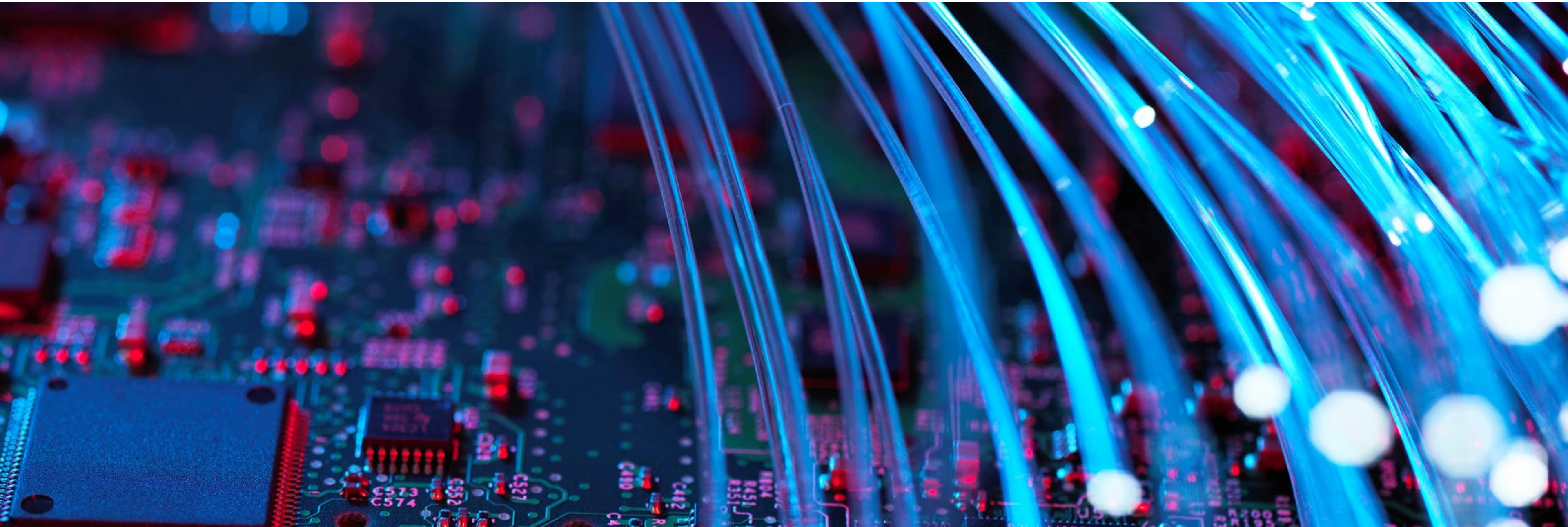
Baker McKenzie.

Legal liability for insecure software – "write once, cause damage anywhere"

27 February 2020

Dr. Lukas Feiler, SSCP, CIPP/E



Overview

1 Are there acceptable vulnerabilities?

2 Liability for off-the-shelf vs. custom software

3 Liability in the SaaS context

4 Software litigation in pratice

1 Are there acceptable vulnerabilities?

Is it OK to produce code with vulnerabilities?

B2C

(EU Digital Content Directive)

- Liability for
  - agreed/usual quality
  - fitness for communicated/usual purpose
- No liability for free OSS

B2B

- Liability for
  - agreed quality

Average/usual quality:

- countless vulnerabilities
- backdoors?
- very severe vulnerabilities? (how severe?)

Practice approach: Defining unacceptable vulnerabilities

Which vulnerabilities are not acceptable? E.g.

- OWASP Top 10 Critical Web App. Security Risks
- 2019 CWE Top 25 Most Dangerous Software Errors
- Vulnerabilities with a Common Vulnerability Scoring System (CVSS) Base Score >= 8
- Use of third-party software with known vulnerabilities (e.g., “vulnerabilities for which a CVE no. was assigned”)

or

- “… disclaims any and all warranties, fitness for any purpose …”

2 Liability for off-the-shelf vs. custom software

Liability for off-the-shelf software

Limitation of liability in practice

- Disclaiming any and all liability
- Not valid under contract law of EU Member States in continental Europe
- B2C
  - Liability cannot be disclaimed
  - What damages?
- B2B: Where software vendor is not established in same country as customer
  - License terms provide choice of foreign law and foreign jurisdiction ;-)

