

TeleTrust "IT-Sicherheitsrechtstag 2020"

Berlin, 24.09.2020

Umsetzung des IT-Sicherheitsgesetzes im Unternehmen

RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte, Vorstand TeleTrust, Leiter AG Recht

Karsten U. Bartels LL.M.*



- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Zert. Datenschutzbeauftragter (TÜV)
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit e. V. (TeleTrust)
- Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e.V.

*Rechtinformatik





- IT-Recht
- IP-Recht
- Arbeitsrecht

- Wirtschaftsberatung
- Berlin - bundesweit
- www.hk2.eu

„HK2 wurde zu den besten
Wirtschaftskanzleien 2020
gewählt“

brand eins/ thema, Heft 16/ 2020



„Bewegungsziele“

- Gesetzliche Compliance
KRITIS/ Non-KRITIS/ Hersteller
- Vertragliche Umsetzung mit
Unterauftragnehmern und
Kooperationspartnern (KRITIS/ Non-
KRITIS)
- Verhältnis zur Umsetzung der
DSGVO
- Verhältnis zur Umsetzung des
GeschGehG

1 2 3 4 5 6 7 8

Ich bewege heute:

- Gesetzliche Compliance
KRITIS/ Non-KRITIS/ Hersteller
- Vertragliche Umsetzung mit
Unterauftragnehmern und
Kooperationspartnern (KRITIS/ Non-
KRITIS)
- Verhältnis zur Umsetzung der
DSGVO
- Verhältnis zur Umsetzung des
GeschGehG

1 2 3 4 5 6 7 8

Prüffrage

Was wäre, wenn wir IT-Sicherheit nicht *state of the art* vertraglich regeln würden?

Es gilt das Gesetz, wenn der Vertrag es nicht richtet.

- Ausfüllung von vertrags- und haftungsrechtlichen Generalklauseln
 - Mangelbegriff
 - deliktsrechtliche Verkehrssicherungspflichten
 - vertraglichen Rücksichtnahmepflichten
 - die „im Verkehr erforderlichen Sorgfalt“ i. R. d. Fahrlässigkeitsbegriffs
- Sicherheitserwartungen des Verkehrs
- Wirkung setzt eine andere Rechtsprechung voraus

Entwicklung der Rechtsprechung zur IT-Sicherheit

Dass die Gerichte sich nicht (nennenswert) mit IT-Sicherheitsfällen befassen, sagt nichts über die IT-Sicherheit in den Unternehmen aus.

KRITIS-Betreiber – Zulieferer Verträge enthalten

- IT-Sicherheitskonzept
- Datenschutzkonzept
- IT-Sicherheitsmaßnahmen
- Dokumentation
- Auditregelungen
- SLA
- ...

§ 8a BSIG

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 **angemessene organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen **maßgeblich** sind. Dabei **soll der Stand der Technik eingehalten werden**. Organisatorische und technische Vorkehrungen sind **angemessen**, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

§ xy Leistungsvertrag

(1) Der Auftragnehmer ist verpflichtet, **angemessene organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen **maßgeblich** sind. Dabei **soll er den Stand der Technik einhalten**.

Lösung

Ein eigener, agiler Vertrag zur konkreten, bilateralen Umsetzung der IT-Sicherheitsanforderungen, der zur Sicherstellung der eigenen Compliance justiziable Ansprüche schafft und gleichzeitig streitvermeidend wirkt.

Lösung

IT-Security Service and Management Agreement (ITSSMA)

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbefchränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
10. Benachrichtigungspflichten
11. Mitwirkungspflichten
12. Eskalationsregime
13. Beweislastregeln
14. Rechtsfolgenregime
15. Sonstiges
16. Anlagen
 - TOM Spezifikationen
 - Vorlagen Reporting, Benachrichtigungen
 - Konzepte des Anbieters (Datenschutz, IT-Sicherheit)

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
 - **Stand der Technik, Allgemein anerkannte Regeln der Technik**
 - **Klarstellung von Referenzen und externen Maßstäben**
 - ...

