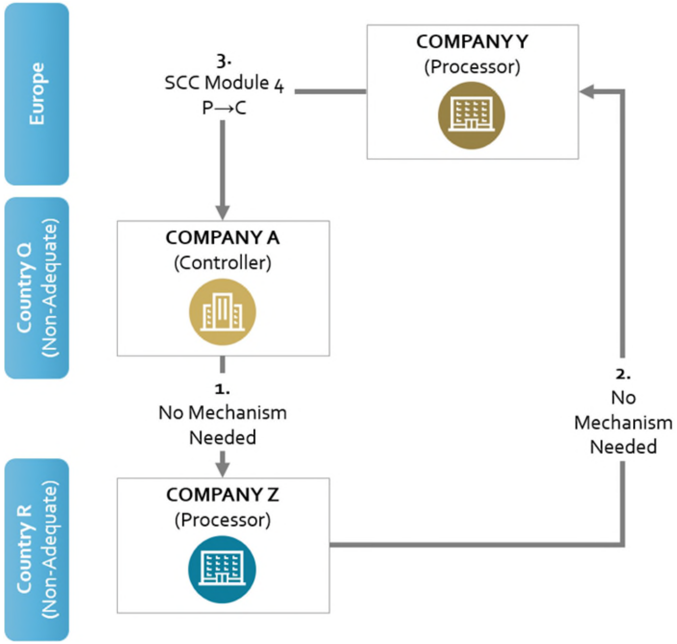
- Background. Company A, located in Country Q, transfers personal data to its processor, Company Z, also located in Country Q. Company Z onward transfers the personal data to its sub-processor, Company Y, located in the EEA. Company Y then onward transfers the personal data back to Company A. Note for purposes of this example Company A is assumed not to be subject to Article 3(2) of the GDPR.
- Transfer 1: No mechanism needed. Company A is not required under the GDPR to put safeguards in place to transfer information to a processor that is also located in Country Q.
- Transfer 2: No mechanism needed. Company Z is not required nder the GDPR to put in place a transfer mechanism when it transmits (exports) personal data to the EEA. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.
- Transfer 3: SCC Module 4. Article 46 of the GDPR requires that a processor that transfers personal data outside of the EEA to a non-adequate country must utilize a safeguard. The EDPB has confirmed that this requirement applies when an EEA processor (Company Y) sends data to a non-EEA controller (Company A).[82] Company Y and Company A should utilize the SCC Module 4.
- Subsequent Onward Transfers from Company A do not require safeguards. Note that if Company A sends data that it received from Company Y to subsequent controllers or processors it is typically not required to put a transfer mechanism in place.
- Transfer Impact Assessments. Clause 14 of SCC Module 4 does not typically require Company Y or Company A to conduct a TIA of the laws of Country Q. Note, however, that a TIA would be required if Company Y combined the personal data that it received from Company Z with its own personal data or with data it

received from a separate company (e.g., did a data enhancement or a data append), and transmitted the combined data to Company A.

- Law enforcement request policy. Clause 15 of SCC Module 4 would not typically require that Company A take specific steps in the event that it receives a request from a public authority for access to personal data. Note, however, that a law enforcement policy might be warranted if Company Y combined the personal data that it received from Company Z with its own personal data or data it received from a separate company (e.g., did a data enhancement or a data append), and transmitted the combined data to Company A.

8.5 Controller A (Non-EEA) → Processor Z (Non-EEA) (different country) → Sub-processor Y (EEA) → Controller A (Non-EEA)

Visual



Description and Implications

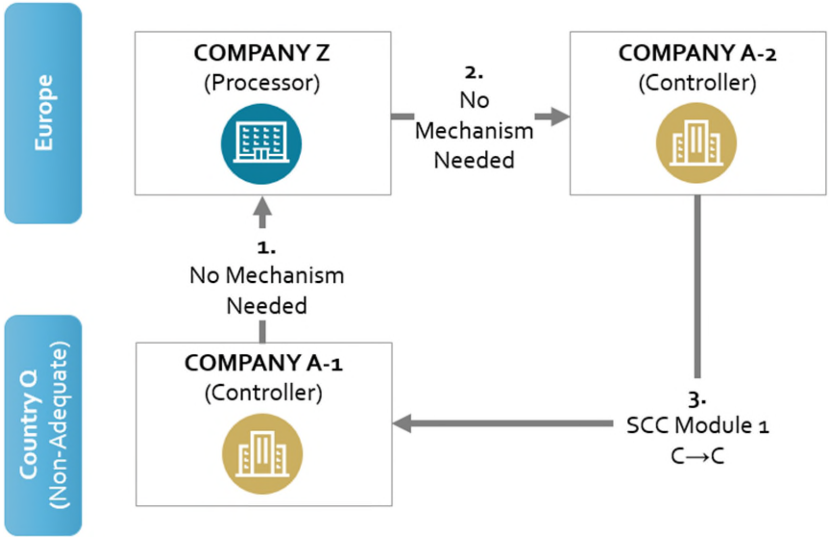
- Background. Company A, located in Country Q, transfers personal data to its processor, Company Z, located in Country R. Company Z onward transfers the personal data to its sub-processor, Company Y, located in the EEA. Company Y then onward transfers the personal data back to Company A. Note for purposes of this example Company A is assumed not to be subject to Article 3(2) of the GDPR.
- Transfer 1: No mechanism required. Company A is not required under the GDPR to put safeguards in place to transfer personal information to a processor that is located in another non-adequate country. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.
- Transfer 2: No mechanism required. Company Z is not required under the GDPR to put safeguards in place to transfer personal information to a processor that is located in the EEA. Unless Country R independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.
- Transfer 3: SCC Module 4. Article 46 of the GDPR requires that a processor that transfers personal data outside of the EEA to a non-adequate country must utilize a safeguard. The EDPB has confirmed that this requirement applies when an EEA processor (Company Y) sends data to a controller (Company A).[83] Company Y and Company A should utilize the SCC Module 4.
- Subsequent Onward Transfers from Company A do not require safeguards. Note that if Company A sends data that it received from Company Y to subsequent controllers or processors it is typically not required to utilize a safeguard.
- Transfer Impact Assessments. Clause 14 of SCC Module 4 would not typically require Company Y or Company A to conduct a TIA of the laws of Country Q. Note, however, that a TIA would be required if Company Y combined the personal data that it received from Company A (via Company Z), with its own personal data or data received from a

separate company (e.g., did a data enhancement or a data append), and transmitted the combined data to Company A.

- Law enforcement request policy. Clause 15 of SCC Module 4 does not typically require that Company A take specific steps in the event that it receives a request from a public authority for access to personal data. Note, however, that a law enforcement policy might be warranted if Company Y combined the personal data that it received from Company A (via Company Z), with its own personal data or data received from a separate company (e.g., did a data enhancement or a data append), and transmitted the combined data to Company A.

