November 2015

Newsletter

Special Edition

Data Transfers from Switzerland to the US post-Safe Harbor

Overview and guidelines from a Swiss perspective

walderwyss attorneys at law

Data Transfers from Switzerland to the US post-Safe Harbor

In the aftermath of the landmark decision of the Court of Justice of the European Union (CJEU) of 6 October 2015 (C-362/14) invalidating the European Commission's US-EU Safe Harbor decision 2000/520/EC, both the Swiss Federal Data Protection and Information Commissioner (the Federal Commissioner) and administrative bodies as well as commentators on both Swiss, EU and EU member state level have published varied reactions and statements.

This Newsletter gives an overview from a Swiss point of view of

- the legal framework for data transfers from Switzerland abroad (see section 1.),
- what needs to be done (see section 2.),
- how to assess whether you are affected (checklist for data exporters; see section 3.), and
- what the future may bring (see section 4.).

By Jürg Schneider
Dr. iur., Attorney at Law
Partner
Phone +41 58 658 55 71
juerg.schneider@walderwyss.com

and Monique Sturny
Dr. iur., LL.M., Attorney at Law
Telefon +41 58 658 56 56
monique.sturny@walderwyss.com

1. Legal framework for data transfers from Switzerland abroad

1.1. Transfers of personal data from Switzerland abroad

If personal data are **transferred from Switzerland to a recipient located in a foreign country,** such transfer is considered processing of personal data and must therefore comply with the Swiss Federal Data Protection Act (**DPA**). Even a mere granting of access to personal data to an individual or legal entity domiciled abroad qualifies as a transfer for the purposes of the DPA. Disclosures from Switzerland to group companies abroad also qualify as transfers abroad.

The DPA prohibits a transfer of personal data abroad if such transfer could seriously endanger the personality rights of the data subjects. Such a danger can exist if the personal data are transferred to a country whose legislation does **not provide for an adequate protection of the personal data** being transferred (art. 6 para. 1 DPA). Unlike the data protection laws of most other countries, the DPA not only protects personal data relating to individuals, but also personal data relating to legal entities. This broad scope of protection can create difficulties in the context of cross-border transfers, as only very few data protection legislations of other countries apply to personal data relating to legal entities. The Federal Commissioner has published a non-binding list of countries which he deems to be providing an adequate data protection level for personal data relating to individuals [1].

1 See <http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de> (last visited on 16 November 2015). With respect to Austria and Liechtenstein, the Federal Commissioner has added a remark stating that the data protection acts of these two countries apply not only to personal data relating to individuals, but also to personal data relating to legal entities. With respect to Denmark, the Federal Commissioner mentions that the Danish data protection act also applies to personal data relating to legal entities under certain conditions. Finally, the Federal Commissioner mentions on the list that the Argentinian data protection act applies not only to individuals, but equally to legal entities domiciled in Argentina.

If personal data shall be transferred to a country that does not provide for an adequate level of data protection for the personal data being transferred, such a transfer may only occur if the conditions set forth in art. 6 para. 2 DPA are fulfilled (see section 2.1 below for more details).

1.2. Transfers to the US in particular

Currently, **neither US federal law nor the laws of any US state are considered to provide an adequate level of data protection from a Swiss point of view.** Until recently, the Federal Commissioner recognised that a certification of the data recipient under the US-Swiss Safe Harbor Framework is considered to provide for an adequate data protection level in the sense of art. 6 para. 1 DPA for transfers of personal data to such recipient.

In the aftermath of the CJEU decision dated 6 October 2015 (C-362/14) declaring the European Commission's Safe Harbor decision (2000/520/EC) to be invalid, **the Federal Commissioner however published a statement on 22 October 2015 according to which he no longer considers a certification of the data recipient under the US-Swiss Safe Harbor Framework as providing for an adequate data protection level.** The Federal Commissioner's statement caused much uncertainty as to what measures actually need to be taken. Some additional guidance was published by the Federal Commissioner on 28 October 2015 (see section 2. below for more details).

As Switzerland is neither a member of the EU nor of the European Economic Area (EEA), the aforementioned CJEU decision (C-362/14) does not have any direct impact on the validity of the US-Swiss Safe Harbor Framework. Neither Swiss courts nor the Federal Commissioner are bound by decisions of the CJEU. However, obviously, the CJEU decision nevertheless has a major practical impact on Switzerland, not least since Switzerland risks to be considered as not providing for an adequate level of data protection from an EU perspective if it still allowed data transfers based on the US-Swiss Safe Harbor Framework. Against this background, the Federal Commissioner's statements did not come as a surprise, even though the Federal Commissioner has in principle no competence to declare the US-Swiss Safe Harbor Framework invalid.

