CYBER SECURITY COALITION.be

Privacy Focus Group

International Data Transfers
Acting on Brexit and Schrems II

Webinar – 25 March 2021
11:00 a.m.

eubelius
advocaten avocats attorneys

Anneleen Van De Meulebroucke

Data Transfers

Anneleen Van de Meulebroucke - 25 March 2021

eubelius

advocaten avocats attorneys

Content of presentation

Data Transfers

outside the European Economic Area

eubelius

advocaten avocats attorneys

1. What is a data transfer?

- Transfer of personal data is a broad concept
  - processing in a third country outside the EEA (or by an international organization)
  - intended to be processed after transfer to a third country (onward transfers)
  - access to data within the EEA from a third country is sufficient!
- Third country: countries (or territories or sectors) outside the EEA (EU27 + Iceland, Liechtenstein and Norway)
- Intragroup data transfers

Examples of data transfers

Example 1

Controller wishes to engage a processor to facilitate its direct marketing mailings. The Processor eventually chosen is located in Vienna, Austria and the personal data will be accessible from there.

→ Vienna is located in the EEA
→ No personal data transfers
→ No additional measures required

Example 2

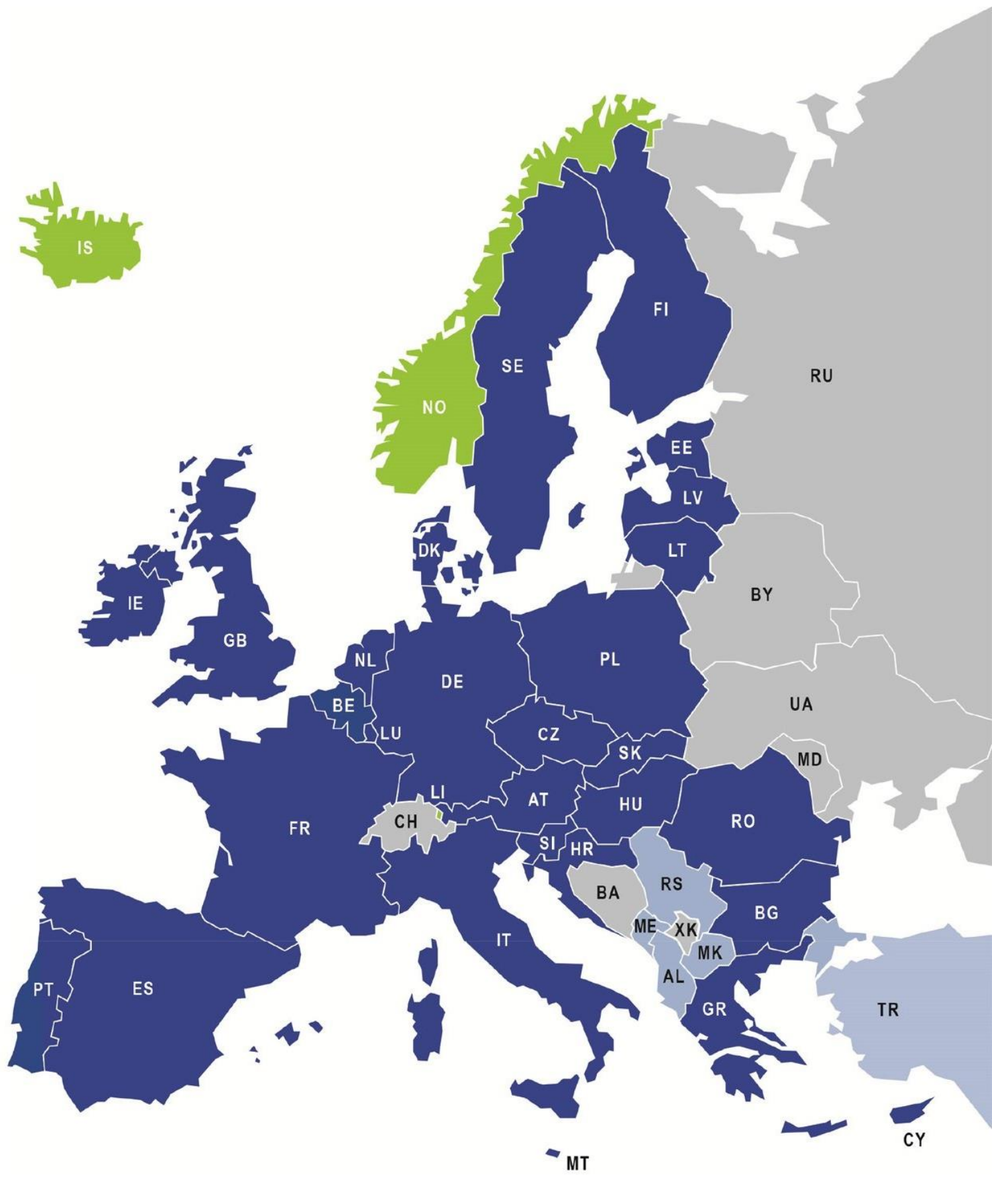
Controller is a large company with offices in Barcelona and Paris. Personal data is collected and stored on the IT systems of the headquarters in Paris. The other EU establishments have access to the main system. Processor provides IT helpdesk services to Controller and operates from India. Processor has, like the other establishments, access to the systems of Controller but no personal data is actually transferred.

