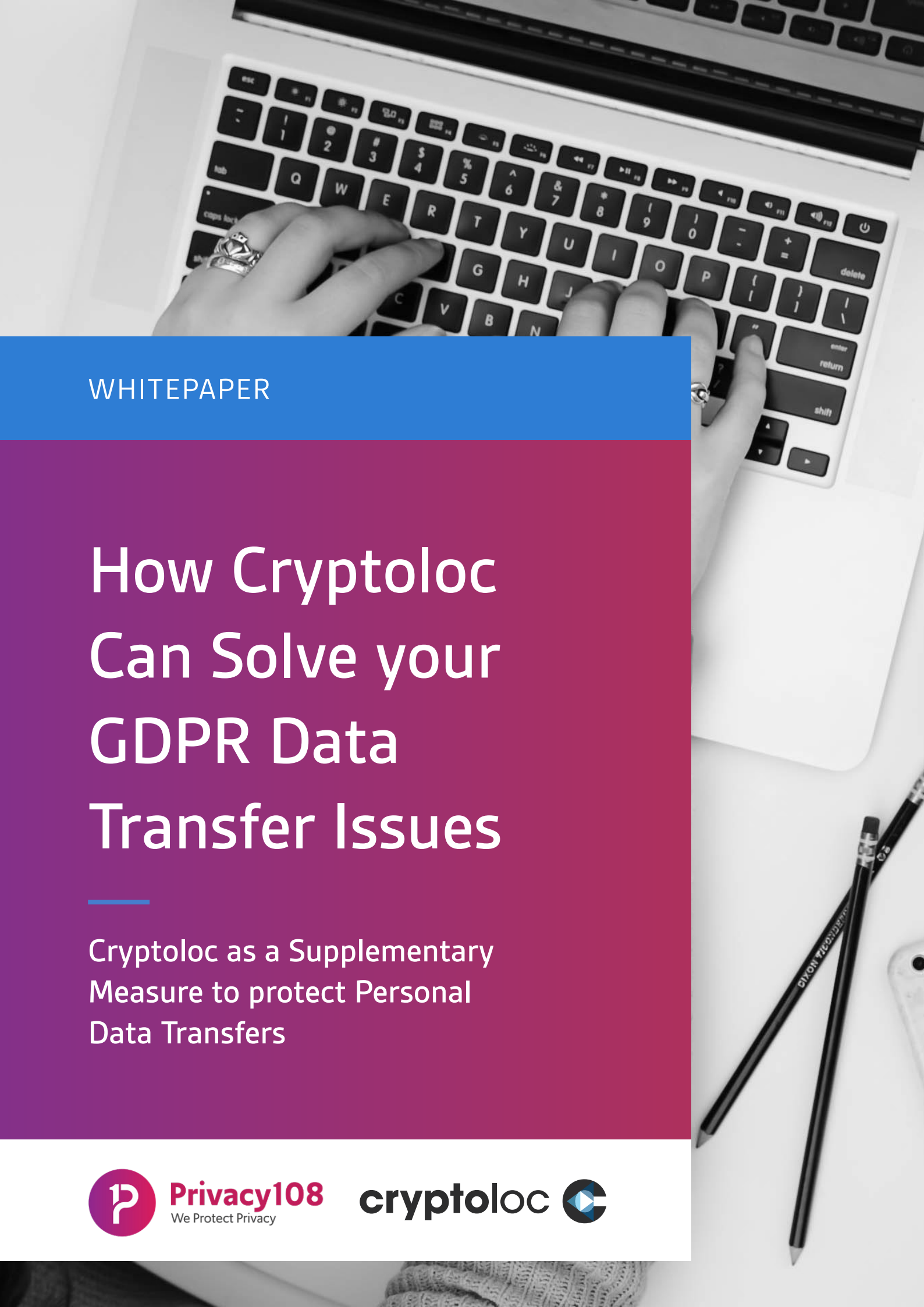


WHITEPAPER

How Cryptoloc Can Solve your GDPR Data Transfer Issues

Cryptoloc as a Supplementary Measure to protect Personal Data Transfers

Privacy108
We Protect Privacy

cryptoloc

Disclaimer

This report (Report) has been produced independently by Dr Jodie Siganto PhD LLM CISSP CIPM CIPP/E of Privacy108 Consulting Pty Ltd on the request of Cryptoloc Technology Group Pty Ltd.

