Data Protection and Cybersecurity Breaches: What Risks of Liability?

Geneva Cybersecurity Law & Policy Conference

Dr. David Vasella, CIPP/E

walderwyss attorneys at law

What is a "breach"?

- Generic obligation on controller(s) and processor(s) to take appropriate security measures
  (Data Protection Act (DPA) and Ordinance (DPO) of 1993)
- "Data Breach": any unauthorized processing (including any breach of a processing principle)
- Specific security obligations in the financial sector (FINMA Circular on operational risks: Banks must implement an IT risk management concept and specifically a risk management concept for dealing with cyber risk)

“Civil Liability” under Swiss Law

“Liability”: Article 28a Civil Code

1 The applicant may ask the court:

1. to **prohibit** a threatened infringement;
2. to order that an existing infringement **cease**;
3. […]

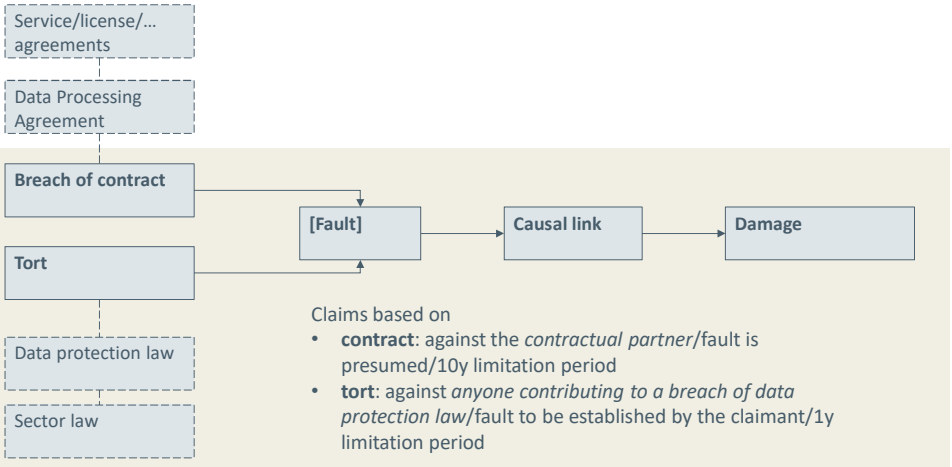
2 […]

3 **Claims for damages and satisfaction** and for **handing over profits** […] are reserved.

} “negatory” action

} “reparatory” action

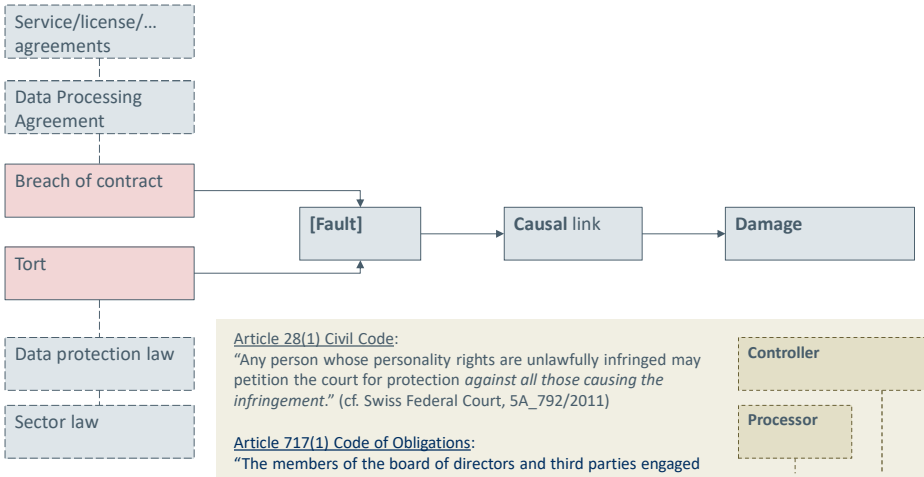
Requirements for Liability under Swiss Law



