

TeleTrust-Konferenz 2019

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Berlin, 28.11.2019

IT-Sicherheit im Geschäftsgeheimnisschutzgesetz

RAin Dr. Johanna Schmidt-Bens LL.M.

HK2 Rechtsanwälte



- IT-Recht
 - IP-Recht
 - Arbeitsrecht
-
- gegründet 2002
 - Wirtschaftsberatung
 - Berlin - bundesweit
 - www.hk2.eu



Zum Einstieg ...

eine Bestandsaufnahme.

Wie setzen Unternehmen das
Geschäftsgeheimnisschutzgesetz
(GeschGehG) in DE um?

Überwiegend gar nicht.

Agenda

1. Das neue GeschGehG
2. Geschäftsgeheimnisse
3. Angemessene
Geheimhaltungsmaßnahmen
4. GeschGehG + DSGVO
5. Schutzkonzept
6. Checkliste



Geheimnisschutz nach dem GeschGehG

StGB

- ✓ §§ 201, 202 – Verletzung der Vertraulichkeit d. Wortes und d. Betriebsgeheimnisses
- ✓ § 202a – Ausspähen von Daten
- ✓ § 203 – Verletzung von Privatgeheimnissen
- ✓ § 204 – Verwertung fremder Geheimnisse
- ✓ § 206 – Verletzung Post- und Fernmeldegeheimnis

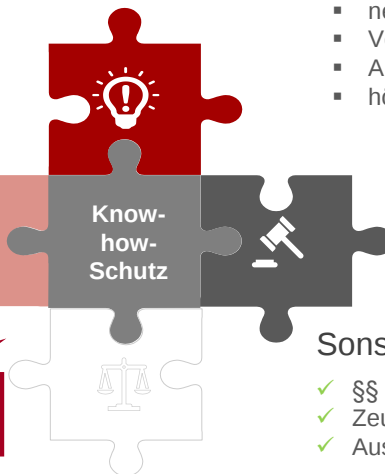
GeschGehG

- Legaldefinition des Geschäftsgeheimnisses
- neue Schutzvoraussetzungen
- Vergleichbarkeit mit Schutz von Immaterialgüterrechten
- Ansprüche des Geheimnisinhabers
- höhere Chancen der gerichtlichen Durchsetzbarkeit

UWG

- § 17 – Verrat von Geschäftsgeheimnissen
- § 18 – Verwertung von Geschäftsgeheimnissen
- § 19 – Verleiten und Erbiten

**§ 23 i.V.m. § 4
GeschGehG**



Sonstige

- ✓ §§ 333 HGB; 85 GmbHG; 395, 404 AktG
- ✓ Zeugnisverweigerungsrechte (§§ 383 I Nr. 6, 384 Nr. 3 ZPO)
- ✓ Ausschluss der Öffentlichkeit (§§ 172 Nr. 2, 173 II GVG)

Geschäftsgeheimnis nach § 2 Nr. 1 GeschGehG

Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb, rechtswidriger Nutzung
und rechtswidriger Offenlegung

Vorliegen eines
Geschäftsgeheimnisses

Information

geheim

wirtschaftlicher Wert aufgrund
der Geheimhaltung

angemessene
Geheimhaltungsmaßnahmen



Entwicklung

- ✓ Erfindungen
- ✓ Designs
- ✓ Konstruktionszeichnungen
- ✓ Zusammensetzungen
- ✓ Rezepturen
- ✓ Eigenschaften von Produkten und Komponenten



Verkauf + Marketing

- ✓ Kundendaten
- ✓ Preise
- ✓ Vertriebswege
- ✓ Distributoren
- ✓ Marktanalysen
- ✓ Verbraucherverhalten
- ✓ Kundenwünsche
- ✓ Logistikinformationen



Strategie, Transaktionen + Wachstum

- ✓ Geschäftsmodelle
- ✓ Personalien
- ✓ Innovationen
- ✓ Business-Pläne
- ✓ Investitionspläne
- ✓ Marketing-Preise
- ✓ Fusionspläne
- ✓ Verkaufs- und Kaufabsichten
- ✓ Expansionspläne
- ✓ Inhalt und Ablauf von M&A-Verhandlungen
- ✓ Marktentwicklung

HK2
Rechtsanwälte

-



Konkret

- was ist zu tun?

