What's new in the revised DPO?

Association of Foreign Banks in Switzerland (AFBS)
November 2, 2022

Plan

I. Introduction

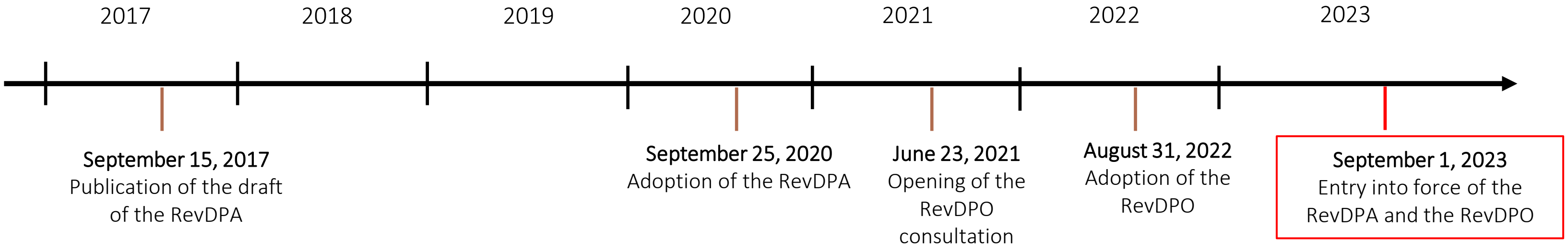
II. What's new in the revised DPO?

III. Practical implementation of the revised DPA

IV. Use of cloud services

V. Annexes (GDPR v/s revised DPA)

I. Introduction



2017 2018 2019 2020 2021 2022 2023

September 15, 2017
Publication of the draft of the RevDPA

September 25, 2020
Adoption of the RevDPA

June 23, 2021
Opening of the RevDPO consultation

August 31, 2022
Adoption of the RevDPO

September 1, 2023
Entry into force of the RevDPA and the RevDPO

Main points of the revision of the Swiss data protection Act (the "RevDPA")

- Preservation of the main principles (in particular: purpose, lawfulness, good faith, proportionality)
- Reinforcement of the duty to inform data subjects
- Accountability principle: a new approach to compliance
- Increased enforcement by an administrative authority (Swiss Data Protection Authority)
- Scope of application
  - Application of the RevDPA only to data of natural persons
  - Harmonization with European law

II. What's new in the revised DPO? (1/5)

Introductory comment: text (fortunately!) revised as compared to the initial draft in June 2021!

A. Data security (criminal liability in case of intentional breach / Article 61 (c) revDPA)

- Safety measures in accordance with
  - Type of data processed (*e.g.*, sensitive data)
  - Processing (*i.e.*, purpose, scope, circumstances) → ⚠ specific mention of *cloud* infrastructures in the explanatory report
  - Risk (*i.e.*, probability and breach's severity)
  - State of current technical and scientific knowledge
- Examples of security measures listed in the explanatory report:
  - Pseudonymization and anonymization of data
  - Encryption of data and identification procedures
  - Employee training

II. What's new in the revised DPO? (2/5)

A. Data security (*continued*)

- Purpose of the measures: to guarantee the C.I.A.T.:

Protection objectives	Technical and organizational measures
Confidentiality	Data access control
	Control of access to premises and systmes
	Usage control
Availability	Control of data carriers
	Memory control
	Transport control
Integrity	Recovery
	Data integrity
	System security
Traceability	Entry control
	Communication control
	Detection / Remediation

II. What's new in the revised DPO? (3/5)

B. Logging (Article 4 DPO)

- Logging is a data *security measure* according to Article 3 RevDPO
- *Scope* for private data controllers:
  - Large-scale automated processing of sensitive data <u>or</u> high-risk profiling
    - ➢ What is a *high-risk profiling* notion ? → see next *slide*
  - When precautionary measures are not sufficient to ensure data protection (→ only theoretical carve-out according to the explanatory report)
- *Content*: Log must provide information on the identity of the person who carried out the processing, the nature, date and time of the processing and, if applicable, the identity of the recipient of the data to allow → for a *posteriori* control *(audit trail)*
- *Retention time*: Log files are kept for at least one year, separately from the system in which the personal data is being processed.