The information, statements, statistics and commentary (together the 'Information') contained in this Report have been prepared by Dr Jodie Siganto from publicly available material and from discussions held with Cryptoloc Technology Group Pty Ltd.

The findings and conclusion of this paper do not constitute legal advice and should not be relied upon as such.

Privacy 108 Consulting Pty Ltd ABN 52 600 425 885 is an incorporated legal practice registered with the Queensland Law Society. Individual liability limited by a scheme approved under Professional Standards Legislation.

Contents

Outline 4

Schrems II Decision 5

Standard Contractual Clauses 5

What are Standard Contractual Clauses? 5

Schrems II and SCCs 6

EDPB Guidance on SCCs, Essential Equivalency and Supplementary Measures 6

SCCs and supplementary measures 7

Encryption as a Supplementary Measure 8

Encryption for storage in a third country 8

Cryptoloc as a Supplementary Measure 9

How does Cryptoloc work? 9

How can Cryptoloc be applied as a technical supplementary measure to the SCC's? 9

What does the Cryptoloc process look like? 10

Cryptoloc and GDPR Requirements 11

Conclusion 11

Outline

The introduction of the General Data Protection Regulation (GDPR)[1] and associated stiffer penalties and increased enforcement activity has highlighted the global importance of ensuring data protection, particularly for entities dealing with personal data on an international basis.

One of the major issues for both the GDPR and other data protection laws is ensuring that protection is not lost by transferring data to an entity in a different jurisdiction and subject to different, less privacy-protective laws.

This has been a particular issue for transfers of data between the EU and the US, where data protection law is more fragmented and sector-based. Regulators from both sides of the Atlantic have previously agreed on systems to ensure the protection of transferred data, with the EU US Safe Harbor originally being established and then replaced by the EU US Privacy Shield program. However, both these arrangements have been found wanting.

In a landmark decision (Schrems II decision) in July 2020, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield as a legal personal data transfer mechanism to cover data transfers from the European Economic Area (EEA) to the US and raised doubts about the sufficiency of the other common basis for data transfers, Standard Contractual Clauses (SCCs).[2] The Schrems II judgement had a seismic impact on all data transfers out of the EU. Many organisations are now looking for steps they can take (such as encryption) to ensure that data transfers are safe from the disruption of similar decisions in the future.

This whitepaper considers the following:

- What are the essential requirements for encryption to be a suitable supplementary measure for transferring data out of the EEA; and
- How the Cryptoloc solution meets those requirements.

Disclaimer: A detailed analysis of the laws of any particular country and the extent to which they may be regarded as not being sufficient for the purposes of data transfers is outside the scope of this paper.

Transatlantic flows of data continue to be the fastest and largest in the world, accounting for over one-half of Europe's data flows and about half of U.S. flows.

'The Transatlantic Economy 2020' – Daniel S. Hamilton and Joseph P. Quinlan Johns Hopkins University Paul H. Nitze School of Advanced International Studies

[1] General Data Protection Regulation (EU) 2016/679

[2] Data Protection Commissioner Facebook Ireland Ltd, Maximillian Schrems (Case C-311/18).

Schrems II Decision

The Schrems II Decision is complex, and much has been written about it.[3] In summary, the CJEU found that interference arising from US surveillance programs (operating pursuant to US laws)[4] did not ensure an equivalent degree of protection for the data of people in the EU being transferred out of the EU to the US. There were two main reasons for this:

- The US government surveillance programs did not grant data subjects actionable rights before the courts against US authorities; and
- There were inadequate remedies available to data subjects to access their personal data or obtain the rectification or erasure of such data.

Consequently, the CJEU found that the Privacy Shield (which was a mechanism agreed between the EU Commission and the Federal Trade Commission to allow for data transfers) did not ensure a level of protection equivalent to that under the GDPR, and thus could no longer be relied upon. In one decision, the main basis for transfer of data from the EU to the US became invalid.

A more detailed explanation of the decision in the Schrems II case is available here.[5]

Aligned to this finding, the CJEU also made some findings regarding Standard Contractual Clauses (SCCs). After the EU US Privacy Shield, SCCs are one of the most commonly used methods to support data transfers out of the EU, including to Australia.