→ India is located outside the EEA
→ Access is enough to constitute a data transfer
→ No adequacy decision
→ SCC must be concluded

Example 3

Controller is located in Antwerp and sends personal data to Processor, which has establishments in EU countries and non-EEA countries. The establishment of Processor that receives the data is located in New Zealand.

→ New-Zealand is located outside the EEA
→ However, adequacy decision!
→ No additional measures required



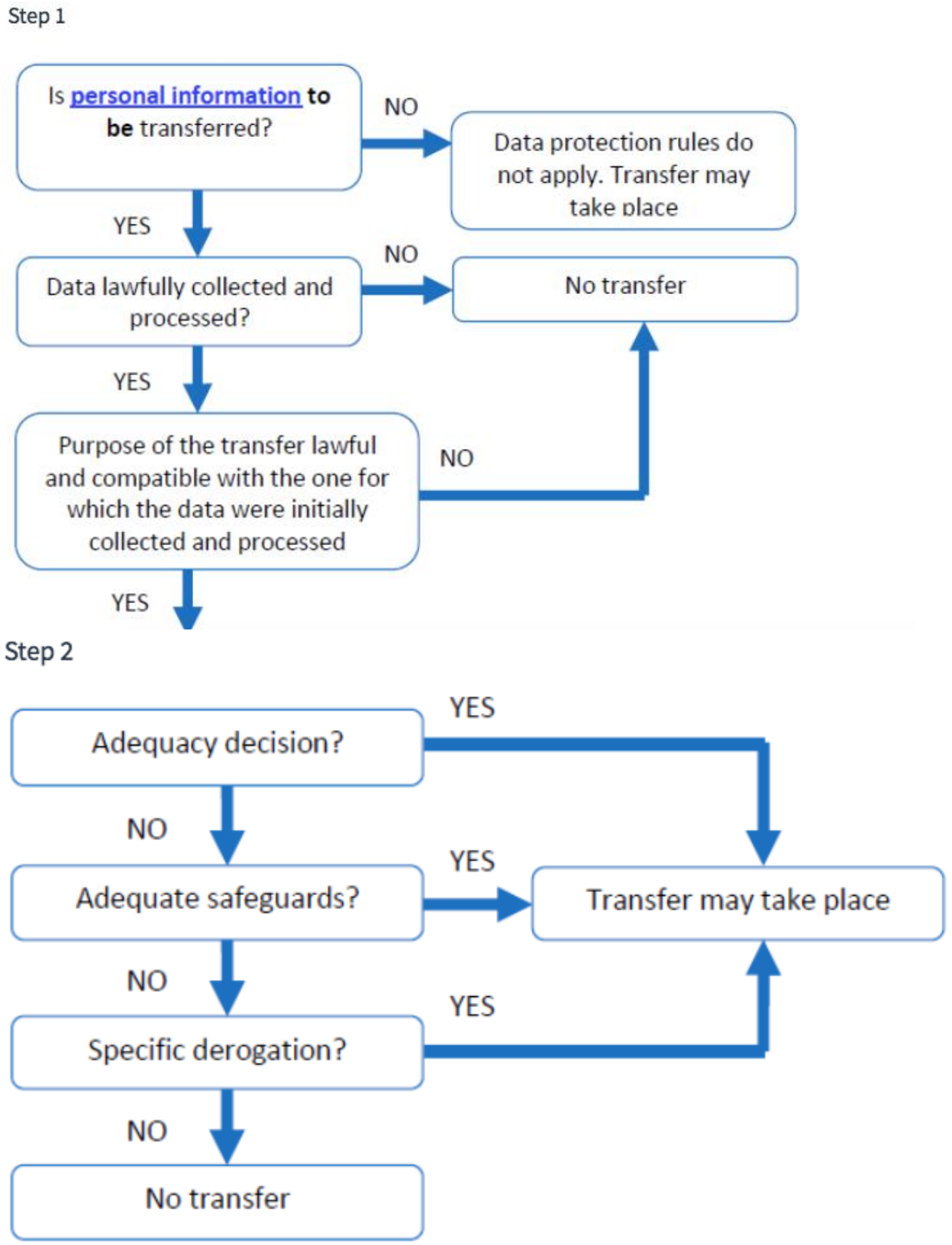
2. What are the risks of data transfers?

