Capgemini

WHITEPAPER

CLOUD MIGRATION & GDPR

Cross-border Data Transfers and Schrems II impact

Executive summary

Adequate data usage is a strong differentiator for organizations, and data masters who do it right can expect higher customer satisfaction, revenue growth and improved margins. In this journey of building data initiatives, the cloud is a strong enabler, bringing efficiency and making state-of-the-art AI and Data Analytics tools easier to access. At the same time, consumers' trust, especially in the use of their personal data, is a strong differentiator, and data privacy, security and fair use are in strong demand from citizens, users, employees, shareholders, and governments.

The Schrems II ruling from the Court of Justice of the European Union (CJEU) in July 2020 has emphasized the need for more collaboration with non-European Cloud Service Providers for organizations dealing with personal data from citizens of the European Economic Area (EEA) to ensure compliance with the requirements defined by the CJEU. The best practices and concrete measures are discussed among actors. Still, we believe that moving to cloud-based infrastructures, platforms and services is an effective strategy to improve business agility and data effectiveness. We believe that embracing positively the privacy requirements and regulations can be done effectively in a cloud-based data estate modernization and has the potential to further accelerate the differentiating power of data. Of course, this requires an understanding of the regulatory landscape and a pragmatic approach.

With the Schrems II ruling invalidating the Privacy Shield agreement between the European Union (EU) and the United Stated (US), organizations can no longer legally transfer data to the US based on the Privacy Shield framework. Other (legal) transfer mechanisms such as the Standard Contractual Clauses (SCCs) remain valid, but organizations must - with appropriate technical and organisational measures - demonstrate that they maintain a level of protection essentially equivalent to that guaranteed by the General Data Protection Regulation GDPR. This means they have to identify precisely the personal data involved in real or potential transfer to the US and deploy a structured and traceable approach to ensure privacy is maintained in line with GDPR and European regulations. In this whitepaper, we provide a brief overview of the Schrems II ruling, and we describe the guidance provided by the European Data Protection Board (EDPB) on the new Standard Contractual Clauses (SCC) and technical, organisational, and contractual measures which contribute to an adequate level of protection. Furthermore, we explain the goals of some technical measures, the requirements when using these measures, and examples on how these measures can be applied in practice. In addition to these, we provide complementary technical measures to consider, and our 3-step approach for identifying risks, assessing gaps in practices and protection, and then implementing correct procedures and technical means. Following this approach, we believe organizations can continue to use cloud services, create a strong competitive advantage by enabling more efficiency, as well as building digital trust.

Table of Contents

1 Introduction

Up to July 2020, the EU-US Privacy Shield agreement helped regulate the GDPR compliance of many organizations transferring personal data using services from US vendors. Then the Court of Justice of the European Union (CJEU) pronounced the Schrems II verdict, invalidating the Privacy Shield and opening a period of uncertainties. As more and more organizations are extending their use of US-based cloud services, clarity is needed on how they can comply with privacy regulations, without weakening their digitalization programs and losing the competitive advantage provided by advanced cloud platforms.

This whitepaper presents these developments and suggests elements of solution and a pragmatic approach to implementing safeguards. Specifically, the following topics are addressed:

- The context of cloud adoption
- The impact of the Schrems II ruling on the usage of cloud services, especially from providers subject to US regulations
- An overview of recommendations from the European Data Protection Board (EDPB)
- Capgemini's methodology to assess and implement necessary measures in a practical and pragmatic way

Please note that this whitepaper is not intending to provide any legal advice in any manner whatsoever. Also, as part of its portfolio offering Capgemini does not provide any legal advice. We share our experience in identifying and implementing key organizational and technical measures necessary for meeting GDPR requirements. In addition to the technical recommendations, organizations should get legal advice with their legal department or law firm.

2 The rise of cloud adoption

Cloud computing allows consumers of IT resources, such as servers and databases, to use them as they need, on demand, from publicly available infrastructures. Amazon started the movement in the early 2000's, with Amazon Web Services (AWS) making available storage and compute services. Other vendors have been positioning since. AWS, Microsoft Azure and Google Cloud are leaders in Gartner's 2021 Magic Quadrant for Cloud Infrastructure and Platform Services[1], with an expanding array of offers and services.

Businesses can gain more autonomy in the use of sophisticated computing resources. They can use advanced tools, such as machine learning frameworks and packaged cognitive applications, paying only based on real usage. They can go fast and experiment without committing to expensive investments. This increases business agility by reducing dependency on overstretched IT infrastructure groups[2].

Innovation is easier, as many advanced tools are readily available, for Artificial Intelligence, data sharing, workflow management, modern user interfaces… Anybody can leverage the high investments made by the major cloud vendors in advanced tools offered in off-the-shelf product suites.

For Chief Data Officers, consolidation on the Cloud also provides better control on data assets, and facilitates data sharing, data quality management, data governance, thus accelerating the use of data across the organization and increasing trust in data. Cloud vendors are putting several billion Dollars per year each on security only[3]. This provides high confidence in their expertise and capability, and you can thus reach high levels of security – at the same time organizations still need to take care of the areas which they are responsible for, such as application-level security and security domains configuration for instance.

For IT departments, the Cloud offers strong capabilities for modernizing existing platforms and delivering new, innovative services. Using cloud services allows to better satisfy business users by authorizing capacities unavailable so far, at competitive costs. Renting IT resources, as opposed to buying them, releases budgets for more strategic investments, making hardware and software platform a commodity.

All in all, the Cloud is a clear facilitator in the journey to being a data powered enterprise[4], enabling data mastery in a faster, easier, safer and cheaper way.

