Data Privacy Act in Switzerland: year one in review

Prof. Philippe Gilliéron
AIBL Geneva

B · M · G
AVOCATS

27.09.24

I. Introductory remarks

B · M · G
AVOCATS

Federal Data Protection Act came into force on 1st september 2023 (FDPA)

Two ordinances by two main ordinances, one related to the FDPA, one to certifications

The FDPA is more a substantial revision than a truly new Act, and still relies upon the same data protection principles

Lawfulness, fairness and transparency; purpose limitation; mnimisation; accuracy; storage limitation; integrity; and confidentiality; accountability

Key points of the revision (selection)

- Only data related to individuals are in scope
- Privacy by design and by default (art. 7)
- Data protection officers (art. 10)
- Code of conducts (art. 11) and certifications (art. 13)
- Register of activities (art. 12)
- Data protection impact assessment (art. 22 and 23)
- Data breach notifications (art. 24)
- Increased rights for individuals (art. 25 et seq.)
- Increased powers of investigations for the Federal Data Protection Commissioner (art. 49 et seq.)
- Increased sanctions (art. 60 et seq.)

Content

What's new with regards to the Federal Data Protection Commission and the FDPA? (II)

What are the current learnings with private entities? (III)

What are the latest developments to be kept in mind? (IV)

II. Federal Data Protection Commission

B·M·G
AVOCATS

I. Before 1 september 2023

LE TEMPS

EN CONTINU MONDE SUISSE ÉCONOMIE R/ÉVOLUTIONS OPINIONS CULTURE SOCIÉTÉ SCIENCES SPORT CYBER ARTICLES AUDIO VIDÉOS PODCASTS

Huit questions pour saisir les enjeux majeurs de la nouvelle loi sur la protection des données

Le 1er septembre est entrée en vigueur en Suisse la nouvelle loi sur la protection des données, imposant une myriade d'obligations aux entreprises et devant protéger mieux les

- Substantial efforts from the Commissionner to ensure the visibility of the new Federal Data Protection Act FDPA).
- Heavily mediated
- Companies aware of the existence of the FDPA and its significance, following the heavily mediated GDPR
- Twice as many phone calls in August and September 2023 as usual

B · M · G
AVOCATS

II. Some figures

Increase of resources at the Federal Data Protection Commission: 27 to 33 FTEs

Federal Data Protection Commission has 4 primary tasks: advice, monitoring, information and legislation

Time allocated

- 53.3% advice (out of which 20.8% to private sector)
- 15.7% monitoring
- 17.8% information
- 13.2% legislation

B·M·G
AVOCATS

II. Some figures

- 15.7% related to monitoring is similar to the existing ratio since 2015

- «Only» 12 in-depth investigations carried out in 2023.

- Intent to shift resources from «information» to «monitoring» to control around 12’000 big and medium-sized companies as well as around 10’000 associations and foundations

B · M · G
AVOCATS

II. Some figures

- Significant increase of complaints and denunciations from individuals: 4091 to 5074 in a year
- Average of 51 letters sent per month to individuals by the Federal Data Protection Commission
- Increased advice requested on AI related projects

B · M · G
AVOCATS

III. Official supporting tools

Federal Data Protection Commissionner has made significant efforts to support the companies and federal authorities in their duties to comply with the FDPA

