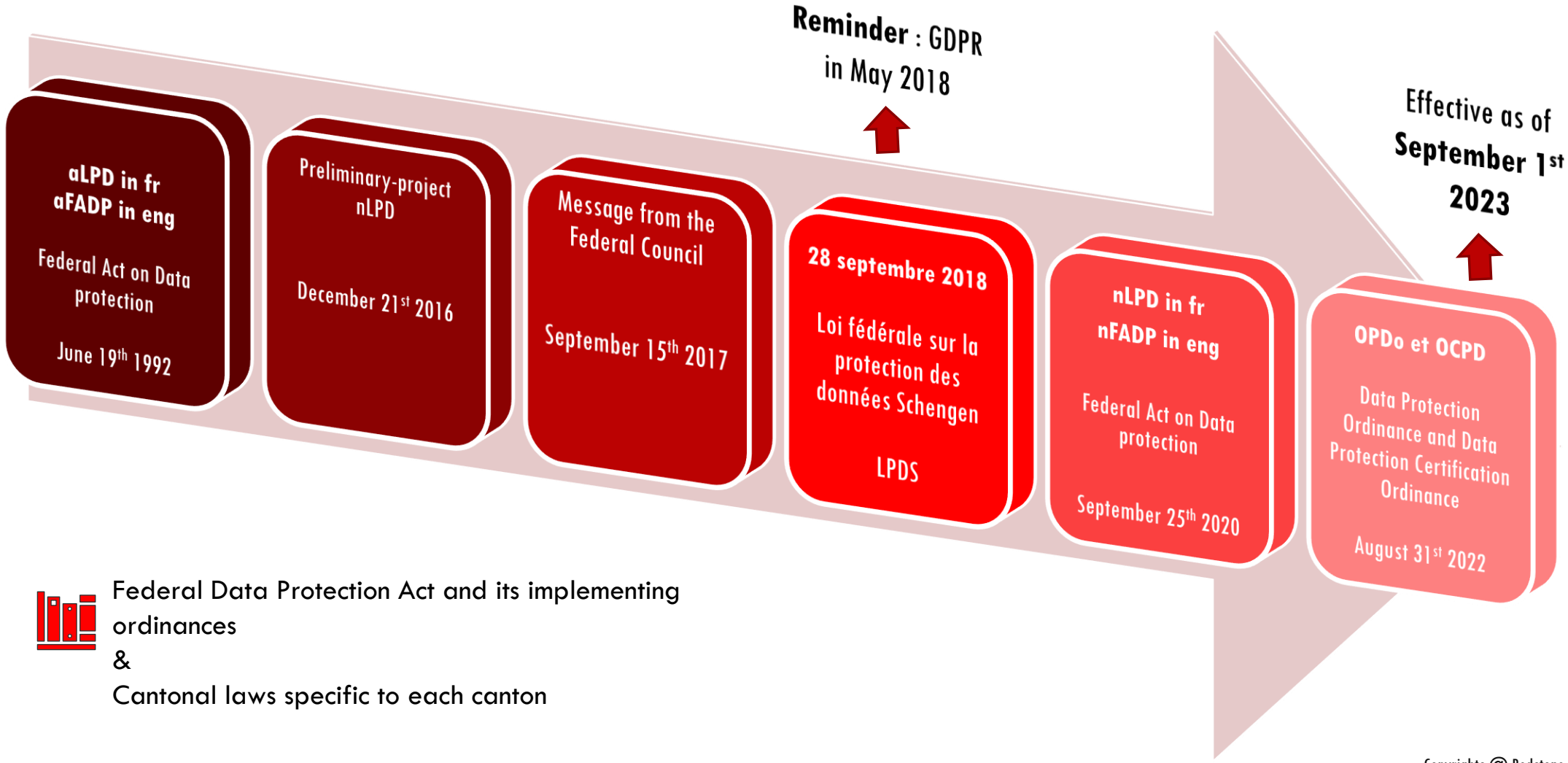
REVISION OF THE SWISS DATA PROTECTION ACT

xxx
2023

REDstone consulting

IN SWITZERLAND?