[1] https://www.gartner.com/en/documents/4004076
[2] https://www.capgemini.com/resources/the-cloud-imperative-for-telcos-data-analytics/
[3] https://www.reuters.com/article/us-tech-cyber-microsoft-idUSKBN15A1GA and more recently: https://www.engadget.com/google-microsoft-billion-invest-cybersecurity-us-biden-231242040.html
[4] https://www.capgemini.com/research/the-data-powered-enterprise/

3 How Schrems II impacts cloud adoption

This section provides an overview of the impact on cloud adoption, privacy regulations and jurisprudence related to this topic. Please note that we provide it as a base for understanding the requirements and the technical impact, and that this document should not be seen as providing legal advice.

3.1 GDPR and the invalidation of the Privacy Shield

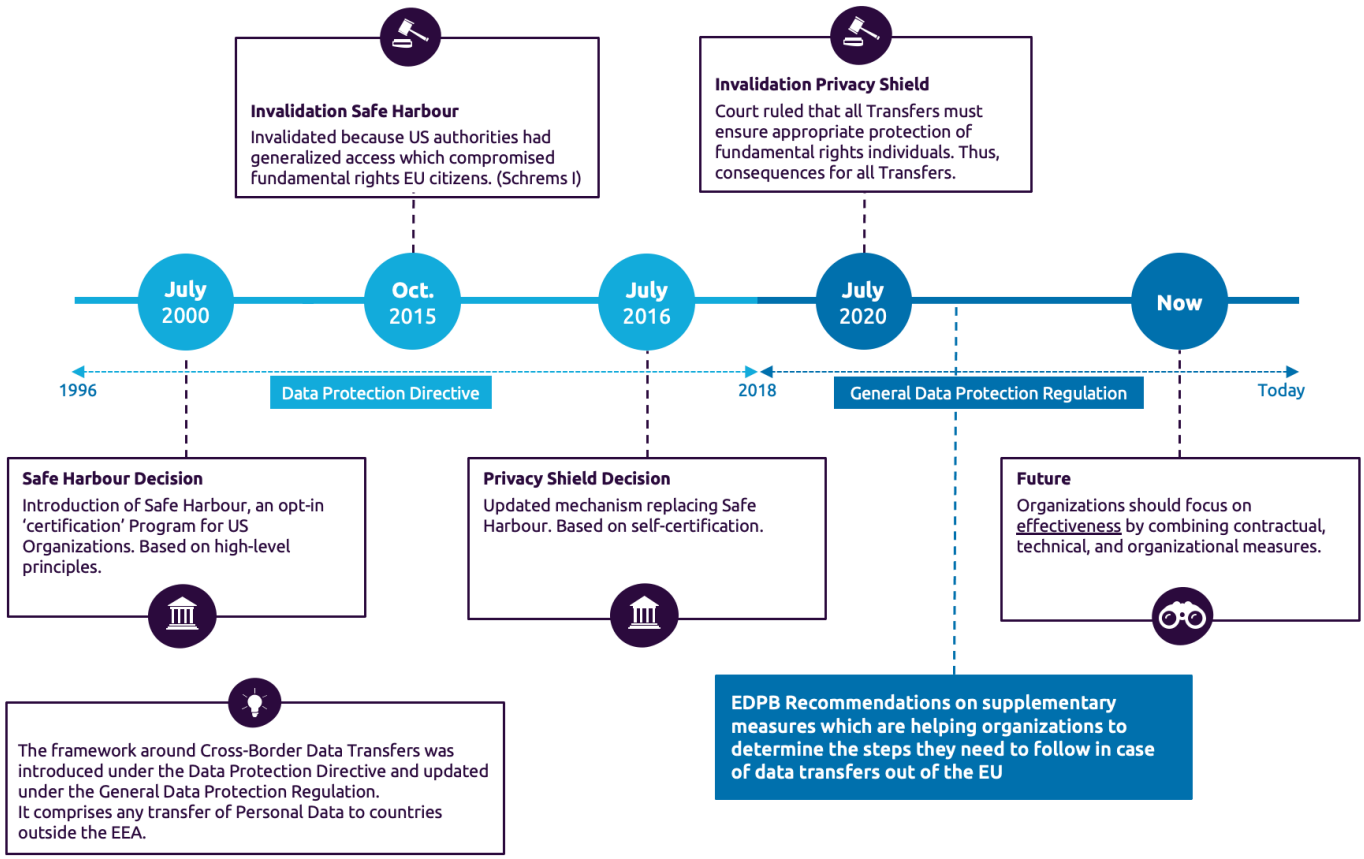
While an increasing number of organizations is moving to the cloud, those subject to the General Data Protection Regulation (GDPR) must ensure that the requirements of cross-border data transfers are satisfied. Reference is made to cross-border data transfers when data is transferred to a country which is not a member of the European Economic Area (in GDPR-terms 'a third country'). We must bear in mind that transfer of data also refers to the mere fact of having distant access from a non-EU country to data hosted in the EU.

In case of data transfer, organizations must ensure that personal data benefits from the same level of data protection as in the EU. It is important to mention that there is a difference in accountability between a Controller and a Processor. The Controller (usually the client/customer of the Cloud Service Provider) determines the purposes and means of the processing of personal data and is therefore responsible for a sufficient level of protection. Personal data can be for instance from customers, employees or users – basically any physical person the organization is processing data about. The Cloud Service Provider will usually be a Processor, processing data on behalf of the Controller, in accordance with its instructions. In the end, the Controller is accountable and should make sure that it only makes use of processors providing sufficient guarantees to implement appropriate technical and organisational measures (see art. 28(1) GDPR).

