Calamu Technologies Corporation
White Paper 02/2021

Data Harbor in a Storm: EU Recommends Supplemental Security Measures Offered by Calamu for Data in the Cloud

Abstract

The Schrems II decision by the Court of Justice of the European Union in July 2020 invalidated the EU-US Privacy Shield framework and suggested a solution to a stalemate with the US over its ability to obtain European's personal data indirectly through cloud platforms subject to US jurisdiction. The decision held that Standard Contractual Clauses should be strengthened to include obligations to implement supplementary measures to provide a level of protection on cloud platforms essentially equivalent to that required in Europe.

This White Paper examines these supplemental measures, and the extent to which organizations that store European personal data using Calamu Protect may be compliant with three of the Use Cases set forth in recommendations issued in November 2020 by the European Data Protection Board.

Calamu is a data protection platform that forms a safe data harbor for computer data. Processed data is immune to the impacts of a data breach and greatly simplifies compliance with the GDPR. This White Paper is authored by the Calamu team with assistance from Patrick Burke (Partner, Phillips Nizer LLP) and Marla Crawford (General Counsel, Compliance).

 |

Table of Contents

I. Overview: Calamu's Data Harbor Meets the GDPR Moment **3**

II. The Cross-Border Regulatory Stalemate That Led The EU To Embrace "Supplementary Measures" Including Advanced Encryption **3**

III. Schrems II: CJEU Invalidated Privacy Shield, Points Regulators Toward SSCs With Supplementary Measures **5**

IV. Europeans Update SCCs and Recommend Supplementary Technical Measures To Prevent US Authorities From Obtaining Readable Personal Data From Cloud Platforms **5**

V. How Calamu Prevents Governmental Authorities Reading Personal Data Obtained From Cloud Platforms **7**

VI. EDPB's Recommendation Annex Offers Examples of Supplementary Measures **7**

VII. Conclusion: Calamu Protect Security and GDPR Compliance Within a Data Harbor **9**

Appendix **11**

Legal Disclaimer

I. Overview: Calamu's Data Harbor Meets the GDPR Moment

European data protection officials have a strong mandate for companies transferring and storing the personal data of EU citizens in cloud platforms located in the United States ("US"): implement "supplementary measures" to render the data as protected as it would have been in the European Union ("EU") countries that the General Data Protection Regulation ("GDPR") protects. Organizations are consequently seeking effective supplementary measures to improve their data security. One way to protect personal data sent to the US under GDPR is to create a safe "Data Harbor" on cloud platforms subject to US jurisdiction. Such a Data Harbor would virtually hold the personal data and protect it from unauthorized access using robust cybersecurity measures, including advanced encryption.

Calamu creates a secure "Data Harbor" that defies the conventional concept of jurisdiction. In effect, Calamu'd data ceases to exist in readable form anywhere.

Calamu offers just the sort of protection described by the European data protection authorities: a safe harbor where data cannot be stolen by hackers or surreptitiously acquired by US law enforcement or intelligence agencies outside of the treaty-approved EU-US Mutual Legal Assistance Treaty ("MLAT"). Calamu creates a secure "Data Harbor" that defies the conventional concept of jurisdiction. In effect, Calamu'd data ceases to exist in readable form anywhere. This is because the data held in a Calamu Data Harbor is fragmented, securely encrypted and subject to strict, detailed permissions. In order to make the data readable, it must be decrypted and reassembled by the Calamu platform.

This White Paper will examine how the July 2020 Schrems II decision invalidated the widely adopted EU-US Privacy Shield framework and encouraged the use of Standard Contractual Clauses ("SCCs") that led to (1) the European Commission's issuance of updated SCCs and (2) the European Data Protection Board's ("EDPB") publication of recommendations providing a roadmap for organizations to implement compliant "supplementary measures." Of particular interest to the EDPB are cloud environments in countries such as the US, where there is a need to create a secure layer of protection over the data, in essence a "Data Harbor." Calamu fits squarely within various Use Cases detailed in the Annex to the EDPB Recommendations (see full text in Appendix). As described below, Calamu provides ingenious and effective supplementary technical measures that exceed the EDPB's Recommendations.