Federal Data Protection Act and its implementing ordinances
&
Cantonal laws specific to each canton

PURPOSE OF THE LAW

The nFADP aims to protect the personality and fundamental rights of physical persons

Whose personal data are processed.

(art. 1)

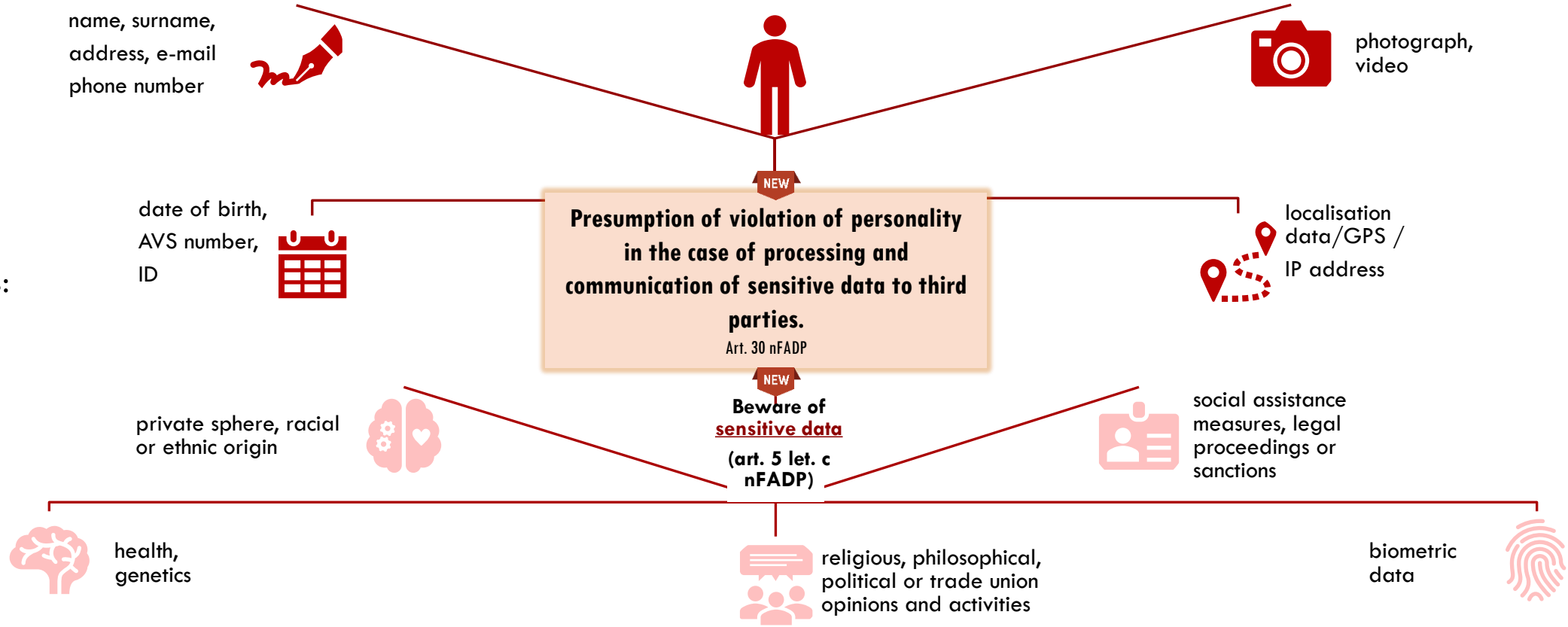
SCOPE OF THE LAW

The nFADP applies to the processing of personal data by private individuals or federal authorities. (art. 2)

DEFINITION: PERSONAL DATA

Any information relating to an *identified* ou *identifiable* (natural) person, *directly* or *indirectly* (art. 5 let.a).

Examples:



DEFINITION: PROCESSING

Any operation relating to personal data, whatever the means and procedures used.