8.6 Controller A-1 (Non-EEA) → Processor Z (EEA) → Controller A-2 (EEA) → Controller A-1 (Non-EEA) (Renvoi)

Visual



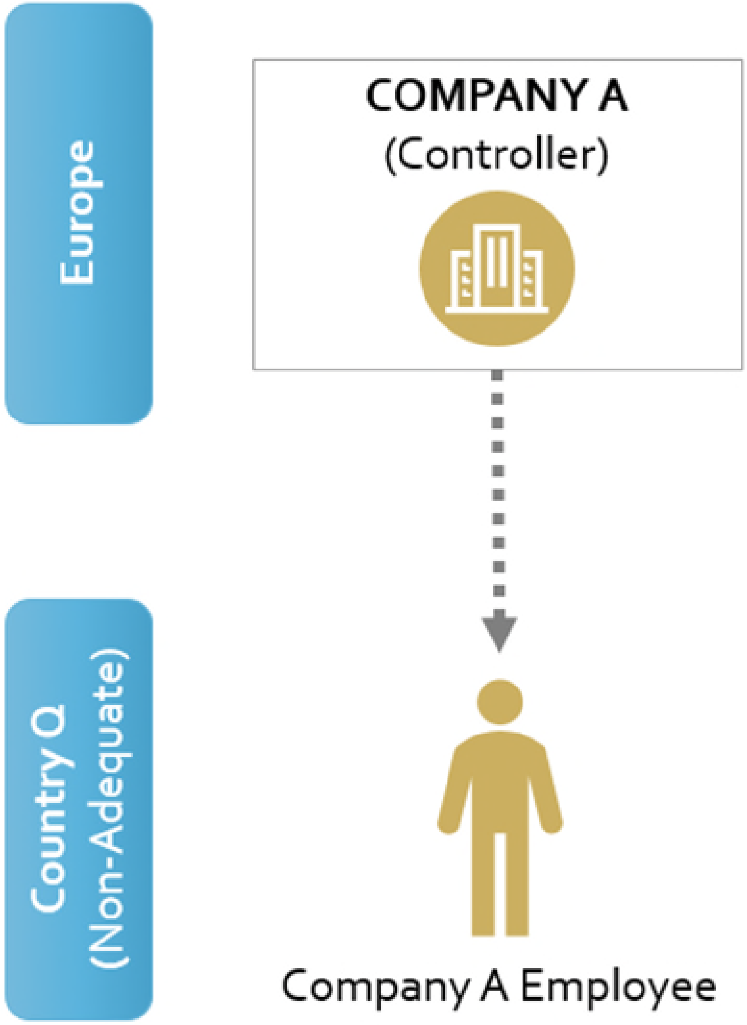
Description and Implications

- Background. Company A-1 and Company A-2 are corporate affiliates that are under common ownership or control, but are separate legal entities. Company A-1, located in Country Q, transfers personal data to its processor, Company Z, located in the EEA. Company Z onward transfers the personal data to Company A-2, located in the EEA. Company A-2 then returns the data back to Company A-1.
- Transfer 1: No mechanism needed. Company A-1 is not required under the GDPR to put safeguards in place to transfer personal data to a processor that is located in the EEA. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed. Note that if Company Z is acting as Company A-1's processor, the parties will need to have a written agreement that complies with Article 28 of the GDPR.
- Transfer 2: No mechanism needed. Company Z is not required under the GDPR to put in place a transfer mechanism when it transmits personal data to another controller within the EEA; this would include a corporate affiliate of Company A-1. Note that if Company Z is acting as Company A-2's processor, the parties will need to have a written agreement that complies with Article 28 of the GDPR.
- Transfer 3: SCC Module 1. Article 46 of the GDPR requires that a controller that transfers personal data outside of the EEA to a non-adequate country must utilize a safeguard. This requirement applies when an EEA controller (Company A-2) sends data to a corporate affiliate (Company A-1).[84] Company A-1 and Company A-2 should utilize the SCC Module 1. In practice, Company A-1 and Company A-2 may decide to put in place an intragroup agreement that incorporates the SCCs as well as any contractual

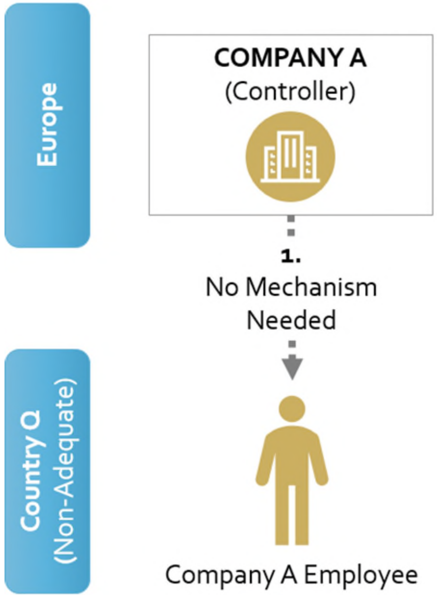
requirements imposed by other countries in which the corporate group transfers personal data.

- Subsequent Onward Transfers from Company A-1. Note that if Company A-1 makes any additional onward transfers the appropriate module of the SCCs would need to be used.
- Transfer Impact Assessments. Clause 14 of the SCCs requires both parties (Company A-2 and Company A-1) to document whether either party has reason to believe that the laws and practices of Country Q prevent the data importer (i.e., Company A-1) from fulfilling its obligations under the SCCs.
- Law Enforcement Request Policy. Clause 15 of the SCCs requires the data importer (Company A-1) to take specific steps in the event that it receives a request from a public authority for access to personal data. As a result, Company A-1 might consider creating a law enforcement request policy.

9. Other Transfers from EEA Controllers to Non-EEA Employees

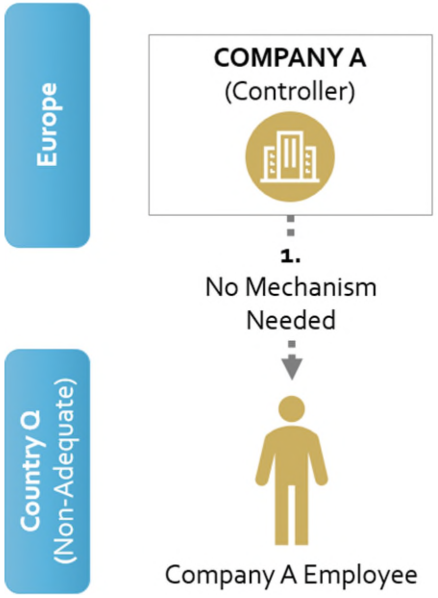


9.1 Controller A (EEA)→ Employee of Controller A (Non-EEA) (on business trip)

Visual	Description and Implications
 Europe COMPANY A (Controller) 1. No Mechanism Needed Country Q (Non-Adequate) Company A Employee	- Background. Company A is a European legal entity that does not have a legal presence in Country Q. Company A has an employee that travels to Country Q on a business trip and from that location performs work by accessing files remotely that contain personal data. - Transfer 1: No mechanism needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA, the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[85] The EDPB provided, as an example, the use-case whereby an employee travels for work to India where he remotely accesses personal data from the EEA. - Transfer Impact Assessments. The EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[86] As a result, Company A might consider conducting a TIA to analyze various risks that may result from the transmission of data to an employee in Country Q. While conducting a TIA might be beneficial, it is important to note that unlike transfers that utilize the SCCs, a TIA is not contractually required. - Law enforcement request policy. The EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[87] As a result, Company A might consider creating a law enforcement request policy to mitigate risks surrounding law enforcement requests received from Country Q.