II. The Cross-Border Regulatory Stalemate That Led The EU To Embrace "Supplementary Measures," Including Advanced Encryption

In late 2020, the European Commission[1] and the EDPB[2] faced a regulatory challenge that threatened becoming a stalemate. They sought to solve the problem of allowing Europeans' personal data to continue to be transferred and stored on US-

1 The European Commission is the executive branch of the EU, responsible for proposing legislation, implementing decisions, upholding EU treaties, and managing the day-to-day business of the EU.

2 The EDPB is composed of representatives of 27 EU Member States and 3 European Economic Area nations, charged to ensure consistent application of the European Union's GDPR.

controlled cloud platforms. The concern was that US government entities could collect data through back-door methods without notification to those defined under GDPR as controllers, processors, or European data subjects.
Over recent years, US authorities expanded their collection of data directly from cloud storage providers. Neither the customers of these cloud providers nor the Europeans' whose personal data was acquired by US law enforcement and agencies had knowledge of their access.

Since the passage of the Foreign Intelligence Surveillance Act ("FISA") in 1978, US federal law enforcement and intelligence agencies (primarily the Federal Bureau of Investigation and the National Security Agency) have utilized a special FISA Court to adjudicate requests for surveillance warrants. With FISA Court approval, US authorities could obtain email communications and other data from cloud storage platforms in their pursuit of national security threats.

US federal law enforcement can also reach data on cloud platforms with warrants approved by US federal courts. It was one such federal warrant issued in 2013 under Section 2703 of the Stored Communications Act[3] ("SCA") directed at Microsoft that prompted a significant shift in the law. That warrant sought the email of a targeted account stored on Microsoft's servers in Ireland. Microsoft challenged the legality of the warrant in court, arguing that the Stored Communications Act could not compel American companies to produce data stored in servers outside of the United States.[4] When Microsoft's legal challenge to the US government's request for the target's e-mail reached the US Supreme Court in 2018, Congress stepped in and passed the Clarifying Lawful Overseas Use of Data Act ("The US Cloud Act"), which explicitly amended the SCA to permit warrants seeking data stored outside of the US. The enactment of the US Cloud Act mooted Microsoft's Supreme Court case (the US government won).[5]

The US Cloud Act[6] requires companies operating cloud platforms to provide US authorities with data sought by warrants regardless of the jurisdiction in which the server is located – allowing the US to acquire European's personal data on Europe-based cloud platforms when the cloud platform is controlled by companies subject to US jurisdiction.

The US Cloud Act's global jurisdictional reach directly contradicts the requirement in GDPR Article 48 that Europeans' personal data should only be obtained by foreign sovereigns in the manner established by treaty between the US and the EU, specifically, the MLAT. US law enforcement and intelligence agencies, however, often prefer avoiding the cumbersome MLAT process, and seek to obtain the data directly through the cloud storage providers by serving warrants that do not require any notification to the cloud customers whose data is exfiltrated.

In addition, the EU data protection authorities are concerned that US agencies could obtain Europeans' personal data that is exported to the US and stored in the controller or processor's cloud storage without any notice to the controller or processor, thereby obviating the EU citizens' fundamental data privacy rights.

---

3 18 U.S. Code §2703.

4 After the US's warrant was upheld against Microsoft's motion to quash by a US Magistrate Judge and a US District Court, the Court of Appeals for the Second Circuit reversed the denial of the motion to quash, holding that requiring Microsoft to disclose the electronic communications in question would be an unauthorized extraterritorial application. See *In re Warrant To Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp.,* 829 F.3d 197, 204–205 (C.A.2 2016).

5 US v. Microsoft Corporation, 138 S. Ct. 1186, 200 L. Ed. 2d 610 (April 17, 2018) (holding case mooted by the US Cloud Act amendments to the Stored Communications Act).

6 H.R. 1625: Consolidated Appropriations Act, 2018, Enacted — signed by President Trump on March 23, 2018.

III. Schrems II Decision: CJEU Invalidates Privacy Shield, Points Regulators Toward Standard Contractual Clauses with Supplementary Measures

The seminal Schrems II decision[7] arose out of a litigation brought by the Austrian privacy activist, Maximillian Schrems. Schrems alleged a violation of his fundamental human right of data privacy as a result of the EU's tolerance of the US government's ready access to his personal data. His case is referred to as Schrems II in recognition of his prior successful lawsuit that resulted in the invalidation of the EU-US Safe Harbor mechanism, the predecessor to the EU-US Privacy Shield framework.[8]