However, the Federal Commissioner has indeed the competence to amend his (non-binding) list of countries which he considers to be providing an adequate data protection level[2]. **Accordingly, the Federal Commissioner has adapted said list, now declaring that the US is not considered to be providing an adequate data protection level, without any exception available based on the US-Swiss Safe Harbor Framework.**

Although the Federal Commissioner's view does not have any legally binding effect, **data exporters are strongly advised to no longer rely on the US-Swiss Safe Harbor Framework for data transfers from Switzerland to the US.**

2 See link in footnote 1 above.

2. What needs to be done from a Swiss perspective

According to the Federal Commissioner's statements of 22 and 28 October 2015, the following two measures should be taken if personal data are disclosed to the US:

- **adequate safeguards** in the sense of art. 6 para. 2 DPA are necessary (see section 2.1 below) and
- an increase of **transparency** vis-à-vis the data subjects concerned (see section 2.2 below) is recommended.

The Federal Commissioner demands of all data exporters concerned to implement the aforementioned measures by the **end of January 2016.** Hence, it seems that waiting for the possible adoption of a new US-Swiss safe harbor framework is rather not an option (see section 4. below).

2.1. Adequate safeguards

Given that the Federal Commissioner no longer considers the US-Swiss Safe Harbor Framework as providing for an adequate data protection level, adequate safeguards in the sense of art. 6 para. 2 DPA are recommended for all transfers of personal data from Switzerland to recipients located in the US.

The most commonly used safeguards are:

- **Contractual agreements:** The Federal Commissioner first of all recommends relying on contractual safeguards pursuant to art. 6 para. 2 letter a DPA. We recommend using the model contracts for the transfer of personal data to third countries issued by the European Commission (**EU Model Clauses**) adapted to Swiss law requirements or other contractual clauses explicitly recognised by the Federal Commissioner. The Federal Commissioner's statements (in particular his statement of 22 October 2015) raised confusion and insecurity on whether he deems any changes to the EU Model Clauses to be necessary. In particular, the Federal Commissioner mentions that parties to contractual agreements in the sense of art. 6 para. 2 letter a DPA should commit to the following:
  - (i) Data subjects whose data are being transferred to the US need to be clearly and comprehensively informed about possible governmental surveillance by US authorities;
  - (ii) Parties to transfer agreements must undertake to provide data subjects whose data are being transferred to the US with the necessary means in order to ensure effective judicial protection, to actually conduct such proceedings and to accept court decisions issued based on such proceedings.

  In our view, and in light of the Federal Commissioner's additional statement of 28 October 2015, there are strong arguments to hold that it is **still possible to rely on the standard EU Model Clauses (adapted to Swiss law requirements)** as they are also used for transfers to other jurisdictions which do not provide for an adequate data protection level. We do not see any valid reason for inserting amendments or additional clauses into the standard EU Model Clauses (beyond the generally recommended slight adaptions to Swiss law requirements).

– **BCRs:** As an alternative to contractual agreements, it is possible to rely on Binding Corporate Rules (**BCRs**) for any intra-group transfers of personal data to the US (albeit BCRs are rarely used in practice due to the complexity of adopting them on a group-wide level) (art. 6 para. 2 letter g DPA).

In the two cases mentioned above (i.e. reliance on either contractual agreements or BCRs), the **Federal Commissioner must be informed in advance** of the contractual safeguards that have been taken or the BCRs that have been adopted (art. 6 para. 3 DPA). If EU Model Clauses (adapted to Swiss law requirements) or other standard contractual clauses explicitly accepted by the Federal Commissioner are used, a mere notification according to art. 6 para. 3 DPA is sufficient and a more in-depth examination procedure of the agreed clauses by the Federal Commissioner can generally be avoided.

According to art. 6 para. 2 DPA, transfers of personal data from Switzerland to a country without an adequate data protection level are also possible in the following scenarios:

– **Consent:** The data subject has consented in an individual specific case (art. 6 para. 2 letter b DPA). Please note that in case of processing of sensitive personal data or personality profiles such consent must be given expressly (art. 4 para. 5 DPA);
– **Performance of a contract:** The processing is directly connected with the conclusion or the performance of a contract and the personal data are those of a contractual party (art. 6 para. 2 letter c DPA);
– **Overriding public interest or legal claims:** Disclosure is essential in the specific case to either safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts (art. 6 para. 2 letter d DPA);
– **Protection of the data subject:** Disclosure is required in the specific case to protect the life or the physical integrity of the data subject (art. 6 para. 2 letter e DPA);
– **General availability:** The data subject has made the data generally accessible and has not expressly prohibited their processing (art. 6 para. 2 letter f DPA).

The further possible safeguards mentioned above (i.e. art. 6 para. 2 letter b–f DPA) can not be used very often in practice as they mostly have a narrow and specific scope of application, making them available typically only for special and singular situations.

2.2. Increase transparency

As it is not and will not be possible to contain data accesses by US authorities by contractual safeguards, the Federal Commissioner is of the opinion that it is important to enhance **transparency** in the sense of art. 4 para. 4 DPA vis-à-vis the data subjects concerned by a data transfer to the US[3]. Accordingly, the Federal Commissioner recommends that persons whose personal data are transferred to the US must be

3 <http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01325/index.html?lang=de&print_style=yes> (last visited on 16 November 2015).

informed fully and clearly about the possible access by US authorities in order to be able to safeguard their rights. In our opinion, the Federal Commissioner clearly overshoots the mark with these requirements. The fact that authorities may access personal data based on local laws is commonly known, neither new nor an issue exclusively arising on US territory. In particular, there is in our view no need to provide data subjects with such additional information with respect to data transfers to the US (or to any other country).