9.2 Controller A (EEA)→ Employee of Controller A (Non-EEA) (on vacation)

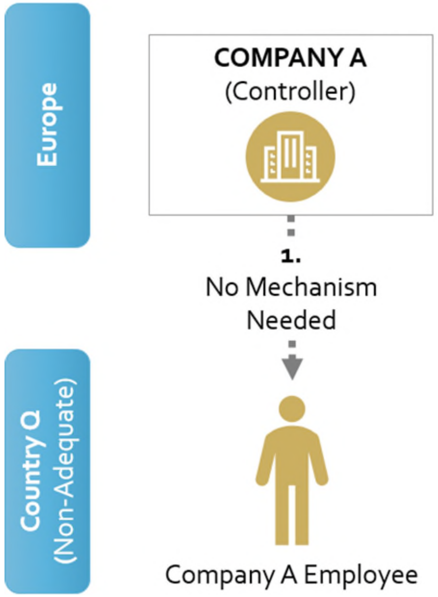
Visual



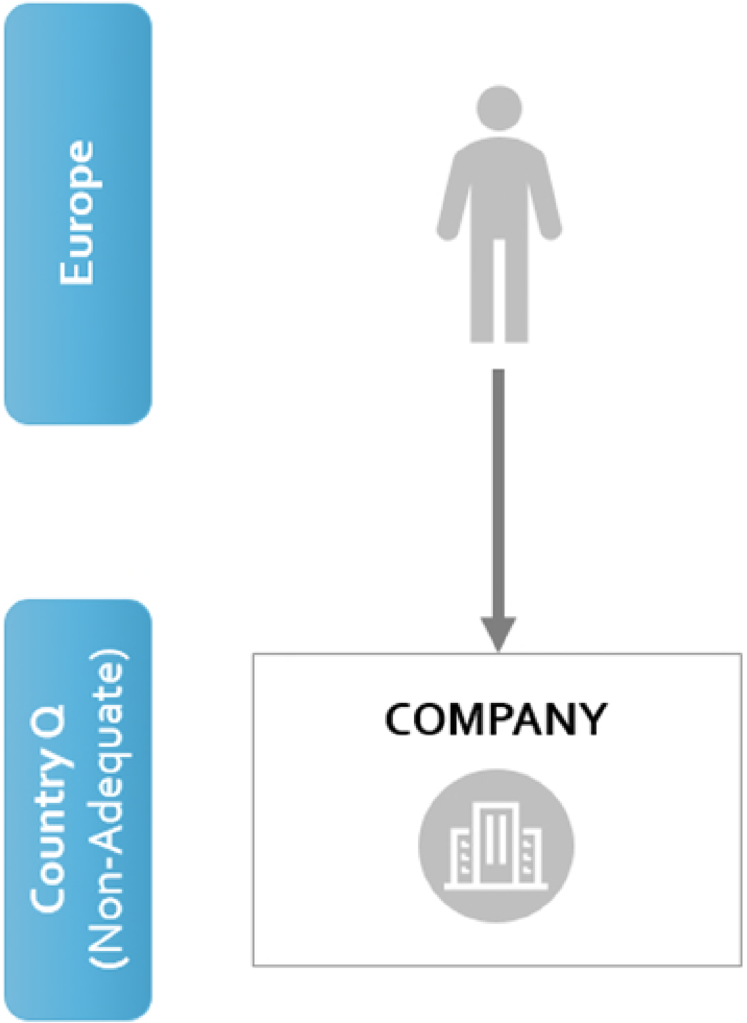
Description and Implications

- Background. Company A is a European legal entity that does not have a legal presence in Country Q. Company A has an employee that travels to Country Q on a vacation and from that location performs work by accessing files remotely that contain personal data.
- Transfer 1: No mechanism needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA, the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[88] The EDPB provided, as an example, the use-case whereby an employee travels for work to India where he remotely accesses personal data from the EEA. Although the EDPB has not specifically discussed the situation where an employee is travelling for personal reasons, the rationale provided by the EDPB in the work-travel use case would likely apply to personal travel as well.
- Transfer Impact Assessments. The EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[89] As a result, Company A might consider conducting a TIA to analyze various risks that may result from the transmission of data to an employee in Country Q. While conducting a TIA might be beneficial, it is important to note that unlike transfers that utilize the SCCs, a TIA is not contractually required.
- Law enforcement request policy. The EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[90] As a result, Company A might consider creating a law enforcement request policy to mitigate risks surrounding law enforcement requests received from Country Q.

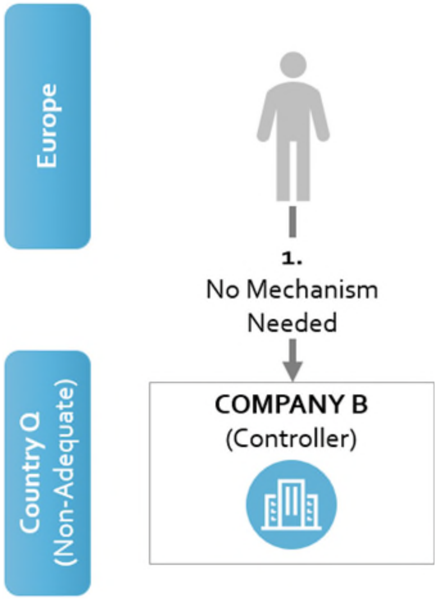
9.3 Controller A (EEA)→ Employee of Controller A (Non-EEA) (remote worker)

Visual	Description and Implications
 Europe COMPANY A (Controller) 1. No Mechanism Needed Country Q (Non-Adequate) Company A Employee	• Background. Company A is a European legal entity that does not have a legal presence in Country Q. Company A has an employee that works from Country Q (e.g., a remote worker). • Transfer 1: No mechanism needed. The EDPB has suggested that when a company transmits personal data to an employee that is located outside of the EEA, the transmission does not constitute a "transfer" of personal information for purposes of Chapter V of the GDPR because the data has not been sent to a separate controller or processor.[91] While the EDPB provided, as an example, the use-case where an employee travels for work to India where he remotely accesses personal data from the EEA, the EDPB's rationale may apply equally to other remote-work situations such as an employee that resides in a non-EEA country, or a remote employee that downloads personal data (as opposed to remotely accesses such data). • Transfer Impact Assessments. The EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[92] As a result, Company A might consider conducting a TIA to analyze various risks that may result from the transmission of data to an employee in Country Q. While conducting a TIA might be beneficial, it is important to note that unlike transfers that utilize the SCCs, a TIA is not contractually required. • Law enforcement request policy. The EDPB has suggested that a controller (Company A) is "accountable for [its] processing activities" which include assessing risks "to conduct or proceed with a specific processing operation in a third country although there is no 'transfer' situation."[93] As a result, Company A might consider creating a law enforcement request policy to mitigate risks surrounding law enforcement requests received from Country Q.