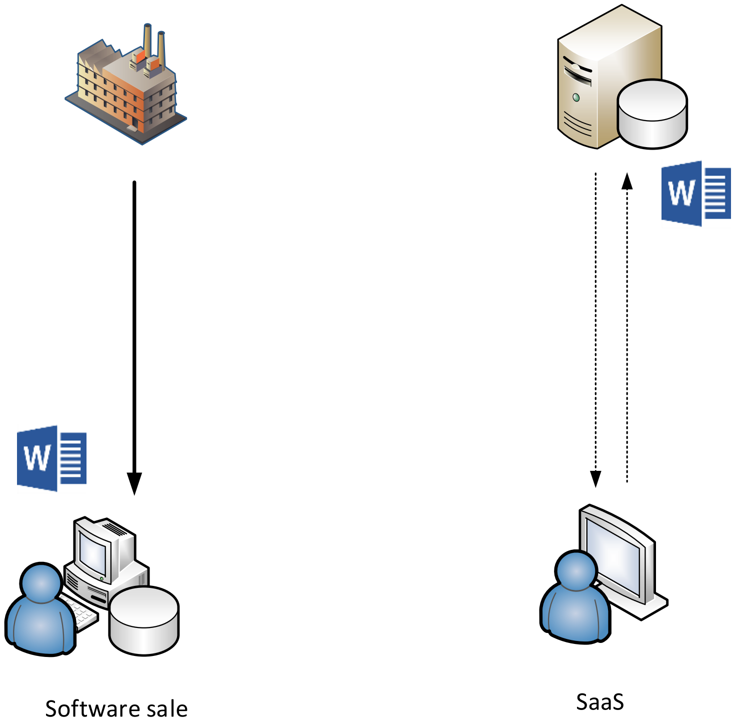
Liability for custom software

Limitation of liability in practice

- Full disclaimer often not possible – less negotiation power for software vendor
- Who is responsible for vulnerability?
  - e.g., customer instructs developer to implement weak encryption
- Use of notoriously unsecure OSS? Obligation to review security of OSS?

3 Liability in the SaaS context

Software sale vs. SaaS



SaaS

- Data remains with vendor → GDPR liability

  possible to limit in contract? (Art. 82(5) GDPR)
- Contractual liability for
  - B2C:
    - agreed/usual quality
    - fitness for communicated/usual purpose
  - B2B
    - agreed quality

4 Software Litigation

Challenges of litigating software security issues

- Time: How valuable is a final judgment in 6-9 years?

- Knowing you are right vs. proving it: Software development projects are often poorly documented

- Complexity: How to make the judge / expert witness understand the technical issues?

Baker McKenzie.

Lukas Feiler
Nikolaus Forgó

EU-DSGVO
EU-Datenschutz-Grundverordnung

VERLAG
ÖSTERREICH

Lukas Feiler
Bernhard Horn

Umsetzung der
DSGVO in der Praxis

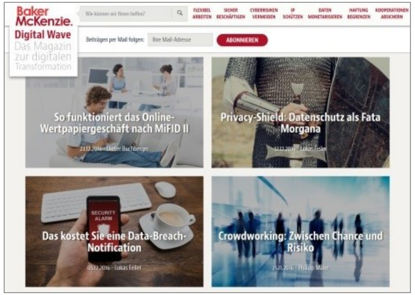
Fragen, Antworten, Muster

VERLAG
ÖSTERREICH

The EU General
Data Protection
Regulation (GDPR):
A Commentary

Lukas Feiler
Nikolaus Forgó
Michaela Weigl

GLP
German Law Publishers



Digital Wave
Das Magazin zur digitalen Transformation

Beiträgen per Mail folgen: Ihre Mail-Adresse

So funktioniert das Online-Wertpapiergeschäft nach MiFID II
23.12.2016 - Dieter Buchberger

Privacy-Shield: Datenschutz als Fata Morgana
12.12.2016 - Lukas Feiler

Das kostet Sie eine Data-Breach-Notification
05.12.2016 - Lukas Feiler

Crowdworking: Zwischen Chance und Risiko
25.11.2016 - Philipp Maier

Lukas Feiler is co-autor of the first Austrian commentary on the GDPR and of the first Austrian book on the practical implementation of the GDPR. He also advises companies on the digital transformation under www.digitalwave.at.

Dr. Lukas Feiler, SSCP CIPP/E
Partner
Head of IP/IT in Vienna

Schottenring 25
1010 Vienna

T: +43 1 24 250
lukas.feiler@bakermckenzie.com

www.bakermckenzie.com

Diwok Hermann Petsche Rechtsanwälte LLP & Co KG ist ein Mitglied von Baker & McKenzie International, einem Verein nach dem Recht der Schweiz mit weltweiten Baker & McKenzie-Anwaltsgesellschaften und kooperiert mit Baker & McKenzie Rechtsanwaltsgesellschaft mbH, Düsseldorf. Der allgemeinen Übung von Beratungsunternehmen folgend, bezeichnen wir als "Partner" einen Freiberufler, der als Gesellschafter oder in vergleichbarer Funktion für ein Mitglied von Baker & McKenzie International tätig ist. Als "Büros" bezeichnen wir die Kanzleistandorte der Mitglieder von Baker & McKenzie International.