3. Checklist for data exporters: Are you affected?

We recommend going through the following checklist in order to assess whether you are affected by the recent statements of the Federal Commissioner:

- **Analysis of data flows:** Are personal data transferred to the US either directly from Switzerland to the US or indirectly (e.g. transfer of personal data from Switzerland to the UK and, thereafter, transfer of said personal data to the US)? E.g.:
  - (i) Storage of personal data or back-up on a server located in the US?
  - (ii) Personal data stored on a server not located in the US, but company or individual located in the US has access to the server and, hence, to the personal data?
- **Proportionality considerations:**
  - (i) As the DPA does not apply to fully anonymised data, are there possibilities to **anonymise** data?
  - (ii) Validate **appropriateness** of data flows, in particular in case sensitive personal data or personality profiles are being transferred abroad.
- Identify whether any transfers of personal data to the US have been based on the **US-Swiss Safe Harbor Framework** so far:
  - (i) **Intra-group transfers** based solely on US-Swiss Safe Harbor Framework? If yes:

    Adequate safeguards are needed, i.e. conclusion of data transfer agreements (ideally based on the EU Model Clauses or other contractual clauses explicitly recognised by the Federal Commissioner) or BCRs, unless one of the other scenarios mentioned in art. 6 para. 2 letter b–f DPA applies (i.e., inter alia, consent in an individual case, transfer relating to a contractual partner, etc., see section 2.1 above).
  - (ii) **Transfers to other third parties (i.e. other than group companies)** based solely on the US-Swiss Safe Harbor Framework? If yes:

    Adequate safeguards are needed, i.e.: conclusion of data transfer agreement (ideally based on the EU Model Clauses or other contractual clauses explicitly recognised by the Federal Commissioner), unless one of the other scenarios mentioned in art. 6 para. 2 letter b–f DPA applies (see section 2.1 above).
- Review and adapt any **privacy policies, notices and contracts** with references to the US-Swiss Safe Harbor Framework.

– **Inform the Federal Commissioner** of any contractual safeguards or BCRs which you rely on instead of the US-Swiss Safe Harbor Framework (art. 6 para. 3 DPA). Be ready to answer questions the Federal Commissioner may raise in this context (in particular relating to the purposes of the data processing, the categories of data recipients, the countries to which the personal data shall be transferred, etc.). The Federal Commissioner has the power to investigate cases in more detail in certain instances (art. 29 para. 1 DPA). In the process of informing the Federal Commissioner according to art. 6 para. 3 DPA, also consider whether there are any data files which should be registered (art. 11a and 29 para. 1 letter b DPA). Such registration can occur alongside with a notification according to art. 6 para. 3 DPA.

Please note that additional or stricter requirements may apply in certain situations and in specific sectors, such as, *inter alia,* rules on banking secrecy or provisions relating to handling personal data relating to employees, or specific blocking statutes.

4. What is ahead?

Whether there will be a new safe harbor framework for transfers from Switzerland to the US (so-called **"Safe Harbor 2.0"**) and whether the requirements for safeguards such as the use of EU Model Clauses or BCRs will be amended in the future largely depends on the respective developments on the EU level:

– Negotiations on a **new "Safe Harbor 2.0" framework** for data transfers from the EU to the US between the European Commission and the US are underway. Commentators agree that the CJEU decision is likely to increase pressure on the US in the negotiations on a new framework. The Article 29 Data Protection Working Party has urged EU Member States and European institutions to continue discussions with US authorities in order to find a new solution[4]. It is hoping that a new framework will be available by the end of January 2016, which seems very ambitious. It is generally expected that Switzerland will adopt a similar, yet separate new framework with the US once a new framework is agreed on an EU level.

– Whether the **EU Model Clauses** will still be considered a valid basis for data transfers to the US in the future is currently under review on an EU wide level. The Federal Commissioner hopes that the future of the EU Model Clauses on an EU wide level will be clear by the end of January 2016[5]. Without explicitly mentioning the future use of the EU Model Clauses for data transfers from Switzerland to the US, the Federal Commissioner clearly intends to follow the approach which will be taken on an EU wide level.

– Additionally, the requirements for the use of **BCRs** for intra-group data transfers to the US may also come under scrutiny. Again, it is highly likely that the Federal Commissioner will autonomously adapt his practice to any changes on the EU level.

4 Statement of the Article 29 Working Party, Brussels, 16 October 2015 (<http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf>, last visited on 16 November 2015).

5 <http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01325/index.html?lang=de&print_style=yes> (last visited on 16 November 2015).

Walder Wyss Ltd.
Attorneys at Law

Phone + 41 58 658 58 58
Fax + 41 58 658 59 59
reception@walderwyss.com

www.walderwyss.com
Zurich, Basel, Berne, Lugano