10. Transfers from European Data Subjects

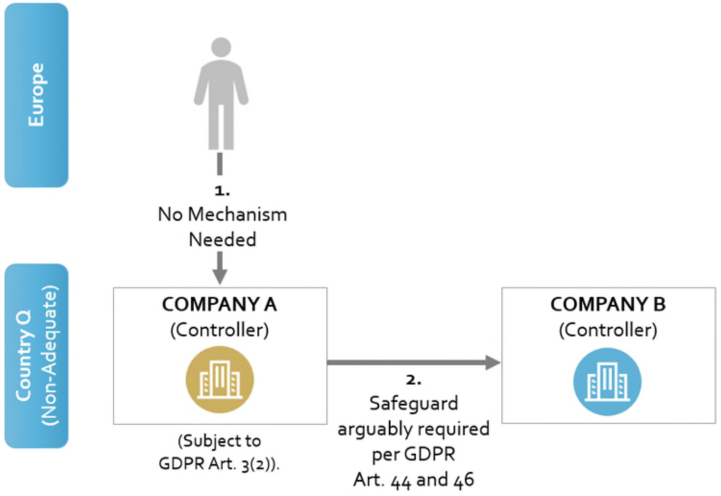


10.1 Data Subject (EEA) → Controller A (Non-EEA)

Visual	Description and Implications
 Europe 1. No Mechanism Needed COMPANY B (Controller) Country Q (Non-Adequate)	● Background. Company B, located in Country Q, collects data directly from a data subject, located in the EEA. For the purposes of this example, it is assumed that the data subject is operating in a personal (as opposed to work or commercial) capacity. ● Transfer 1: No mechanism needed. The EDPB has taken the position that a data subject "cannot be considered a controller or processor."[94] As a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to transfers performed by data subjects. In addition, the transfer of personal data from the EEA to Country Q arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulation does not apply to processing done by a "natural person in the course of a purely personal or household activity."[95] The net result is that a controller outside of the EEA that receives personal data directly from a data subject does not need to utilize the SCCs, or any other safeguards.

10.2 Data Subject (EEA) → Controller A (Non-EEA) → Controller B (Non-EEA) (same country)

Visual

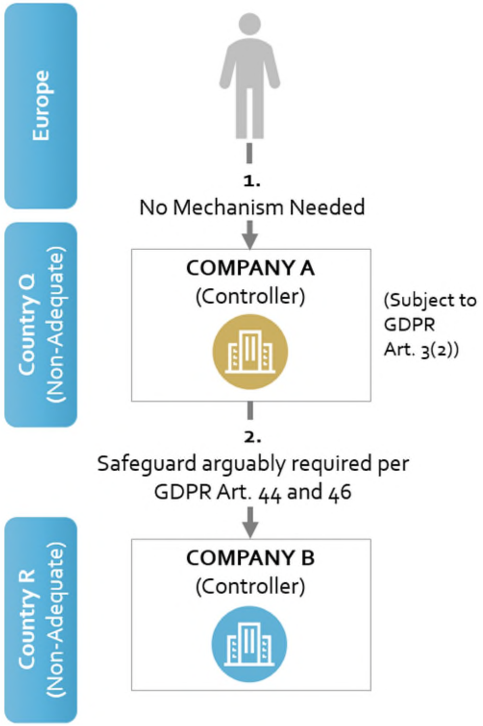


Description and Implications

- Background. Company A, located in Country Q, collects data directly from a data subject, located in the EEA. Company A onward transfers the data to Company B, also located in Country Q. For the purposes of this example, it is assumed that the data subject is operating in a personal (as opposed to work or commercial) capacity.
- Transfer 1: No mechanism required. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[96] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[97] No mechanism is needed to transfer personal data from the data subject to Company A.
- Transfer 2: Safeguard may be required. If Company A is subject to the GDPR (e.g., it offers goods or services to data subjects in the European Union or monitors their behavior in the European Union) then Company A is required to comply with the cross-border transfer restrictions in GDPR Chapter V when transferring personal data "to a third country."[98] The European Commission has suggested that transfers to another company "in the same [non-EEA] country," should utilize a safeguard mechanism such as the SCCs.[99] In this situation the parties should consider the use of SCC Module 1 for transfers from a controller to another controller. Note that if Company A is not subject to the GDPR, then no additional steps need to be taken in order to transfer personal data to Company B.
- Transfer Impact Assessments. If the parties utilize SCC Module 1, Clause 14 of the SCCs would require Company A and Company B to conduct a TIA to analyze various risks that may result from the transmission of data to a second controller in Country Q.
- Law Enforcement Request Policy. If no SCCs are signed, neither Company A nor Company B would be directly subject to Clause 15 of the SCCs that require specific steps in the event that a company receives a request from a public authority for access to personal data. If the parties utilize SCC Module 1, Company B might consider putting in place a law enforcement request policy as part of demonstrating its compliance with Clause 15.

10.3 Data Subject (EEA) → Controller A (Non-EEA) → Controller B (Non-EEA) (separate country)

Visual

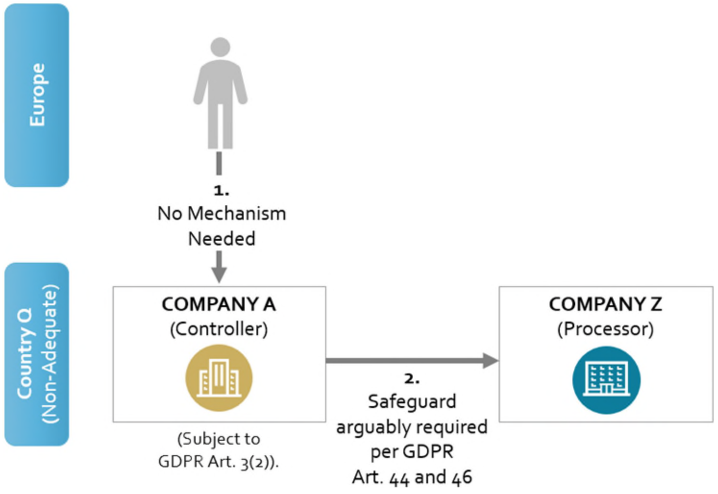


Description and Implications

- Background. Company A, located in Country Q, collects data directly from a data subject, located in the EEA. Company A onward transfers the data to Company B, located in Country R. it is assumed that the data subject is operating in a personal (as opposed to work or commercial) capacity.
- Transfer 1: No mechanism required. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[100] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[101] As a result no mechanism is needed to transfer personal data from the data subject to Company A.
- Transfer 2: Safeguard may be required. If Company A is subject to the GDPR (e.g., it markets products or services to individuals in the EEA) then Company A is required to comply with the cross-border transfer restrictions in GDPR Chapter V when transferring personal data "to a third country."[102] In this situation the parties should consider the use of SCC Module 1 for transfers from a controller to another controller. Note that if Company A is not subject to the GDPR, then no additional steps need to be taken in order to transfer personal data to Company B.
- Transfer Impact Assessments. If the parties utilize SCC Module 1, Clause 14 of the SCCs would require Company A and Company B to conduct a TIA to analyse various risks that may result from the transmission of data to Country R.
- Law Enforcement Request Policy. If no SCCs are signed, neither Company A nor Company B would be directly subject to Clause 15 of the SCCs that require specific steps in the event that a company receives a request from a public authority for access to personal data. If the parties utilize SCC Module 1, Company B might consider putting in place a law enforcement request policy as part of demonstrating its compliance with Clause 15.

