SWISS INFOSEC

ISSS BERNER TAGUNG
19. NOVEMBER 2019

RECHTLICHE ASPEKTE BEI IT BESCHAFFUNGEN AUS SICHT INFORMATIONSSICHERHEIT

Reto C. Zbinden
CEO/Rechtsanwalt
Swiss Infosec AG

AGENDA
THEMENÜBERSICHT

Swiss Infosec AG
Hauptsitz in Sursee

01 EINLEITUNG

02 VERTRAG: GARANTIE/GEWÄHRLEISTUNG

03 GESETZLICHE HAFTPFLICHT

04 PRODUKTHAFTPFLICHT

05 VERTRAGSGESTALTUNG

06 ZUSAMMENFASSUNG – FRAGEN/DISKUSSION

SWISS INFOSEC

KAPITEL 01

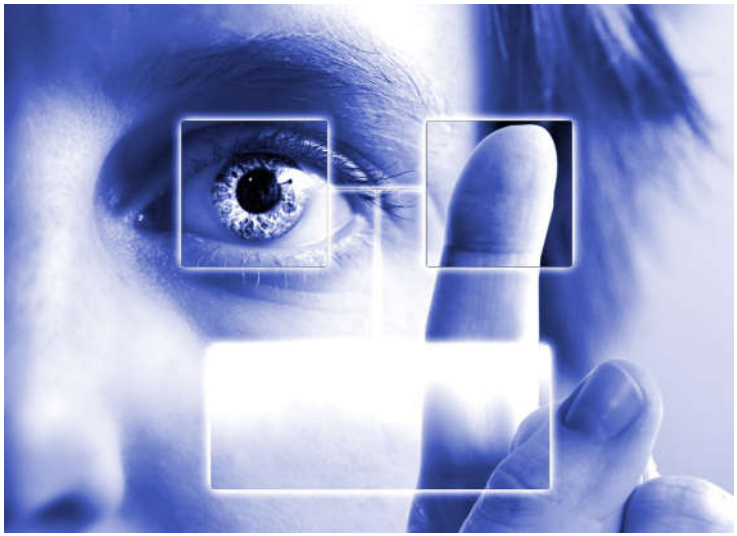
EINLEITUNG

IT-LEISTUNGEN: VIELFALT AN RECHTSVERHÄLTNISSEN

- Kaufvertrag →
  vertragliche Haftpflicht +
  Garantie/Gewährleistung
- Werkvertrag →
  vertragliche Haftpflicht +
  Garantie/Gewährleistung
- Auftrag →
  vertragliche Haftpflicht
- Miete →
  vertragliche Haftpflicht

WEITERE ANSPRÜCHE

- Ausservertragliche gesetzliche Haftpflicht
- Kausalhaftung wie z.B. Produkthaftpflicht



SWISS INFOSEC

KAPITEL 02

GARANTIE / GEWÄHRLEISTUNG

VERTRAG: VORTEILE

- Verschuldensunabhängige Rechtsbehelfe und Haftung beim Kauf für unmittelbare Schäden
- für absichtlich verschwiegene Mängel gilt eine Verjährungsfrist von 10 Jahren

VERTRAG: NACHTEILE

- Enger Mangelbegriff:
  zugesicherte Eigenschaften/Tauglichkeit zum vorausgesetzten Gebrauch
- Strenge gesetzliche Rügeobliegenheit («sofort»)
- Rechtsbehelfe Preisminderung oder Rückgabe gegen Vergütung bei IT-Produkten oft nicht zielführend
- Ansprüche nur gegenüber Käufer/Besteller, nich gegenüber den Vor- oder Zulieferanten
- Und last but not least: häufiger Ausschluss in Lieferanten-AGBs

