Your data in the cloud? Data protection do's and don'ts for a cloud-based project

Association of International Business Lawyers

Philipp Fischer
March 31, 2023

Plan

I. Introduction

II. Cross-border transfer of personal data

III. Transfer of data to the United States

IV. Use of the cloud

Source: https://subscription.packtpub.com/book/cloud-and-networking/9781838555276/3/ch03lvl1sec10/introducing-the-cloud

I. Introduction (1/3)

Is a disclosure of data a "processing activity" (Article 2 (1) revDPA)?

1. Concept of "personal data"

- Personal data: "all information relating to an identified or identifiable person" (Article 5 (a) revDPA).
- A person is identifiable if he/she can be identified on the basis of additional information with reasonable efforts.
- Case-by-case analysis taking into account, amongst others, the technical possibilities available to the recipient (→ evolving approach depending on technological developments).

Case n° 1: anonymized data

- Data is anonymized if the reference to a person is irreversibly eliminated. In other words, there is no remaining possibility to link the data to the data subject.
- In such situation, the information does not relate to an identifiable person and is therefore out of the scope of the DPA.

I. Introduction (2/3)

Case n° 2: pseudonymous data

- There is pseudonymous data if the reference to a person is reversibly eliminated. For instance, when data is encrypted, the use of the encryption key allows access to the personal data.

- In such a situation, even though the data subject is not directly identified through pseudonymous data, he/she remains identifiable to the person holding the encryption key, who may decode the encrypted data and access personal data. However, a third party that does not have access to the encryption key may not identify the data subject.

Message relating to the revised DPA, FF 2017 6640

- *La loi ne s'applique pas aux données qui ont été anonymisées si une ré-identification par un tiers est impossible (les données ont été anonymisées complètement et définitivement) ou* ***ne paraît possible qu'au prix d'efforts tels qu'aucun intéressé ne s'y attèlera****.* ***Cette dernière règle vaut aussi pour les données pseudonymisées*** (NB: unlike under the GDPR).

Decision n° HG190107-O of 4 May 2021 of the Handelsgericht of the canton Zurich

- In the case of pseudonymous data, if a third party does not have access to the encryption key and may therefore not reestablish the link between the data and the data subject, the information is in principle not personal data and is out of scope of the DPA (from the point of view of the third party).

- In its decision, the *Handelsgericht* however tempers this approach and specifies that if the third party receiving the data may, provided reasonable efforts, gain access to the encryption key or otherwise gain access to information that allows identification of the data subject, the data is covered by the scope of the DPA (which was the case in this decision).

I. Introduction (3/3)

2. Concept of "processing"

Article 5 (d) revDPA: processing means "any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, **disclosure**, archiving or destruction of data " (highlight added).

- A disclosure of personal data to a recipient in Switzerland or in a foreign country therefore constitutes a data processing activity within the meaning of the DPA (and the revDPA)

II. Cross-border transfers of personal data (1/4)

1. Introduction

- Distinction between two scenarios:

  a) **Scenario 1**: the receiving country has a legislation guaranteeing an "adequate" level of protection.

  b) **Scenario 2**: the receiving country does not have a legislation guaranteeing an "adequate" level of protection.

- Note: online publication of data in order to inform the public (media) does not qualify as a disclosure to a foreign country, even if the data is available from abroad (Article 18 revDPA).

II. Cross-border transfers of personal data (2/4)

2. Scenario 1 – Disclosure to an "adequate" country (Article 16 (1) revDPA)

- Concerned countries

  a) All countries that (i) adhered to the (revised) Convention 108 of the Council of Europe and (ii) effectively implement it.

  b) The "list of the Data Protection Commissioner" (Article 7 of the current DPO) will be replaced by the list in Appendix 1 of the new Ordinance.

  c) In practice: all Member States of the European Union will feature on this list.

- Consequences

  a) Transfer of personal data to these countries will not trigger additional requirements.

  b) The general principles of data protection must nevertheless be complied with (Article 6 revDPA: lawfulness / good faith / proportionality / finality)

II. Cross-border transfers of personal data (3/4)

3. Scenario 2 – Disclosure to a "non-adequate" country

Option 2A – specific guarantees (Article 16 (2) et (3) revDPA)

Contractual possibilities

a) *Contract between the disclosing party and the receiving party*

- Use of standard data protection clauses already recognized by the Commissioner (for example, "standard contractual clauses for the EU", cf. *slide* n° 15) (Article 16 (2) (d) revDPA) → ⚠ implementation of *Schrems II* (cf. *slide* n° 13 s.)
- Possibility also to use *ad hoc* clauses specially drafted and incorporated in the contract between the disclosing party and the receiving party that have to be communicated to the Commissioner before the transfer (Article 16 (2) (b) revDPA)

b) *Within a group of companies:* use of *Binding Corporate Rules* (BCR / "intra-group contract") approved by the Commissioner or by the data protection authority of an "adequate" foreign country (Article 16 (2) (e) revDPA).