10.4 Data Subject (EEA) → Controller A (Non-EEA) → Processor Z (Non-EEA) (same country)

Visual

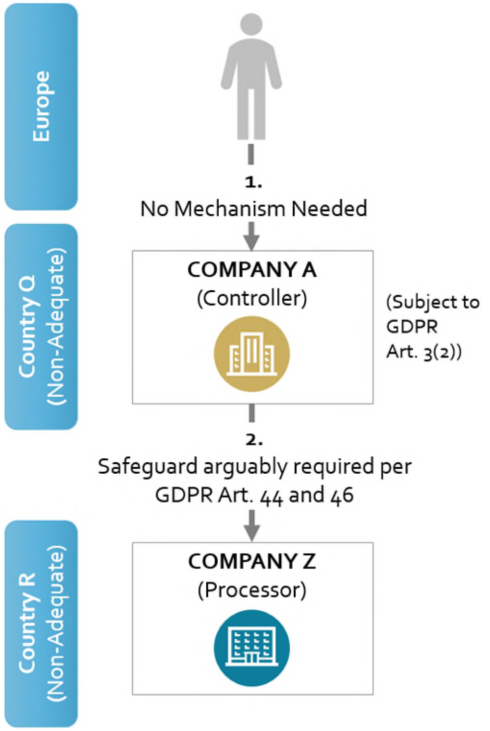


Description and Implications

- Background. Company A, located in Country Q, collects data directly from a data subject, located in the EEA. Company A onward transfers the data to its processor, Company Z, also located in Country Q. Note that in this example it is assumed that the data subject is operating in a personal (as opposed to work or commercial) capacity.
- Transfer 1: No mechanism required. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[103] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[104] As a result no mechanism is needed to transfer personal data from the data subject to Controller A.
- Transfer 2: Safeguard may be required. If Company A is subject to the GDPR (e.g., it markets products or services to individuals in the EEA) then Company A is required to comply with the cross-border transfer restrictions in GDPR Chapter V when transferring personal data "to a third country."[105] The European Commission has suggested that transfers to another company "in the same [non-EEA] country," should utilize a safeguard mechanism such as the SCCs.[106] In this case the parties should consider the use of SCC Module 2 for transfers from a controller to a processor. Note that if Company A is not subject to the GDPR, then no additional steps need to be taken in order to transfer personal data to Company B.
- Transfer Impact Assessments. If the parties utilize SCC Module 2, Clause 14 of the SCCs would require Company A and Company Z to conduct a TIA to analyze various risks that may result from the transmission of data a second controller in Country Q.
- Law Enforcement Request Policy. If no SCCs are signed, neither Company A nor Company B would be directly subject to Clause 15 of the SCCs that require specific steps in the event that a company receives a request from a public authority for access to personal data. If the parties utilize SCC Module 2, Company Z might consider putting in place a law enforcement request policy as part of demonstrating its compliance with Clause 15.

10.5 Data Subject (EEA) → Controller A (Non-EEA) → Processor Z (Non-EEA) (different country)

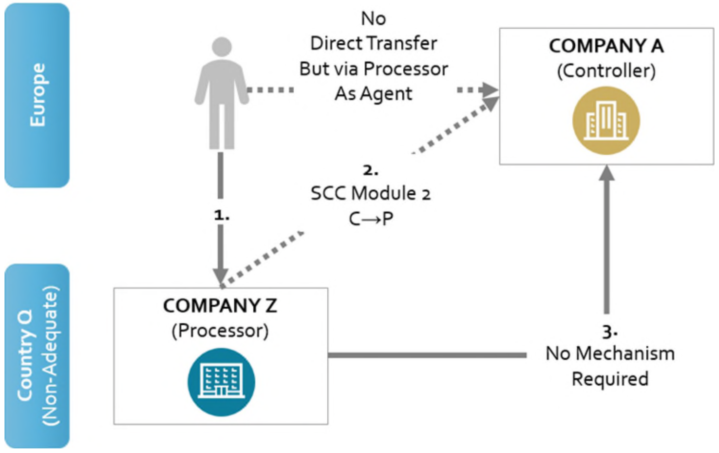
Visual	Description and Implications



- Background. Company A, located in Country Q, collects data directly from a data subject, located in the EEA. Company A onward transfers the data to its processor, Company Z, located in Country R. Note that in this example it is assumed that the data subject is operating in a personal (as opposed to work or commercial) capacity. Note that in this example it is assumed that the data subject is operating in a personal (as opposed to work or commercial) capacity.
- Transfer 1: No mechanism required. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[107] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[108] As a result no mechanism is needed to transfer personal data from the data subject to Controller A.
- Transfer 2: Safeguard may be required. If Company A is subject to the GDPR (e.g., it markets products or services to individuals in the EEA) then Company A is required to comply with the cross-border transfer restrictions in GDPR Chapter V when transferring personal data "to a third country."[109] In this situation the parties should consider the use of SCC Module 2 for transfers from a controller to a processor. Note that if Company A is not subject to the GDPR, then no additional steps need to be taken in order to transfer personal data to Company Z.
- Transfer Impact Assessments. If the parties utilize SCC Module 2, Clause 14 of the SCCs requires Company A and Company Z to conduct a TIA to analyze various risks that may result from the transmission of personal data to Country R.
- Law Enforcement Request Policy. If no SCCs are signed, neither Company A nor Company Z would be directly subject to Clause 15 of the SCCs that requires specific steps in the event that a company receives a request from a public authority for access to personal data. If the parties utilize SCC Module 2, Company Z might consider putting in place a law enforcement request policy as part of demonstrating its compliance with Clause 15.

10.6 Data Subject (EEA) → Processor Z (Non-EEA) → Controller A (EEA)

Visual



Description and Implications

- <u>Background</u>. Company A retains Company Z (non-EEA) to collect personal information from data subjects on its behalf. In this scenario the data subject is directly transferring personal information to a processor that is not in the EEA, but that processor is acting at the instruction of a controller that is in the EEA. The solid line indicates the data flow; the dashed line indicates the contractual relationship.
- <u>Transfer 1 and Transfer 2: Possible use of SCC Module 2.</u> The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[110] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[111] However, because Company Z is working on behalf, and at the direction of, Company A, an argument could be made that the data subject is not making the decision to directly transfer personal data outside of the EEA – that decision has been made by Company A. Based upon that rationale, Company A and Company Z might consider utilizing SCC Module 2 wherein Company A would conceptualize itself as constructively exporting personal data from the EEA to its processor in Country Q.
- <u>Transfer 3: No Mechanism</u>. The GDPR does not require a company that transmits data from a non-adequate country to the EEA to utilize a safeguard mechanism. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.
- <u>Transfer Impact Assessments.</u> If the parties utilize SCC Module 2, Clause 14 of the SCCs requires Company A and Company Z to conduct a TIA to analyze various risks that may result from the transmission of data to Country Q.
- <u>Law Enforcement Request Policy</u>. If the parties utilize SCC Module 2, Company Z might consider putting in place a law enforcement request policy as part of demonstrating its compliance with Clause 15.