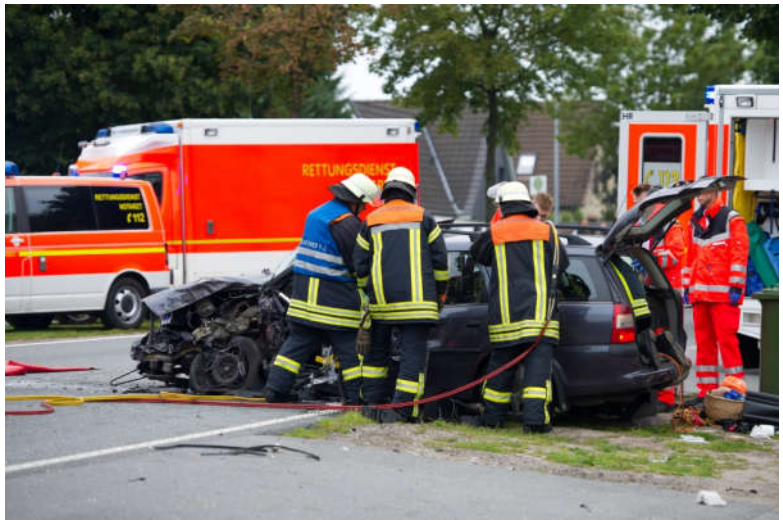
SWISS INFOSEC

KAPITEL 03:

GESETZLICHE HAFTPFLICHT

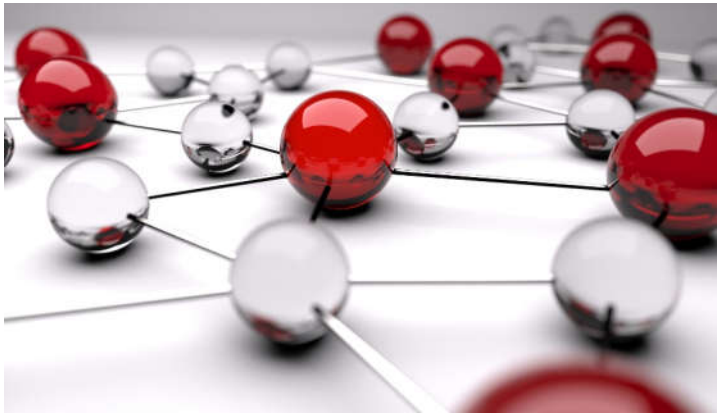
ÜBERSICHT

«Wer einem andern widerrechtlich Schaden zufügt, sei es mit Absicht, sei es aus Fahrlässigkeit, wird ihm zum Ersatz verpflichtet»



VORTEILE

- Gilt auch dann, wenn kein Vertrag abgeschlossen wird
- Keine sofortige Mängelanzeige nötig, aber einjährige Verjährungsfrist (ab Kenntnis von Schaden und Verursacher), die zehn Jahre nach Schadenseintritt dann definitiv verjährt



NACHTEILE

- Schadenersatz ist an ein Verschulden (Vorsatz/Fahrlässigkeit) gekoppelt, das nachgewiesen werden muss
- Nachweis regelmässig anspruchsvoll, dass Schaden nach allgemeiner Lebenswartung die gewöhnliche Folge des vorgeworfenen Verhaltens ist
- Auch hier:
  häufiger Ausschluss in Lieferanten-AGBs

ZUSATZ GESCHÄFTSHERRENHAFTUNG

- Haftung für Hilfspersonen, aber nur bei Subordinationsverhältnis (teilweise aber nicht gegeben gegenüber IT-Provider weil dazu ihnen gegenüber eine Weisungsbefugnis bestehen müsste)
- Verschulden wird vermutet, aber Sorgfaltsbeweis möglich: sorgfältige Auswahl, Instruktion, und Überwachung

PRODUZENTENHAFTUNG – "SCHACHTRAHMENFALL"*

Beim Verlegen des von einem Bagger angehobenen Schachtrahmens wurde ein Arbeiter erheblich verletzt, weil sich eine Aufhängeschlaufe aus der Verankerung gelöst hatte. Ursache war die **unzureichende Sicherheitsprüfung** der Verankerung.

Das Bundesgericht bejahte die Haftung des Herstellers des Rahmens, weil er in seinen Betrieb die Sicherheitsprüfung seiner Produkte vernachlässigt hatte: sog. "**Organisationsverschulden**".

PRODUZENTENHAFTUNG – "SCHACHTRAHMENFALL"*

Dieser Entscheid kann für vergleichbare Folgen aus mangelhafter Prüfung von Anlagen, Komponenten in der Maschinen- und IT-Branche herangezogen werden.