- The GDPR offers an adequate level of protection for personal data located within the EEA. Third countries might not offer such a protection

- The risk of an international transfer = there is no guarantee that personal data will be treated according to the safeguards the GDPR offers
  - access by foreign authorities (cf. **Schrems II**)
  - the third country does not offer the same protection or does not impose the same obligations to controllers
  - the rule of law and legal protections for fundamental (human) rights and freedoms are lacking in the non-EEA country

- Before a data transfer takes place, additional **adequate measures** or **appropriate safeguards** must be taken in order to create protection

3. How to organize a data transfer (the basics)?



Safeguards and measures for data transfers (chapter V GDPR)		
Principle	No transfer of data to third countries because there is no adequate level of protection	
Exception	**1. Adequacy decision** *Article 45 GDPR*	‘**White list’** of third countries
	2. **Appropriate safeguards** *Article 46 GDPR* A. without permission DPA	Instrument between public authorities or bodies
		Binding corporate rules
		Standard data protection clauses after approval EC
		Standard data protection clauses after approval DPA and EC
		Approved code of conduct
		Approved certification mechanism
	B. with permission DPA	Contractual clauses
		Administrative arrangements between public authorities or bodies
	3. **Derogations** for specific situations *Article 49 GDPR* *Exceptional* *Occasional* *Non-repetitive*	Explicit consent of the data subject
		Performance of a contract between the controller and the data subject
		Performance of a contract in the interest of the data subject
		Important reasons of public interest
		Legal claims
		Vital interests and data subject is incapable to consent
		Public record
		Compelling legitimate interest if not repetitive, limited number of persons involved and subject to notification to the DPA
		EU or Member State law provisions for important reasons of public interest

Countries with an Adequacy Decision (“white list”)

Andorra

Argentina

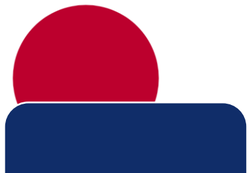
Canada

Faroe Islands

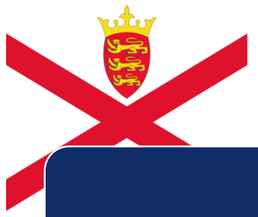
Guernsey

Israel

Isle of Man



Japan



Jersey

New Zealand

Switzerland

Uruguay

~~The United States of America (limited to the Privacy Shield Framework)~~

Appropriate safeguards - Standard contractual clauses

What are Standard Contractual Clauses?

- Listed as an appropriate safeguard under article 46 GDPR
- According to the CJEU, SCC are a transfer tool that may serve to ensure contractually an essentially equivalent level of protection for data transferred to third countries
- At the moment, there are two sets of SCC;
  - EU controller to non-EU or EEA controller
  - EU controller to non-EU or EEA processor
- New obligation to investigate law of data importer (see EDPB guidance)

New set of Standard Contractual Clauses:

- New SCC contain several modules to be used by companies, depending on the transfer scenario and designation of the parties under the GDPR, namely:
  (i) controller-to-controller transfers,
  (ii) controller-to-processor transfers,
  (iii) processor-to-processor transfers and
  (iv) processor-to-controller transfers.
- In addition to the general clauses, controllers and processors should select the module applicable to their situation, which makes it possible to tailor their obligations under the SCC to their corresponding role and responsibilities re data processing.
- It should be possible for more than two parties to adhere to the SCC.
- Additional controllers and processors should be allowed to accede to the SCC as data exporters or importers throughout the life cycle of the contract of which those clauses form a part.

4. So what changed with Schrems II?

- In the Schrems II judgment (C-311/18) rendered on 16 July 2020, the Court of Justice ruled on a number of questions related to the export of personal data.