Other possibilities

a) International treaty (article 16 (2) (a) nLPD)

c) Specific guarantees established by a federal body and communicated to the Commissioner (Article 16 (2) (c) revDPA) (applicable to the public sector)

d) Other guarantees provided by the Federal Council (Article 16 (3) revDPA)

II. Cross-border transfers of personal data (4/4)

3. Scenario 2 – Disclosure to a "non-adequate" country (continuation)

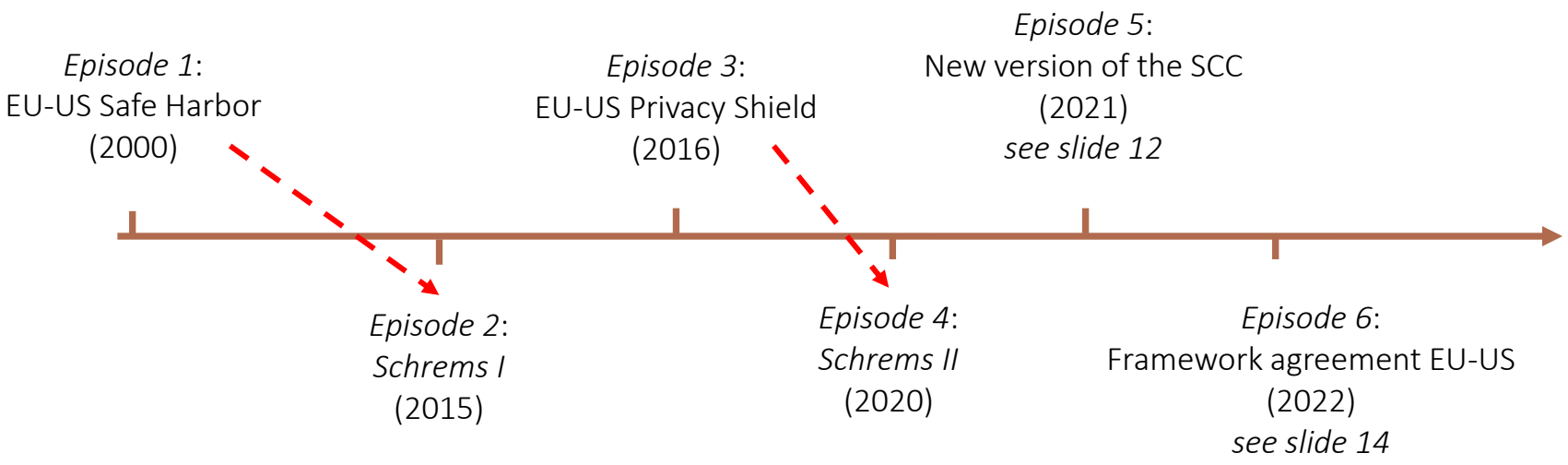
Option 2B – 7 derogations (Article 17 revDPA)

1. Explicit consent of the concerned person
2. Transfer is directly connected to the conclusion or the performance of a contract:
   a) Between the controller and the data subject
   b) Between the controller and its contracting partner in the interest of the data subject [new]
3. To safeguard an overriding public interest
4. For the recognition, exercise or defense of legal claims before a court or *another competent foreign authority [new]*
5. Protection of life or physical integrity
6. The data subject has made the personal data publicly accessible and has not expressly prohibited its processing
7. *The data originates from a register provided for by law and which is accessible to the public or to persons with a legitimate interest [new]*

→ In red: on demand, said information must be disclosed to the Commissioner, which requires, from a data controller's perspective, a greater duty to document in order to answer a possible request from the authority

III. Transfer of personal data to the United States (1/3)

Timeline



III. Transfer of data to the United States (2/3)

Episode 5: New version of the SCC (2021)

In the EU

Modules

- **Module 1**: Transfer of liability from controller to controller
- **Module 2**: Transfer of liability from controller to processor
- **Module 3**: Transfer of liability from processor to processor
- **Module 4**: Transfer of liability from processor to controller

Appendices

- **Appendix I –** list of parties, description of transfers, competent supervisory authorities *[applicable to all]*
- **Appendix II –** technical and organisational measures *[applicable to modules 1, 2 and 3]*
- **Appendix III –** list of secondary processors *[applicable to modules 2 and 3]*

Implementation

- Since 27 September 2021, the SCC must be used for new transfers outside of the EEA.
- As of 27 [EU] / 31 [CH] December 2022, the SCC must be used for all transfers outside of the EEA (including already existing transfers).