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
 - **Anforderungen nach IT-Sicherheitsgesetz**
 - **Anforderungen nach DSGVO**
 - **Technische und organisatorische Maßnahmen**
 - **Umgang mit 1. „harten“ und 2. „weichen“ Anforderungen (Bsp.: 1. Stand der Technik und 2. konkrete Einsatz)**
 - **Dokumentationstiefe**
 - **Nachweis**

Bsp.: Verpflichtungen zum Stand der Technik

- Konkrete Verpflichtung auf den Stand der Technik
- Festlegung der Schutzmaßnahmen
 - Maßnahmenbeschreibung
 - Verknüpfung mit IT-Sicherheitszielen
- Methode
 - Nachweis zur Praxiserprobung
 - Nachweis zum Grad der Fortschrittlichkeit
 - Ggf. Standards/ Normungen und Veröffentlichungen von Fachverbänden/ Experten als Maßstab
- Dokumentation
 - Detailtiefe
 - Struktur
- Prüfung und Überprüfung
- Rechtsfolgen
- *Beachte*
 - *Perspektive AG/ AN*
 - *Angemessenheitserwägungen, planmäßiges Unterschreiten des SdT*

ITSiG 2.0 RefENT

„(1a) Die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene

organisatorische und technische Vorkehrungen zur Vermeidung von Störungen nach Absatz 1 Satz 1 zu treffen, umfasst auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung **haben dem jeweiligen Stand der Technik zu entsprechen**. Die **Einhaltung des Standes der Technik wird vermutet**, wenn die Systeme der **Technischen Richtlinie [Bezeichnung] des Bundesamtes** in der jeweils geltenden Fassung **entsprechen**.

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
 - **Verfahren für einzufordernde Änderungen** (vgl. Change Request Management in IT-Verträgen)
 - Anforderungen, Angebot zu bekannten Konditionen, keine unbegründete Ablehnung
 - Fristen für das Verfahren
 - Fristen für Leistung
 - Verhandlung
 - **Zusagen zur Verfügbarkeit weiterer Leistungen des AN**
 - **Berücksichtigung Life Cycle des Produkts**
 - **Nachlaufende Update-Pflichten**

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. **Unterbeauftragungsbeschränkungen**
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
10. Benachrichtigungspflichten
11. Mitwirkungspflichten
12. Eskalationsregime
13. Beweislastregeln
14. Rechtsfolgenregime
15. Sonstiges
16. Anlagen
 - TOM Spezifikationen
 - Vorlagen Reporting, Benachrichtigungen
 - Konzepte des Anbieters (Datenschutz, IT-Sicherheit)

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbeschränkungen
7. **Umgang mit Audits, Testaten und Zertifikaten**

Bsp.: Audit-Klausel

- Internes oder externes Audit/ Anforderungen an den Prüfer
- Verdachtsabhängig oder -unabhängig
- Konkretisierung der Prüfungsinhalte
- Angemessene Ankündigungsfrist/ Terminierung
- Wahrung der Geheimhaltungsinteressen
- Wahrung der Vertraulichkeit und Datensicherheit
- Rechtsfolgen
- Geheimhaltung der Audit-Ergebnisse
- Übernahme der Kosten
- Haftung

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbefchränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. **Entscheider und Vertretungsregelungen**
9. Kommunikation
10. Benachrichtigungspflichten
11. Mitwirkungspflichten
12. Eskalationsregime
13. Beweislastregeln
14. Rechtsfolgenregime
15. Sonstiges
16. Anlagen
 - TOM Spezifikationen
 - Vorlagen Reporting, Benachrichtigungen
 - Konzepte des Anbieters (Datenschutz, IT-Sicherheit)

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbeschränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
 - **jour fixe**
 - **Teilnehmer**
 - **Protokoll inkl. Zuständigkeiten**
 - **Reporting**
 - **eingesetzte Tools**

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbeschränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
10. Benachrichtigungspflichten
 - als „Derivat“ der gesetzlichen Meldepflichten
 - zusätzliche Benachrichtigungspflichten
 - Benachrichtigungsverbote

§ 8b BSIG

(4) Betreiber Kritischer Infrastrukturen haben die **folgenden Störungen unverzüglich** über die Kontaktstelle an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem **Ausfall oder zu einer erheblichen Beeinträchtigung** der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen **geführt haben**,
2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem **Ausfall oder zu einer erheblichen Beeinträchtigung** der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen **führen können**.

Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der **vermuteten oder tatsächlichen Ursache**, der **betroffenen Informationstechnik**, der **Art der betroffenen Einrichtung** oder **Anlage** sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung enthalten.