Chapter V of the GDPR contains several articles that refer to “Transfers of personal data to third countries or international organizations.” In art. 44 GDPR and beyond, the general principles for data transfers to third countries are mentioned and specific “transfer instruments” (or mechanisms) are described. It is important to note that some countries out of the EU/EEA may be recognised by the European Commission as providing an adequate level of protection, hence not requiring the implementation of a specific transfer mechanism. The list of such countries is made available on the European Commission website and may be updated from time to time. In the absence of such an adequacy decision, other mechanisms (appropriate safeguards) for cross-border data transfers must be used to ensure compliance with the GDPR. In art. 46(2) GDPR these mechanisms are mentioned: standard data protection clauses, approved codes of conducts, approved certification mechanisms, Binding Corporate Rules (BCRs), and legally binding and enforceable instruments between public authorities or bodies. These mechanisms are seen as appropriate safeguards which can be used for transferring personal data to third countries.

Most Cloud Service Providers (CSPs) have their headquarters in the Unites States (Amazon, Microsoft, Google), and thus other laws and regulations may apply in addition to European regulations. Back in 2016, the European Commission and the United States had agreed on a bilateral agreement referred to as Privacy Shield, where organizations could demonstrate compliance with EU Data Protection laws via a self-certification mechanism. The Privacy Shield replaced the previous bilateral agreement know as Safe Harbor previously invalidated. In 2018, the Cloud Act[5], constrained under certain conditions US-based service providers to give access from their users when requested to do so by the US authorities, thus potentially revealing personal data from EU citizens. In July 2020, the Schrems II ruling from the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield in particular on account of the Cloud Act and invasive US surveillance programs, thereby making transfers of personal data on the basis of the Privacy Shield illegal. At the same time, the CJEU confirms that the other transfer mechanisms such as the Standard Contractual Clauses (SCCs) and the Binding Corporate Rules (BCRs) remain valid but may no longer be sufficient on their own to transfer data as further described below.

TIMELINE
CROSS-BORDER DATA TRANSFERS



[5] The Clarifying Lawful Overseas Use of Data Act

3.2 The Schrems II ruling

This section provides a brief summary of the content and consequences of the Schrems II[6] ruling. For anyone new to this topic, we recommend reading the official press release or the FAQ written by the European Data Protection Board (EDPB).[7]

Austrian citizen Maximillian Schrems questioned the legitimacy of two mechanisms[8] used for the protection of personal data by Facebook Ireland Ltd. In the Schrems II ruling from July 2020, the CJEU answered some of his preliminary questions.

Summary of Court Decision

- Invalidation of the EU-US Privacy Shield Agreement, because it did not offer the level of protection required under the GDPR.
- The Standard Contract Clauses ("SCCs") remain valid but are - by themselves - not sufficient to ensure a level of protection equivalent to the GDPR.
- For organizations to ensure that an adequate level of protection is provided, they should understand the protection offered by the legal system in the third country, as well as the measures required to ensure that an equivalent level of protection is provided by the complete combination of contractual, organizational, and technical measures implemented by the parties involved.

Following the Schrems II ruling, organizations cannot anymore base their data transfers to the US solely on transfer mechanisms (e.g. contractual clauses); they must ensure that measures are implemented in order to mitigate the impact of legislations which may enable public authorities to request access to data including personal data. As such, organizations must carry out assessments on a case-by-case basis and document them, to ensure an adequate level of protection in case of existing or potential transfer of data to a third country.[9]

There are multiple reasons why the Schrems II ruling is challenging for organizations. Firstly, the ruling resulted in legal uncertainty, and thus organizations were seeking further clarifications and guidelines from the European data protection authorities. In particular, organisations were waiting for guidance as to what are the different steps companies need to take when transferring personal data on the basis of SCCs or the BCRs, in the new context. The EDPB has published on 18 June 2021 its '*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*'.

Secondly, further to this decision, many organizations may have realised that they need to have a better knowledge of the data transferred on their behalf.

Finally, stopping a migration to the cloud might not be the best and safest answer even with regards to data privacy. Moving to the cloud is a chance for organizations to improve the overall level of security of their IT environment, and mitigate other potential security and privacy risks by implementing Security and Privacy by Design from the start. As such, this is a question of balancing between different risks and requirements.

---

[6] CJEU C-311/18 (Schrems II)

[7] press release: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf and EDPB FAQ: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en.

[8] (Legal) mechanisms or adequate safeguards to transfer data to third countries: adequacy decisions, standard contractual clauses, binding corporate rules, certification mechanism, codes of conduct, derogations)

[9] A third country in the context of this paper is a country outside the European Economic Area ("EEA").

3.3 Examples of recent cases

While the interpretation and application of the Schrems II ruling has taken some time, there are already examples were authorities acted upon the conclusion of the CJEU, especially from national or regional data protection authorities. Below is a brief description of three cases.

- **The Portuguese National Statistical Institute**[10]

  The Portuguese Data Protection Authority (Comissão Nacional de Proteção de Dados) ordered the Portuguese National Statistical Institute to suspend processing of personal data in any third country that lacks adequate privacy protections, including the United States. The Statistics institute was undertaking the 2021 census by collecting data through forms via their website. For this, they were using services of Cloudflare, a Cloud Service Provider headquartered in the United States. An investigation by the Portuguese Data Protection Authority showed that when the cloud service is used, there are no guarantees that the data will be processed within the European Union and will not be sent to inadequate countries. Furthermore, the investigation showed that the National Statistical Institute had not carried out the necessary Risk Assessment (DPIA) for this particular processing and did not seek the DPA's advice. Making use of Standard Contractual Clauses does not mean that there is no obligation for the controller to guarantee a sufficient level of protection when data is transferred to third countries. Reference is made to the CJEU Schrems II Judgment, regarding the implementation of additional measures and a relationship is made with the accountability principle from art. 5 GDPR.