- **the EU-US privacy shield** (article 45 GDPR) is annulled as the law of the USA does not provide for an adequate level of data protection, essentially equivalent to that of the EEA

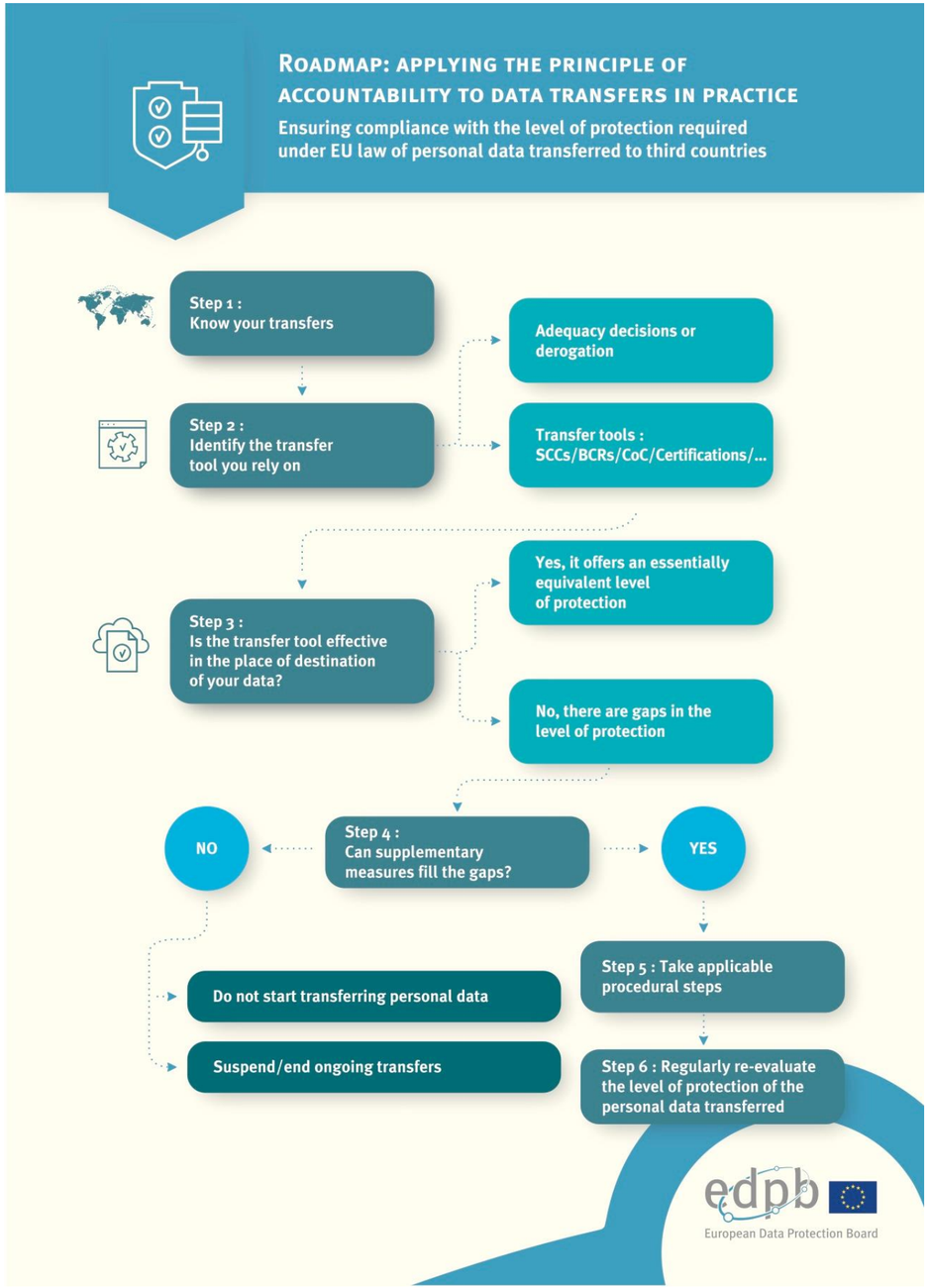
- **SCC** (article 46 GDPR) remain valid

  - Controllers relying on SCC are required to verify, on a case-by-case basis (and in collaboration with the recipient of the data in the third country outside the EEA), whether the legislation of the third country ensures a level of protection that is essentially equivalent to that guaranteed in the European Economic Area.

  - If such a level of protection is not ensured, the data exporter should either cease the transfer of personal data to the third country or implement **supplementary measures** following a data transfer impact assessment in order to ensure a level of data protection as required by EU law.