Standard Contractual Clauses

What are Standard Contractual Clauses?

SCCs are one of the mechanisms organisations can use under GDPR to transfer personal data to a third country (i.e. countries outside the EEA that do not have privacy laws affording an essentially equivalent level of protection to the GDPR). SCCs contractually bind third parties that receive the personal data of EU citizens to provide privacy protections consistent with the processing requirements of the GDPR. Many organisations opt to use them as a transfer mechanism.

The SCCs include GDPR mandated data protection provisions, such as support of data subject rights, use of sub-processors, audit rights, data accuracy and minimisation and retention and deletion requirements.

In November 2020, the European Data Protection Board (EDPB) released a new draft version of the SCCs, updating the current clauses to better reflect the use of new and complex processing operations involving multiple parties, complex processing chains and evolving cross-border relationships.

This was a welcomed update in light of the Schrems II Decision, as the new SCC's provide additional safeguards for cross-border data transfers, including obligations on the data importers in third countries in the event of government requests to access data.

The new SCCs require the data importer to notify the data exporter (and data subject, where possible) of a legally binding request from a public authority for disclosure of relevant personal data, or if it becomes aware of any direct access to such data by public authorities. Additionally, there are obligations for the importer to obtain a waiver on any prohibition on notification and to provide the exporter with

[3] See for example:
I) Article by Hunton Andrews Kirth
II) Norton Rose Fulbright Analysis
III) Minter Ellison Analysis
IV) Bird and Bird Analysis
V) Schrems II Tracker

[4] The particular US laws examined as part of the Schrems II decision are reviewed in "SCCs White Paper – US".

[5] "GDPR Cross-border Transfers: Draft SCCs and Supplementary Measures"

the greatest possible amount of information regarding requests received, to the extent permissible.

Binding Corporate Rules (BCRs) have the same effect as the SCCs, however they can only be applied to entities within the same organisational group that are receiving such data.

Schrems II and SCCs

As SCCs and BCRs only bind the parties of the contract (the entities receiving the data), they do not have any impact on the types of government surveillance which the CJEU identified as being problematic and inconsistent with the principles of the GDPR.

In the Schrems II decision, the CJEU emphasized that, although SCCs can be used, before that use, parties must review the laws of the destination country (and in particular the powers of local security agencies) and consider reinforcing the SCCs with additional safeguards (or supplementary measures). This applies to transfers to the US or any other country that the EU considers not to provide an adequate level of data protection i.e. any country where there is not an existing adequacy decision.[6]

The CJEU explained that, to rely on SCCs for such transfers, the exporting organisations must undertake a case-by-case assessment of the transfer to ensure an essentially equivalent level of protection for the EEA personal data under the third country's laws, and that in certain circumstances "supplementary measures" may be necessary to ensure such protection.

The biggest issue post Schrems II is trying to identify which country's laws may be regarded as offering 'essentially equivalent' protection to that provided under the GDPR, and what that might mean. And, if not essentially equivalent, what supplementary measures might be required.

EDPB Guidance on SCCs, Essential Equivalency and Supplementary Measures

Following the Schrems II Decision, the European Data Protection Board (EDPB) has issued guidance on establishing essential equivalency.

The EDPB expects organisations to assess the laws of the data importer's country and any impediment to compliance with transfer obligations. This assessment is becoming known as a 'transfer impact assessment.' In particular, data exporters will have to:

- Verify if data subjects rights in the context of international transfers (such as access, correction and deletion requests for transferred data) can be effectively exercised in practice and are not thwarted by law in the third country of destination; and
- Verify the presence of any relevant laws, which may require disclosure of personal data to public authorities or give public authorities powers of access, and then verify that any such requirements or powers:
  - » are limited to what is necessary and proportionate in a democratic society; and
  - » may not impinge on the commitments contained in the transfer tool the exporter is relying on.

Where that assessment shows that the laws of the importing country are not essentially equivalent, then supplementary measures are required.

Conducting the required foreign law assessment will be challenging in those jurisdictions where data access by public authorities is not regulated in a transparent way or where the regulatory landscape is complex and uncertain. Also, against the backdrop of *Schrems II*, it is hard to see how companies can use the SCCs to transfer personal data to recipients in communist or other countries which may not be truly democratic. Since the assessment test developed in EU case law is that public authority interference should not go beyond what is *"necessary in a democratic society"*, transfers to countries without a democratic foundation appear to be off-limits.