- **Unlawful use of newsletter tool by a German company**[11]

  The Bavarian Data Protection Authority (BayLDA) considered the use of the newsletter tool Mailchimp by a Bavarian-based company in a specific case unlawful under the GDPR. This Bavarian-based company transferred email addresses from its newsletter subscribers to the US-based company behind the trademark Mailchimp. The BayLDA was involved via a complaint lodged by a data subject claiming unlawful transfer of its personal data outside the EU/EEA, namely the US. BayLDA stated there are at least indications that Mailchimp may qualify as an 'electronic communication service provider' under US surveillance law and therefore may be subject to data access by US intelligence services. Hence, although standard contractual clauses were in place, the BayLDA took the view that the use of Mailchimp is unlawful in this case because the Bavarian-based company failed to evaluate whether the implementation of "additional measures" according to the ECJ's Schrems II decision was necessary. After the BayLDA's intervention, the company immediately refrained from further using Mailchimp and rightfully stated that relevant authority guidelines concerning such "additional measures" were not in place at that time. BayLDA did not issue any further measures in this case, including no fines.

[10] CNPD - Deliberação/2021/533

[11] BayLDA - LDA-1085.1-12159/20-IDV

- **Doctolib and AWS**[12]

  The French Ministry of Solidarity and Health uses several service providers to manage appointments for vaccines on the internet. Several organizations have asked the judge to end the partnership with one of the providers, Doctolib, because the data was processed via Amazon Web Services (AWS) and thus transferred data to the subsidiary of a US-based company. They stated this was not compliant with the GDPR. The outcome of the decision is interesting. Namely that due to the various measures taken it is assumed that - in this context - the data will not be processed outside the EU: "*Doctolib and AWS have concluded a complementary addendum on data processing establishing a specific procedure in the event of requests for access by a public authority to data processed on behalf of Doctolib, providing in particular for the contestation of any general request or one that does not comply with European regulations. Doctolib has also set up a security system for data hosted by AWS through an encryption procedure based on a trusted third party located in France in order to prevent the reading of data by third parties."* Another important aspect to mention in this case is that the data processed via AWS was not regarded as "health data", even if it indeed was private data. So, with the measures in place and the data concerned, the level of protection cannot be regarded as inadequate in the light of the risk of infringement of the GDPR.

[12] CE - 450163

4 EDPB Recommendations: data protection authorities' view on how to proceed after Schrems II

This section will provide an overview on the Recommendations adopted by the European Data Protection Board (EDPB), which was much expected by organizations in need of ensuring their compliance with GDPR in the post-Schrems II environment. Here again the below developments do not constitute a legal advice but a mere reading of the EDPB Recommendations.

Subsequent to the Schrems II verdict, the EDPB developed Recommendations on how organizations could respond and comply with the new jurisprudence. The EDPB has defined an approach with specific steps that organizations can follow to understand the impact of Schrems II on their organization, analyse whether these issues can be solved with supplementary measures, and remain compliant in the future.

In addition to a description of the 'How', the EDPB also worked out the 'What' by describing a few scenarios in which cross-border data transfers take place by using services from US Cloud Providers. In short, the EDPB provides various technical, organizational, and contractual safeguards to increase the level of protection to a level equivalent to the EU.

EDPB's six-step plan for assessing and protecting global data flows:

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

Whatever measures you decide to implement, always keep in mind that you should verify the effectiveness of the measures. Using a methodical, standardized way to assess the use of these Cloud Services will benefit your organization in terms of speed, effectiveness, and level of compliance. Maintaining documentation also enables you to demonstrate that you carefully considered all aspects related to data protection. See below a brief summary of the most relevant aspects of the EDPB as visualized in the steps above and other means which we think can be used to complement the approach suggested by the EDPB. See more on Capgemini's way to tackle these challenges in the *Capgemini Approach* section below.

The EDPB introduces a six-step approach that may assist organizations in taking appropriate actions to maintain compliance with data protection regulations.

Scan the QR for more information.

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Scan the QR for more information

4.1 Know your transfer

Companies are expected to know where their data is transferred to and/or accessed from. Although the GDPR was already requiring companies to map their data processing activities and flows of data, the CJEU decision brings back to the forefront the need for companies to have a clear view on which data is being transferred cross-border, across their subcontractors, services providers and infrastructures. In complex ecosystems with multiple providers this can be a complex exercise.

4.2 Appropriate transfer mechanism

The Schrems II ruling invalidated the Privacy Shield mechanism. However, in practice, we know that some CSPs already relied on Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) as their primary mechanism for the cross-border data transfers.[13] Hence this means that companies which were already relying on the Privacy Shield will need to make sure that they now adopt and implement either SCCs or BCRs.

In this context of intense discussions on data transfers, it has to be noted that on 4 June 2021, the European Commission issued modernized standard contractual clauses[14] under the GDPR. They replaced the three sets of SCCs that were adopted under the previous Data Protection Directive 95/46.[15] The new SCCs aim to reflect both the updated regulations (GDPR), and the Schrems II ruling. They are modular, more detailed, and introduce a high standard of accountability for both Data Importers and Data Exporters. Since 27th September 2021, organisations entering into new contracts must refer to these new SCCs. For contracts entered into before the EU Commission Decision on 2021, organisations have until December 2022 to amend their transfer mechanism and replace it with the new SCCs.

A few examples of changes in the SCCs are:

- Stricter onward transfer restrictions
- Broad third-party beneficiary rights for Data Subjects
- Broad transparency requirements for Controllers importing Personal Data
- Obligation to evaluate laws of third country
- Obligation to notify in case of government access requests, and obligation for Data Importer to review, assess, and - if legality of request is questioned - challenge requests from public authorities.[16]

In practice, the new SCCs still require organizations to implement appropriate measures which are further developed under the Recommendations of the EDPB.

