# The Revised Swiss FDPA and the GDPR

## Key differences and their implications for compliance

December 10, 2020

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

# Agenda

**01** When and why a revised Swiss Federal Data Protection Act (Revised FDPA)

**02** How the FDPA compares to the GDPR, with a focus on

- Transparency
- High-risk profiling
- Data subject rights
- Outsourcing
- International data transfers
- Data breach notifications
- Documentation and governance
- Enforcement

**03** Practical tips for operationalization of compliance

# Introduction

# Today's Speakers

**Thomas Steiner**

Partner

LAUX LAWYERS (Zurich, Switzerland)

- Works with Swiss and international companies on building compliant and sustainable data protection programs (GDPR and Swiss FDPA)
- Focus on regulated sectors in digital transformation, including health, insurance and finance

# Today's Speakers

**François Charlet**

Chief Privacy Officer

Vaudoise Assurances (Lausanne, Switzerland)

- Chief Privacy Officer at Vaudoise Assurances, a major Swiss insurance company
- Develops and implements privacy management framework (GDPR and Swiss FDPA) at Vaudoise

# Disclaimer

Our opinions are our own and not those of our firm, company, or clients.

# Purposes and Goals

- Learn about the conceptual differences between the (Revised) FDPA and the GDPR
- Understand how the Revised FDPA compares to the GDPR, and where nuances or stricter requirements may require changes to data protection programs
- Offer practical compliance tips regarding the implementation of the requirements of the Revised FDPA in Swiss companies, and in companies with data processing operations affecting data subjects in Switzerland

# When and why a revised Swiss Federal Data Protection Act (Revised FDPA)?

# Revised FDPA: when?

## January 1, 2022 – more likely July 1, 2022

- Revised FDPA adopted in final vote of Federal Parliament on September 25, 2020
- Referendum unlikely
- Federal Department of Justice to draft revised Ordinance on FDPA (Revised FDPO)
- Entry into force likely July 1, **2022**
- Applicable from entry into force – **no transition period**!

# Revised FDPA – why?

- Key objectives of the (total) revision of FDPA 1992:
  - to implement the requirements of the **revised Convention 108 of the Council of Europe**, and
  - to **align** the FDPA **with the GDPR**, particularly pending European Commission's adequacy review
- Drivers of the revision
  - Perceived lack of transparency in the wake of big data analytics and cloud computing
  - Perceived loss of control over "own" personal data when using digital services
  - Increased data security risks (data breaches)
  - Algorithms take over selection and decision making

# How the Revised FDPA compares to the GDPR

# Conceptual differences (1|2)

## GDPR: Principle of Prohibition

- GDPR: The **default rule** is: “verboten” (prohibited)
- Controllers need a “good reason” (statutory exemption) in order to lawfully process personal data
- At least one of the **legal bases** listed in Article 6(1) GDPR must apply
- Controllers need to actively **inform** individuals (data subjects) on legal bases relied on, and to **document** their choice of legal bases


# Conceptual differences (2|2)

## (Revised) FDPA: Processing of personal data generally allowed

- Under (Revised) FDPA, private organizations are generally **allowed** to process personal data if they comply with the **data processing principles**
- Controllers to **justify** their processing of personal data, in order to …
  - lawfully **disclose sensitive personal data** to third parties (excluding processors)
  - continue processing despite data subject's **explicit objection**
  - process personal data **for further purposes**, for longer than necessary, or otherwise not in accordance with data processing principles

→ Justification of otherwise unlawful **personality rights infringement**

→ Justification based on (Swiss law) legal obligation, consent, or prevailing private (including necessity for performance of contract with data subject) or public interests

Prohibited

# Revised FDPA: Aligned with GDPR requirements

**Fed. Agencies**: Legal Basis
(**Private organizations**: basis for justification, where necessary!)

Processing Principles
(lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, accuracy, security)

**Transparency**
(Duties to inform data subjects; changes to **privacy notices** recommended)

Data Subject Rights
(rights of access and information, **objection**, rectification erasure and data portability, **+ restriction etc.**)

Documentation / Governance

Requirements for Outsourcing of Processing Operations (processing on behalf of controller)

Int'l Data Transfers (across Swiss border; **list of import countries** required in privacy policy)

Autom. Decision-making, incl. Profiling (right to object) / **high-risk profiling**