* BG Entscheid 110 II 456

http://www.servat.unibe.ch/dfr/c2110456.html

SWISS INFOSEC

KAPITEL 04

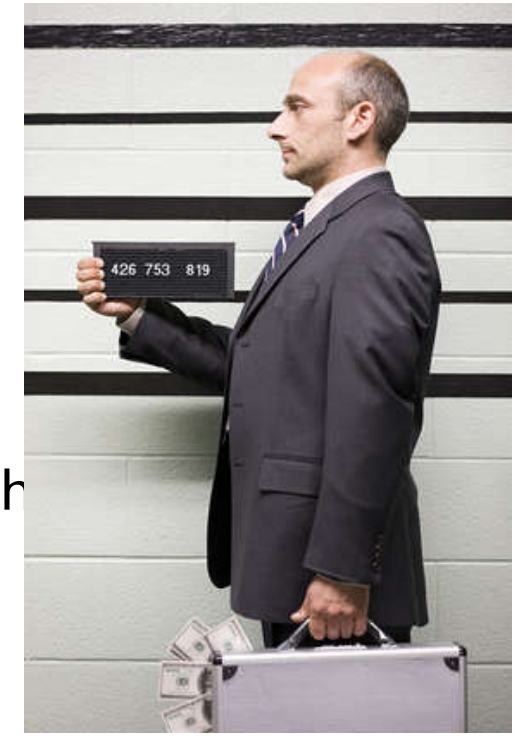
PRODUKTHAFTPFLICHT

ÜBERSICHT

„Die herstellende Person (Herstellerin) haftet für den Schaden, wenn ein fehlerhaftes Produkt dazu führt, dass:

a) eine Person getötet oder verletzt wird;
b) eine Sache beschädigt oder zerstört wird, die nach ihrer Art gewöhnlich zum privaten Gebrauch oder Verbrauch bestimmt und vom Geschädigten hauptsächlich privat verwendet worden ist.

Die Herstellerin haftet nicht für den Schaden am fehlerhaften Produkt.“



VORTEILE

- Kein Ausschluss in Provider-AGB möglich
- Auch Mängel von Komponenten eines Produkts erfasst
- Alle ”Hersteller”, d.h. der Verkäufer und dessen Vor- oder Zulieferanten haften solidarisch für die Folgen eines Produktefehlers

NACHTEILE

- Körperliches Produkt vorausgesetzt (beim Bereitstellen von Cloud-Services wie Rechenleistung und Softwareapplikationen nicht gegeben)
- Enger Anwendungsbereich: Personenschaden und (nur) für Konsumenten Sachschaden (aber nicht am fehlerhaften Produkt)→ primär Konsumentenschutz
- Beispiel: also nicht Totalschaden des fehlehrhaften Autos, sondern nur das beim Unfall beschädigte Reisegepäck

ZWISCHENFAZIT

- Für Schäden bei Verletzungen der IT-Sicherheit ist gesetzliches Haftungsregime zu wenig griffig
- Einzige Einflussmöglichkeit: Vertrag (um damit gleich auch widersprechende Lieferanten-AGBs zu übersteuern) → vertragliche Haftpflicht
- Praxisempfehlung für das Submissionsverfahren: Ein ausformulierter Vertrag wird zum Eignungskriterium gemacht (ev. in Zusammenspiel mit SIK-AGB) und dieser den Ausschreibungsunterlagen beigelegt

SWISS INFOSEC

KAPITEL 05

VERTRAGSGESTALTUNG

WICHTIGE VERTRAGSELEMENTE ZUR INFORMATIONSSICHERHEIT (1/2)

- Datenstandort
- Audit/Kontrollrechte
- Beizug Subunternehmen/Weiterreichung von Pflichten
- Informationspflichten (etwa über built-in accounts, Schlüssel für Systemzugriffe, Vulnerabilities, Incidents, Infosec-(Re)-Zertifizierungen)
- Sinnvoller Abnahmeprozess
- *Möglichst* keine/wenige Ausschlüsse zu: Haftung/Gewährleistung, evtl. auch bezüglich Drittprodukten
- Pflicht zum Abschluss einer Vermögens-Haftpflichtversicherung, die auch Schäden bei Verletzungen der Informationssicherheit abdecken

WICHTIGE VERTRAGSELEMENTE ZUR INFORMATIONSSICHERHEIT (2/2)

- Detaillierte Regelung technisch-organisatorischer Massnahmen (TOM)
- Wartungs-/Supportmodalitäten
- Evtl. Source Code Escrow
- Evtl. Recht zum Reverse-Engineering für eigenständige Sicherheitsüberprüfung
- Evtl. Recht zu Penetration Tests für eigenständige Sicherheitsüberprüfung
- Datenmigration (Rückgabemodalitäten)

NEUE BUSSENBESTIMMUNG E-DSG (1/2)