---

[13] Example of Statement Microsoft on reliance on SCC: https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/

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

[15] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[16] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847

4.3 Supplementary measures

In Annex II of their Recommendation the EDPB has multiple scenarios for which it identifies supplementary measures. The EDPB distinguishes three types of measures: (i) Technical measures, (ii) Contractual measures, (iii) Organizational measures. According to the EDPB, contractual measures 'will generally consist of unilateral, bilateral or multilateral contractual commitments.' [17] Organisations must ensure that they enter into strong data protection clauses with the cloud providers they rely on. Organisations can check the Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors GDPR. Besides, the EDPB describes that organisational measures 'may consist of internal policies, organisational methods, and standards controllers and processors could apply to themselves and impose on the importers of data in third countries.'[18] The EDPB lists some examples of organisational measures that exporters can implement, albeit the list is not exhaustive and other measures may also be appropriate: Internal policies for governance of transfers especially with groups of enterprises; Transparency and accountability measures; Organisation methods and data minimisation measures; Adoption of standards and best practices.

In the section below we present the goals of some technical measures mentioned by the EDPB, the requirements when using these measures, and examples on how these measures can be applied in practice. In the next chapter we describe measures which can be used to complement the approaches suggested by the EDPB.

4.4 Technical measures as supplementary safeguards

Technical privacy measures help to prevent unauthorized identification of data subjects, or in any other way derive information about them in that specific context or another context where data is combined with data from other data sets.

4.4.1 Encryption of data-at-rest, in transfer and in use

When organizations use a CSP to store, process or backup data, they can use encryption as a technical measure, thus preventing another player, including public authorities, from being able to access the data, even if authorities obligate the respective CSP to provide it.

For encryption to be an effective measure, it should meet at least the following requirements:

- State-of-the-art encryption algorithm and parametrization, such as post-quantum cryptographic algorithms and use of large key lengths;
- Properly maintained software that implements the encryption algorithm flawlessly, preferably with certification by a competent authority;
- Reliable encryption keys management with a trustworthy public-key certification authority;

[17] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, p.36

[18] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, p.43

- Retaining of encryption keys by the data exporter or by a provider of the data exporter located in the EU and regulated only by EU laws.

Encryption of data at rest and in transfer is a fairly standard measure. Encrypting data in use requires the use of specific algorithms (please refer to the section below on homorphic encryption) or confidential computing – where memory in virtual machines is kept encrypted[19].

Example – Microsoft Double-Key Encryption

A good example of Service that appears to enable organizations to meet this requirement is Microsoft Double Key Encryption ("DKE"). It uses two keys to protect data; one key in your control and a second key stored securely in Microsoft Azure. Viewing data protected with Double Key Encryption requires access to both keys.

An organization can use DKE encryption in Office 365 to ensure that data is not readable by Microsoft. This does mean that this limits some of the functionality within Office 365.

Example – Thales HSM as a Service with Google Cloud

With an External Key Manager in Google Cloud security architecture, you can use an external provider to protect some of your Google Cloud services, such as BigQuery and Compute Engine. Typically, the Hardware Security Modules (HSM) as a service from well-known security firm Thales is certified to be compatible with Google Cloud – this is important as Thales is a European company, locating its infrastructures in Europe and used to work in high security environment such as Defence.

4.4.2 Pseudonymized Data

When using a CSP for certain processing activities such as data analytics, you might be able to replace identifiers with scrambled and/or aggregated versions, thus making it impossible to get back to the original identities. Under certain boundaries, this can still allow statistical analysis and machine model training, for instance. When using pseudonymisation, the data exporter replaces identifiers with pseudonyms, and keeps the original identifier at a distinct location. For pseudonymisation to be effective, the following conditions should be satisfied and documented:

- Personal data can no longer be attributed to a specific data subject, nor allow to single out a data subject in a group without the use of additional information;
- The additional information is held exclusively by the data exporter and kept separate, or is completely erased if not needed;
- Disclosure or unauthorized use of that alternative information is prevented by appropriate technical or organizational measures;

[19] https://confidentialcomputing.io/

- A thorough analysis has been carried out to ensure that no external party is able to attribute/link data they might have access to, to the pseudonymized data of an individual.

Example – Pseudonymized data

A telecom operator wishes to perform statistical analysis on consumption data (Call Data Records, or CDRs) from their customers, using a cloud-based AI platform. Transferring CDRs as-is would mean revealing personal and sensitive data. They have chosen to pseudonymize them: replacing the customer id and phone numbers by one-way hashes.

Then if the operator wants to be able to use the insights derived from the analysis (identify risk of churn, or potential fraud for instance), they can reconciliate the insights with a table of hashes to real numbers kept on their on-premise platform. If the analysis is only for statistical purpose, this mapping is not even necessary.

4.4.3 Multi-party processing

Multi-party processing requires a Data Exporter to split data in such way that no part an individual processor receives suffices to reconstruct the data in whole or in part. The Data Exporter splits the data before transmission to distinct processors and merges the results after receiving them back. The final result could constitute personal or aggregated data. If a data exporter wishes to use this technology, it should ensure the following requirements are met:

- The data exporter must split the data in two or more parts, each of which can no longer be interpreted or attributed to a specific individual without the use of additional information;
- Each piece is transferred to a different processor in a different jurisdiction;
- Optionally: the processors process the data jointly, e.g. using Multi-Party Computing (“MPC”) in a way that no new information is revealed;
- The algorithm used is secure against active adversaries;
- There is no evidence of collaboration between public authorities in the different jurisdictions, or evidence that public authorities in one of the countries is able to use its power in both jurisdictions;
- The Controller has established by means of a thorough analysis of the data in question that the pieces of personal data it transmits cannot be attributed to an identified or identifiable individual.

Example – Multi-party processing for auctioning on sugar beets in Denmark

A real-life application of multi-party processing can be found in Denmark, for auctioning on sugar beets between beet farmers and Danisco, the only beet processor on the Danish market[1]. Farmers have to make offers for volume and prices, and then the market price and volumes are determined based on market demand. Farmers do not want to reveal their economic positions and productivities, especially to Danisco, and having a third party as auctioneer would be risky and expensive.