(art. 5 let. d nFADP)

Collection

- Survey
- Questionnaire
- Online form
- Interviews
- Online activity monitoring observation
- Data exchange (internal or external)

Using

- Recording
- Storage
- Consultation
- Updating
- Transmission
- Archiving

Deletion

- Remove
- Destruction
- Portage
- Anonymisation

ACTORS

NEW

Causal responsibility

The data controller remains responsible, even in the event of sub-contracting (proactivity).

(art. 9 nFADP)

DATA SUBJECT	DATA CONTROLLER	DATA PROCESSOR
Individual whose personal data is processed (art. 5 let. b). The data of legal entities are no longer personal data within the meaning of the nFADP (art. 5 let. a FADP a contrario).	The **private individual** (*legal entity or individual*) or **federal authority** (*federal authority or service or natural person entrusted with a public task by the Confederation*) **which alone or jointly determines the purposes and means of processing personal data.**	Processes personal data on behalf of and in accordance with the instructions of the data controller. - Inform the data subject (art. 19 al. 2 let. c) - Provide for compliance with business/manufacturing/professional secrecy - Authorization required for 2nd tier subcontracting (general or specific) - Obligation to assist the controller in the event of an access request.

Data processing agreement

CHF 250'000.- (art. 61 let.b nFDAP)

EXTRATERRITORIALITY

The nFDAP applies to factual situation that **have an effect in Switerland**

Even if they occurred abroad.

(art. 3)

Case law confirmed: ATF 138 II 346 (Google Street View) – *strong link with Switzerland*

Example: The FADP applies to images taken in Switzerland and published on a website from abroad, where they are processed and made available to people in Switzerland..

EXTRATERRITORIALITY - GDPR

The GDPR also has **extraterritorial scope** (art. 3 GDPR).

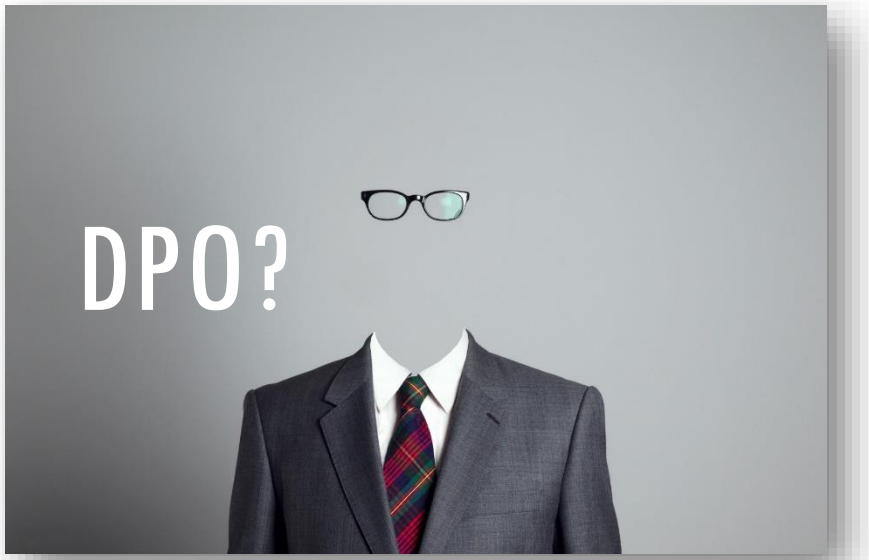
Data processing carried out in the context of the activities of an establishment[1] on the territory[2] of the Union, whether or not the processing takes place in the EU, and whether or not the data relate to residents of the EU or elsewhere.

[1] *Establishment:*

Broad concept, independent of legal form. A real and effective activity, even if minimal, by means of a permanent establishment is sufficient.