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbeschränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
10. Benachrichtigungspflichten
11. Mitwirkungspflichten
 - **Garantieerklärung (§ 9b Abs. 2 ITSiG Ref.ENT)**
 - **überschießende Inhalte ggü. Mindestanforderungen nach Allgemeinverfügung des BMI**

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbefchränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
10. Benachrichtigungspflichten
11. Mitwirkungspflichten
- 12. Eskalationsregime**
- 13. Beweislastregeln**
14. Rechtsfolgenregime
15. Sonstiges
16. Anlagen
 - TOM Spezifikationen
 - Vorlagen Reporting, Benachrichtigungen
 - Konzepte des Anbieters (Datenschutz, IT-Sicherheit)

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbeschränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
10. Benachrichtigungspflichten
11. Mitwirkungspflichten
12. Eskalationsregime
13. Beweislastregeln
14. Rechtsfolgenregime
 - **Schadenersatz**
 - **Vertragsstrafen (auch No-Spy-Klausel)**
 - **Kündigung**
 - **Folgen der Kündigung**

IT-Security Service and Management Agreement (ITSSMA)

1. Ziel, Anwendbarkeit, Verknüpfung mit weiten Verträgen, Rangfolge der Regelungen
2. Definitionen
3. Technische und Organisatorische IT-Sicherheitsmaßnahmen
4. IT-Security Change Management
5. Vergütung
6. Unterbeauftragungsbefchränkungen
7. Umgang mit Audits, Testaten und Zertifikaten
8. Entscheider und Vertretungsregelungen
9. Kommunikation
10. Benachrichtigungspflichten
11. Mitwirkungspflichten
12. Eskalationsregime
13. Beweislastregeln
14. Rechtsfolgenregime
15. **Sonstiges**
16. **Anlagen**
 - **TOM Spezifikationen**
 - **Vorlagen Reporting, Benachrichtigungen**
 - **Konzepte des Anbieters (Datenschutz, IT-Sicherheit)**

Umsetzung des IT-Sicherheitsgesetzes mit Leistungen von USA-ansässigen Anbietern



EU-U.S. Privacy Shield

Angemessenheitsbeschluss der Kommission, Art. 45 DSGVO



EuGH, Urteil vom 16.07.2020, Az. C-311/18 Privacy Shield ist ungültig

- Sachverhalt

Maximilian Schrems forderte die irische Datenschutzbehörde auf, Facebook Ireland die Übermittlung seiner personenbezogenen Daten an die Konzernmutter in die USA zu untersagen.

- Entscheidung

Der EUGH erklärt das **Privacy Shield** (Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO) aus 2016 für ungültig. Die Befugnisse der US-Geheimdienste und die Rechtslage in den USA können kein angemessenes gleichwertiges Datenschutz-Niveau im Vergleich zum EU-Recht sicherstellen.

Die von der Kommission im Jahr 2010 beschlossenen **Standardvertragsklauseln (Standard Contractual Clauses (SCC))**, 2010/87/EU vom 05.02.2010, sind weiterhin gültig.

EU-Standardvertragsklauseln Art. 46 Abs. 2 c DSGVO



Checkliste

Datentransfer an Unternehmen mit Sitz USA

Anwendung/ Tool Vertragspartner	[...] [..., USA]
Vorfrage: Bedeutung der Anwendung im eigenen Unternehmen	<ul style="list-style-type: none"> ▪ [Kurzbeschreibung]
Zumutbarkeit alternativer Dienste mit Sitz des Vertragspartners in EU /EWR	<ul style="list-style-type: none"> ▪ [Ergebnis eines Marktüberblicks] ▪ [Schlussfolgerung und Begründung]
Verlagerung der Datenverarbeitung in die EU/ EWR oder ein Land mit Angemessenheitsbeschluss	<ul style="list-style-type: none"> ▪ [ja/ nein] ▪ [Land/ Region] ▪ [Kurzbeschreibung (z. B. Anpassung der Hosting-Konfiguration)]
Zusätzliche Maßnahmen und Garantien	<ul style="list-style-type: none"> ▪ [Verschlüsselung, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann] ▪ [Anonymisierung oder Pseudonymisierung, bei der nur der Datenexporteur die Zuordnung vornehmen kann] ▪ [Entzug der Zugriffsberechtigung über der Berechtigungsmanagement („Kill switch“ für Konzerntöchter)] ▪ [...]
Abschluss der Standardvertragsklauseln nach Orientierungshilfe des LfDI Baden-Württemberg	<ul style="list-style-type: none"> ▪ [ja/ nein. Ggf. Verwendung des Musters]
Ausnahme gem. Art. 49 DSGVO (wenn weder Angemessenheitsbeschluss, noch Garantien bestehen)	<ul style="list-style-type: none"> ▪ ausdrückliche Einwilligung, Art. 49 Abs. 1 lit. a DSGVO ▪ Vertragserfüllung, vorvertragliche Maßnahmen, Art. 49 Abs. 1 lit. b DSGVO ▪ Abschluss oder Erfüllung eines Vertrags mit anderer Person im Interesse des Betroffenen, Art. 49 Abs. 1 lit. c DSGVO ▪ wichtige Gründe des öffentlichen Interesses, , Art. 49 Abs. 1 lit. d DSGVO ▪ Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, , Art. 49 Abs. 1 lit. e DSGVO ▪ Schutz lebenswichtiger Interessen, wenn Einwilligung nicht möglich, Art. 49 Abs. 1 lit. f DSGVO ▪ Übermittlung aus Register nach Anforderungen des Art. 49 Abs. 1 lit. g DSGVO