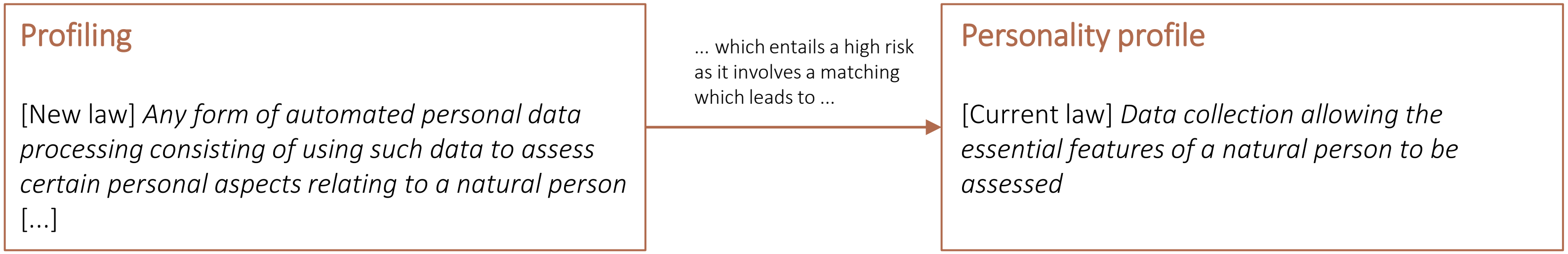
II. What's new in the revised DPO? (4/5)

French text: *appariement*
German text: *Verknüpfung*

B. Logging (Article 4 DPO) (*continued*)

Notion of *high-risk profiling* (Article 5 (g) RevDPA)

- Legal definition: "any profiling that entails a high risk for the personality or fundamental rights of the data subject, because it leads to a *matching* of data that allows the *essential features of the natural person's personality to be assessed* " (emphasis added).



Profiling

[New law] *Any form of automated personal data processing consisting of using such data to assess certain personal aspects relating to a natural person* [...]

... which entails a high risk as it involves a matching which leads to ...

Personality profile

[Current law] *Data collection allowing the essential features of a natural person to be assessed*

- High risk profiling in case of "personality profile"?
  - Profiling that does *not* lead to a personality profile should not be qualified as "high risk profiling".
  - The notion of "personality profile" under the current law is assessed on a case-by-case basis, according to the duration and context of the processing (TAF A-4232/2015, *Moneyhouse*, c. 5.2.1).

II. What's new in the revised DPO? (5/5)

C. Processing regulations (Article 5 RevDPO)

- *Scope* for private data controllers:
  - Large-scale automated processing of sensitive data or high-risk profiling
- *Content*: information regarding:
  - Internal organization
  - Procedure for data processing and control
  - Measures to ensure data security

III. Practical implementation of the RevDPA (1/3)

A. Transitional provisions

1. *Principle*: The RevDPA will apply to all data processing as of September 1, 2023

   → No transitional period!

2. *Exception*: The following provisions will not apply to processing that (i) started before the RevDPA comes into force, provided that (ii) the purposes of the processing remain unchanged and (iii) *no new data are collected*:

   - Article 7 RevDPA: data protection by design and by default
   - Article 22 RevDPA: data privacy impact assessment (DPIA)
   - Article 23 RevDPA: prior consultation of the Data Protection Authority (in connection with certain DPIAs)

III. Practical implementation of the RevDPA (2/3)

B. Steps to take before the RevDPA enter into force

1. Acquiring the internal know how

   → training

2. Assessing the current situation, in particular:

   - Listing the processing of personal data

     → register of processing activities

   - Reviewing the governance and the internal regulations regarding data protection