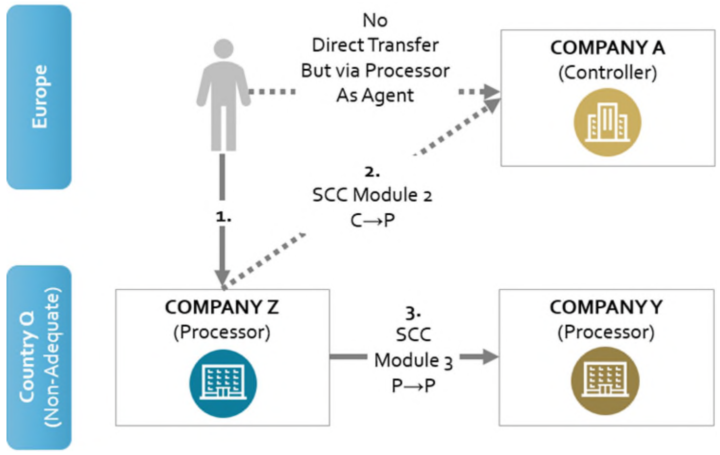
10.7 Data Subject (EEA) → Processor Z (Non-EEA) → Processor Y (Non-EEA)

Background. Company A retains Company Z in Country Q to process personal data (e.g., collect personal data from data subjects). Company A instructs Company Z to transmit the personal data to Company Y, which is a second processor in Country Q. There are two general strategies for how the transfer could be structured.

Visual

Description and Implications

Option 1

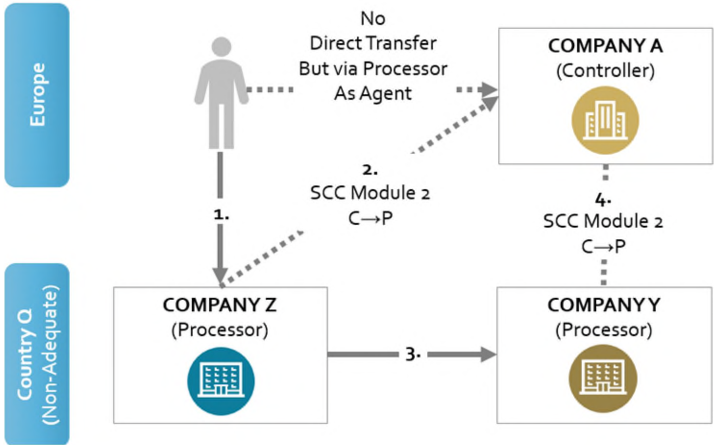


- Transfer 1 and Transfer 2: Possible use of SCC Module 2. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[112] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[113] As a result, an argument could be made that no mechanism is needed to transfer personal data from the data subject to Company Z. However, because Company Z is working on behalf, and at the direction of, Company A, an argument could be made that the data subject is not making the decision to directly transfer personal data outside of the EEA – that decision has been made by Company A. Based upon that rationale, Company A and Company Z might consider utilizing SCC Module 2 (First SCC) wherein Company A would conceptualize itself as constructively exporting personal data from the EEA to its processor in Country Q.
- Transfer 3: Possible use of SCC Module 3. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions must also utilize the SCCs (appropriate module). According to Clause 8.7, transfers "in the same [non-EEA] country," should also utilize a safeguard mechanism such as the SCCs.[114] In this case the transfer from Company Z to Company Y could be conceptualized either as a processor-to-processor transfer (where Company Y is acting at the direction of Company Z), or as a controller-to-processor transfer (where Company Y is acting at the direction of Company A). The former structure (depicted to the left) might be most appropriate to the extent that Company Y has been selected by Company Z, is a sub-processor of Company Z, and/or takes instruction directly from Company Z.

<table>
<tr><th>Visual</th><th>Description and Implications</th></tr>
<tr><td></td><td>

- Transfer Impact Assessments. If the SCCs are utilized, Clause 14 of the SCCs requires all parties (Company A, Company Z, and Company Y) to document whether any party has reason to believe that the laws and practices of Country Q prevent the data importers (i.e., Company Z and Company Y) from fulfilling their obligations under the SCCs. The TIA could take the form of a single document reviewed and approve by all parties, or separate documents that reflect the specific factors applicable to Company Z and to Company Y.
- Law Enforcement Request Policy. If the SCCS are utilized, Clause 15 of the SCCs requires the data importers (Company Z and Company Y) to take specific steps in the event that they receive a request from a public authority for access to personal data.

</td></tr>
<tr><td colspan="2">Option 2</td></tr>
<tr><td>



</td><td>

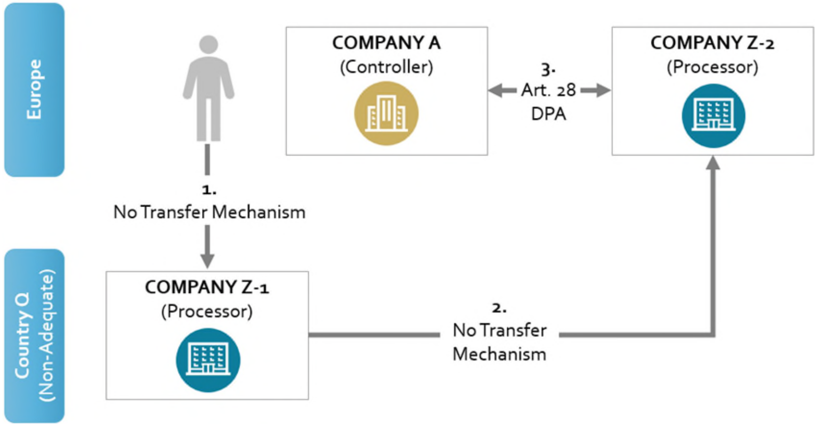
- Transfer 1 and Transfer 2: Possible use of SCC Module 2. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[115] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[116] As a result, an argument could be made that no mechanism is needed to transfer personal data from the data subject to Company Z. However, because Company Z is working on behalf, and at the direction of, Company A, an argument could be made that the data subject is not making the decision to directly transfer personal data outside of the EEA – that decision has been made by Company A. Based upon that rationale, Company A and Company Z might consider utilizing Module 2 (First SCC) wherein Company A would conceptualize itself as constructively exporting personal data from the EEA to its processor in Country Q.
- Transfer 3 and Transfer 4: Possible use of SCC Module 2. Pursuant to Clause 8.7 of the First SCC, all subsequent onward transfers to non-adequate jurisdictions must also utilize the SCCs (appropriate module). According to Clause 8.7, transfers "in the same [non-EEA] country," should also utilize a safeguard mechanism such as the SCCs.[117] In this case the transfer from Company Z to Company Y could be conceptualized either as a processor-to-processor transfer (where Company Y is acting at the direction of Company Z), or as a controller-to-processor transfer (where Company Y is acting at the

</td></tr>
</table>

Visual	Description and Implications
	direction of Company A). The latter structure (depicted to the left) might be most appropriate to the extent that Company Y has been selected by Company A, is a direct processor of Company A, and/or takes instruction directly from Company A. • Transfer Impact Assessments. If the SCCs are utilized, Clause 14 of the SCCs requires all parties (Company A, Company Z, and Company Y) to document whether any party has reason to believe that the laws and practices of Country Q prevent the data importers (i.e., Company Z and Company Y) from fulfilling their obligations under the SCCs. The TIA could take the form of a single document reviewed and approve by all parties, or separate documents that reflect the specific factors applicable to Company Z and to Company Y. • Law Enforcement Request Policy. If the SCCs are utilized, Clause 15 of the SCCs requires the data importers (Company Z and Company Y) to take specific steps in the event that they receive a request from a public authority for access to personal data.