Art. 8 Bearbeitung durch Auftragsbearbeiter

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

[2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

[3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

[4] …

NEUE BUSSENBESTIMMUNG FÜRS DSG (2/2)

Art. 55 Verletzung von Sorgfaltspflichten

Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich:

b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 8 Absätze 1 und 2 erfüllt sind;

AUDIT/KONTROLLRECHTE

EU-DSGVO verlangt für den Vertrag, dass «dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt“

DSG sagt, dass sich „der Auftraggeber sich insbesondere vergewissern muss, dass der Dritte die Datensicherheit gewährleistet“

AUDIT/KONTROLLRECHTE

- milde Varianten: Zusendung von regelmässig erstellten Security Berichten (Management Summary) oder reines Nachfragerecht
- Häufigkeit und Zeitpunkt
- Interne Kosten der Kontrollen berücksichtigen: Kunden auferlegen, mindestens wenn damit nicht wesentliche Mängel bemerkt wurden
- Vorbehalt Datenschutz Dritter

BEIZUG SUBUNTERNEHMER

- Starre Lösung: «Der Auftragsbearbeiter darf seine Verpflichtungen aus diesem Vertrag nicht ohne vorherige schriftliche Zustimmung des Verantwortlichen an einen Unterauftragsbearbeiter weitergeben.»

- Flexible Lösung: «Der Auftragsbearbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung (…), und der Verantwortliche hat das Recht, sich derartigen Änderungen aus wichtigem datenschutzrechtlichen Grund zu widersetzen, wozu er innert X Tagen schriftlich oder per E-Mail beim Auftragsbearbeiter Einspruch zu erheben hat (…).»

HAFTUNGSBEGRENZUNG

- Vorsicht vor Kleingedrucktem

- Haftungsausschlüsse sind möglich, aber nur innerhalb bestimmter Bandbreite:
  - ≠ Vorsätzliche/grob fahrlässig begangene Handlungen
  - ≠ Körperschäden

Häufige Formulierung,
um Ungültigkeit von Freizeichnungs-Klauseln zu vermeiden:
„soweit gesetzlich zulässig…“

HAFTUNGSBEGRENZUNG

- Ausschluss/Begrenzung der Haftung für Hilfspersonen aber auch für Vorsatz und Grobfahrlässigkeit oft möglich

- Handkehrum: «Unlauter handelt insbesondere, wer AGB verwendet, die (…) zum Nachteil der Konsumentinnen und Konsumenten ein erhebliches und ungerechtfertigtes Missverhältnis zwischen den vertraglichen Rechten und den vertraglichen Pflichten vorsehen.“ (Art. 8 UWG)

→ Standpunkt: Im B2C-Verhältnis Ausschluss der Hilfspersonenhaftung bei Vorsatz/Grobfahrlässigkeit unzulässig

LAST BUT NOT LEAST: KEIN TUNNELBLICK AUF INFORMATIONSSICHERHEIT

- Passt Kostenverteilung (auch implizite bzw. im Kleingedruckten platzierte) zu auferlegten Pflichten?
- Haftungsregelung: Vorsicht vor weitgehenden Gewährleistungs- und Haftungsausschlüssen, auch in Bezug auf Drittprodukte (dann mind. Rechteabtretung zusichern lassen)
- In jeden Vertrag mit internationaler Tragweite sollte das auf den Vertrag anwendbare Recht und die örtliche Zuständigkeit bei Streitigkeiten bestimmt werden

SWISS INFOSEC

reto.zbinden@infosec.ch | +41 79 446 83 00

MEET SWISS INFOSEC!
Sicherheit im Fokus

Zürich Flughafen
13 bis 17 Uhr, anschliessend Apéro
www.infosec.ch/msi

Haben Sie schon den kostenlosen Newsletter abonniert?
www.infosec.ch/news
infosec@infosec.ch

SWISS INFOSEC

ISSS BERNER TAGUNG
PORTRAIT

Reto C. Zbinden

RETO C. ZBINDEN
Rechtsanwalt, CEO
CISSP, CISM, CRISC, BSI-zertifizierter ISO 27001 Lead Auditor

Reto.Zbinden@infosec.ch
Mobile: +41 79 446 83 00

SPEZIALGEBIETE

- Datenschutz, Recht
- Informationssicherheit (ISMS)
- Zertifizierung nach ISO 27001
- Archivierung
- Cloud Security
- Krisenmanagement
- Business Continuity Management
- Risikomanagement