Zum Nachlesen

- Urteil des EuGH vom 16.07.2020 (C-311/18)
- <https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfe-des-Ifdi-bw-was-jetzt-in-sachen-internationaler-datentransfer/> (2. Auflage)
- Handlungsempfehlung HK2 Rechtsanwälte
- Aktuelle Sachstands-Information „Datentransfer ohne Privacy Shield - Sofortmaßnahmen auf Sichtweite“ und Checkliste „Transferproblematik“

HK2 – Der Rote Faden

Sehr geehrter Herr Bartels,

meine Lieblings-Sentenz von Julian Nida-Rümelin ist: „Ich bin affizierbar durch Gründe.“ Gedankenpause: Wunderbar. Ich auch. Gründe muss man manchmal auch suchen. Das dachte sich wohl auch die Post, die jetzt tatsächlich eine „Briefankündigung im E-Mail Postfach“ als neuen Service anbietet. Mir werden hier Scans der Umschläge der Briefe, die ich postalisch erhalte, vorab gemalt. Nur die Umschläge. Begründung: „Immer und überall informiert“ zu sein. Andere digitalisieren die Welt, wir scannen Briefumschläge. Was für ein possierlicher Unfug.

Die Verlinkung zum Dienst habe ich nicht vergessen, aber ich kann Euch/ Ihnen auf Wunsch gern den Roten Faden ausgedruckt im Kuvert schicken und vorab das Bild vom Umschlag malen. Vielleicht gibt's ja doch Gründe ...

Nun denn – den Roten Faden spinnen wir in dieser Ausgabe unter anderem um die Fragen, wann eine rechtliche Information – zum Beispiel im Zusammenhang mit der Corona-Pandemie – unzulässig sein kann, wie unterschiedlich Gerichte Influencer-Marketing beurteilen und warum fehlende Querverweise in AGB womöglich taktisch gar nicht so hilfreich sind wie gedacht.

Viel Spaß bei der Lektüre

wünscht Euch/ Ihnen

Karsten U. Bartels

P.S.: meine besten Glückwünsche an Matthias und die weiteren HK2-AutorInnen zur Buchveröffentlichung, siehe unten!

Red Flags

Wiederverkauf nach Änderung der Firmware verboten

Wer etwa ein Auto kauft, darf es wieder verkaufen, auch wenn darauf die Marke des Herstellers angebracht ist. Dieses Verständnis dürfte den meisten so trivial erscheinen, dass sie darüber kaum je nachdenken. Bei Privatverkäufen ist das auch unproblematisch, weil das Markenrecht auf diese keine Anwendung findet. Im geschäftlichen Verkehr dagegen unterliegt dieser „Erschöpfung“ genannte Grundsatz als Ausnahme vom Markenschutz Grenzen. Er gilt ggf. nicht für Importwaren aus Staaten außerhalb des EWR oder für **veränderte Produkte**. Und eine solche Veränderung liegt – so das LG München I (17 HK O 1703/20) – auch vor, wenn ein Händler die **abgespeckte Firmware** gebrauchter Router einer Sonderedition gegen die aktuelle, **funktionsreichere Firmware** des Router-Herstellers für die Standard-Geräte gleichen Typs austauscht. Dass dies zu einer **Verbesserung** führt oder, dass es sich um die **Original-Firmware** des Herstellers für diesen Router-Typ handelt, spielt dabei keine Rolle.