5. And what happened next?

- 2 EDPB recommendations
  - Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
  - Recommendations 02/2020 on the European Essential Guarantees for surveillance measures



Recommendations 01/2020 - Step-by-Step approach

Step 1 – Know your transfers

Map all transfers of personal data to third countries (including onward transfers, remote access, use of cloud storage solutions etc.).
Document all transfers internally, *e.g.* by using the record of processing activities.

Step 2 – Identify the relevant transfer tools

For each transfer, identify the relevant transfer tool of Chapter V GDPR (*e.g.* standard contractual clauses, binding corporate rules, derogations, *etc.*). If the transfer cannot be based on an adequacy decision or on a derogation as provided for by art. 49 GDPR, proceed with Step 3.

Recommendations 01/2020 - Step-by-Step approach

Step 3 – Assess whether the Article 46 GDPR transfer tool is effective in the light of all the circumstances

Selecting an Article 46 GDPR transfer tool (such as standard contractual clauses or binding corporate rules) is not sufficient in itself. The data exporter is required to assess the effectiveness of this transfer tool, i.e. whether the circumstances of the transfer ensure a level of protection guaranteed by EU law.

If legislation exists in the third country that might impinge on the effectiveness of the transfer tool, the data exporter should examine this legislation on the basis of the European Essential Guarantees (EDPB Recommendations 02/2020)

If the third country does not have legislation that impinges on the effectiveness of the transfer tool, the data exporter should take into account other objective elements enabling the third country's authorities to require or gain access to the personal data being transferred (such as reported incidents, practice, legal powers and technical, financial and human resources at its disposal).

Recommendations 01/2020 Step-by-Step approach

Step 4 – Adopt supplementary measures:

If the result of the assessment in Step 3 shows that the legislation of the third country might impinge on the effectiveness of the transfer tool, the data exporter should take supplementary measures (i.e. contractual, technical and organisational measures).

If appropriate measures cannot be adopted, the transfer should not proceed without notification to the competent supervisory authority.

Step 5 – Procedural steps if you have identified effective supplementary measures

These procedural steps may differ depending on the Article 46 GDPR transfer tool you are using or envisage using. For example, putting in place standard contractual clauses, binding corporate rules, implementing supplementary measures, consulting with the competent supervisory authority if ad hoc transfer terms are used, ...

Step 6 – Re-evaluate at appropriate intervals

Data exporters should re-evaluate at appropriate intervals whether the level of protection accorded to the data transferred to third countries is still sufficient and should monitor whether there have been or will be any developments that may affect the level of protection.

Supplementary measures

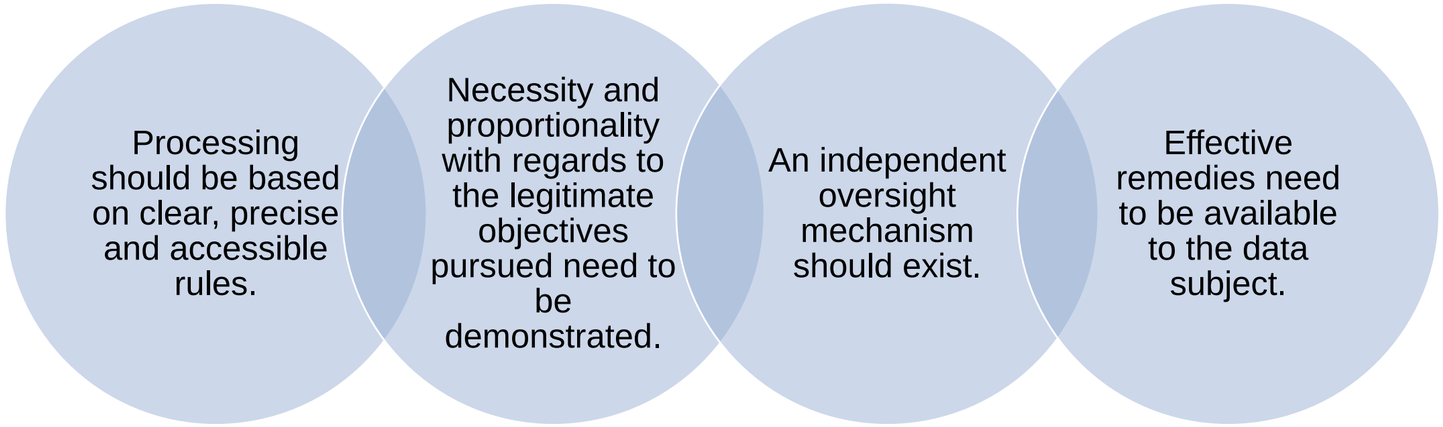
- Annex 2 to the 01/2020 recommendations contains a non-exhaustive list of examples of supplementary measures to ensure essential equivalency.
- The supplementary measures are divided into (i) technical, (ii) contractual and (iii) organizational safeguards.
  - contractual and organisational measures alone are not sufficient, as they generally do not overcome access to personal data by public authorities;
  - technical measures are the most important measures for reaching the required standard of protection to render access by third country public authorities to personal data ineffective