3. Carry out a gap analysis

III. Practical implementation of the RevDPA (3/3)

B. Steps to take before the RevDPA enter into force (*suite*)

4. Taking the necessary corrective measures, in particular:

- Preparing or updating the privacy notices
- Preparing or updating the data processing agreements

  → additional contractual guarantees may be required in case of transfer / access of personal data outside of Switzerland
- Defining a data protection governance
- Establishing a process to centralize and manage responses to data subjects' requests (*e.g.,* right to access, right to erasure)
- Defining a process for data security breaches
- Defining a process for future processing of personal data (data privacy impact assessments)

IV. Use of cloud services (1/6)

1. Subcontracting

A. Conditions

The law gives the controller the possibility to entrust personal data to a processor under the following conditions:

1. Subcontracting must be provided for:
   - in a contract between the controller and the processor; or
   - by law
2. The processor may only carry out processing operations that the controller would be able to carry out.
3. There is no legal or contractual obligation to maintain secrecy.

B. Obligations of the controller and the processor

In particular, the data controller must ensure that the processor is able to guarantee the security of personal data.

The processor itself may outsource processing to a third party only with the prior consent of the data controller.

The processor must comply with the same general obligations as the data controller.

IV. Use of cloud services (2/6)

2. Cross-border communication

A. Introduction

- Distinction between two assumptions:

  a) Hypothesis 1: The State of destination has regulations ensuring an "adequate" level of protection.

  b) Hypothesis 2: The State of destination does not have regulations ensuring an "adequate" level of protection.

IV. Use of cloud services (3/6)

2. Cross-border communication

B. Hypothesis 1 - Communication to an "adequate" state (Article 16 (1) RevDPA)

States concerned

a) All States that (i) have acceded to the Council of Europe Convention (Revised) 108 and (ii) are effectively implementing it.

b) The "list" of the Data Protection Authority (Article 7 OLPD) will be replaced by an ordinance of the Federal Council.

c) In practice: All the Member States of the European Union will be included in this list.

Consequences

a) The transfer of personal data to these States does not trigger any additional requirements.

b) The general principles of data protection (Article 5 RevDPA: lawfulness / good faith / proportionality / purpose) must nevertheless be respected.

IV. Use of cloud services (4/6)

2. Cross-border communication

B. Hypothesis 2 - Communication to a "non-adequate" state

Option 2A - specific guarantees (Article 16 (2) and (3) RevDPA)

Contratual options

Regulation in the agreement between the communicator and the recipient:

a) Use of *standard data protection clauses already recognized* by the Data Protection Authority (*e.g.,* "EU standard contractual clauses") (Article 16 (2) (d) RevDPA) → implementation of *Schrems II* ⚠

b) It is also possible to use *specific standard clauses to be approved* by the Data protection Authority (time limit for taking a position: in principle three months).

c) *Within groups of companies*: Use of *Binding Corporate Rules* (*BCR* / "intra-group contract") approved by the Data Protection Authority or by an authority of an "adequate" state (Article 16 (2) (e) RevDPA).

Other possible options

a) International Treaty (Article 16 (2) (a) RevDPA).

b) Specific guarantees established by a federal body and communicated to the Data Protection Authority (Article 16 (2) (c) RevDPA) (applicable to the public sector)

c) Other guarantees provided by the Federal Council (Article 16 (3) RevDPA) (*e.g.*, historically, the Swiss-US Privacy Shield)

IV. Use of cloud services (5/6)

2. Cross-border communication

C. Hypothesis 2 - Communication to a "non-adequate" state (continued)

Option 2B - Seven exemptions (Article 17 RevDPA)

1. "Express" consent of the data subject
2. Communication in connection with the conclusion or performance of a contract:

   a) between the controller and the data subject

   b) between the controller and the data importer, in the interest of the data subject [new]
3. Safeguarding of an overriding public interest
4. Establishment / exercise / defense of a right before a foreign court *or a foreign authority [new]*
5. Protection of life or physical integrity
6. The data subject has made the data accessible to everyone and has not expressly objected to the processing
7. *Data in a register provided for by law and access to this register is made in a lawful manner [new]*