In Switzerland ("*Swiss finish*")

- The last version of the SCC was approved by the Commissioner rapidly after their implementation in the EU (Position paper of the Commissioner dated 27 August 2021).
- According to the Commissioner, the data controller (or processor) that exports personal data must adjust the SCC with regard to certain points (cf. next *slide*).

	Case 1: Data transmission is exclusively subject to the FADP[13]	Case 2: The data transfer is subject to both the FADP and the GDPR.[14]	
		Option 1: The parties provide for two 'separate' arrangements for data transfers under the FADP and under the GDPR	Option 2: The parties adopt the GDPR standard for all data transfers
Competent supervisory authority in Annex I.C under Clause 13	Mandatory FDPIC	Parallel supervision: FDPIC, insofar as the data transfer is governed by the FADP; EU authority insofar as the data transfer is governed by the GDPR (the criteria of Clause 13a for the selection of the competent authority must be observed)	
Applicable law for contractual claims under Clause 17	Swiss law or the law of a country that allows and grants rights as a third party beneficiary	Swiss law or the law of a country that allows and grants rights as a third party beneficiary for contractual claims regarding data transfers pursuant to the FADP; law of an EU member state for those according to the GDPR (free choice for Module 4)	Law of an EU member state (free choice for Module 4)
Place of jurisdiction for actions between the parties pursuant to Clause 18 b[15]	Free choice	Free choice for actions concerning data transfers pursuant to the FADP; court of an EU member state for actions concerning data transfers pursuant to the GDPR (free choice for Module 4)	Courts of an EU member state (free choice for Module 4)
Adjustments or additions concerning the place of jurisdiction for actions brought by data subjects	The SCCs must be supplemented with an annex specifying that the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c.		
Adjustments or additions regarding references to the GDPR	The SCCs must be supplemented with an annex specifying that references to the GDPR are to be understood as references to the FADP	The SCC must be supplemented with an annex specifying that the references to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP.	
Supplement until the entry into force of the revFADP[16]	The SCCs are to be supplemented with an annex in which it is specified that the clauses also protect the data of legal entities until the entry into force of the revised FADP.		

Source: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html

III. Transfer of personal data to the United States (3/3)

Episode 6: Framework agreement EU-US

In the EU

- On March 25, 2022, the European Commission and the United Stated announced that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the *Schrems II* decision of July 2020.
- Decision generally expected in 2023.

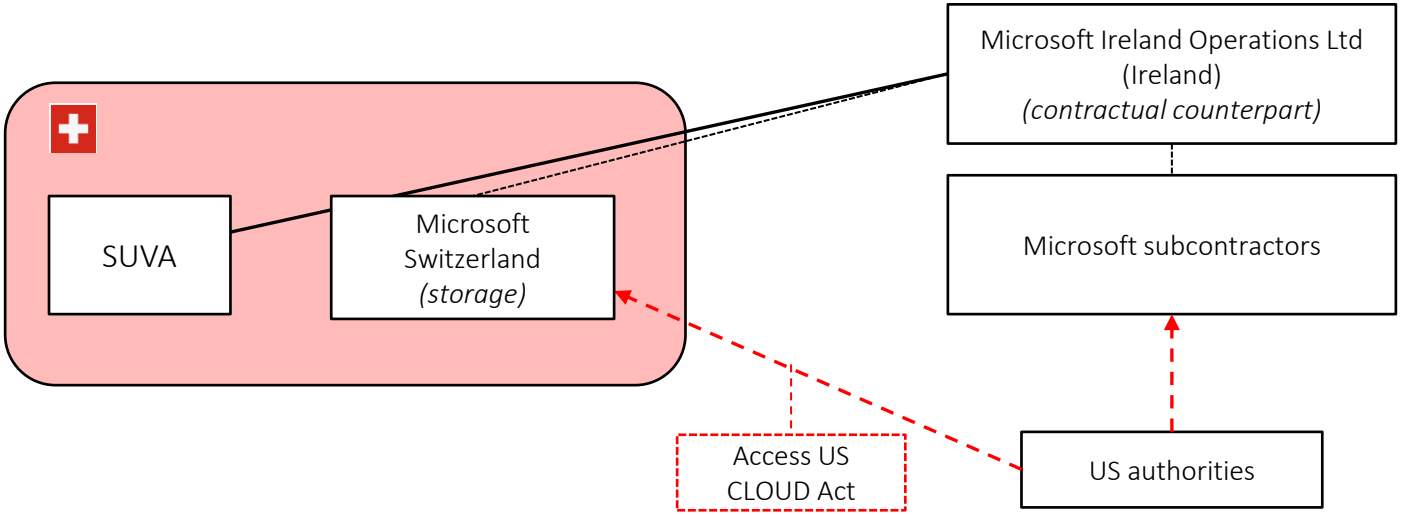
In Switzerland

- Switzerland has not yet made such an announcement.
- Switzerland will probably wait for the implementation of the EU/US framework agreement to adopt a similar approach.