- ✓ Angemessene Geheimhaltungsmaßnahmen treffen
- ✓ Dokumentieren
- Schutzkonzept erstellen

Angemessene Geheimhaltungsmaßnahmen

- Objekt der Maßnahme (Informationen)
- Schutzbedarf
- Geheimhaltungsmaßnahmen
 - technisch
 - organisatorisch
 - rechtlich
- Angemessenheit
 - Einzelfall / individuell-konkrete Betrachtung
 - Maßstab / Technologie-Niveau

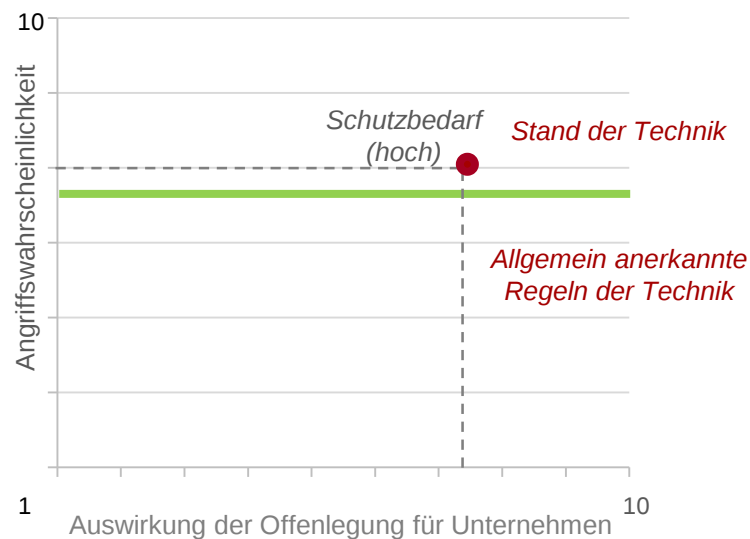
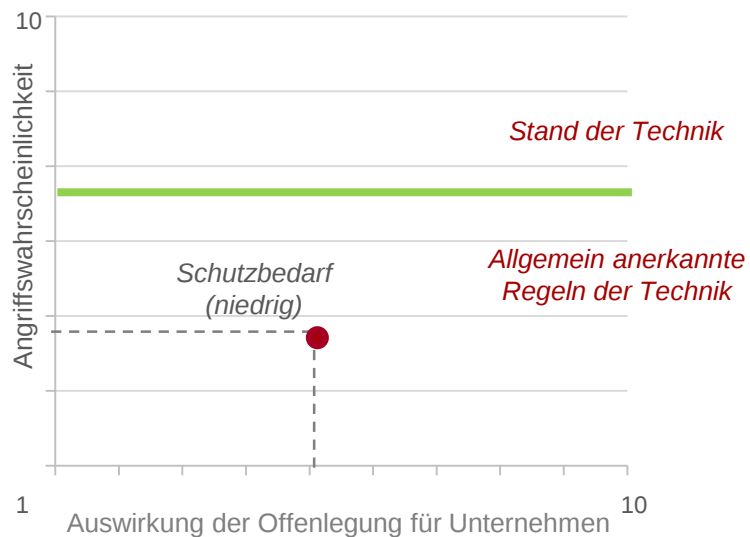
Angemessenheit der Geheimhaltungsmaßnahmen

- Faktoren (*Gesetzesbegründung*)
 - Wert des Geschäftsgeheimnisses
 - Entwicklungskosten
 - Natur der Information
 - Bedeutung für das Unternehmen
 - Größe des Unternehmens
 - Übliche Geheimhaltungsmaßnahmen des Unternehmens
 - Art der Kennzeichnung
 - Vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern
- Konkretisierung durch die Rechtsprechung beachten

Stand der Technik?