Technical measures	Contractual measures	Organizational measures
• Encryption • Pseudonymization • Recipients that are exempt from government access, e.g. by duty to professional secrecy • Split or multi-party processing, i.e. the data importer receives data that is split in such a way that no part of the data suffices to reconstruct the data or to attribute the data to a specific data subject • …	• Obligations on the data importer to use specific technical measures • Additional transparency obligations on the data importer • Obligations on the data importer to take specific actions, e.g. the commitment to review the legality of any order to disclose the data • Empowering data subjects to exercise rights, e.g. data may only be accessed with the express of implied consent of exporter and/or data subject • …	• Internal policies and procedures regulating intra group data transfers • Transparency and accountability measures, e.g. publication of transparency reports • Organizational methods and data minimization, e.g. adoption of strict and granular data access and confidentiality policies • Adoption of standards and best practice, e.g. data security and data privacy policies, codes of conduct or international standards such as ISO norms • …

Recommendations 02/2020 - European Essential Guarantees

- Recommendations 02/2020 supplement Recommendations 01/2020 and contain a framework of four guarantees to help the data exporter assess in Step 3 whether the legislation of a third country (including possible public authority surveillance measures and government access to data) can be regarded as a justifiable interference with the rights to privacy and protection of personal data under the EU Charter of Fundamental Rights.

- The European Essential Guarantees are key element in the data transfer impact assessment. The four guarantees that must be considered as part of the overall assessment are:



- '*These guarantees require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework*.' - EDPB

Use of cloud services – judgment of French Conseil d'État on the usage of Amazon Web Services (AWS)

FACTS

The French Ministry of Health decided to integrate the medical portal Doctolib, which uses hosting services provided by AWS Luxembourg, into its online booking system for COVID-19 vaccinations

Several associations and trade unions considered that the use of AWS would constitute a serious and manifestly unlawful breach of personal data protection rights (cf. Schrems II) on the grounds that:

- AWS Luxembourg is a subsidiary of AWS US, and;
- there is a risk of unauthorised access to the data by US authorities.

The Council of State rejected the request (albeit in an interlocutory decision) for two reasons.

1. NO HEALTH DATA

The Council of State noted that the data collected in the context of the vaccination arrangements are **not health data** because they do not reveal the medical reasons for eligibility for vaccination.

The data only relate to the **identification** of the persons and to making vaccination **appointments**.

These data are also **deleted at the latest after three months** from the date of the appointment, and data subjects can also delete them directly online.

2. ADDITIONAL SAFEGUARDS

The agreement between Doctolib and AWS Luxembourg would provide for a specific **addendum on access requests** by a foreign authority, which would provide that AWS **challenges** any access request in violation of European regulations.

Furthermore, the data was stored in the European Economic Area, namely in **France and Germany**

Doctolib has also set up a **security system** for the personal data hosted by AWS based on an **encryption** procedure carried out by **a trusted third party** located in France, in order to prevent third parties from reading the data.

Brexit

Data transfers to the UK

eubelius

advocaten avocats attorneys

EU-UK Trade & Cooperation Agreement

UK as a third country

As a result of Brexit, the UK is a **third country** in relation to the GDPR, as of 1 January 2021

The EU-UK Trade and Cooperation Agreement includes a **bridging mechanism** on further exchange of personal data between the EU and the UK

This mechanism lasts for a transition period of four months initially (until 30 April 2021) with the possibility of extending it for another two months (until 30 June 2021)

During the transition period

Transmission of personal data from the EU to the UK shall not be considered as transfer to a third country under EU law, provided that

(i) the UK adheres to the conditions listed in the agreement and

(ii) no adequacy decision is adopted during the transition period

If an adequacy decision is adopted by the EC, this bridging mechanism will cease and instead the adequacy decision will apply (see next slide)

After the transition period

The free flow of data to the UK will no longer be possible without

(i) an adequacy decision from the European Commission, or

(ii) the implementation of a data transfer tool as listed in Chapter V of the GDPR.

If no adequacy decision is adopted by the EC, personal data can only be transferred based on the appropriate safeguards and derogations listed in Articles 46 or 49 GDPR, e.g. standard contractual clauses, binding corporate rules, …

To adequacy or not to adequacy?