Data Protection Impact Assessment / Privacy-by-Design and Default

Data Breach Notification

Data Security

Enforcement

# Scope of Revised FDPA

## Articles 2–3 and 14 Revised FDPA

- Personal and material scope: processing of personal data, whether **automated or manual** (!)
  - by businesses, organizations, or (in the context of business activities only) natural persons
  - by Federal authorities (note: Chapter 6 Revised FDPA only applies to processing by Federal authorities)
- Territorial scope
  - Revised FDPA applies to processing operations with an **effect in Switzerland**, even if initiated abroad
  - Private International Law Act: Revised FDPA applicable if effect on personality rights of data subjects in Switzerland reasonably foreseeable (or due to choice of Swiss law once infringement occurred)
- **Swiss representative** required if *controller* abroad
  - in connection with offering goods or services to, or monitoring behavior of data subjects in, Switzerland,
  - engages in extensive and regular processing involving a **high risk** for data subjects in Switzerland

# **Transparency:**
# Do we have to change our privacy notices?

# Do we have to change our privacy notices? (1|3)

## Article 19 Revised FDPA

- **Privacy notices** are **a must** under the Revised FDPA
- Shorter list of **minimum elements of information** (Art. 19 para. 2 Revised FDPA ; comp. Arts 13–14 GDPR)
  - The identity and contact details of controller
  - Purposes of the processing
  - The recipients or categories of recipients of the personal data, if any
  - The categories of personal data concerned (if not obtained from the data subject)
  - If controller intends to transfer personal data to a recipient outside of Switzerland, **the countries** and, where applicable, reference to the safeguards or derogations the controller relies on for the data transfer
- Exceptions and limitations apply (Art. 20 Revised FDPA)

# Do we have to change our privacy notices? (2|3)

## Article 19 para. 2; and Articles 10 para. 3 let. d, 14 para. 3 and 21 para. 1 Revised FDPA

- **Additional information**, *as far as necessary for exercising data subject rights and for transparent processing* (Art. 19 para. 2 Revised FDPA)
  - may require types of information listed in Art. 13 para. 2 (or 14 para. 2) GDPR; and
  - information about the **existence of high-risk profiling**
- **Supplementary**, where applicable, and if not published elsewhere
  - the contact details of the data protection advisor – DPO (Art. 10 para. 3 let. d Revised FDPA)
  - the name and address of the Swiss representative (Art. 14 para. 3 Revised FDPA); and
  - the existence of automated individual decision-making (Art. 21 para. 1 Revised FDPA)

# Do we have to change our privacy notices? (3|3)

## Article 19 Revised FDPA

→ **Practical tips for changes to privacy notices**

- add **list of countries** to which personal data is transferred (also applies where recipient is a *group company* or a *processor*) and safeguards or derogations relied on for the data transfer; may require (internal and external) **fact-finding**, e.g., based on questionnaires!
- inform about existence of **high-risk profiling**
- refer to **applicable data protection laws** rather than GDPR provisions; e.g., that data subject rights may be subject to exemptions or derogations under applicable data protection laws

# **High-risk profiling:** Do we really need express consent?

# High-risk profiling (1|2)

## Article 5 let. f–g and Article 6 paras 6–7 Revised FDPA

- High-risk profiling – a concept introduced late in the Parliamentary debate
  - **High-risk profiling**: profiling [cf. Art. 5 let. f Revised FDPA] which involves a **high risk to the personality** or fundamental rights of the data subject, as it creates a **pairing between data that enables an assessment of essential aspects of the personality** of a natural person (Art. 5 let. g Revised FDPA)
  - ***If*** consent of the data subject is required, consent is valid only if it is informed, freely given, and specific (Article 6 para. 6); and, in the case of high-risk profiling, it has to be *express* (Art. 6 para. 7 let. b Revised FDPA)

→ **Express consent <u>not</u> required for every** high-risk-profiling! (despite the fuss around it)

→ Express consent needed only **if justification required** (e.g., further processing despite objection or for further purposes) and if **no other suitable basis for justification** (e.g., legal or contractual obligation)

# High-risk profiling (2|2)

Article 5 let. f–g and Article 6 paras 6–7 Revised FDPA

→ **Practical tips**

- Inform about (high-risk) profiling in **privacy notices** to ensure transparent processing
- Build trust by explaining **how and why –** in separate communication or FAQ on website
- Perform data protection impact assessment (**DPIA**) in order to assess *actual risk* of high-risk profiling
- Consider if you can rely on **necessity to perform a contract** with the data subject or to **comply with legal obligation** (laid down in Swiss law), or on **prevailing legitimate interest** to justify high-risk profiling for further purposes or if data subject objects