The Court of Justice of the European Union ("CJEU") ruled in July 2020 and agreed with enough of Schrems' concerns about US government access to Europeans' data to invalidate the popular EU-US Privacy Shield framework. The Privacy Shield, which had been a widely used legal mechanism under the European Union's GDPR, authorized US organizations to store Europeans' personal data on US cloud platforms. In invalidating the Privacy Shield, the Court held that it did not protect the privacy rights of EU citizens because it failed to require supplementary security measures to prevent US authorities from collecting decrypted copies of Europeans' personal data. The Court found that while the US was treaty-bound to seek Europeans' data exclusively through the MLAT, it was nonetheless obtaining Europeans' personal data directly from those cloud platforms without notice to the Europeans whose personal data was obtained. The US Cloud Act had extended the US authorities' jurisdictional wingspan, allowing them to reach data worldwide in violation of the GDPR. With the Privacy Shield transfer tool invalidated, the CJEU encouraged a more rigorous approach via another transfer tool: SCCs.

IV. Europeans Update Standard Contractual Clauses and Recommend Supplementary Technical Measures To Prevent US Authorities From Obtaining Readable Personal Data From Cloud Platforms

The CJEU's Schrems II affirmation of SCCs encouraged the European data protection bureaucracy to craft a solution to protect Europeans' personal data from acquisition by the US government through cloud platforms. Their suggested fix: The GDPR would support storage of European personal data on cloud platforms susceptible to US warrants ***if*** the exporter agreed to employ "supplementary measures" to protect the data during transfer and storage from US surveillance on cloud platforms, including advanced data security techniques. Export could be in compliance with the EU GDPR if the exporter creates a "Data Harbor" that provides a level of protection "essentially equivalent" to that required under the GDPR, and capable of preventing US authorities from obtaining the data in readable, unencrypted form. The effect is to neutralize US authorities' ability to assert its jurisdiction over the data without transparency.

7 Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ("Schrems II"), C311/18.

8 Judgement of 6 October 2015, Maximilian Schrems v Data Protection Commissioner ("Schrems I"), C-362/14.

The EU's public encouragement of safe, cloud-based Data Harbors – promoting the use of SCCs that provide for the use of "supplementary measures" to ensure protection from US government data collection – was announced in November 2020:

1. The EDPB publicly adopted its "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" ("EDPB Recommendations"). These include specific "use cases" that describe various characteristics of a Data Harbor. The EDPB Recommendations focused on one of the few GDPR mechanisms still available to data exporters to the US, data transfer agreements known as Standard Contractual Clauses, recommending that such agreements include "supplemental transfer tools" that would foil US government attempts to gain Europeans' personal data directly from the operators of the cloud platforms where the data is transferred and stored. These recommended "supplementary measures" would permit the European personal data to be stored on US-controlled cloud platforms only if it is maintained in encrypted formats that would deny US authorities the ability to read it; and,

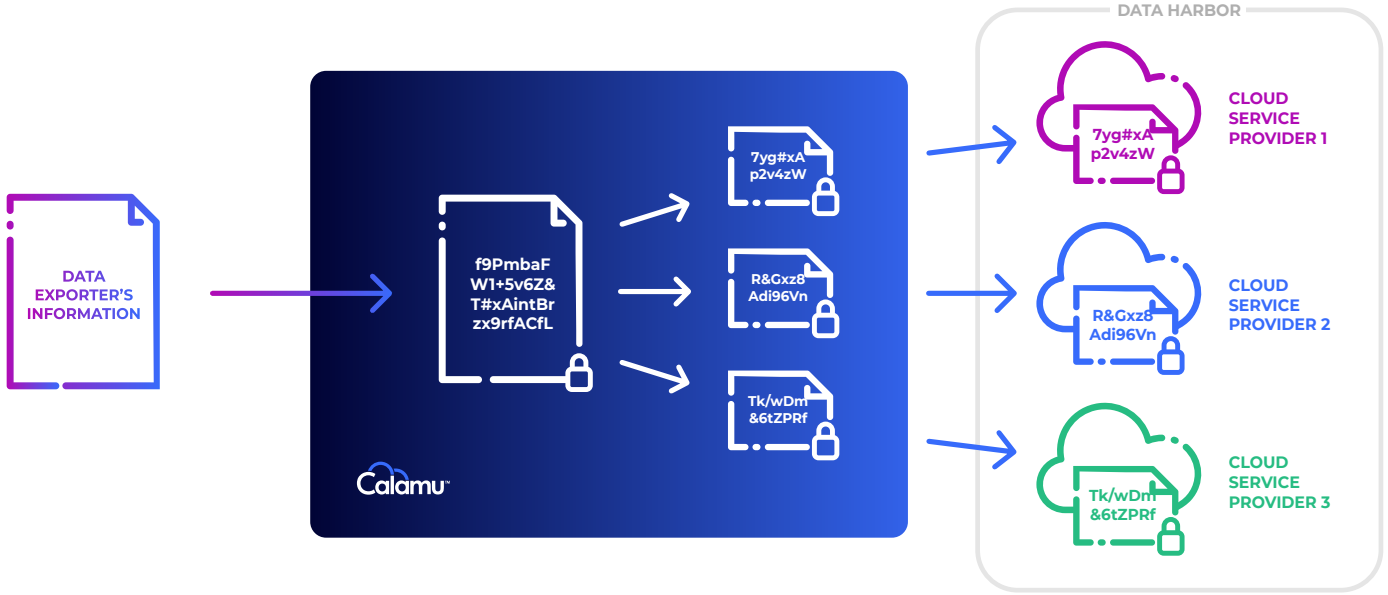
2. The European Commission released updated SCCs for consultation, updated versions of approved SCCs – the first updates since the GDPR went into effect in May 2018. Moreover, these encourage supplementary technical or organizational measures to ensure security and confidentiality, including an implied expectation for "supplementary measures" to be implemented based on the EDPB Recommendations.