→ In red: information to the Data Protection Authority (upon request of the authority; therefore increased duty of documentation for the data controller in order to be able to respond to possible requests of the authority

IV. Use of cloud services (6/6)

3. Methodology

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 Data Protection Authority (article 6 (3) LPD) / not necessary under the RevDPA)
- 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/DPA)

Step 2: Review of technical and operational guarantees

- Catalog of TOMs according to the identified risks
- Data localization issue in terms of application of possible US legislation

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 "conductor")
- 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: Management decision making

Thank you for your attention

Antoine Amiguet

aamiguet@obersonabels.com

Philipp Fischer

pfischer@obersonabels.com

OBERSON ABELS

Comparative table GDPR / RevDPA (1/5)

<table>
<tr><th>Provisions</th><th>GPDR</th><th>RevDPA (September 25, 2020)</th></tr>
<tr><td><i>Entry into force</i></td><td>May 25, 2018</td><td>September 1, 2023</td></tr>
<tr><td><i>Sensitive personal data</i>
Art. 9 GDPR / Art. 6 (7) (a) RevDPA</td><td>- Principle: prohibition of processing of sensitive data
- Exception based on:
• Explicit consent: main legal basis for the processing of sensitive data by a private organization
• Other possible legal basis: EU/Member State law, safeguarding vital interests, data made public by the data subject, etc.</td><td>- <i>A priori</i>, all <i>legal basis</i> can be used
• Case-by-case analysis based on the principle of proportionality
• If consent is the legal basis for the processing of sensitive data, it must be express.</td></tr>
<tr><td rowspan="2"><i>Compulsory consent (processing for which the legitimate interest is not an adequate legal basis)</i>
Art. 22, 49 (1) (a) GDPR / Art. 17 (1) (a) RevDPA</td><td>Consent required for:
- Automated individual decision making
• Other possible legal basis: permitted by a legal provision, necessary for the execution of a contract</td><td>N/A: There is no instances in which the consent is specifically required as a legal basis for a data processing.</td></tr>
<tr><td colspan="2">- Transfer of personal data to a State which does not benefit from an EC / Federal Council adequacy decision and in the absence of appropriate safeguards
• Other possible legal basis: performance of a contract, important reasons of public interest, exercise of legal rights, protection of vital interests, based on a register provided for by law</td></tr>
</table>

Comparative table GDPR / RevDPA (2/5)

<table>
<tr><th>Provisions</th><th>GPDR</th><th>RevDPA (September 25, 2020)</th></tr>
<tr><td><em>Processing of data of children</em>

Art. 8 GDPR</td><td>Where services are offered to a child on the Internet and where consent is the legal basis for the processing, this consent must be provided by the legal representative when the child is under 16 years old (this threshold may be lowered to 13 years old by the Member States)</td><td><em>No specific provision in this respect</em></td></tr>
<tr><td rowspan="2"><em>Right of information</em>

Art. 13, 14 GDPR /
Art. 19-21 RevDPA</td><td colspan="2">- Identity and contact details of the data controller
- Purpose of the processing
- Recipients or categories of recipients to whom personal data is transferred
- Existence of automated decisions making</td></tr>
<tr><td>- More extensive information right:
• DPO contact details
• Legal basis of the processing (including the nature of the legitimate interest of the controller or third party if applicable)
• Retention period
• Rights of the data subject
• Consequences for the data subject of refusal to provide personal data</td><td>- Necessary information for the data subject to exercise his/her rights
- + List of foreign States in case of cross-border transfer
- Restrictions / exceptions to the provision of information (more extensive list):
• Overriding interests of a third party / or of the controller (if no transfer to third party)
• Information prevents to achieve the purpose of the processing</td></tr>
</table>

Comparative table GDPR / RevDPA (3/5)