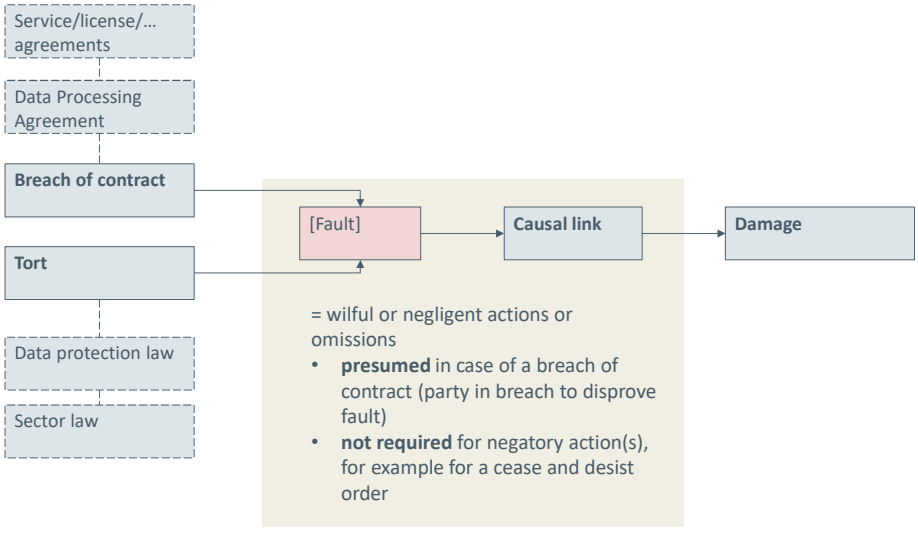
Claims based on

- **contract**: against the *contractual partner*/fault is presumed/10y limitation period
- **tort**: against *anyone contributing to a breach of data protection law*/fault to be established by the claimant/1y limitation period

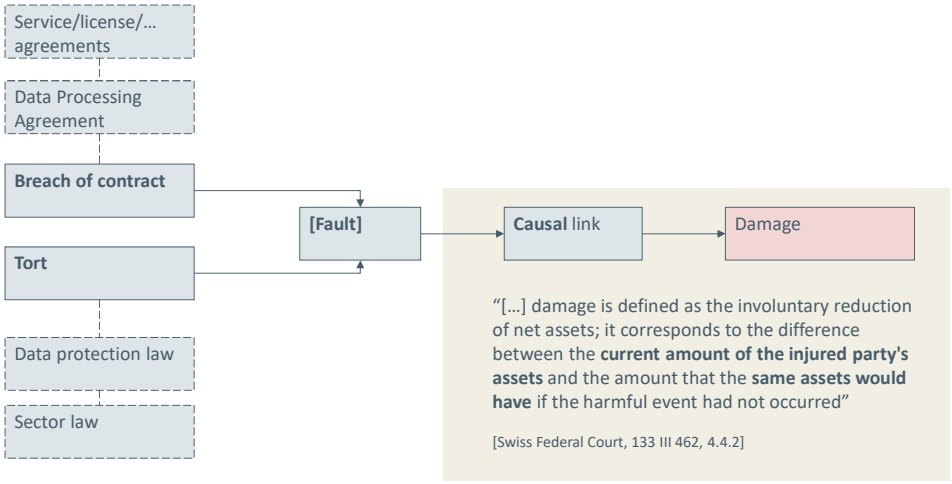
Who's at risk?



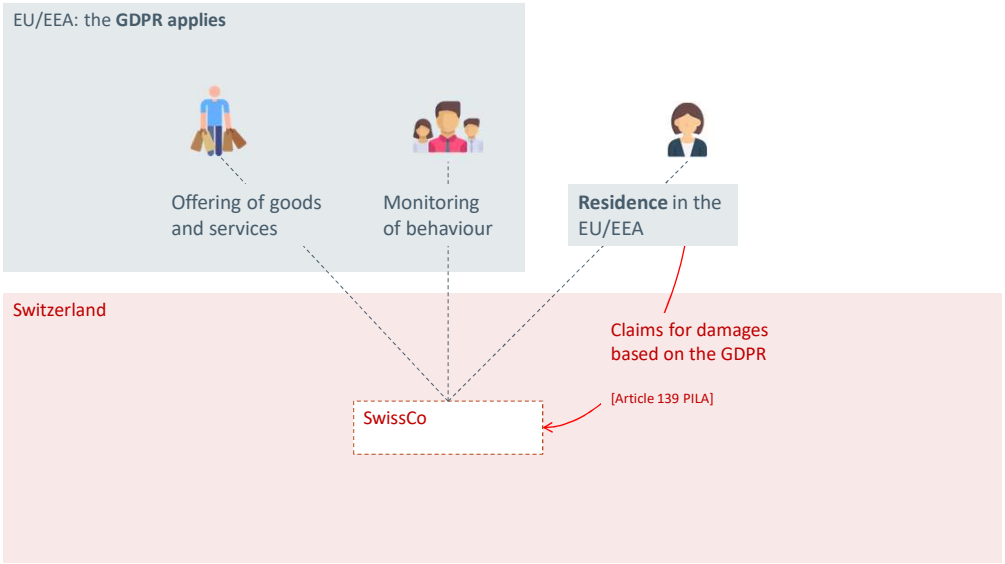
"Fault"