Philip Koch

Irreführung durch Kundeninformationen

Ob Gutscheine statt Rückzahlung, abweichende Lieferbedingungen oder Informationen zur Umsatzsteuerenkung, **Unternehmen informieren ihre Kunden** über Corona bedingte Besonderheiten in der Vertragsbeziehung. Werden in Kundeninformationen **Rechtsansichten** geäußert, können sie **wettbewerbswidrig** sein. Unzulässig laut BGH (I ZR 85/19):

- Die Behauptung einer eindeutigen Rechtslage, die nicht besteht.
- Für den Kunden ist nicht erkennbar, dass es sich um eine Rechtsansicht handelt, sondern er versteht die Äußerung als Feststellung.
- Objektiv falsche Aussagen auf eine ausdrückliche Nachfrage des Kunden.

Rechtsansichten sind als Meinungsäußerungen zulässig, wenn der Kunde sie als solche erkennen kann. **Es kommt also auf die ganz konkrete Formulierung an.**

Die Kommunikation mit dem Kunden bedarf daher immer einer rechtlichen Prüfung. Selbst bei der Formulierung von **Zahlungsaufforderungen** oder **Kündigungsschreiben** besteht das Risiko, die vom BGH aufgezeigten Grenzen des Zulässigen zu überschreiten.



Nadja Marquard



BGH zur AGB-Auslegung beim Verwenden mehrerer Klauselwerke

Es gibt Anbieter, die AGB als verbundene, epische Patchworks verstehen. Das geht leider schief.

So hatte der BGH (VIII ZR 289/19) kürzlich über die Wirksamkeit einer in AGB enthaltenen Inkassokostenpauschale zu entscheiden. Dabei hat er sich auch zur Auslegung von AGB beim **Verwenden mehrerer Klauselwerke** geäußert und eine Einbeziehung von separaten Urkunden, auf die in der jeweiligen Klausel nicht gesondert hingewiesen worden war, verneint.

Zwar seien bei der Auslegung einer AGB-Klausel grundsätzlich auch inhaltlich verbundene Bestimmungen eines „Gesamtpaketwerks“ zu berücksichtigen. Dagegen seien aber Bestimmungen, die in **gesonderten Urkunden** niedergelegt sind und auf die die beanstandete Formalklausel nicht konkret Bezug nimmt, grundsätzlich nicht zur Auslegung dieser Klausel heranzuziehen. Dem Kunden kann insbesondere nicht **abverlangt** werden, **verschiedene Klauselwerke nach Anhaltspunkten zu durchforsten**, wie ein bestimmter Begriff noch weiter zu verstehen sein könnte.



Ronja Hecker



Influencer Chaos auch in den Berufungsinstanzen

Die Frage, ob ein Influencer auch **kommerzielle Posts ohne Gegenleistung** zu kennzeichnen hat, wird auch von den **Berufungsinstanzen unterschiedlich** gesehen.

Schon das LG München (4 HK O 14312/18) hatte entschieden, dass im Fall prominenter Personen mit hoher Followerzahl für den **Nutzer offensichtlich** ist, dass **kommerzielle Interessen** verfolgt werden und Beiträge mangels Irreführung nicht zu kennzeichnen sind. Dieser Ansicht ist nun das OLG Hamburg (15 U 142/19) gefolgt.

Das OLG München (29 U 2333/19) geht noch einen Schritt weiter: Unentgeltliche Posts seien schon **keine kommerzielle Handlung**. Das allgemeine Interesse, sich durch Publikationen für Werbeverträge interessanter zu machen, genügt nicht. Die **Absatzförderung der Produkte** sei nur ein **zufälliger Reflex** eines ansonsten redaktionellen Handelns.

Das OLG Braunschweig (2 U 78/19) und das OLG Frankfurt a. M. (6 W 68/19) haben das anders gesehen und gehen von einer **generellen Kennzeichnungspflicht** aus.

Wann und ob der **BGH die Gelegenheit** bekommt, diese Unstimmigkeit zu klären, ist noch ungewiss.



Sina Schmiedefeld



HK2 Insights

KI & Recht kompakt

Künstliche Intelligenz ist eine **Basistechnologie**, die in allen Bereichen des täglichen Lebens, in allen Produkten und in der Arbeitswelt, eine Rolle spielen wird.

Die Auswirkungen dieser technologischen Revolution sind noch gar nicht absehbar.

Schon jetzt wirft KI in vielen Rechtsbereichen aber ganz **praktische, juristische Fragen** auf. Wir freuen uns – und sind auch ein wenig stolz – gemeinsam mit **exzellenten Autoren**, die sich mit KI bereits länger intensiv auseinandersetzen, in dem soeben bei Springer Vieweg erschienenen Buch **KI & Recht** zur Diskussion der Implikationen von KI in der Rechtspraxis beizutragen.