- On 19 February 2021, the EC launched the process towards the adoption of two adequacy decisions for transfers of personal data to the United Kingdom:
  - an adequacy decision under the General Data Protection Regulation (GDPR); and
  - an adequacy decision under the Law Enforcement Directive (LED).

- The EC assessed the UK's law and practice on personal data protection (based on comprehensive explanatory material formally provided by the UK to the EC in March 2020), including the rules on access to data by public authorities and secret services. It concludes that the UK ensures a level of data protection essentially equivalent to the level guaranteed under the GDPR and LED.

- The decisions will be formally adopted after;
  - the European Data Protection Board has issued a non-binding (although likely persuasive) opinion in relation to the decision; and
  - the decisions have been approved by the EU Member States acting through the European Council.

- Once adopted, the decisions would be valid for a first period of four years, with a possibility to renew the adequacy finding if the level of protection in the UK would continue to be adequate after those 4 years.

Questions ?

For more information, please contact:

Anneleen Van de Meulebroucke

Counsel

+32 2 543 32 07

Anneleen.vandemeulebroucke@Eubelius.com

CRANIUM

Bart Van Buitenen

CRANIUM

Supplementary measures Schrems II: a technical perspective.

CRANIUM

Spoiler Alert

Summary of this presentation:

The EDPB has basically said that full compliance for the most common use cases of transferring data to third countries is currently impossible.

We are left with applying the **risk based approach** to take the measures that we *can* take, and focus on **accountability** to document them to the best of our abilities until new SCCs arrive.

Cases may then be taken to court, where case-by-case the risk based approach and the relevant documentation will be assessed.

Overview

Supplementary measures in theory

- EDPB guidance on supplementary measures
- Draft SCCs (including EDPS & EDPB joint opinion)

Supplementary measures in practice

- Conseil d’Etat AWS case
- Measures implemented by processors in my experience
- Example response by US based processor while awaiting new SCCs

Technical measures

Supplementary technical measures in theory

EDPB guidance

- Supplementary measures may be contractual, technical or organizational in nature.
- Contractual and organizational will generally not suffice.
- I will focus on technical measures as defined by a number of use cases in the guidance

EDPB guidance context

From the guidance:

The following measures are examples of supplementary measures you could consider when you reach **Step 4 “Adopt supplementary measures”. This list is not exhaustive.** Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. You should select those supplementary measures that can effectively guarantee this level of protection for your transfers.

Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment “Schrems II” if and to the extent that it **addresses the specific deficiencies identified in your assessment of the legal situation in the third country**. If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data.

EDPB guidance: Use Case 1

Storing data in third country for backup purposes that do not require access to data in the clear.

If

- Strong encryption before transmission
- Encryption algorithm and setup state of the art and not crackable
- Strength encryption vs. how long should data be confidential (e.g. avoid long term cracking thus exposure)
- Encryption is flawlessly implemented with conformity proof (eg certification)
- Keys are reliably managed
- Keys retained under control data exporter, or trusted entities wihtin EU

In other words: encrypted (before sending!) backups storage is fine.

EDPB guidance: Use case 2

A data exporter first pseudonymises data it holds, and then transfers it to a third country for analysis, e.g., for purposes of research.

If

- a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject,
- that additional information is held exclusively by the data exporter and kept separately in a Member State or adequate third country,
- disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and
- 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 country may possess that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

In other words: data is anonymized before sending.

EDPB guidance: Use case 3

Encrypted data is transferred through third country on its way to adequacy.

- State of the art transport encryption
- Decryption only possible outside third country
- Trustworthy PKI
- Protection against passive + active attacks
- If necessary also end to end encrypted on application level, state of the art, taking ito account time info needs to be confidential, flawlessly implemented, no backdoors exist,
- Keys reliably managed

In other words: end-to-end encryption by trusted provider

EDPB guidance: Use case 4

Data importer in third country is protected by that country's law, e.g. for provision of medical care or legal services.

If

- Resident data importer is exempt from providing access due to professional secrecy
- The exemption covers all information that may provide access to data
- Importer does not forward data to processor or other party that may in turn give access to data
- Data in transit it encrypted
- Decryption key only available to importer
- Data exporter verifies that encryption key matches decryption key by importer

In other words: importer is only one with access to the data and this access is protected by strong legal guarantees such as professional secrecy (doctor, lawyer).