# **Data Subject Rights:** Do we have to change our policies and procedures?

# Right of access

## Article 25 Revised FDPA

- Same concept as Art. 15 GDPR
- Similar list of minimum elements of information (Art. 25 para. 2 Revised FDPA ; comp. Art. 15 GDPR)
- Includes a right to receive a **copy** (e.g., a print-out or extract of a data set) of the personal data undergoing processing (Art. 25 para. 2 let. b Revised FDPA; similar to Art. 15 para. 3 GDPR)
- **Additional information**, *as far as necessary for exercising data subject rights and for transparent processing,* therefore data subject may ask for other useful information, such as
  - types of information listed in Art. 19 para. 3 (categories) or para. 4 (import countries and safeguards for international transfers), but not in Art. 25 para. 2 Revised FDPA, and
  - information on data subject's rights (cf. Art. 15 para. 2 GDPR) or additional information of such listed in Art. 13 para. 2 (or 14 para. 2) GDPR
- 30-day for (first) response

# Data portability right

## Article 28 Revised FDPA

- Introduced in the Parliamentary debate
- Copied from Article 20 GDPR
  - Nuance: “commonly used electronic format” (Art. 28 para. 1 Revised FDPA) vs. “structured, commonly used and machine-readable format” (Art. 20 para. 1 GDPR)
  - Limitation to cases where data is “processed with consent of the data subject” or “in direct connection” with a contract (Art. 28 para. 1 let. b Revised FDPA) is modelled after Art. 20 para. 1 let. a GDPR, but will not provide the same limitations since legal basis does not have to be determined or documented under Revised FDPA

# Limitations of rights of access and data portability

## Articles 26 and 29 Revised FDPA

→ **Practical tips**

- Art. 26 (or Art. 29 by reference to Art. 26) Revised FDPA provides for limitations: access / data portability may be denied, limited or deferred
  - if Swiss law so provides, in particular, in order to protect a professional secrecy,
  - if it is necessary for the purposes of prevailing interests of third parties,
  - If the access or data portability request is manifestly unfounded, in particular, if it pursues a purpose that is contrary to data protection or is obviously of a frivolous nature, or
  - if it is necessary for the prevailing interests of the controller and the controller does not disclose the personal data to third parties (→ rather weak protection of business secrets!)
- Amend your internal policies, procedures and standard responses to reflect these limitations
- **Structure** your customer data in ways that will allow you to provide copies / extracts of personal data (e.g., in Excel) without having to redact personal data of other customers

# Right to object (or to restrict or erase)

## Article 30 para. 2 let. b Revised FDPA

- Art. 30 para. 2 let. b Revised FDPA (processing against the express will of the data subject) is effectively a **right to object** (identical to Art. 12 para. 2 let. b FDPA 1992)
- The courts have interpreted the right to object to include
  - a **right to erasure** (delete, destroy or anonymize) and
  - a **right to restriction of processing**
- **Limitations**: Contractual or legal obligations or overriding private or public interests may prevail over interest to discontinue, restrict processing or to erase personal data (Art. 31 Revised FDPA)

→ **Practical tip**: amend internal policies, procedures and standard responses to reflect

# Right to rectification and further rights and remedies

## Article 32 Revised FDPA

- Art. 32 para. 1 let. b Revised FDPA (remedies) sets out a right to have inaccurate personal data **rectified**
- Limited exceptions – rectification may be denied
  - if a (Swiss law) statutory obligation prohibits the change, or
  - if personal data is being processed for archiving purpose in the public interest

→ **Practical tip**: amend internal policies, procedures and standard responses to reflect that exceptions are very limited!

→ **Practical note**: The Revised FDPA grants data subjects all rights granted under GDPR, and potentially more, as remedies available in cases of personality rights infringements under the Civil Code are also available under the Revised FDPA (cf. Art. 32 para. 2 Revised FDPA)

# **Outsourcing:**
# Do we have to change our data processing agreements?

# Data processing agreements

## Article 9 Revised FDPA

- Same concept as Art. 28 GDPR
- Data processing agreements (controller-to-processor) pursuant to Art. 28 para. 3 GDPR will normally suffice for the purposes of the GDPR; **but** need to get international data transfers right!

→ **Practical tips**

- Refer to **applicable data protection laws** rather than GDPR or Revised FDPA provisions
- Make sure "Swiss data protection law" is included in definition of applicable data protection law (note: Revised FDPA is not a law implementing or supplementing GDPR)
- Make sure provider is **contractually bound to inform on import countries** in cases of data transfers outside of Switzerland (you will need this information for your privacy notices)

# **International Data Transfers:** Do we have to change intra-group data sharing agreements or agreements with service providers?