[2] *Marktort-Prinzip – Principle of market location:*

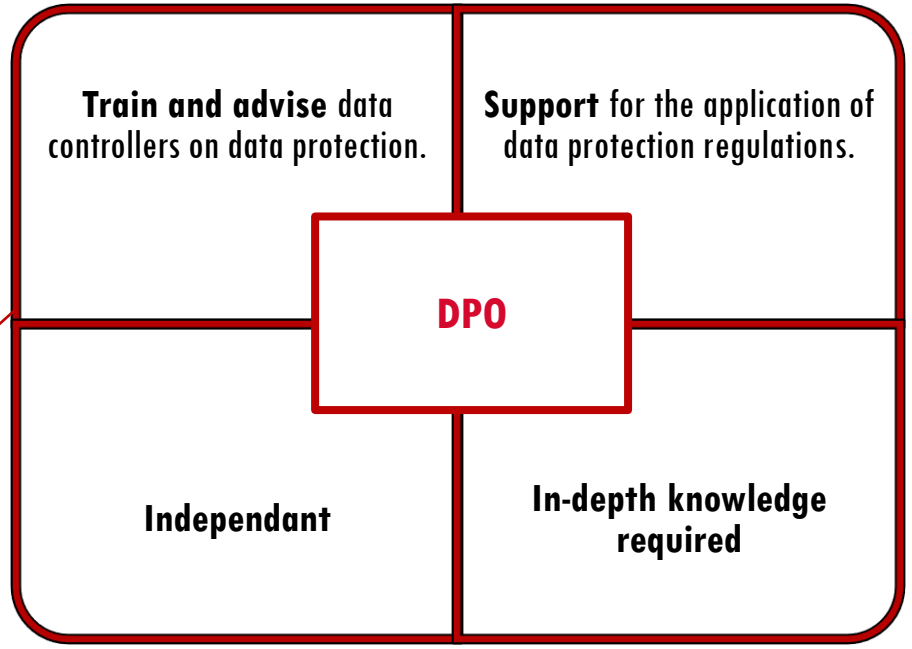
i. the personal data of an EU resident is processed in connection with goods and/or services offered to him/her (offer of goods or services);
ii. or the behaviour of individuals within the EU is "tracked" (behavioural tracking).



Private data controllers ***may*** appoint a **data protection officer**

(art. 10 nFADP et 23ss OPDo)

≠ GDPR



There is no need to consult the PFPDT (FDPIC) for the impact assessment with the remaining high risks.

SWISS REPRESENTATIVE NEW

Foreign private data controller

→ ***regular large-scale treatment*** which presents a **high risk**

→ must appoint a **Swiss representative** (art. 14 nFADP)

PRINCIPLES

NEW

Presumption of violation of personality in the case of treatment:

1) in violation of the principles (art. 6 et 8 nFADP)

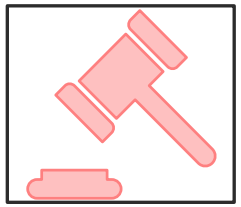
<u>or</u>

2) against the express wish of the data subject

Art. 30 nFADP

Lawfulness

Art. 6 al. 1 nFADP



Any processing of personal data requires, in principle, a **justification**

(art. 31 nFADP : law, consent*, publicor private interest).

Good faith

Art. 6 al. 2 nFADP & 2 CC

No data process without the knowledge or against the wishes of the data subject.

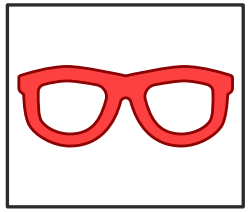
Proportionality

Art. 6 al. 3 FADP

- Only suitable and necessary data for achieving the intended purpose may be processed.
- **Avoid** non necessery process
- **Minimize** process

Transparency

Art. 6 al. 2 nFADP



Purpose and collection must be recognisable.

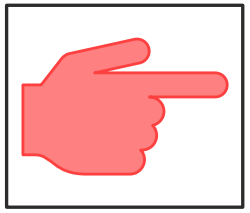
Purpose limitation

Art. 6 al. 3 nFADP

Process data solely for the purpose stated at the time of collection.

NEW Recognizability

Art. 6 al. 3 nFADP



Collection of data and its purposes must be recognisable and communicated to the data subject.

NEW Accuracy

Art. 6 al. 5 nFADP

Data must be complete and up-to-date.