Schutzbedarfsanalyse



GeschGehG Schutzkonzept

Schützenswerte Geheimnisse	Schutzniveau der Geschäftsgeheimnisse	Geheimhaltungsmaßnahmen		Prozesse und Zuständigkeiten	...
		Maßnahme objektiv	Angemessenheit		

Exkurs

Dokumentation der „TOM“ nach Art. 32 DSGVO

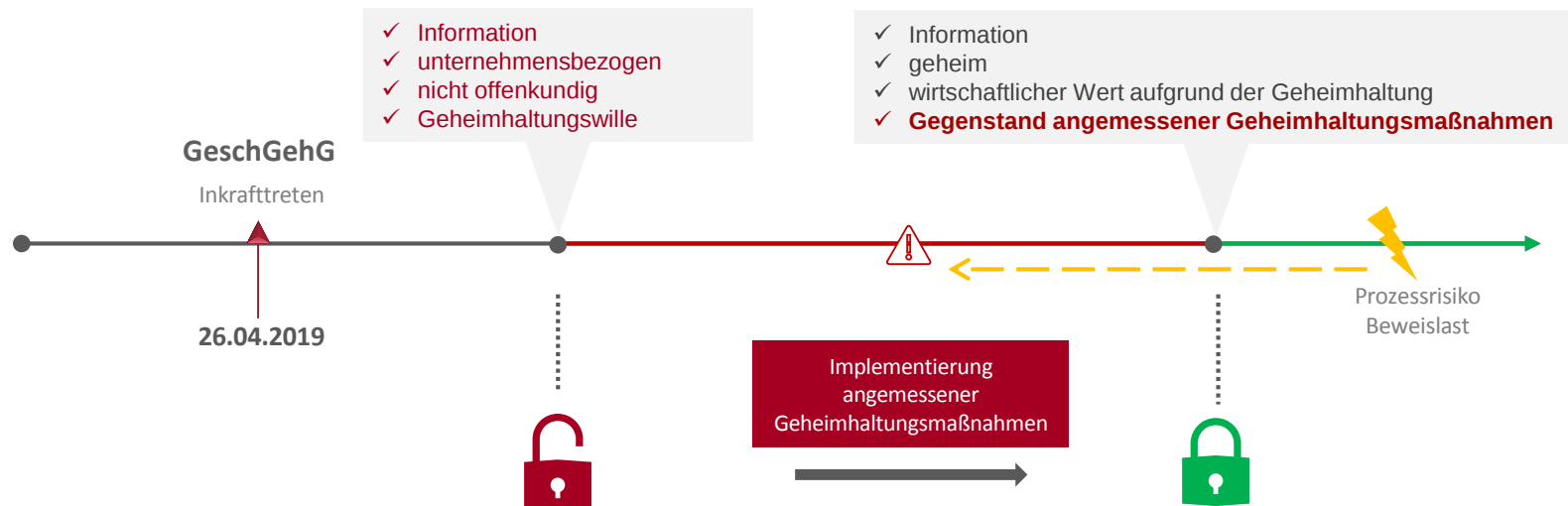
Maßnahmen	Beschreibung	Stand der Technik		Schutz- bedarf	Wirksam- keits- prüfung
		objektiv-technisch	subjektive Auswahl		

GeschGehG

Ansprüche bei Rechtsverletzungen

§ 6	Beseitigung und Unterlassung
§ 7	Vernichtung; Herausgabe; Rückruf; Entfernung und Rücknahme vom Markt
§ 8	Auskunft über rechtsverletzende Produkte; Schadensersatz bei Verletzung der Auskunftspflicht
§ 10	Haftung des Rechtsverletzers
§ 11	Abfindung in Geld
§ 12	Haftung des Inhabers eines Unternehmens
§ 13	Herausgabeanspruch nach Eintritt der Verjährung