Taken together, the EU's pragmatic approach requires exporters of Europeans' personal data to verify whether the law or practice of the third country where the data would be stored in any way impinges on the effectiveness of appropriate safeguards contained in the GDPR Article 46 transfer tools. The EDPB Recommendations effectively describe supplementary measures that would constitute a GDPR-compliant Data Harbor for European personal data on US-controlled cloud platforms and ensure that the transfer and storage of EU data meets the essentially equivalent level of protection that EU law requires.

Three of the EDPB's recommended "supplementary measures" describe methods for preventing the US authorities from obtaining usable data from cloud platforms (these are set out in the Appendix to this White Paper). As discussed below, these "supplementary measures" largely describe the features offered by Calamu.

In short, European data regulators – taking a cue from the CJEU's Schrems II decision – have reached a conclusion: if European's personal data is to be sent abroad to reside on US cloud platforms, those exporters must create a safe "Data Harbor". This Data Harbor would contain the personal data, but protect it from surveillance using effective cybersecurity measures, including advanced encryption.

V. How Calamu Protects EU Data on Cloud Platforms



1. Data Exporter's information (native data).

2. The data exporter's Information is hashed, compressed, encrypted, and fragmented using Calamu.

3. The fragments are scattered to independent cloud service providers creating a data harbor.

Figure 1 - Calamu process example of protecting data using a Data Harbor.[9]

VI. EDPB's Recommendation Annex Offers Examples of Supplementary Measures

The EDPB's Recommendation Annex clarifies how exporters can transfer and store Europeans' personal data on cloud platforms subject to US jurisdictional reach by following the guidance in Schrems II in favor of SCCs with "supplementary measures." These supplementary technical measurements "will be especially needed where the law of that country imposes on the data importer obligations which are contrary to the safeguards of Article 46 GDPR transfer tools and are, in particular, capable of impinging on the contractual guarantee of an essentially equivalent level of protection against access by the public authorities of that third country to that data."[10]

9 This figure depicting the Calamu process is a simplified version of a complex process. For those interested in a deeper understanding of the process, please contact Calamu for a demonstration.

10 EDPB Recommendations Annex at §72.

The EDPB Recommendations Annex details seven Use Cases of "supplementary technical measures" that data exporters may use in combination with SCCs in order to comply with the GDPR for the transfer and storage of data on US cloud platforms. At least three of these Use Cases cover various technical measures addressed by Calamu that would support compliance with the GDPR under various circumstances (these are set forth in the Appendix to this white paper). The Annex makes clear that the Use Cases "describe specific circumstances, and measures taken. Any changes to the scenarios may give rise to different conclusions."[11]

Three of the Use Cases describe technical measures offered by use of Calamu's current technology:

> **Use Case No. 1: Data storage for backup and other purposes that do not require access to data in the clear.** "A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes."
>
> **Use Case 3: Encrypted data merely transiting third countries.** "If a data exporter transfers personal data to a data importer in a jurisdiction ensuring adequate protection, the data is transported over the internet, and the data may be geographically routed through a third country not providing an essentially equivalent level of protection."
>
> **Use Case 5: Split or multi-party processing.** "The data exporter wishes personal data to be processed jointly by two or more independent processors located in different jurisdictions without disclosing the content of the data to them. Prior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part. The data exporter receives the result of the processing from each of the processors independently, and merges the pieces received to arrive at the final result which may constitute personal or aggregated data."