Security

Art. 8 nFADP

Ensure confidentiality and protect data against unauthorised processing by using appropriate technical and organisational measures.

NEW

*<u>Consent</u>

Frea and clear

Art. 6 al. 6 et 7 nFADP

Free, clear, specific and unequivocal

Art. 4 GDPR

NEW

Personal data must be protected **by design** and **by default**

Art. 7 nFADP

THE DATA SUBJECT'S RIGHTS

NEW

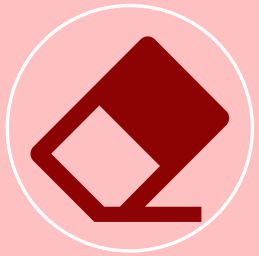
Right of access / to information

Response:
30 days (nFADP) et 1 month (GDPR) + free

Right to object to the processing

Right to have personal data rectified

Right to limitation



Right to be forgotten / erased

Right of portability

(art. 28ss nFADP et 20 OPDo)

Delivery: electronic form

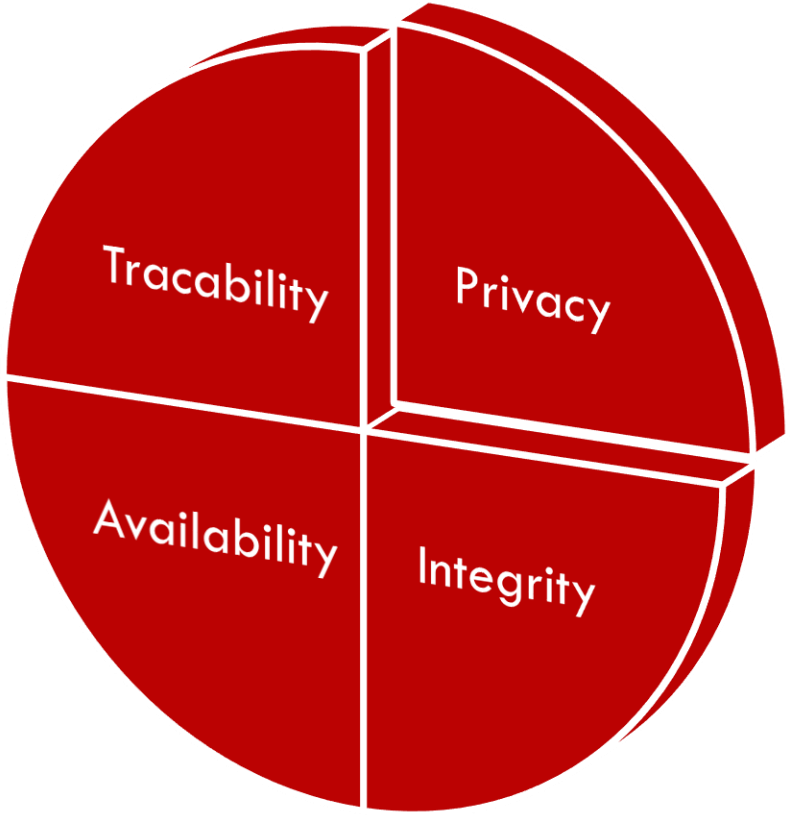
CHF 250'000.- (art. 61 let. a nFADP)