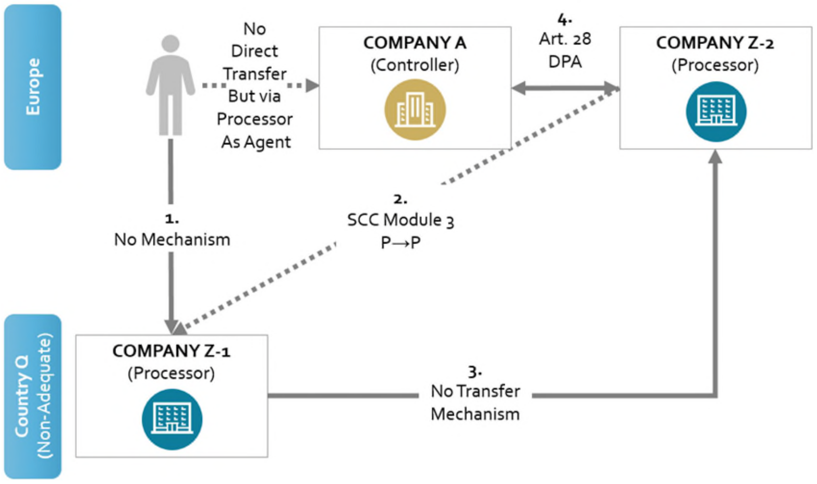
10.8 Data Subject (EEA) → Processor Z-1 (Non-EEA) → Processor Z-2 (EEA) → Controller A (EEA)

Background. Company A retains Company Z-2 (EEA) to collect personal data from data subjects on its behalf. Company Z-2 utilizes its affiliate in Country Q as a sub-processor to collect the personal data. In this scenario the data subject is physically transferring personal information to the sub-processor that is not in the EEA, but that sub-processor is acting at the instruction of the processor, and ultimately the controller, that is in the EEA. There are three strategies for how the transfer could be conceptualized and structured.

Visual	Description and Implications
Option 1	
 Europe Country Q (Non-Adequate) COMPANY A (Controller) 3. Art. 28 DPA COMPANY Z-2 (Processor) 1. No Transfer Mechanism COMPANY Z-1 (Processor) 2. No Transfer Mechanism	• Transfer 1: No Mechanism Needed. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[118] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[119] As a result, no mechanism may be needed to transfer personal data from the data subject to Company Z-1. • Transfer 2: No Mechanism Needed. The GDPR does not require a company that transmits data from a non-adequate country to the EEA to utilize a safeguard mechanism. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed. Note, however, that per Article 28 of the GDPR a written subprocessing agreement must be in place between Company Z-1 and Company Z-2 • Transfer 3: Article 28 DPA. The initial agreement governing the processing of personal data by Company Z-2 on behalf of Company A must be governed by a written contract between Company A and Company Z-2 that complies with the requirements of Article 28 of the GDPR. The GDPR does not, however, require a cross-border transfer safeguard mechanism for data that is transferred from a company in the EEA to another company in the EEA.

Visual | **Description and Implications**

Option 2



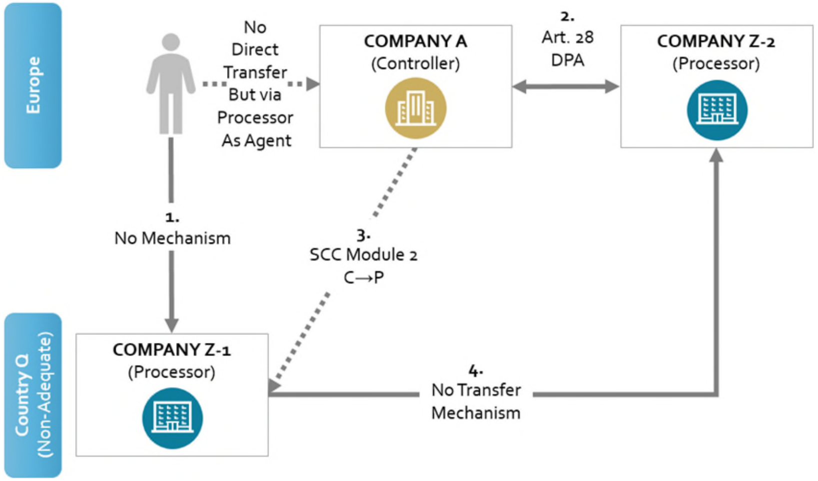
- Transfer 1 and Transfer 2: Possible Use of SCC Module 3. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[120] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[121] However, because Company Z-1 is ultimately working on behalf, and at the direction of, Company Z-2, an argument could be made that the data subject is not making the decision to transfer personal data outside of the EEA – that decision has been made by Company Z-2 (acting at the instruction of Company A). Based upon that rationale, Company Z-2 might consider entering into the SCC Module 3 with Company Z-1 wherein Company Z-2 conceptualizes itself as constructively exporting personal data from the EEA to its sub-processor in Country Q.
- Transfer 3: No Mechanism. The GDPR does not require a company that transmits data from a non-adequate country to the EEA to utilize a safeguard mechanism. Unless Country Q independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed.
- Transfer 4: Article 28 DPA. The initial agreement governing the processing of personal data by Company Z-2 on behalf of Company A must be governed by a written contract between Company A and Company Z-2 that complies with the requirements of Article 28 of the GDPR. For the ultimate transfer of personal data from Company Z-2 to Company A, the GDPR does not require a safeguard mechanism for data that is transferred from a company in the EEA to another company in the EEA (a written contract compliant with Article 28 may be required).
- Transfer Impact Assessments. If Company Z-1 and Company Z-2 utilize SCC Module 3, Clause 14 of the SCCs would require the parties to conduct a TIA to

Visual | **Description and Implications**

analyze various risks that may result from the transmission of data a second controller in Country Q.

- Law Enforcement Request Policy. If Company Z-1 and Company Z-2 utilize SCC Module 3, Company Z-1 might consider putting in place a law enforcement request policy as part of demonstrating its compliance with Clause 15.

Option 3



- Transfer 1 and Transfer 3: Possible use of SCC Module 2. The EDPB has taken the position that a data subject "cannot be considered a controller or processor,"[122] and, as a result, the restrictions on cross-border data transfers that apply to controllers and processors do not apply to data subjects.[123] However, because Company Z-1 is ultimately working on behalf, and at the direction of, Company A, an argument could be made that the data subject is not making the decision to transfer personal data outside of the EEA – that decision has been made by Company A. Based upon that rationale, Company A might consider entering into the SCC Module 2 with Company Z-1 wherein Company A conceptualizes itself as constructively exporting personal data from the EEA to its processor in Country Q.
- Transfer 2 and Transfer 4: Article 28 DPA. The initial agreement governing the processing of personal data by Company Z-2 on behalf of Company A must be governed by a written contract between Company A and Company Z-2 that complies with the requirements of Article 28 of the GDPR. For the ultimate transfer of personal data from Company Z-2 to Company A, the GDPR does not require a safeguard mechanism for data that is transferred from a company in the EEA to another company in the EEA. Similarly the GDPR does not require a company that transmits data from a non-adequate country to the EEA to utilize a safeguard mechanism. Unless Country Q

Visual	Description and Implications
	independently requires a cross-border transfer mechanism, no cross-border transfer mechanism will be needed. • Transfer Impact Assessments. If Company A and Company Z-1 utilize SCC Module 2, Clause 14 of the SCCs requires the parties to conduct a TIA to analyze various risks that may result from the transmission of data a second controller in Country Q. • Law Enforcement Request Policy. If Company A and Company Z-1 utilize SCC Module 2, Company Z-1 might consider putting in place a law enforcement request policy as part of demonstrating its compliance with Clause 15.