“Damage”: Quantifiable Financial Impact



Role of the GDPR



Data breach affecting a data processor

Claims against the controller:

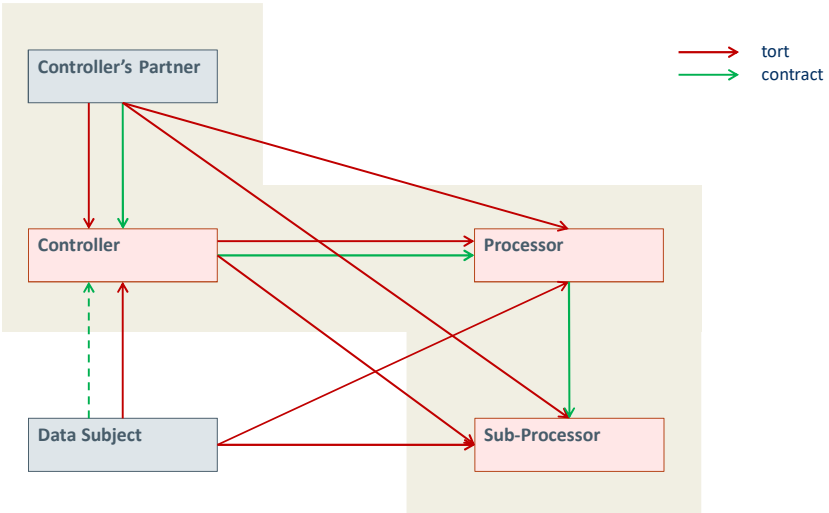
- based on liability for the processor
  (under the GDPR as well as Swiss law)
- **data subjects** for damages (data subjects in the EEA: including for non-material damages)
  (based on tort)
- the controller's **contractual partners**
  (based on contract and potentally tort)
- **authorities** (investigation; potentially fines)

Claims against the processor:

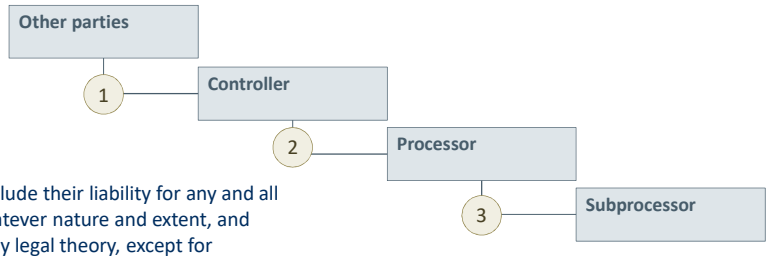
- **data subjects** for damages (data subjects in the EEA: including for non-material damages)
  (based on tort)
- the **controller(s)**
  (based on contract and/or tort)
- the controller's **contractual partners**
  (based on tort)
- **authorities** (investigation; potentially fines)

joint and several liability (article 50 et seq. and 99(3) CO)

Data breach affecting a data processor or sub-processor



Risk allocation



1
2
3

"The Parties exclude their liability for any and all damages of whatever nature and extent, and arising under any legal theory, except for damages caused willfully or with gross negligence. [*The Parties exclude any liability for their auxiliaries.*]"

2
3

[Article 28(4) GDPR: *"Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."*]

1
2
3

"[…] shall indemnify, defend and hold harmless […]": =?

Questions?

Dr. David Vasella, attorney at law, CIPP/E
david.vasella@walderwyss.com
direct: +41 58 658 52 87

walderwyss attorneys at law