B · M · G
AVOCATS

III. «Official» supporting tools

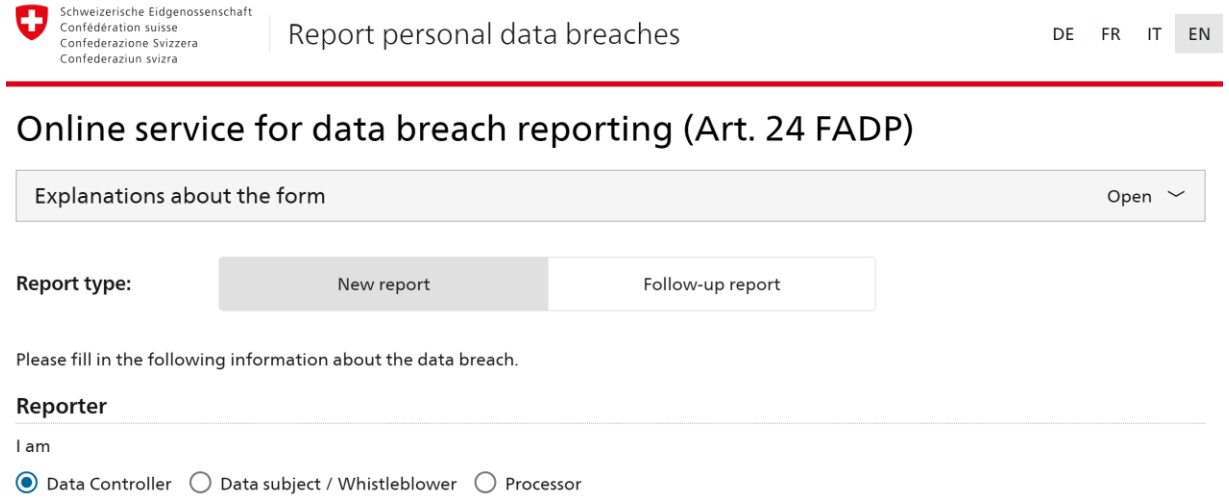
- **Register of processing activities** can be recorded **for federal authorities** through an interface provided by the Federal Data Protection Authority

- Datareg.edoeb.admin.ch

B·M·G
AVOCATS

III. Official supporting tools

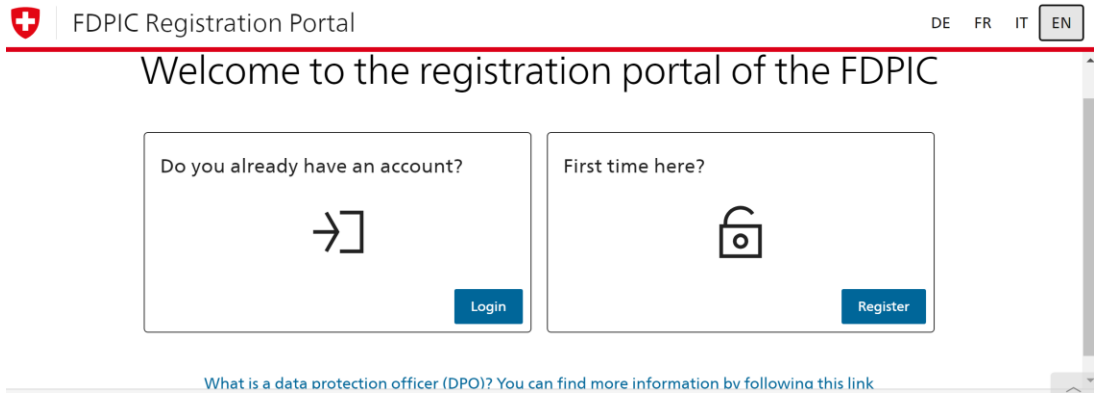
- **Data breaches** can also be notified through an online portal
- Most data breaches are notified through this portal
- 245 notifications since May 9, 2023, most of the time related to subprocessors
- 57 have required follow-up with additional information