APPLYING THE PRINCIPLES: TOM'S

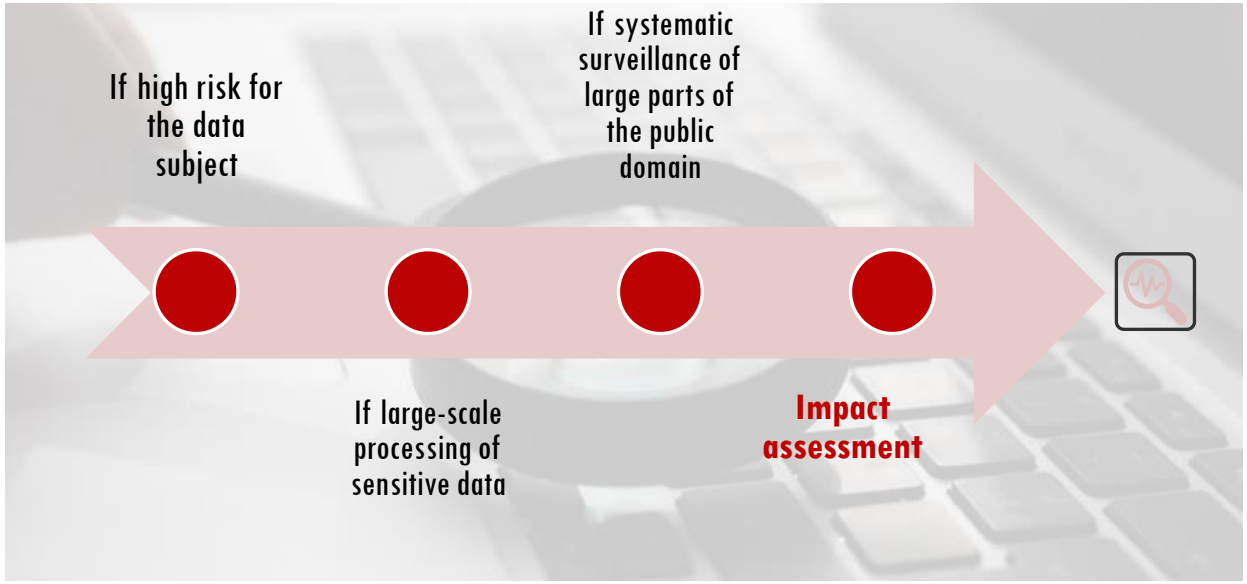
No presumption of compliance.

Articles 5(2) and GDPR require data controllers to demonstrate their ***compliance*** with the principles and the ***effectiveness*** of the measures taken.

Cf. Message LPD, pp. 6592 and 6794, articles 4 and 5 OLPD on security measures from which the principle of responsibility is deduced.



IMPACT ASSESSMENT (DPIA – 22 LPD) NEW



Examples:

- Physical risks (health data, false treatment)
- Material risks (bank card abuse)
- Immaterial risks (social disadvantages)

If necessary, carry out an impact assessment (art. 22 nFADP)

In case of new project, self-assessment of the most sensitive processing operations that involve a higher risk for the individual or fundamental rights:

- *Respect for principles*
- *Respect for rights*
- *Risk analysis*

9 criteria

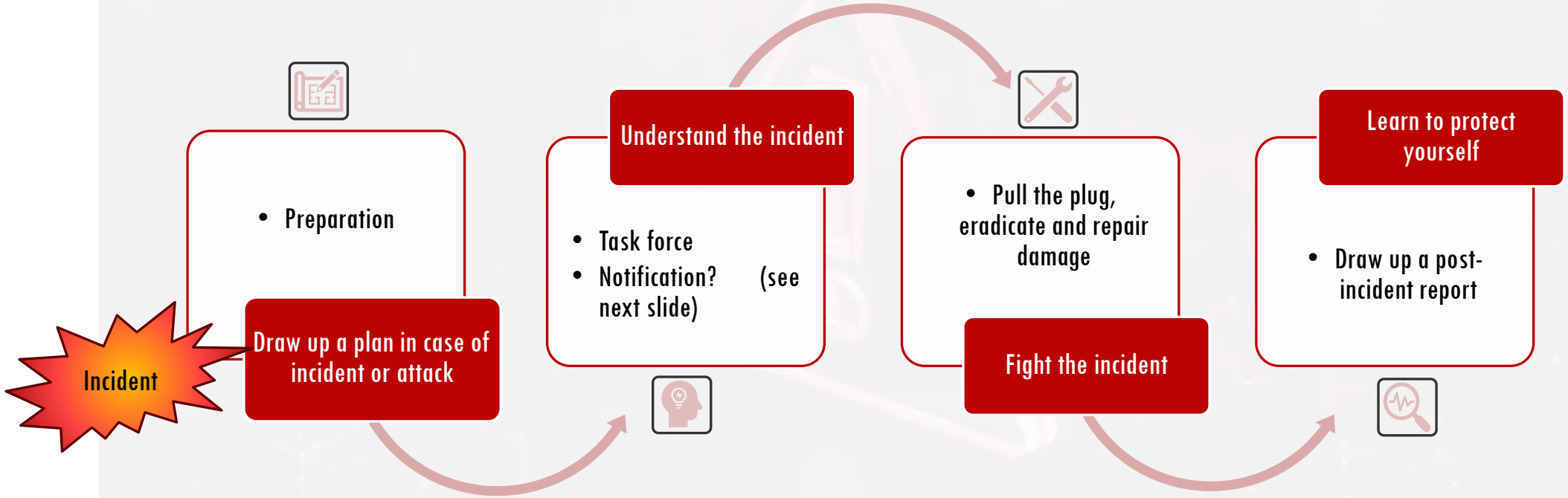
- Evaluation/scoring (including profiling)
- Automatic decisions with legal or similar effect
- Systematic monitoring
- Sensitive or highly personal data
- Large-scale collection
- Cross-referencing of data
- Vulnerable persons
- Innovative use
- Exclusion from a right/contract/service