Given these issues with the assessing of foreign laws, the use of supplementary measures becomes even more important.

[6] Countries which have an adequacy determination are listed here: Adequacy decisions | European Commission (europa.eu)

SCCs and supplementary measures

Where it may not be possible to establish that there is essential equivalency, the EDPB has recommended additional safeguards to support SCCs[7], such as encryption and pseudonymisation of data, which would also require that the data cannot be decrypted by national security agencies.[8]

The purpose of these supplementary measures is to elevate the protection afforded to data in the local country so that it rises to the appropriate level of protection under the EU standards.

The supplementary measures at issue may be contractual, technical, and organisational.

The EDPB provides a non-exhaustive list of suggested supplementary measures, including:

- **Technical measures:** such as forms of encryption, and pseudonymisation.
- **Additional contractual measures:** such as obligations to implement the technical measures discussed above, transparency obligations regarding the level of access available to government authorities in the recipient jurisdiction and the measures taken to prevent access to personal data, and reinforced power for the data exporter to conduct audits of the data importer. Non-EU transferees may also be required to review the legality of any access requests received by them and to challenge such requests where appropriate.
- **Organizational measures:** such as adoption of internal policies with clear allocation of responsibilities for data transfers and operating procedures in the event of an access request, transparency and accountability measures including documentation of access requests, and ensuring data minimization.

You may need to combine several measures to ensure the appropriate level of protection, including the use of encryption as a technical measure where the recipient in the third country is exposed only to encrypted data.

It is worth remembering that the CJEU recognised that government intelligence gathering can be a perfectly legitimate aim to process personal data - even if it includes the use of secret surveillance measures - as long as adequate and effective guarantees against abuse are in place.

[7] EDPB Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[8] The adversary in this instance is a nation state so the measures will need to be robust – which may mean cumbersome or expensive to use. U.S. companies should use commercially available encryption, or else they may need a special license to export the software, since U.S. export laws regard such unique software as a "munition" under 15 C.F.R. 742.15.

Encryption as a Supplementary Measure

The EDPB has provided recommendations on its expectations for encryption to be considered an adequate and appropriate supplementary measure.

For example, encryption keys must be retained solely under the control of the data exporter, or other entities entrusted with this task, residing in the EEA or a third country with an adequate level of protection.

The EDPB has provided some examples of encryption in specific use cases.

Encryption for storage in a third country

If a data exporter uses a hosting service provider in a third country to backup data, encryption in this instance would only be deemed an effective supplementary measure if:

1. the personal data is processed using strong encryption before transmission;
2. the encryption algorithm and its parameterisation (e.g., key length, operating mode) 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 an 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 or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured.

Other EDPB guidance covers transferring data which is geographically routed over the internet via a third country which is not an adequate jurisdiction.

Encryption in this instance would be deemed an effective supplementary measure (in combination with end-to-end encryption if so required) if, it is used to protect the data in transit and it provides effective protection having regard to the resources known to be available to the public authorities of the third country; if decryption is only possible outside the third country in question. In addition to other measures, there must also be a reliable key management system and the existence of backdoors (in hardware and software) must be ruled out.

Additionally, the EDPB specifies that any interference with the fundamental right to privacy and data protection for the purpose of surveillance should be subject to an effective, independent and impartial oversight system that must be provided for, either by a judge or by another independent authorised body.

Encryption keys must not be disclosed to public authorities unless such conditions and safeguards are observed.

Cryptoloc as a Supplementary Measure

How does Cryptoloc work?

Cryptoloc's patented technology combines three different encryption algorithms into one unique multilayer process that can be deployed across a wide range of applications, including file storage and document management and counterfeit prevention and detection solutions.

The Cryptoloc secure escrow model provides a mechanism by which a trusted, neutral third party, can assist in recovering access to a user's documents. Neither the escrow agent nor the cloud provider has any access to view the content of any user's documents during the recovery process.

In a Cryptoloc – based solution, document owners use a locally generated private/public key-pair (4096-bit RSA) to protect the encryption key for each document upload to the cloud. Document owners also use a password authenticated account to access the cloud-hosted Cryptoloc – based solution.