B·M·G
AVOCATS

III. Official supporting tools

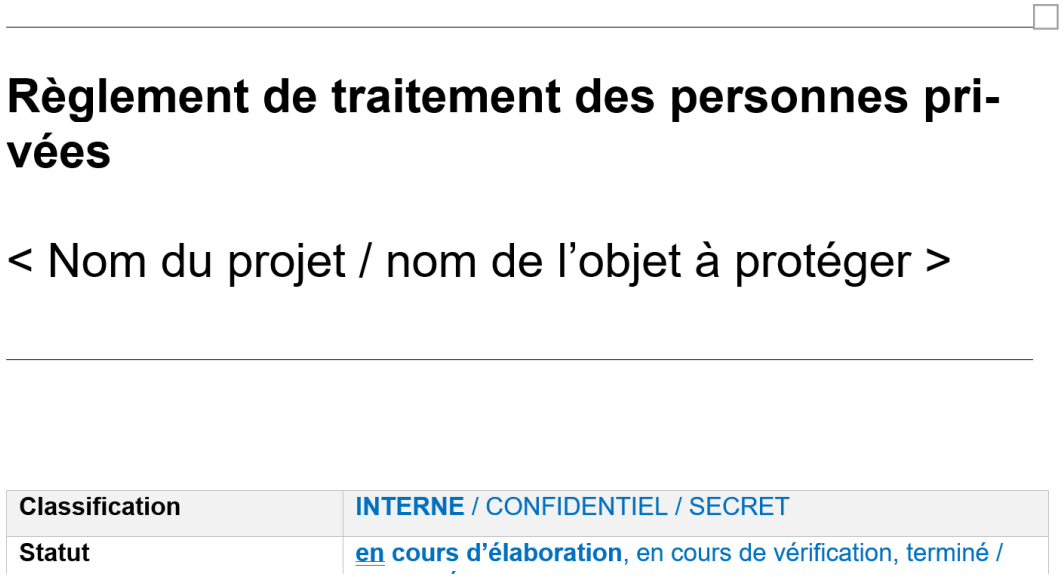
- **Data Protection Officers** portal
- Mandatory for federal authorities
- Optional for private entities
- More than 2000 recorded so far
- Dpo-reg.edoeb.admin.ch



B·M·G AVOCATS

IV. Official templates

- Federal authorities (art. 6 Ord.) and private authorities (art. 5 Ord.) sometimes have to adopt a **processing regulation** (high risk profiling; processing of sensitive data at scale



Règlement de traitement des personnes privées

< Nom du projet / nom de l'objet à protéger >

Classification	**INTERNE** / CONFIDENTIEL / SECRET
Statut	**en cours d'élaboration**, en cours de vérification, terminé /

B · M · G
AVOCATS

IV. Official templates

- Data Protection Commissionner provides a template for **Subject Access Request (SAR)**

Expéditeur:

Prénom/nom .....

Adresse .....

NPA/localité .....

Lieu et date .....

Recommandé

Responsable du traitement .....

.....

.....

Demande d'accès

Mesdames, Messieurs,

Me fondant sur l'art. 25 de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD), je vous prie de bien vouloir me donner par écrit et gratuitement, dans un délai de 30 jours dès réception de la présente, les informations suivantes :

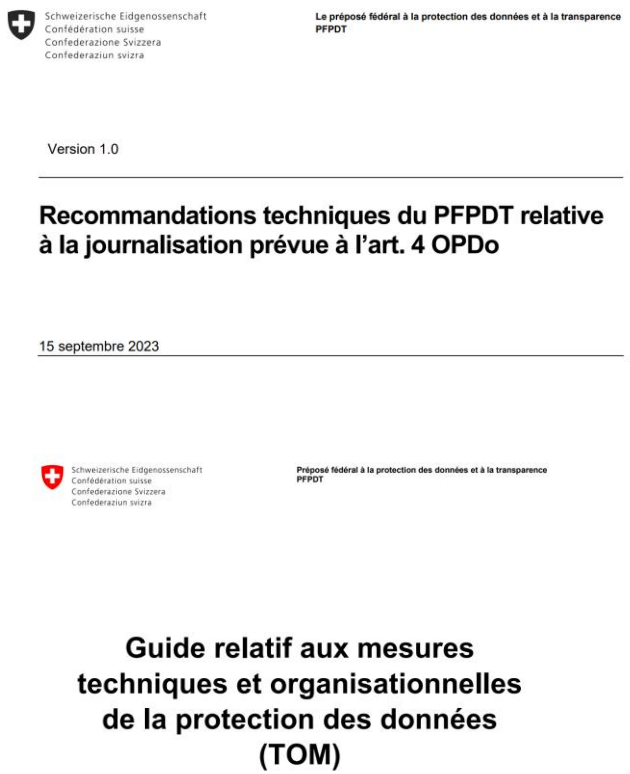
1. l'identité et les coordonnées du responsable du traitement;
2. les données personnelles traitées en tant que telles;
3. la finalité du traitement;
4. la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères pour fixer cette dernière;
5. les informations disponibles sur l'origine des données personnelles, dans la mesure où ces données n'ont pas été collectées auprès de la personne concernée;
6. le cas échéant, l'existence d'une décision individuelle automatisée ainsi que la logique sur laquelle se base la décision;
7. le cas échéant, les destinataires ou les catégories de destinataires auxquels des données

B·M·G AVOCATS

V. Official guidelines

- Guidelines also exist with regards to the requirements to store **logs** (art. 4 Ord.)