Das Buch behandelt die technischen Grundlagen und die Auswirkungen im Zivil-, Urheber-, Datenschutz-, Straf- und Arbeitsrecht.

Matthias Hartmann,
Jörg Hennig,
Bernhard Kloos und Anika Nadler



KI & Recht kompakt

EBOOK INSIDE Springer Vieweg



dunkelrot

Schluss mit den Geheimprozessen?

Das **Bundesverfassungsgericht** meint es ermt mit fairem Verfahren, auch im **Wettbewerbsrecht**. Es hat nun bestätigt, dass die für das **einseitige Verfügensverfahren** aufgestellten **Grundsätze zur prozessualen Waffengleichheit** (wie zu erwarten) auch im **Wettbewerbsrecht** gelten (1 BvR 1379/20).

Elverfahren sind im gewerblichen Rechtsschutz und Außenrecht besonders beliebt, um Unterlassungsansprüche schnell und effektiv durchzusetzen. Der Gegner wird wegen der vermeintlichen **Dringlichkeit in der Praxis in aller Regel nicht angehört**, obwohl die Nachanhörung gesetzlich nur als Ausnahme festgelegt ist.

2018 **korrigierte** das Bundesverfassungsgericht die **praktische Umkehr des Regel- Ausnahmeverhältnis** in zwei Entscheidungen aus dem Presse- und Außenrecht (BVerfG, 1 BvR 1782/17, II.2.a und 1 BvR 1783/17, II.2.b).



Sina Schmiedefeld

Compliance & Data Protection

Die Kolumne der HK2 Connection GmbH



Auch für Kreative: EDSA-Leitlinie zur Einwilligung

Bereits im Mai hat der **Europäische Datenschutzausschuss (EDSA)** eine aktualisierte **Leitlinie zur DSGVO-konformen Einwilligung** veröffentlicht. Anlass für die Aktualisierung war u. a. das **Cookie-Urteil des EuGHs 2019** (wir berichteten). Dennoch nicht die EDSA, entgegen der vielerorts geweckten Erwartung, war nicht so ausführlich auf die **Cookie-Einwilligung ein**. Allein Beispiel 6a stellt klar, dass ein **Cookie-Banner**, das die **Linkliste** eine Webseite verdeckt und erst nach Einwilligung zugänglich macht, keine wirksame Einwilligung ermöglicht. Daneben enthält die Leitlinie zahlreiche weitere **Praxisbeispiele** für wirksame und unwirksame Einwilligungen inkl. einiger **kreativer Ansätze**, wie das Smartphone im Uhrzeigersinn zu drehen. Wer also mit **unkonventionellen Einwilligungstechniken** experimentieren will, dem sei diese EDSA-Leitlinie als Lektüre empfohlen.

Kein allgemeiner Anspruch auf Unterlassung

Bei mir um die Ecke **„schlechtes Abschneidegut“**, folgt man dem **Datenschutz in dies** Bezug auf die **Klage** Videoüberwachung e kürzlich, die **DSGVO er** **„Anspruch auf Unterlassung“** **„schlechter“** weil **rechtswidriger, Datenverarbeitung**. Die **DSGVO** **keine** eben nur **Rechte des Betroffenen** wie **Löschung** und **Berichtigung**. Diese **Kriterien** dann auch **ganzlich** geltend gemacht werden. Ansonsten bliebe nur die **Beschwerde** bei der **Aufsichtsbehörde**. Da die **DSGVO** die **Rechtsbezüge** **abschließend regelt**, sei die **allgemeine Leistungsklage** auf Grundlage eines **zivilrechtlichen Unterlassungsanspruchs nicht statthaft**.



Lukas Wagner LL.M.
Datenschutzbeauftragter der HK2 Connection GmbH



Michael Schramm LL.M. (Minnesota)
Datenschutzbeauftragter der HK2 Connection GmbH

hk2.eu/newsletter

Haben Sie Fragen?

HK2
Rechtsanwälte



HK2
Rechtsanwälte

Rechtsanwalt
Karsten U. Bartels LL.M.

Hausvogteiplatz 11 A
10117 Berlin

Telefon +49 (0)30 27 89 00 - 0
Telefax +49 (0)30 27 89 00 - 10
E-Mail bartels@hk2.eu
www.hk2.eu

www.hk2.eu

www.comtection.de