Provisions	GPDR	RevDPA (September 25, 2020)
Data subjects rights Art. 13-21 GDPR / Art. 19, 20, 25, 26, 6 (5), 32 (1) (3), 32 (2) (c), 28, 29 RevDPA	- Right of information - Right of access - Right to rectification - Right to erasure - Right to data portability	
	- Right to restriction of processing: limit the processing of personal data (*e.g. only* with the consent of the data subject or for the exercise of legal rights) when: • Accuracy of personal data is challenged • Unlawful processing • Personal data no longer needed for the processing, but necessary for the exercise of legal rights • Objection of the data subject to the processing and weighing of the overriding legitimate grounds for processing against the interest of the data subject - Right to object when the processing is based on the legitimate interest of the controller or a third party	*No specific provision on this respect*

Comparative table GDPR / RevDPA (4/5)

<table>
<tr><th>Provisions</th><th>GPDR</th><th>RevDPA (September 25, 2020)</th></tr>
<tr><td rowspan="2"><em>Profiling</em>

Art. 13 (2) (f), 21, 22 GDPR / Art. 5 (g), 6 (7) (b), 31 (2) (c) (1) RevDPA</td><td colspan="2">- When profiling is used for automated decision making:
• Additional guarantees to be provided (right to be heard, right to human intervention)</td></tr>
<tr><td>- When profiling is used for automated decision making:
• Consent of the data subject necessary (unless permitted by a legal provision / necessary for the execution of a contract)
• Additional information to be provided

- Right to object where profiling is based on legitimate interest, except if the controller can prove that compelling legitimate grounds override the interests of the data subject.
- Unrestricted right of objection of the data subject when profiling is used for marketing purposes</td><td>- Additional notion of <em>high-risk profiling</em> when profiling leads to a data matching that allows the assessment of <em>essential characteristics of the personality of an individual</em>
→ If consent is the legal basis: express consent required
→ When profiling is used to assess the <em>creditworthiness</em> of a person, the legal basis for such processing cannot be the legitimate interest of the data controller</td></tr>
</table>

Comparative table GDPR / RevDPA (5/5)

<table>
<tr><th>Provisions</th><th>GPDR</th><th>RevDPA (September 25, 2020)</th></tr>
<tr><td rowspan="2">*Data protection impact assessment (DPIA)*
Art. 35 GDPR / Art. 22 RevDPA</td><td colspan="2">Necessary in case of:
- *High risk* to the rights and freedoms of the data subject
- Large-scale processing of sensitive data
- Systematic monitoring of publicly accessible area on a large scale</td></tr>
<tr><td>- Required in the case of profiling only if it is carried out as part of automated decision making producing legal effects with respect to the data subject</td><td>- The data controller may refrain from conducting a DPIA when the system / product / service used is certified by an approved certification body or complies with a code of conduct submitted to the FDPIC</td></tr>
<tr><td rowspan="2">*Approval / Information of the supervisory authority*
Art. 47, 36, 46 (3) GDPR / Art. 16 (2) (e), 23, 16 (2) (b) RevDPA</td><td colspan="2">- Binding corporate rules: *Approval*</td></tr>
<tr><td>- DPIA: *Consultation* in case of high residual risk
- Transfer of data to a country that does not benefit from an adequacy decision when the following safeguard is implemented:
• *Authorization* for contractual clauses between the parties (excluding standard clauses)</td><td>- DPIA: *Consultation* in case of high residual risk unless the DPO has been consulted.
- Transfer of data to a country that does not benefit from an adequacy decision when the following safeguard is implemented:
• Prior *information* for contractual clauses between the parties (excluding standard clauses)</td></tr>
<tr><td>*Data breach*
Art. 33, 34 GDPR / Art. 24 RevDPA</td><td>- Notification to the supervisory authority in case of *risk* to the rights and freedoms of data subjects
- Notification to the data subjects in case of *high risk* for their rights and freedoms
- Deadline for notification: within 72 hours</td><td>- Notification to the supervisory authority in case of a *high risk* to the personality or fundamental rights of data subjects
- Notification to the data subjects when necessary for their protection or when required by the DPIC
- Deadline for notification: at the earliest</td></tr>
</table>