The three Use Cases above can be satisfied by the use of Calamu's platform (see full text in Appendix). By using Calamu, the data is hashed, encrypted, fragmented, re-encrypted, and scattered to separate cloud service providers. Calamu's technology utilizes industry standard and certified methods to perform hashing, encryption, key management and secure transmission of the data. Calamu's proprietary, patented technology contains built-in randomization so that no two fragments are alike, and the data is segregated in a manner that eliminates the possibility of reconstructing the data contained within any one cloud service provider should it be accessed by an unauthorized third-party. Further, Calamu's technology is designed to automatically heal the data should any one cloud service provider become compromised due to a data breach or outage while also benefiting from no downtime or data loss. Beyond the ability to simply store data for backup or archival purposes, Calamu's technology can also be used to securely and privately transfer data between two parties while supporting overall compliance.

Adoption of Calamu technology as part of supplementary measures can also bring compliance advantages from elsewhere in the GDPR. For example, discussing compliant "prior measures and risk assessment" with respect to ransomware risks in the EDPB's January 14, 2021 "Guidelines 01/2021 on Examples regarding Data Breach Notification,"[12] the guidelines state:

---

11 EDPB Recommendations Annex at §77.

12 See Guidelines 01/2021 on Examples regarding Data Breach Notification by EDPB.

> "In this example, the attacker had access to personal data and the confidentiality of cipher text containing personal data in encrypted form was compromised. However, any data that might have been exfiltrated cannot be read or used by the perpetrator, at least for the time being. The encryption technique used by the data controller conforms to the state-of-the-art. The decryption key was not compromised and presumably could also not be determined by other means. In consequence, the confidentiality risks to the rights and freedoms of natural persons are reduced to a minimum barring cryptanalytic progress that renders the encrypted data intelligible in the future"[13]

Calamu's Data Harbor protects data from being breached or hacked consistent with GDPR guidance, as well as other data protection laws and regulations around the US and the world.

VII. Conclusion: Calamu Provides Security and Supports GDPR Compliance Within a Data Harbor

Calamu's technology enables organizations to securely move European personal data to cloud storage platforms subject to US jurisdiction while supporting compliance with the GDPR. The Court of Justice of the European Union's July 2020 Schrems II decision – while invalidating the EU-US Privacy Shield framework – pointed the way for lawful adaptation of SCCs to counteract the US government's expanding claim of jurisdiction over data held on cloud platforms controlled by companies subject to US jurisdiction.

The EDPB's November 2020 Recommendations set out seven "Use Cases" providing "supplementary measures" providing a level of protection "essentially equivalent" to that required under the GDPR. Three of the EDPB Recommendations' Use Cases – pertaining to transfer to, and storage on, cloud platforms and dividing data among multiple platforms – describe technical capabilities currently offered by Calamu.

Calamu enables organizations to create a protected virtual environment, called a Data Harbor, which fits within the recommended Use Cases. Calamu'd data is not only encrypted, it is decomposed into encrypted fragments spread over at least three physically separate cloud platforms or servers. Safe in its Data Harbor, Calamu'd data cannot be acquired or read by unauthorized parties because – until reconstituted – the original data no longer exists. And because the file does not exist in any one location, it cannot be intercepted, acquired or revealed without proper authentication.

Moreover, Data Harbors are more resilient than current industry best practices. A breach to any single location is futile, because Calamu automatically detects and disables the breached location. There is virtually no possibility of data manipulation or exfiltration of the original information and downtime or loss of productivity.

Calamu offers a solution to bridge the GDPR compliance gap and to permit the benefits of storing Europeans' personal data in cloud platforms without the risk of GDPR violations. Moreover, Calamu significantly improves the security and confidentiality of the data.