- Same for **technical and organisational measures**



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le préposé fédéral à la protection des données et à la transparence
PFPDT

Version 1.0

Recommandations techniques du PFPDT relative à la journalisation prévue à l'art. 4 OPDo

15 septembre 2023

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

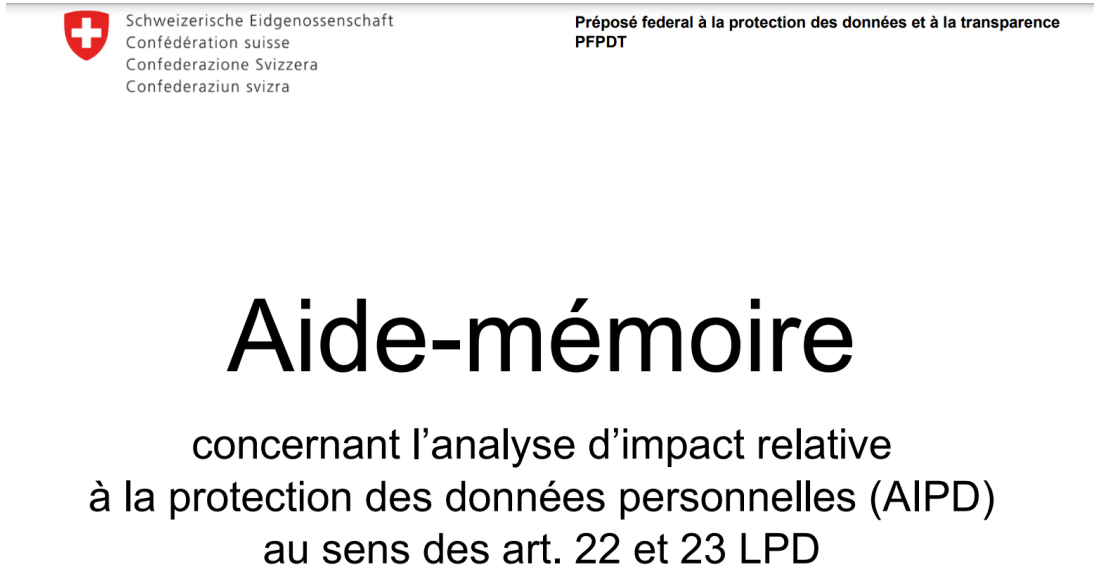
Préposé fédéral à la protection des données et à la transparence
PFPDT

Guide relatif aux mesures techniques et organisationnelles de la protection des données (TOM)

B·M·G
AVOCATS

V. Official guidelines

- Guidelines related to **data protection impact assessment** (DPIA, art. 22 and 23 FDPA)



B·M·G
AVOCATS

VI. Monitoring activities

- As seen above, these activities remain limited so far.
- Current investigations (at least publicly released) were launched prior to the coming into force of the FDPA.
- Forum Civique Suisse: collecting publicly available data of priests to build a database, send them a questionnaire as to their religious convictions and then publicly release the data ➔ Forum Civique agreed not to publicly release the answers from the one refusing it, but refused to delete these data ➔ formal investigation launched in December 2023

B · M · G
AVOCATS

VI. Monitoring activities

- Real estate agency is not allowed to ask women whether they are or are about to become pregnant. The argument according to which such question would be meant to assess and allocate bigger apartments to future families cannot be considered a prevailing interest and exceeds the principle of minimization. Mère consent is not acceptable as not freely given.
- Digitec Galaxus did not comply with its duty to inform and the principle of proportionality by asking too many data and preventing customers to make a purchase without having to first create an account. Galaxus agreed to comply and the Commissioner will have to assess whether Galaxus has implemented the required modifications.