Starting in 2008, a multi-party cryptographic processing between Danisco, the beet farmers' association and the European public tenders office was used to obtain cooperatively an optimal market place without any party having the view on all the offers.

5 Complementary measures to consider

In this section, we want to mention other measures which can be used to complement the approaches suggested by the EDPB.

5.1 Standard cybersecurity practices

Standard security practices should be applied to ensure your data protection practices are adequate, for which we recommend a Zero-trust environment. A Zero-trust environment is a strategic security approach, going beyond only using technology. A Zero-trust Approach requires organizations to:

- Trust, but verify all identities (users, systems, services, and applications), meaning authenticate these identities and authorise these identities in a continuous mode.
- Encrypt all data in transit and depending on the risk also in use and at rest;
- Monitor all activities in the environment (implementing security monitoring and response capabilities);
- Use (Micro) segmentation, so a compromised segment cannot compromise other segments;
- Assume you are breached, so detection, response and recovery measures must be in place.

Implementing Zero-trust should focus on the security processes, security technology, organisation of security and governance of security and its implementation. In addition, standard data protection & privacy solutions should also be considered. For example:

- Privacy by Design, to take privacy requirements into account before and during the design;
- Data retention, to reduce the exposure from old data, half-forgotten and badly catalogued;
- Automated record of processing activities (data register), to have a clear overview of all personal data (including cross-border data transfers) processed within the organisation.
- Data Minimization practices, to limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose.

5.2 Homomorphic encryption and Federated learning

Homomorphic encryption and federated learning are two privacy-enhancing mechanisms, making sure processing can be done, and specifically machine learning models can be trained, with reduced need for decrypting sensitive data.

Specifically, homomorphic encryption allows machine learning and advanced analytics models to be executed on encrypted data[20]. No decryption of data is necessary, the algorithm computes directly on encrypted data and still can extract information with no need to reveal sensitive individual information. While still young and very experimental, this technology is promising, as it could allow large data sets to be made available widely, within an

[20] https://homomorphicencryption.org/introduction/

organization or across organizations, while keeping data safe – as some homomorphic encryption algorithms are considered as safe even from quantum computers.

Federated learning addresses the shared learning issue. Let us say a consortium of banks in a specific country wants to cooperate to fight against fraud. They would need to train fraud detection machine learning models on all their data, but they do not want to actually share data. They could rely on a joint venture or commonly supported non-profit organization, but then would need to trust this organization with sensitive data. It can be done, but it puts a heavy security and privacy constraint.

Alternatively, the consortium could use federated learning to collaboratively train their machine learning models[21]. Starting from an initial model, each party (each bank) can refine an initial model on their own environment, and then combine the refined models to create a new stronger, collaboratively trained model. Under certain conditions, with adequate algorithms, the new combined model can approach the performance of a model trained globally, on all the data, while being much safer. This approach is already used typically on Gboard on Android[22] for predicting your next keys and words.

None of these approaches fulfil the requirements of protecting private data, but they allow some forms of sharing and utilization while keeping data confidential and encrypted, which complements encryption mechanisms and restricts the need for unencrypted data.

5.3 Reinforce the data protection governance

Full identification and qualification of data moving to the Cloud is required, as inventory of explicit and potential data movements. Having a Data Trust policy, covering data lineage, data catalogue, data quality, data lifecycle management and reference management is necessary for a sound data estate modernization with the Cloud. This policy now strongly supports the Privacy requirements entailed by GDPR and Schrems II, and Data Protection has to work closely with Data Governance.

With GDPR, Data Protection also becomes a compliance function. A strong framework such as the three lines of defence now standard for financial crime prevention and for risk management[23] can provide inspiration in setting up the right organization:

- The first line of defence is operational management, owning and managing the risks, overseeing their prevention on a day-to-day basis;
- The second line of defence is the risk management function, setting up processes, supporting policies identifying emerging risks, providing expertise and monitoring the effectiveness of control;
- The third line of defence is internal audit, ultimately in charge of evaluating the adequacy and efficiency of internal practices and standards to comply to regulations.

Furthermore, companies also need to define how they would handle and address requests they may receive from public authorities.

[21] http://researchers.lille.inria.fr/abellet/talks/federated_learning_introduction.pdf

[22] https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[23] https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf#:~:text=In%20the%20Three%20Lines%20of,independent%20assurance%20is%20the%20third

5.4 European Cloud Providers

In parallel to the largest CSPs, which are all US- or China-based, we have a few offerings from European companies with infrastructures located within the EU, such as OVHcloud. According to an upcoming study by Capgemini Research Institute, a majority of organizations consider data residency and local cloud providers as adequate for securing control and privacy compliance. As of today, European vendors are mainly providing infrastructure services, sill limited in platform services and missing the depth, ease of use and richness we can get from Google Vertex AI, Azure Synapse or Amazon Sagemaker, to name only a few.

Recent announcements from large European players partnering with US cloud platform vendors could change the game: joint ventures are being set up with full European nationality and control, located in Europe, promising to deliver a full range of cloud infrastructure and platform services based on US technology. This could provide the best of both worlds: a rich set of capabilities based on solid and proven technology, while being subject solely to European laws and thus exempt from the questioning on data transfer / data access.

In a parallel movement, US cloud vendors are moving to be more European in their daily operations to provider stronger guarantees: in addition to providing choice of data localization, they are move closer to data sovereignty by setting up subsidiaries fully based in European countries and in some cases offering the option of having operations and support fully performed by European teams. In this way, they can commit that no personnel from an organisation outside of EEA will be physically able to get access to any data owned by their clients, and also that the contractual relationship will be fully owned by a European organization.