11. Endnotes

[1] In 2021, the European Commission also approved a second set of standard contractual clauses that could be used for transfers within Europe (i.e., standard contractual clauses that addressed only Article 28 processor requirements). When this Handbook refers to SCCs it is only referring to the Standard Contractual Clauses intended for use with cross-border transfers of personal information.

[2] Companies are also permitted to transfer personal data outside of the EEA if the transfer is subject to one of the exceptions or "derogations" found within Article 49 of the GDPR (e.g., if the data subject has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers).

[3] The Controller-Controller Set I can be downloaded at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32001D0497 (last viewed 15 June 2022). The Controller-Controller Set II can be downloaded at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915 (last viewed 15 June 2022).

[4] The Controller-Processor Standard Contractual Clauses can be downloaded at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 (last viewed 15 June 2022).

[5] Commission Implementing Decision of 4.6.2021 at Recital 7.

[6] European Commission, The New Standard Contractual Clauses – Questions and Answers *available at* https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf.

[7] Search of secondary sources conducted on Lexis.

[8] Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II), Case No. C-311/18 (2020) at para. 134.

[9] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) 18 June 2021.

[10] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) at para. 30, 18 June 2021.

[11] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) at para. 47-48, 18 June 2021.

[12] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) at para. 47-48, 18 June 2021.

[13] New Standard Contractual Clauses (all Modules) Clause 14(a).

[14] New Standard Contractual Clauses (all Modules) Clause 14(c).

[15] New Standard Contractual Clauses (all Modules) Clause 14(d).

[16] *Schrems II* at para. 134.

[17] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) 18 June 2021.

[18] SCC Clause 14(b)(ii) (all Modules).

[19] SCC Clause 14(b)(ii) (all Modules).

[20] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) adopted on 18 June 2021 at ¶ 37.

[21] SCC Clause 14 (all Modules) fn 12.

[22] SCC Clause 14 (all Modules) fn 12.

[23] SCC Clause 14 (all Modules) fn 12.

[24] SCC Clause 14 (all Modules) fn 12.

[25] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) adopted on 18 June 2021 at ¶ 37.

[26] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) adopted on 18 June 2021 at ¶ 37.

[27] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) adopted on 18 June 2021 at ¶ 37.

[28] SCC Clause 14(b)(i) (all Modules).

[29] SCC Clause 14(b)(i) (all Modules).

[30] SCC Clause 14(b)(i) (all Modules).

[31] SCC Clause 14(b)(i) (all Modules).

[32] SCC Clause 14(b)(i) (all Modules).

[33] SCC Clause 14(b)(i) (all Modules).

[34] SCC Clause 14(b)(i) (all Modules).

[35] SCC Clause 14(b)(i) (all Modules).

[36] SCC Clause 14(b)(i) (all Modules).

[37] SCC Clause 14(b)(iii) (all Modules).

[38] SCC Clause 14(b)(iii) (all Modules).

[39] SCC Clause 14(b)(iii) (all Modules).

[40] *See* New SCC Module 1 at 8.7. The position that a transfer between companies in the same non-EEA country requires a safeguard also accords with Article 44 of the GDPR which requires that "*any* transfer of personal data . . . after transfer to a third country" must take place pursuant to the restrictions in Chapter V of the GDPR.

[41] New SCC Module 1 at 8.7 (similar provisions in Module 2 and Module 3). The position that a transfer between companies in the same non-EEA country requires a safeguard also accords with Article 44 of the GDPR which requires that "*any* transfer of personal data . . . after transfer to a third country" must take place pursuant to the restrictions in Chapter V of the GDPR.

[42] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 15 and 16.

[43] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[44] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[45] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 15 and 16.

[46] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[47] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[48] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 16.

[49] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 16.

[50] GDPR, Art. 44.

[51] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 16.

[52] GDPR, Art. 44.

[53] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 15 and 16.

[54] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 15 and 16.

[55] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[56] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[57] *See* New SCC Module 1 at 8.7. The position that a transfer between companies in the same non-EEA country requires a safeguard also accords with Article 44 of the GDPR which requires that "*any* transfer of personal data . . . after transfer to a third country" must take place pursuant to the restrictions in Chapter V of the GDPR.

[58] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[59] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[60] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[61] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[62] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[63] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[64] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[65] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[66] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[67] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[68] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[69] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[70] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[71] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[72] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[73] GDPR, Art. 28(3)(a). *See also* EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, at paras. 116 and 117.

[74] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 16.

[75] GDPR, Art. 28(3)(h).

[76] GDPR, Art. 28(3)(a). *See also* EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, at paras. 116 and 117.

[77] GDPR, Art. 28(3)(a). *See also* EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, at paras. 116 and 117.

[78] Commission Implementing Decision of 4.6.2021 at para. 3.

[79] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 13.

[80] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 13.

[81] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 13.

[82] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 13.

[83] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 13.

[84] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 13.

[85] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[86] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[87] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[88] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[89] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[90] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[91] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at paras. 14, 15.

[92] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[93] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 17.

[94] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[95] *See* GDPR, Article 2(2)(c).

[96] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[97] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[98] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 10.

[99] New SCC Module 1 at 8.7 (similar provisions in Module 2 and Module 3). The position that a transfer between companies in the same non-EEA country requires a safeguard also accords with Article 44 of the GDPR which requires that "*any* transfer of personal data . . . after transfer to a third country" must take place pursuant to the restrictions in Chapter V of the GDPR.

[100] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[101] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[102] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 10.

[103] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[104] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[105] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 10.

[106] New SCC Module 1 at 8.7 (similar provisions in Module 2 and Module 3). The position that a transfer between companies in the same non-EEA country requires a safeguard also accords with Article 44 of the GDPR which requires that "*any* transfer of personal data . . . after transfer to a third country" must take place pursuant to the restrictions in Chapter V of the GDPR.

[107] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[108] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[109] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at para. 10.

[110] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[111] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[112] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[113] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[114] *See* New SCC Module 1 at 8.7. The position that a transfer between companies in the same non-EEA country requires a safeguard also accords with Article 44 of the GDPR which requires that "*any* transfer of personal data . . . after transfer to a third country" must take place pursuant to the restrictions in Chapter V of the GDPR.

[115] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[116] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[117] *See* New SCC Module 1 at 8.7. The position that a transfer between companies in the same non-EEA country requires a safeguard also accords with Article 44 of the GDPR which requires that "*any* transfer of personal data . . . after transfer to a third country" must take place pursuant to the restrictions in Chapter V of the GDPR.

[118] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[119] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[120] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[121] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).

[122] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR at n.10.

[123] The transfer of data from Europe to the United States arguably constitutes "processing" by the data subject and, therefore, is not subject to the GDPR at all, as the regulations do not apply to processing done by a "natural person in the course of a purely personal or household activity. GDPR, Art. 2(2)(c).