B·M·G
AVOCATS

III. Learnings from private companies

B·M·G
AVOCATS

I. General remarks

FDPA did not have significant impact on multinational companies that had already made most of the work to implement the GDPR

FDPA obviously had more impact on SMEs BUT:

Unlike GDPR, fines are limited because:

- - Commissionner cannot impose them;
- - Fines are only pronounced by criminal authorities
- - Subject to a criminal complaint
- - Only up to CHF 250’000
- - For a limited number of breaches

➔ Little incentive to raise significant budgets

I. General remarks

Incentive comes more from:

- Reputation (customer/public relations)
- Cybersecurity issues
- Potential audit (although risk remains limited for small companies)

Willingness to limit compliance to «MUST BE» rather than «NICE TO HAVE» (budget constraints) ➔ no need for a Rolls Royce

B·M·G
AVOCATS

II. What is the «must be» ?

- Contractual documents (external: privacy policy, cookie policy, data processing agreement/internal: employee privacy notice, retention policy)
- Guidelines to address subject access requests
- Data breach process
- Register of activities (if need be, but good exercice to assess and control data flows) – sometimes difficult to get it done internally

B · M · G
AVOCATS

III. Concerns

- International transfers have drawn much scrutiny
- In the absence of transfer to a country having an adequate level of protection, you need certain safeguards (typically contractual clauses)
- Health industry is subject to additional requirements as a result of its processing of health related data, i.e. sentitive data.
- Double problems: data protection (consent required) and professional secret (art. 321 Criminal Code) ➔ transfer abroad could lead to breach of professional secret as recipient is not bound by art. 321 Criminal Code

B · M · G
AVOCATS

IV. Latest developments: international transfers

B·M·G
AVOCATS

Two good news

I. Introduction

- 2020: ECJ rules that (1) the EU-US Privacy Shield does not comply with the GDPR and that (2) the existing standard contractual clauses still requires a risk assessment to be carried out.

- 4 June 2021: new EU standard contractual clauses implemented by the European Commission, however requiring a risk assessment to be carried out ➔ fairly heavy, notably for SMEs

- In practice, it usually is up to the processor to provide a risk assessment and ensure that the transfer does not represent a significant risk for the individuals, or that such residual risk is mitigated.

- Heavy solution

B · M · G
AVOCATS

II. Swiss-US Privacy framework

- July 2023: EU and US had already adopted the EU-US Data Privacy Framework.
- Question to assess whether such framework was also applicable to the transfers to Switzerland had not been addressed
- 14 August 2024: Federal Council has approved the Swiss-US Data Privacy Framework

B · M · G
AVOCATS

II. Swiss-US Privacy Framework

Self certification process to be renewed on a yearly basis

Rights of data subjects have been increased: right to access their data

Companies are accountable to transfers downstream to subprocessors and compliance with the framework

Opt in requirement for any processing not initially contemplated

These companies are subject to the surveillance of the FTC, to which a complaint can be filed, as well as to the Federal Data Protection Commissioner

In the absence of resolution, arbitration to the ICDR (International Center for Dispute Resolution) may be filed

II. Swiss-US Privacy Framework

Other key point to ensure adequacy for the US: access by authorities.

Access by authorities and its limitations has been more clearly defined, with the appointment within authorities of DPOs, subject to the Privacy and Civil Liberties Oversight Board

Data Protection Review Court in place since 7 October 2022 (E.O. 14086) re: surveillance from US authorities

US considered an adequate country (for these companies) as of 15 September 2024

B · M · G
AVOCATS

III. Switzerland as adequate country

After the enactment of the revised FDPA, Switzerland had to go through a new assessment of its legislation from the EU to be considered as an adequate country

15 January 2024: EC Commission confirmed Switzerland on its list of adequate countries

B · M · G
AVOCATS

Many thanks for your attention!

B · M · G
AVOCATS

Prof. Philippe Gilliéron
Philippe.gillieron@bmglaw.ch