

Update

Newsflash February 2017

Revision of Swiss Federal Data Protection Act

On 21 December 2016, the Swiss Federal Council initiated the consultation on its preliminary draft ("Draft") for a revised Swiss Federal Data Protection Act ("DPA"), which lasts until 4 April 2017. The revisions will strengthen individuals' protection of personal data, respond to developments in technology and align the DPA with new EU rules on data protection. This will allow Switzerland to uphold its status as country adequately protecting personal data from an EU perspective (adequacy decision), which allows for easier transfer of personal data from the EU and to ratify the Convention ETS 108 of the Council of Europe.

1. The revision's goals

The revision will strengthen the rights of data subjects, increase transparency of data processing, and generally increase the obligations of data controllers ("**Controllers**") and processors ("**Processors**") while providing for certain reliefs. It will align the DPA with international rules on data protection in order to comply with the upcoming revision of Convention ETS 108 and the EU **General Data Protection Regulation 2016/679 ("GDPR")**. The revised DPA is expected to enter into force in early 2018.

2. Reduction in scope and other relief

a) No more data protection for legal entities

The DPA Draft removes the protection of personal data relating to legal entities. This will ease cross-border disclosure to jurisdictions that do not protect such personal data, such as most EU and other countries.

b) No general notification duty for data files

The duty to notify data files to the Federal Data Protection and Information Commissioner ("**FDPIC**"), which applied to all private parties who regularly (i) disclosed personal data to third parties or (ii) processed sensitive personal data, is removed.

3. Increased or new obligations and sanctions

a) For Controllers

- › **Extended information duties:** the information to be provided to the data subjects by the Controller is more detailed than before and in particular includes Controller's identity and contact information, processed personal data or its categories, purpose of processing, and – in case of disclosure to third parties – the identity of recipients and processors or their categories.
- › Controllers must take **appropriate measures** to avoid breaches of privacy (*privacy by*

design) and provide for data protection-friendly presets (*privacy by default*).

- › Controllers must conduct an **impact assessment** if processing of personal data may lead to an increased risk for the data subject's privacy or fundamental rights (e.g. if main activities of the Controller consist of data processing). Controllers must notify the FDPIC of the outcome of their impact assessments.
- › Controllers must **notify the FDPIC** in case of unlawful processing or loss of personal data.
- › Controllers must **inform the data subject about automated decisions** (*i.e.* decisions taken solely on the basis of automated data processing) which produce legal effects concerning him / her and give him / her the opportunity to comment on such decisions.

b) For Processors

- › A Processor may not appoint a **subprocessor** without prior written consent of the Controller.

c) Sanctions

- › In case of **breach of any duty** under the DPA (such as information, notification and cooperation duties, compliance measures, e.g., regarding security or impact assessments), **finances of up to CHF 500'000** can be imposed. This constitutes a significant change from the current sanction regime which foresees moderate fines of up to CHF 10'000 for a limited list of duties only.
- › If a fine does not exceed CHF 100'000 and the **breach is committed within a company**, the prosecutor may decide not to prosecute the responsible person and instead sentence the company to the payment of the fine.

4. Selected other changes

a) Cross-border transfer system generally maintained

- › Cross-border disclosure is still permitted to **jurisdictions providing adequate protection** of personal data.

- › The **Federal Council** (instead of the FDPIC under the current DPA) decides on the jurisdictions providing adequate protection (**adequacy decision**).
- › For transfers to **countries not providing adequate protection** (such as, currently, the US), data exporting Controllers (or Processors) may rely on treaties (such as bilateral privacy shields), contractual clauses, binding corporate rules or other guarantees:
 - In case of treaty frameworks, such as the new US-Swiss Privacy Shield, neither approval nor notification to the FDPIC is required (*see* our Newsflash "Privacy Shield" of February 2017).
 - In case of standard contractual clauses which were pre-approved by the FDPIC, notification to the FDPIC (but no approval) is required.
 - In case of (non-standard) contractual, corporate or other guarantees, approval by the FDPIC is required.

