Data Protection and Cybersecurity Breaches: What Risks of Liability?

Geneva Cybersecurity Law & Policy Conference
Dr. David Vasella, CIPP/E

- 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)

What is a “breach”?
“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.

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?

- Service/license/... agreements
- Data Processing Agreement
- Breach of contract
- Tort
- Data protection law
- Sector law

Article 28(1) Civil Code:
"Any person whose personality rights are unlawfully infringed may petition the court for protection against all those causing the infringement." (cf. Swiss Federal Court, 5A_792/2011)

Article 717(1) Code of Obligations:
"The members of the board of directors and third parties engaged in managing the company's business must perform their duties with all due diligence and safeguard the interests of the company in good faith."

“Fault”

- Service/license/... agreements
- Data Processing Agreement
- Breach of contract
- Tort
- Data protection law
- Sector law

= wilful or negligent actions or omissions
  - presumed in case of a breach of contract (party in breach to disprove fault)
  - not required for negatory action(s), for example for a cease and desist order
“Damage”: Quantifiable Financial Impact

Damage is defined as the involuntary reduction of net assets; it corresponds to the difference between the current amount of the injured party’s assets and the amount that the same assets would have if the harmful event had not occurred.

[Swiss Federal Court, 133 III 462, 4.4.2]

Role of the GDPR

EU/EEA: the GDPR applies

- Offering of goods and services
- Monitoring of behaviour
- Residence in the EU/EEA

Switzerland

Claims for damages based on the GDPR

[Article 139 PILA]
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 potentially 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

Controller's Partner

Controller

Processor

Data Subject

Sub-Processor

<table>
<thead>
<tr>
<th>red</th>
<th>tort</th>
</tr>
</thead>
<tbody>
<tr>
<td>green</td>
<td>contract</td>
</tr>
</tbody>
</table>
"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.]

[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.”]

“[...] shall indemnify, defend and hold harmless [...]”