IV. Use of cloud-based services (1/4)

1. Situation

- In case of use of cloud services, the data is often not directly stored in a country that does not offer an adequate level of protection, but may be accessed from such a country.
- For example, when using Microsoft's M365 services, the data may be stored in Switzerland and the processor is the Irish entity of the Microsoft Group.
- Does this situation lead to a transfer of data to the US? The Commissioner published a position paper relating to a project of the *Caisse nationale suisse d'assurance en cas d'accidents* (SUVA) regarding the use of Microsoft's M365 cloud services (Outlook and Teams).



IV. Use of the cloud (2/4)

2. Legal issues

Transfer of personal data abroad according to Swiss law (Article 6 DPA / Articles 16 et seq. revDPA)?

- Transfer to a country providing an adequate level of protection → transfer possible
- Transfer to a country which does not provide an adequate level of protection (*e.g.*, the United States) → transfer possible only if an adequate level of protection may in another way be guaranteed (for example contractually).
  - ➢ Due to the surveillance measures available to US authorities, contractual measures are not always sufficient to guarantee an adequate level of protection (cf. decision Schrems II).

US CLOUD Act?

- The US CLOUD Act obliges certain IT service providers that have a link to the US to disclose data to US authorities (irrespective of the place of storage of said data), provided that the proceedings in which such data is requested concern serious crimes.

IV. Use of the cloud (3/4)

3. Position of the SUVA

- The SUVA has identified in its analysis of the project a risk that the data stored on the cloud may be accessed by US authorities pursuant to the US CLOUD Act.

- After analyzing said risks, the SUVA considers that access to said data by US authorities is, in this context, highly unlikely ("*höchst unwahrscheinlich*") and that the use of M365 services is lawful with regard to the DPA.

4. Position of the Commissioner

- The Commissioner considers that the existence of a risk of disclosure of personal data to the US pursuant to the US CLOUD Act triggers, in itself, the application of the provisions of the DPA applicable to crossborder transfers of personal data, regardless of the "Swiss" character of the project (*e.g.,* data controller in Switzerland and storage of the data in Switzerland on the servers of the processor).

- Then, the Commissioner maintains his position according to which, if there is (*even a minimal*) risk of access by authorities of a country that does not provide an adequate level of protection, no personal data may be transferred to the importer (regardless of the use of Standard Contractual Clauses).

IV. Use of the cloud (4/4)

Step 1: Review of contractual guarantees: main issues

- Obtaining the latest version of the contractual package for the Swiss market
- Integration of Standard Contractual Clauses with Swiss finish (+ notification to the Commissioner (article 6 (3) LPD) / not necessary under the RevDPA)
- Financial institutions (FINMA requirements):
  - Notion of "personal data" vs. "CID"
  - Limitation of liability in accordance with Swiss law
  - Right of audit in favor of all Group entities that benefit from the solution
  - Information on cyber incidents (FINMA requirements go beyond the GDPR/RevDPA)

Step 2: Review of technical and operational measures (TOMs)

- Catalog of TOMs according to the identified risks
- Data localization issue in terms of application of possible US legislation (with extra-territorial reach)

Step 3: Conduct a documented Transfer Impact Assessment (TIA) (sometimes a sub-chapter of the Data Privacy Impact Assessment / DPIA)

- Organize a workshop bringing together the various stakeholders within the Bank (project manager, regulatory affairs, IT security, IT department, DPO) with the representative of the legal department (or an external lawyer) playing the role of *chef d'orchestre*
- Points to address (examples):
  - Likelihood that a foreign authority has a lawful access right to the data and intends to enforce it against the provider.
  - Probability that a foreign authority will actually succeed in asserting this access right against the provider.
  - Likelihood of lawful access through a mass surveillance mechanism.

Step 4: Decision by the management

Thank you for your attention

Philipp Fischer
Associé, LL.M. (Harvard)

pfischer@obersonabels.com

+41 58 258 88 88