Each time a document is stored, a new random encryption key is generated client-side (i.e., on their local device: PC, smartphone or tablet). Uploading to the cloud via Cryptoloc involves sharing the secret (the encryption key) for each document between each of the three different parties (the document-owner, the cloud-host and an escrow agent). This has the effect of hiding the key material until it is needed to decrypt the document again.

By having the document in a monitored place on the cloud server, all attempts to access or modify the encrypted document can be monitored and audited. All transit between the cloud server and the user or receiver is through encrypted transport layer security (TLS) tunnels, meaning that the already encrypted documents are then encrypted again for TLS transit, ensuring that a document cannot be compromised in transit.

How can Cryptoloc be applied as a technical supplementary measure to the SCC's?

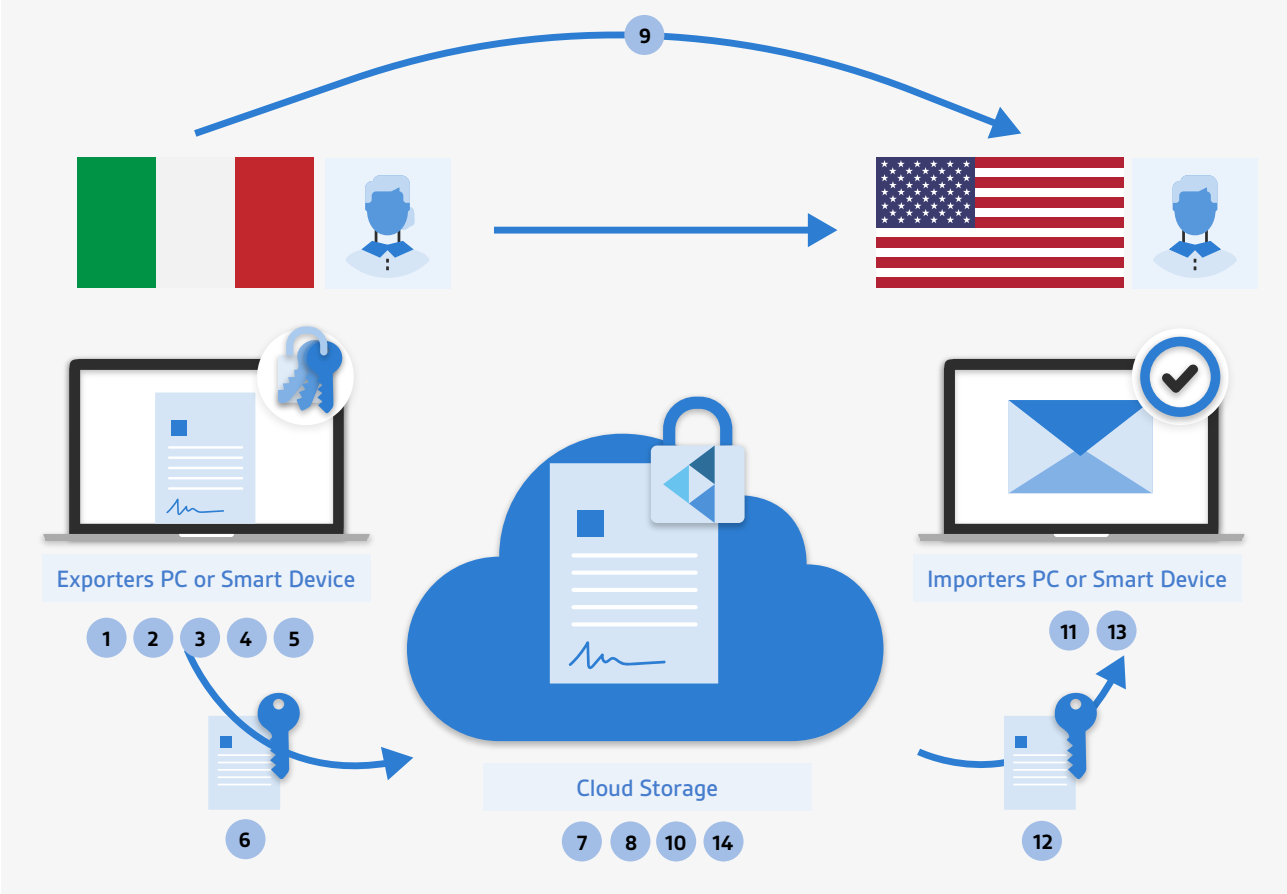
The state-of-the-art security measures and encryption protocols provided by Cryptoloc's technology will enable data exporters to elevate the level of protection afforded to personal data transferring to (or via) a third country, when adopted as a technical measure to supplement the SCCs.