6 Capgemini Approach

Capgemini is one of the leading global companies in cloud transformation. As such, we assist large organizations in public and private sector all over the world with tackling the challenges mentioned above. Experience shows us that most organizations struggle with addressing the privacy and security topics. Moreover, the variety of services used, type of data, maturity levels, risk appetite, and sometimes lack of alternatives, results in the necessity for almost every organization to setup a specific (tailor-made) approach for this topic. Our 3-step approach (based on the recommendations of the EDPB and previous experience) helps organizations to tackle this in a structured and pragmatic.

Capgemini has developed a methodology combining a variety of subject matter expertise in order to help organizations in making confident and well-informed decisions, fitting their situation, maturity level and sector. With a multidisciplinary team consisting of all relevant expertise, we can carry out all steps of our methodology within a relatively short period of time. In three steps Capgemini aims at helping organizations to move forward in a manner they feel comfortable with. By taking a risk-based approach, we assist organizations to focus on the most important challenges they are facing, while improving their maturity level for the future.

Our three-step approach

IDENTIFY

First, we start with identifying and analysing the environment. This can be both the current IT landscape, that is scheduled to be moved to the cloud, together with the modernization plan, plus systems and services that have already been moved to the cloud. Based on the information collected during this phase, we analyse the risks at stake at different levels. This assists organizations in tackling the highest risks first.

In practice it can be difficult for organizations to maintain all this information in a properly managed overview that is updated regularly. As such, we often need to involve multiple stakeholders and/or sources to get a complete view. Below are some examples of the sources that the Capgemini team will use for input.

- An overview of all processing activities outside the EU
- The parties potentially involved in data transfer: vendors, subcontractors, partners, etc.
- The types of personal data involved
- The amount of personal data involved
- The number of parties involved
- Internal stakeholders (HR, Finance, Marketing, etc.)
- The mechanisms on which is relied for data transfers

- Privacy management software used by the organization
- If available an extract of the personal data processing record
- The organization's Configuration Management Database (CMDB)
- Interviews with key stakeholders such as Business Owners, System Owners, Legal, CISO, and the DPO
- Relevant information gathered from a Contract Management Systems
- Data Management Tooling used for Data Governance, such as Informatica, OneTrust, or other brands

Depending on the agreed scope, the outcome of this stage is an overview of systems which might be involved in cross-border transfer of personal data, the relevant factors impacting the level of risk, a risk level, and if needed a prioritization. In addition, we provide a management report including a general overview of our observations, findings and risks identified during our mapping and prioritization phase, and recommendations on how to address these issues in the future.

This step provides senior management with a general understanding of the impact of Schrems II on their organization and the number of services impacted by it. Moreover, they have a better understanding of the potential risks. Having an initial overview of the current situation enables you to address the biggest issues first. This way Senior Management can make an informed decision on the scope and next steps.

ASSESS

The second phase is an in-depth analysis of the specific risks at stake. During the first phase we focused on identifying the most relevant systems and services. In the second phase, we will finalize our analysis of the services in scope by carrying out a gap assessment based on our Capgemini Data Protection Framework. The gap assessment involves (i) collecting more detailed information required to understand the specific risks (impact) for the individual whose personal data is processed due to the data transfer, (ii) the safeguards required to effectively mitigate these risks for the data subject, and (iii) the costs of these safeguards. Optionally we can also give advice on alternative solutions to mitigate specific risks.

INPUT

- Information required to analyse the specific risks related to the respective data transfer. This includes for example a good understanding of the legal system of the country in scope, the protection of fundamental rights of citizens and other individuals. This may also include data available on corruption, court decisions, and other sources that can be considered as relevant and trustworthy
- In depth understanding of the data transferred to the respective countries and their state (pseudonymized, encrypted, etc.)
- A clear view on the end-to-end data lifecycle enabling us to understand which additional measures could be taken, prior to the data transfer

HOW

- First, identify all potential risks for the data subjects due to the cross-border data transfer
- Second, we review the end-to-end processing activity to assess what measures are needed to mitigate these data protection risks. These measures can be commercial (terms and conditions with suppliers), organizational (setting up specific process with vendors and internal teams), technical (implementing additional encryption devices).
- Finally, we produce a report in which we provide a clear overview of the risks, recommended measures (and potential residual risks), and optionally an estimation of the costs to mitigate the risks. Additionally, we can also help organizations to explore alternative solutions

OUTCOME

- An in-depth understanding of the risks related to the respective data transfers
- A set of measures that can be decided on to mitigate the major risks at stake
- A detailed plan / roadmap on how to mitigate the risks and an estimation of the costs and efforts involved

IMPLEMENT

The final step focuses on taking action by implementing technical, organizational and contractual measures within the organization, based on the plan and priorities built during the first two phases. Organizations need to consider the required skills, and the availability within their teams. Often, there is a need for changes across departments, requiring a range of expertise not readily available.

A risk-based approach requires understanding the variety of stakes and requirements, and choosing a mix of the most important aspects and the quick wins which can be achieved rapidly. As in the previous steps, Capgemini can assist with a multi-disciplinary team of professionals with experience in Privacy & Data Protection, Cybersecurity, Cloud Architecture, Data Architecture and Data Science industrialization, as well as specific expertise with the technical environments from the relevant vendors and hyperscalers. Capgemini has close contacts with the major Cloud Service Providers and independent software vendors, facilitation analysis and quick execution. Capgemini's involvement provides access to world-class experts, with track record in many other organizations with similar constraints, and allows to scale fast, getting results rapidly to create trust in the process.

7 Conclusion

Privacy regulations are developing around the world, enforcing organizations to implement safeguards to ensure the protection of personal data, bringing higher trust from customers, employees, users, patients, citizens, and enabling the development of a digital society for the people. The Schrems II ruling from the CJEU and subsequent publications from the EDPB will help in satisfying those higher standards and ensuring European citizens that their personal data is indeed safe and secure. This ruling from the CJEU requires organization to understand the impact of the new regulatory landscape and jurisprudence and to take a closer look at their transfers of personal data. It is also creating uncertainties while the exact consequences are drawn out and the adequate responses are being established.