# International data transfers (data export)

## Article 16–17 Revised FDPA

- Same concept as Arts 44 et seq. GDPR
- Transfers of personal data from Switzerland to recipients in other countries (data exports) allowed
  - based on adequacy decision by Swiss Federal Council;
  - subject to appropriate safeguards (e.g., Standard Contractual Clauses or Binding Corporate Rules); or
  - derogations for specific situations

→ **Practical tips**

- Perform (internal and external) **fact-finding**, e.g., based on questionnaires or checklists, to identify data transfers from Switzerland to other countries (and onward transfers)
- Absent adequacy decision by Federal Council, implement safeguards or determine derogations
- Use EU Standard Contractual Clauses also for purposes of Art. 16 FDPA; make sure "Swiss data protection law" is included in definition of applicable data protection law (note: Revised FDPA is not a law implementing or supplementing GDPR)

# **Data Breach Notifications:** Do we have to change our policies and procedures?

# Data breach notification

## Article 24 (and Article 5 let. h) Revised FDPA

- Substantially identical definition of personal data breach (Art. 5 let. h Revised FDPA)
- Same obligation to notify processors
- Notification of FDPIC only in cases of “high risk”, and “as soon as possible” (Art. 24 para. 1 FDPA)
- Notification of (high-risk) data breach to data subjects
  - if this is necessary for the protection of the data subject, or
  - if the FDPIC so requests
- No 72 hour-deadline; no obligation to document data breaches

→ **Practical tip**: amend internal policies, procedures and templates for notifications to reflect that FDPIC may have to be notified in addition to EU supervisory authorities

# **Documentation/Governance:** Do we need a Data Protection Officer in Switzerland?

# Documentation and governance

## Articles 10 and 12 Revised FDPA

- Identical obligation to maintain records of processing activities (Art. 12 Revised FDPA); exemptions apply
- No obligation to appoint data protection officer
- Appointment of **data protection advisor** (Article 10 Revised FDPA) incentivized
  - If data protection advisor participates in DPIA, controller may abstain from consulting the FDPIC where DPIA shows high risk despite mitigation measures (Art. 23 para. 4 Revised FDPA)

→ **Practical tip**: amend internal policies and data protection organization (group internal functions) to reflect roles, responsibilities and competencies as regards compliance with Revised FDPA; if necessary, establish relationship with external advisors.

# **Enforcement:**
# What are the risks of sanctions and remedies?

# Private enforcement

## Art. 32 Revised FDPA

- Revised FDPA provides private rights of actions against infringements of personality rights under the Revised FDPA. In particular, data subjects may request that:
  - a specific data processing be prohibited;
  - a specific disclosure of personal data to third parties be prohibited; or that
  - personal data be deleted or destroyed.
- Also, (cf. the reference to Art. 28a Civil Code) data subjects may request that a court require controllers (or processors) to comply with specific obligations under the Revised FDPA; or bring claims for compensatory damages, moral damages, or disgorgement of profits
- No court fees are charged in data protection proceedings (revised Art. 113 para. 2 let. g Civil Procedure Code)

# Administrative law enforcement

## Art. 51 FDPA

- FDPIC may take corrective measures, i.e., oblige controllers (or processors) to correct, suspend, or cease certain processing of personal data, or to delete personal data entirely or partially
- FDPIC may also require controllers (or processors) concerned to comply with specific obligations under the Revised FDPA
- FDPIC may not issue administrative fines
- **But** criminal enforcement: public prosecutors may fine responsible natural person (up to CHF 250,000) in case of willful non-compliance with an FDPIC decision or the decision of appellate courts (**indirect fines**) (Art. 63 Revised FDPA)

# Criminal law enforcement

## Art. 60–66 FDPA

- The state prosecutors enforce the criminal law provisions, *on complaint* from data subjects
- Natural persons may be fined up to CHF 250,000, if they are responsible for willful violation of
  - certain information and notification requirements, e.g., willfully providing incomplete or false information to data subjects (pursuant to Art. 19, 21 or 25 Revised FDPA) (Art. 60 Revised FDPA)
  - certain duties of care in connection with the transfer of data abroad, outsourcing (engaging processors), or minimum data security requirements (Art. 61 Revised FDPA),
  - professional secrecy duties (Art. 62 Revised FDPA), or
  - *ex officio*, (**indirect fine**) a decision by the FDPIC or appellate courts (Art. 63 Revised FDPA)
- Controller or processor may be held liable for a fine of up to CHF 50,000 if determining who in the organization is responsible would require disproportionate investigative efforts (Article 64 Revised FDPA)

# Questions

**Thomas Steiner**
Partner
**LAUX LAWYERS**
thomas.steiner@lauxlawyers.ch
www.lauxlawyers.ch/thomas-steiner

**François Charlet**
Chief Privacy Officer
**Vaudoise Assurances**
fcharlet@vaudoise.ch
www.francoischarlet.ch