---

13 Id. at §20.

About Calamu

Calamu was founded by leaders in cyber security and data privacy and is managed by experienced executives and an advisory board of industry experts. Our technology eliminates the risk of data breaches and ransomware attacks, and dramatically simplifies regulatory requirements around data privacy and protection.

www.calamu.com

Acknowledgments

Paul Lewis, Founder and CEO of Calamu, and the Calamu team produced this White Paper, and express their appreciation for the valuable analytical contributions of:

Patrick Burke
Partner, Cybersecurity & Data Technology, Phillips Nizer LLP, New York, NY.

Patrick has practiced in data protection and cybersecurity as a corporate in-house lawyer, regulator, law professor and, now, as outside counsel. Prior to launching the Data Technology & Cybersecurity practice at Phillips Nizer, he served as a Deputy Superintendent at the New York State Department of Financial Services ("DFS"), where he founded and headed DFS's Office of Financial Innovation and supervised its cybersecurity examination team. He served seven years as in-house counsel at Guidance Software, and five years on the faculty of the Benjamin N. Cardozo School of Law in Greenwich Village.

Marla Crawford
General Counsel, Compliance, A System One Division, New York, NY.

Marla is a respected attorney, strategic advisor, and thought leader who speaks regularly on legal technology, electronic discovery, and information governance issues. She is currently the General Counsel of Compliance, a System One division, which provides control, innovation, and ease through an innovative suite of legal eDiscovery solutions. Marla spent 22 years practicing law at the prestigious international law firm, Jones Day. She also served as an Associate General Counsel at Goldman Sachs for 11 years where she led the firm's global eDiscovery practice and focused on complex commercial and securities litigation and regulatory investigations. Marla earned a bachelor's degree in public policy from Duke University and graduated magna cum laude from Boston University, where she earned her Juris Doctor.

Appendix (Excerpts from the EDPB Recommendations Annex)

Below is the wording of the three Use Cases from the EDPB Recommendations Annex that describe "supplementary technical measures" that align with the functionality of Calamu Protect.

Use Case No. 1: Data storage for backup and other purposes that do not require access to data in the clear. A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes. If

1. the personal data is processed using strong encryption before transmission,
2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them;
3. The strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved;
4. The encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification;
5. The keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked; and
6. The keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one of more specified sectors within a third country, or at an international organization for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured.

Use Case 3: Encrypted data merely transiting third countries. If a data exporter transfers personal data to a data importer in a jurisdiction ensuring adequate protection, the data is transported over the internet, and the data may be geographically routed through a third country not providing an essentially equivalent level of protection.

1. Transport encryption is used for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of the third country;
2. Decryption is only possible outside the third country in question;
3. The parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure;
4. Specific protective and state-of-the-art measures are used against active and passive attacks on transport-encrypted;
5. In case the transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal data is also encrypted end-to-end on the application layer using state-of-the-art encryption methods,
6. The encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) confirm to the state-of-the-art and can be considered robust against cryptanalysis performed by public authority in the transiting country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them;
7. The strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved;
8. The encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification;

9. The existence of backdoors (in hardware or software) has been ruled out; and
10. The keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked), by the exporter or by an entity trusted by the exporter under a jurisdiction offering an essentially equivalent level of protection.

Use Case 5: Split or multi-party processing. The data exporter wishes personal data to be processed jointly by two or more independent processors located in different jurisdictions without disclosing the content of the data to them. Prior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part. The data exporter receives the result of the processing from each of the processors independently, and merges the pieces received to arrive at the final result which may constitute personal or aggregated data. If:

1. A data exporter processes personal data in such a manner that it is split into two or more parts each of which can be longer be interpreted or attributed to a specific data subject without the use of additional information,
2. Each of the pieces is transferred to a separate processor located in a different jurisdiction,
3. The processors optionally process the data jointly, e.g., using secure multi-party computation, in a way that no information is revealed to any of them that they do not processes prior to the computation,
4. The algorithm used for the shared computation is secure against active adversaries,
5. There is no evidence of collaboration between the public authorities located in the respective jurisdictions where each of the processors are located, which would allow them access to all sets of personal data held by the processors and enable them to reconstitute and exploit the content of the personal data in a clear form in circumstances where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects. Similarly, public authorities of either country should not have the authority to access personal data held by processors in all jurisdictions concerned,
6. The controller has established by means of a thorough analysis of the data in question, taking into account any information that the public authorities of the recipient countries may possess, that the pieces of personal data it transmits to the processors cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.