INTERNAL PROCEDURE IN THE EVENT OF A BREACH

NEW

Reminder

A breach is the loss, destruction, modification and/or unauthorised disclosure of and/or access to processed data, regardless of whether this is accidental or unlawful, and regardless of whether there is any damage.



NOTIFICATION IN THE EVENT OF A VIOLATION

NEW

Notify *data breach* (art. 24 nFADP et 15 OPDo et 33 GDPR)

In Switzerland – To the **PFPDT (FDPIC) as soon as possible** if the nFADP is applicable and the data security breach is likely to result in a high risk to the data subject's personality or fundamental rights.

In Europe- To the **relevant authority** in **72 hours** if GDPR is applicable.

When must the data subject be notified?

When necessary for its protection or if required by the PFPDT (FDPIC).

Your subcontractors also need to be informed.

Préposé fédéral à la protection des données et à la transparence PFPDT (FDPIC) (admin.ch)

CONSEQUENCES OF A BREACH

NEW

SWITZERLAND

Administrative procedures (see next slide)

- PFPDT (FDPIC)
- Enquiry and non-binding sanctions

Criminal procedure (see next slide)

Ordinary prosecution authorities

- Penalty of up to CHF 250,000 (physical person)

Civil procedure

- Civil authorities with jurisdiction over the subject matter and the value in dispute
- Compensation for damage

EUROPE

Administrative procedures

Data Protection Authorities (DPA)

Link: [Archived content]Data Protection Authorities - European Commission (europa.eu)

In there's an incident, the DPA may:

- Issue a call to order;
- Enjoin the processing operation;
- Temporarily or permanently restrict processing;
- Suspend the flow of data:
- Order or require compliance with the rights of data subjects;
- Impose an administrative fine :RGPD:
  - up to €20 million or up to 4% of annual worldwide turnover

DIRECT IMPACT

1. Updated internal documents
   - Personal data processing activities register
   - Confidentiality policies
   - Rights and obligations of employees (future and current) / Internal regulations
   - Security of information
   - Retention and deletion policy
2. TOM's
3. Review
   - contracts (DPA, HR, . . .)
   - websites and mailing (not. privacy policy, cookies and disclaimers)
4. Cross-border communications
5. Internal procedure:
   - if there is a violation
   - to respect data subject's rights
6. Duty to disclosure (PFPDT (FDPIC))
7. Training and awareness-raising for all
8. Identify the impact analyses to be carried out
9. Appoint a DPO where needed

CONTACT

Nicolas Vernaz – Founder & CEO

Redstone Consulting SA
Esplanade de Pont-Rouge 4 - 1212 Lancy
Tél.: +41(0) 78 762 77 81
nv@redstoneconsulting.ch
Web : www.redstoneconsulting.ch