Capgemini offers a pragmatic three-step approach to help organizations in assessing their situation and implementing and monitoring their compliance to GDPR in the post-Schrems II environment. We also offer concrete technical measures, which can be selected for the implementation.

As organizations are implementing their digital transformation and using the cloud as a key enabler, they need to manage their data more closely, especially where it can relate to personal data and when processed via subcontractors. Data management will ensure data is better controlled, in full compliance with regulations. It will thus create a strong competitive advantage for the organizations which embrace it by enabling better efficiency, as well as generating trust with customers, employees, shareholders.

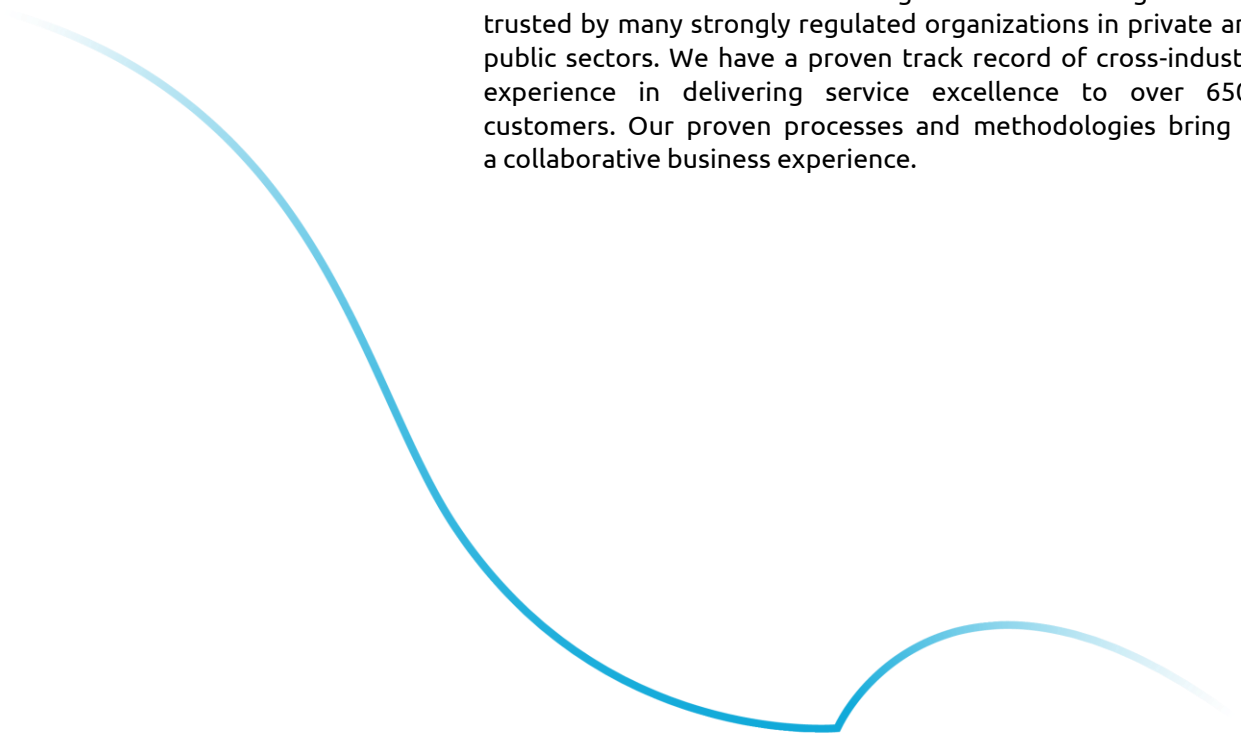
For more information, please reach out to Yannick Martel (yannick.martel@capgemini.com) or Robert Kreuger (robert.kreuger@capgemini.com)

8 Glossary and abbreviations

BCR	Binding Corporate Rules
CJEU	Court of Justice of the European Union
CMDB	Configuration Management Database
CSP	Cloud Service Provider
EEA	European Economic Area
GDPR	General Data Protection Regulation
SCC	Standard Contractual Clauses

Why Capgemini?

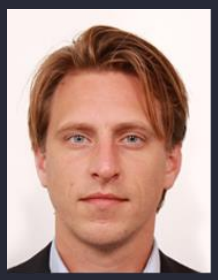
Capgemini is an end-to-end transformation enabler, with competencies from strategy definition, management advisory, to implementation and operations. We are able to mobilize multidisciplinary teams with combined subject matter expertise on privacy, security and cloud, along with customer experience, business re-invention and intelligent manufacturing. We are trusted by many strongly regulated organizations in private and public sectors. We have a proven track record of cross-industry experience in delivering service excellence to over 650+ customers. Our proven processes and methodologies bring in a collaborative business experience.



Yannick Martel

Yannick is Group offer lead for Data &AI in the Telecom industry. Yannick has more than 25 years of experience working in the Telecom and Banking industries, helping organizations implement their digital and data transformation and better serve their customers.

Email: **yannick.martel@capgemini.com**
https://www.linkedin.com/in/ymartel/



Robert Kreuger

Robert is Senior Manager within the Data Protection & Privacy team of the Cybersecurity Unit in the Netherlands. He has extensive knowledge and experience as a privacy consultant, designing and implementing practical solutions related to data protection, information management and digital security.

Email: robert.kreuger@capgemini.com
https://www.linkedin.com/in/robert-kreuger-b3584324/

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 290,000 team members in nearly 50 countries. With its strong 50 year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2020 global revenues of €16 billion.

Get the Future You Want | www.capgemini.com