b) Role of data protection authority (FDPIC)

- › The FDPIC may investigate and issue **binding administrative decisions** (instead of recommendations under the current DPA) regarding Controllers and Processors (e.g. modify or terminate unlawful processing).
- › Self-regulation is promoted, thus the industry (upon approval by the FDPIC) or the FDPIC (after consultation with the industry) may make **good business practice recommendations**. Controllers and Processors will generally be deemed to comply with the DPA if they comply with such good business practice recommendations.
- › The FDPIC has **no power to impose criminal sanctions** (unlike most other European data protection authorities). Any sanction must be imposed by the competent court.

c) No court costs

No court costs are charged in disputes relating to data protection and no fee shall be charged to

data subjects for exercising their right of access.

d) Sanctions for breach of professional secrecy

Willful breach of professional secrecy is punishable by imprisonment of up to three years or monetary penalty. This **new sanction is not limited to the usual bearers of professional secrets** (such as banks or securities dealers under art. 47 Swiss Banking Act or attorneys, auditors, doctors etc. under art. 321 Swiss Penal Code) but shall **extend to any profession for which protection of confidentiality is essential**.

e) Rejected proposals

Certain proposals and concepts were considered but rejected, in particular (i) the collective exercise of rights (so-called **class actions**), (ii) the right to **data portability** (as in the EU GDPR), and (iii) the power of the FDPIC to enact **generally binding data protection rules**.

5. Next steps for Controllers and Processors in Switzerland

The final wording of the revised DPA is not yet determined. It can be expected that most of the changes will be implemented as proposed. Controllers and Processors operating in Switzerland should thus **consider taking the**

following steps or precautions:

- › Consider participating in the ongoing **consultation**, either individually or jointly with peers and industry organizations.
- › Review existing **data processing agreements** with third parties (Processors and sub-processors), e.g., with a view to technical and organizational measures or Processor rights to appoint subprocessors (which will be restricted going forward).
- › Proactively **plan measures** to avoid breaches of privacy (*privacy by design*) and include data protection-friendly presets (*privacy by default*) in future products and services involving processing of personal data.
- › Consult and align with peers and industry organizations to prepare **good business practice recommendations** for approval by the FDPIC.
- › Document the processing of personal data in preparation for possible **impact assessments** to be conducted under the revised DPA.

Please do not hesitate to contact us in case of any queries.

Legal Note: The information contained in this Newsflash is of general nature and does not constitute legal advice. In case of particular queries, please contact us for specific advice.

Your contacts

Geneva / Lausanne

Guy Vermeil
guy.vermeil@lenzstaehelin.com
Tel: +41 58 450 70 00

Daniel Tunik
daniel.tunik@lenzstaehelin.com
Tel: +41 58 450 70 00

Yaniv Benhamou
yaniv.benhamou@lenzstaehelin.com
Tel: +41 58 450 70 00

Zurich

Lukas Morscher
lukas.morscher@lenzstaehelin.com
Tel: +41 58 450 80 00

Stefan Bürge
stefan.buerge@lenzstaehelin.com
Tel: +41 58 450 80 00

Leo Rusterholz
leo.rusterholz@lenzstaehelin.com
Tel: +41 58 450 80 00

Our offices

Geneva

Lenz & Staehelin
Route de Chêne 30
CH-1211 Genève 6
Tel: +41 58 450 70 00
Fax: +41 58 450 70 01

Zurich

Lenz & Staehelin
Bleicherweg 58
CH-8027 Zürich
Tel: +41 58 450 80 00
Fax: +41 58 450 80 01

Lausanne

Lenz & Staehelin
Avenue du Tribunal-Fédéral 34
CH-1005 Lausanne
Tel: +41 58 450 70 00
Fax: +41 58 450 70 01

www.lenzstaehelin.com