Geschäftsgeheimnisse nachträglich geschützt



Checkliste GeschGehG

Aufgabe	Details	zuständig	erledigt
Geschäftsgeheimnisse identifizieren	Klassifizieren		
Schutzbedarfsanalyse	Risiken ermitteln		
Angemessene Geheimhaltungsmaßnahmen ermitteln	Technische, organisatorische und rechtliche Maßnahmen bestimmen anhand des Schutzbedarfs		
Dokumentation und Schutzkonzept	Umsetzung der Maßnahmen in der Unternehmenspraxis feststellen und planen		
Revision	Mindestens jährliche Überprüfung		
Organisation und Schulung im Unternehmen	Verfahren, Zuständigkeiten, Vorgaben, Ziele		
Monitoring Rechtsverletzungen	Wie wird beobachtet, dass Geheimnisse nicht unbefugt verwendet werden?		
Verträge schließen/ anpassen → <i>Checkliste Geheimhaltungsklauseln</i>	✓ Arbeitsverträge ✓ Verträge mit freien Mitarbeitern ✓ Subunternehmerverträge ✓ Kooperationsverträge ✓ Lizenzverträge ✓ Forschungs- und Entwicklungsverträge ✓ NDA		

7 Punkte zum GeschGehG

Alles oder nichts:
Keine angemessenen Geheimhaltungsmaßnahmen, keine Ansprüche.

Beweislast liegt beim Geheimnisinhaber.

Umsetzung im Team:

- IT
- IT-Sicherheit
- Fachabteilungen
- Recht
- (IT-)Compliance
- und ggf. DSB.

GeschGehG ist Geschäftsleitungsthema.

Konsolidierte Umsetzung und
Dokumentation: TOM und
Maßnahmen nach GeschGehG.

Verlust der Ansprüche nach GeschGehG bewerten. Probealarm!

Schutzkonzept erstellen und nachhalten!

ki-und-recht.de

it-sicherheit-und-recht.de

geheimnisschutz.eu

HK2 – Der Rote Faden

Sehr geehrter Herr Bartels,

besonders gern schreibe ich das Editorial, wenn wir neue Kolleginnen oder Kollegen bei uns begrüßen können. Heute darf ich das gleich zweifach: Johanna und Lukas - seid herzlich willkommen in der HK2-Familie! Wir freuen uns, Euch bei uns zu haben. Sie lernen die beiden noch kennen, nicht nur weiter unten im Text.

Wir berichten in dieser Ausgabe von Polizeidaten in der Amazon-Cloud und den Folgen, Mangelfolgeschäden mit Folgen und Sternchenhinweisen ohne (die gewünschten) Folgen. Zudem kündigt sich ein IT-Sicherheitsgesetz 2.0 und eine Klärung zur Klagebefugnis bei Datenschutzverstößen an.

Wenn Sie Matthias Hartmann und mich übrigens mal in Aktion sehen möchten, finden Sie hier den [Link zum Video](#) zum 6. Deutschen IT-Rechtstag.

Viel Spaß bei der Lektüre!

Ihr/ Euer
Karsten U. Bartels LL. M.



Red Flags

Ich war noch niemals in New York...

Für Ihre Daten dürften die meisten Deutschen wollen, dass das auch so bleibt. Die **Datenverarbeitung in den USA** wird oft kritisch gesehen. Um den besorgten Europäern ihre Dienste trotzdem schmackhaft zu machen, bieten viele US-Anbieter Serverstandorte in Europa an. Allerdings haben mit dem **CLOUD Act** aus dem letzten Jahr US-Straßverfolgungsbehörden auch Zugriff auf Daten auf **Servern außerhalb der USA**. Als nun herauskam, dass die **Aufnahmen der Bundespolizei-Bodycams** in der **Amazon Cloud** gespeichert werden, war die Kritik groß. Sensible Daten würden dem Zugriff der USA ausgesetzt. Der Bundesdatenschutzbeauftragte Kelber forderte eine **Speicherung bei einem deutschen**

Das könnte auch für Privatunternehmen das sensible Daten nicht mehr bei US- gespeichert werden dürfen. „Richtig frei“ sind Daten eher jenseits des Atlantik.

hk2.eu/newsletter



www.geheimnisschutz.eu

www.hk2.eu

www.comtection.de

HK2
Rechtsanwälte

Kontakt

Dr. Johanna Schmidt-Bens LL.M.

Rechtsanwältin

schmidt-bens@hk2.eu

HK2 Rechtsanwälte

Hausvogteiplatz 11 A

10117 Berlin

Telefon: +49 30 2789000

Telefax: +49 30 27890010