Update

Newsflash September 2017

Revision of Swiss Federal Data Protection Act

On 15 September 2017, the Swiss Federal Council adopted a draft ("Draft") for a revised Swiss Federal Data Protection Act ("DPA"). This follows the preliminary draft of 21 December 2016 and the consultation process which ended on 4 April 2017. The revision aims at strengthening the individual protection of personal data and aligning the DPA with new EU rules on data protection (see our Newsflash "EU Data Protection law: Required measures for Swiss companies" of September 2017).

1. The revision's goals

The Draft strengthens the rights of data subjects, increases the transparency of data processing, and tightens the obligations of data controllers ("**Controllers**") and processors ("**Processors**"). It aligns the DPA with international rules on data protection in order to comply with the upcoming revision of Convention ETS 108 of the Council of Europe and the **EU General Data Protection Regulation** 2016/679 ("**GDPR**"). This will allow Switzerland to maintain its status as country providing adequate protection of personal data from an EU perspective, thus facilitating data transfers between Switzerland and the EU, and to ratify the Convention ETS 108.

The Draft is currently expected to **enter into force by 1 August 2018** but its final wording is still subject to parliamentary debates and is therefore subject to change.

2. Key differences to the GDPR

Compared to the GDPR (see our Newsflash "EU Data Protection law: Required measures for Swiss companies" of September 2017), the Draft provides in particular no right to data portability, no extra-territorial scope, lower requirements with respect to consent, certification mechanisms and codes of conduct and limited sanctions (as regards scope of offences and level of fines).

3. Reduction in scope and other relief

a) No more personal data for legal entities

The Draft excludes legal entities from the scope of the definition of "personal data", which is strictly limited to data relating to a natural person. This will ease cross-border disclosure of data relating to legal entities to jurisdictions that do not consider such data as personal data under their data protection legislation, such as most EU member states 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.

4. Increased or new obligations and sanctions

a) For Controllers

› **Extended information duties**: the detailed information to be provided to data subjects by the Controller shall include at least the Controller's identity and contact information and the purpose of processing. In case of disclosure to third parties, such information shall include the identity of recipients or their categories and, in case of cross-border disclosure, the jurisdictions where the data has been transferred to and the respective implemented guarantees. Controllers may limit, postpone or waive such information in particular if overriding interests of third parties so require or if the information might hinder the purpose of processing (e.g. processing of data for the preparation of trial).

› 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 may lead to a high risk for the data subject's privacy or fundamental rights (e.g. in case of extensive processing of sensitive personal data or profiling). If such risk is confirmed, the FDPIC must be consulted prior to the processing. No impact assessment is required if the Controller is certified by a recognized certification body, or complies with a code of conduct. In case of multiple similar processing activities, the Controller may conduct a general impact assessment which applies across all processing activities.

› Controllers may appoint a **Data Protection Officer (DPO)**, which under certain circumstances releases Controllers from the requirement of prior consultation of the FDPIC.

› Controllers must **notify the FDPIC**, and under certain circumstances also the data subject, in case of data security breaches which might result in a high risk to the data subject's privacy and fundamental rights.

› Controllers must upon request **inform the data subject about automated decisions** (i.e. decisions taken solely on the basis of automated data processing) which result in legal consequences or significant impairment and give him / her the opportunity to comment on such decisions. Controllers may waive such information duties in particular if the data subject has expressly consented to such processing or if the decision relates directly to the execution or performance of a contract.

b) For Processors

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

c) Sanctions

› In case of a willful **breach of a material duty** under the DPA (such as information, notification and cooperation duties, compliance measures, e.g., regarding security or impact assessments), **fines of up to CHF 250'000** 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 DPA violations only.

› If a fine does not exceed CHF 50'000 and the **breach is committed within a business**, the prosecutor may decide not to prosecute the responsible person and instead hold the business liable for the payment of the fine.

5. Selected other changes

a) Cross-border transfer regime generally maintained

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

› 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 and non-standard contractual clauses or binding corporate rules, the respective guarantee must be (pre-) approved by the FDPIC.

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, as professional or trade associations whose bylaws authorize them to safeguard their members' economic interests may submit **codes of conduct** to the FDPIC. Controllers may not infer any rights from a positive assessment by the FDPIC but they may expect that the FDPIC will not issue any adverse administrative decisions. In addition, they may be released from the obligation of impact assessments.

› The FDPIC has **no power to impose criminal sanctions** (unlike most other European data protection authorities). Any sanction must be imposed by the competent criminal prosecution authorities.

c) No court costs / Exercise of right of access

No court costs are charged in disputes relating to data protection. Further, no fee shall be charged to data subjects for exercising their right of access, subject to any exceptions that may be provided for by way of ordinance.

6. Expected key implementation 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**:

› Identify and review (and document, as required) all **data processing activities** (complete and dynamic data mapping), including a determination of role played (Controller, Joint Controller, Processor) with respect to each type of personal data.

› 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 sub-processors (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 the relevant associations to prepare **codes of conduct** to be submitted to the FDPIC.

› Prepare for possible **impact assessments** to be conducted under the revised DPA.

› Implement data governance, rules and responsibilities (including as regards technical capability) to **respond to requests** of data subjects based on extended rights.

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

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
Brandschenkestrasse 24
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