Cryptoloc's unique three key architecture can be implemented as a stand-alone system, which could potentially be owned and controlled by an EEA entity, with an EEA based escrow agent, using only cloud storage based physically in the EEA. The system can be customised to allow for comprehensive oversight by the trusted escrow agent, as well as the provision of notice in the event of law enforcement or a relevant public authority requesting access to an encryption key.

Furthermore, the contract between the parties sharing the data will properly document the specifications of Cryptoloc and its efficacy as a supplementary measure in order to comply with the accountability principle of the GDPR.

The contract will also contain provisions mandating the handling of government requests for access to personal data, as well as any technical controls to be applied to limit the use of the personal data.

What does the Cryptoloc process look like?



1. A data exporter in the EEA wishes to transfer a file to (or via) a third country.
2. Cryptoloc creates 3 unique key-splits which combine to create a document encryption key.
3. Cryptoloc encrypts the document with the document encryption key using AES256.
4. Cryptoloc then encrypts the key-split pairs with the RSA 4096 bit public key of the 3 parties; owner, cloud and escrow using RSAES-OAEP.
5. 2 of the 3 key splits are encrypted with the public key of the data exporter, the Cryptoloc software and an escrow agent, so that 2 of the 3 party's key splits are required to make the full key.
6. The encrypted file and the encrypted key splits are then uploaded to the cloud through an encrypted TLS tunnel.
7. The escrow agent and the cloud software each only have part of the key, such that neither can decrypt the file alone.
8. The file is now securely stored at rest in the cloud.
9. The data exporter shares the file with the data importer through the software interface or API.
10. Cryptoloc encrypts the data importer's key splits with a temporary key. (If they are a system user, it will use their public key).
11. The data importer receives an email notification containing a link to the software supplier for download.
12. The data importer downloads the encrypted file and the encrypted key splits through an encrypted TLS tunnel.
13. The receiver uses multi factor authentication, including an SMS code, to decrypt the file in their browser.
14. Cryptoloc tracks and audits all access and modifications to the file on the cloud server.

Cryptoloc and GDPR Requirements

GDPR Requirement	cryptoloc
The Encryption algorithm can be considered robust against cryptanalysis performed by public authorities and foreign government agencies	The Cryptoloc algorithm regularly updates their modular algorithms to use the latest and most robust RSA standards
The strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved	The Cryptoloc algorithm uses the latest and most robust RSA standards by default, but also offers the capability to modify and scale the encryption strength as required.
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	Cryptoloc is an ISO27001:2013 complaint company and the algorithms utilised in the technology are set by the accepted RSA standards.
The keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked)	The technology manages the keys such that a file encryption key is never stored in its entirety or in a decrypted format. Each file has a unique encryption key, that is only available to the verified users granted access.
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 jurisdiction with an adequacy decision	The technology requires two of three parties to provide their key part to decrypt a file (the data exporter, the Cryptoloc software and an escrow agent). Alone neither the software provider nor the escrow agent can decrypt a file.

Conclusion

The advent of the GDPR has highlighted the increasing importance of ensuring data protection, especially for parties dealing with the transfer of data in a global context or across international borders. With legislative and regulatory requirements becoming more stringent and stiffer penalties for non-compliance, organisations must look for steps they can take (such as encryption) to ensure that data transfers are safe from the disruption of similar decisions in the future.

Cryptoloc's technology with its unique three key encryption architecture and state-of-the-art security measures, provides a ready-made solution that meets the essential requirements under the GDPR.

Subsequently Cryptoloc's solution negates the requirement for an organisation to undertake case-by-case assessments of the transfer to ensure an essentially equivalent level of protection for the EEA personal data under the third country's laws and enables these organisations to comply with the GDPR.