EDPB guidance: Use case 5

Data is split and then sent to two different parties in third countries, one part of the data does not allow identification of individuals

If

1. Data is split where each part does not allow identification of individuals and is transferred to two different processors in two different jurisdictions,
2. The processors process jointly (secure multi-party computation) but no information is revealed to them other than one part of the data
3. No public authority in the two jurisdictions has access to both data sets

Then the split data processing provices an effective supplementary measure.

In other words: splitting data into anonymous datasets and sending them to different processors. Not familiar with any practical application of this use case.

EDPB guidance: No effective measures!

Use cases 6 and 7 are situations where EDPB does not find effective technical measures:

- Use case 6: Cloud service provider needs access to the data to provide its service and provider is located in jurisdiction that does not provide sufficient guarantees (= most US cloud providers such as Microsoft Teams & Azure, AWS, Google services, etc)
- Use case 7: transfers between entities of an organization where these entities need access to the data and the entity is located in jurisdiction that does not provide sufficient guarantees (= BCR's should still cover this, no mention on approved BCR review)

In other words: the EDPB was not able to provide effective technical measures for the most common use cases out there.

Draft SCCs (including EDPB & EDPS comments)

New SCCs have not yet approved, info below refers to ANNEX Part III in the draft SCCs proposed by Commission (1/2)

- Must include concrete security measures, not generic descriptions
- Includes examples subjects without concrete information, but provides insight to what is expected for additional measures.
- Pseudonimization, encryption
- Ensuring CIA and resilience or processing systems and services
- Ability to restore availablity and access to personal data in event of physical or techincal incident
- Process for testing, assessing and evaluating the effectiveness of measures

Draft SCCs (including EDPB & EDPS comments)

New SCCs have not yet approved, info below refers to ANNEX Part III in the draft SCCs proposed by Commission (2/2)

- User identification and authorization
- Protection of data during transmission and storage
- Physical security
- Event logging
- Systen configuration, including default configs
- Internal IT and IT security governance and management
- Requirements for certification

Technical measures

Supplementary technical measures in practice

Technical measures by processors

Regardless of the many use cases described, the EDPB basically stated that **full comliance is currently impossible** for the most common use cases out there.

Data flows will not suddenly stop, so we need to revert to one of the most basic principles in GDPR: risk based approach.

TIAs are the advised instrument: they will document this **risk based approach** and will provide you with the required **“accountability”** on why certain transfers continue even when full compliance will need to wait for new SCCs.

Following slides document examples of measures that can help to document why the risk has been sufficiently reduced.

Technical measures by processors

Recent example: Conseil d'Etat case regarding Doctolib & AWS

- Data minimization: data transferred was not sensitive (art 9)
- Storage limitation: limited retention time (3 months)
- Control for data subject: option for data subject to remove the data manually online
- Addendum with AWS regarding government access *(for what it's worth)*
- Security: use of third party to encrypt the data and prevent unauthorised access
  - Third party manages key (Atos, FR company)
  - Used "Bring your own key" mechanism in AWS

Technical measures by processors

Examples which should *(should = until verified in legal proceedings this is what we think will be enough)* provide sufficient guarantees:

- On-device processing: detailed data is processed on user devices and only aggregated data is sent for further processing
- End-to-end encryption: third parties only handle encrypted data
- Anonymization: data was anonymized before transfer to third countries (aggregation, not third party anonymization)
- “external” on-device encryption and anonymization: use third party SDKs to anonymize or encrypt data before transferring onward e.g. to US based clouds

Measures by processors:

Example response by a US based processor following a number of detailed questions after Schrems II:

- All data are encrypted with AES256 in transit and at rest
- Confirmation that no requests have been received in context of FISA
- No court has found the processor a FISA 702 “electronic communication service provider”
- They will not comply with a FISA bulk surveillance request
- Will take all legally available action to challenge such requests and non-disclosure provisions should it happen
- They will publish transparency reports every 6 months
- Will proactively notify if anything happens that means they can no longer comply with SCCs or additional safeguards

Presentation by

Bart van Buitenen

bart@cranium.eu

Linkedin: https://www.linkedin.com/in/bartvanbuitenen/

Sources

- http://curia.europa.eu/juris/document/document.jsf;jsessionid=AB489A81EEB06DAADB45CF01C300E296?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3358660
- https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
- https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_annexjointopinion_202102_art46sccs_en.pdf
- https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en
- https://www.essentialguarantees.com
- https://interhop.org/2021/03/10/reponse-franceinter-doctolib
- https://tanker.io/tanker-whitepaper.pdf

CYBER SECURITY
COALITION.be

Thank you