

IT-Sicherheitsrechtstag 2019

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Berlin, 14.11.2019

Umsetzung des Geschäftsgeheimnisschutzgesetzes im Unternehmen

RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte, Vorstand TeleTrust, Leiter AG Recht

Karsten U. Bartels LL.M.*



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

*Rechtsinformatik



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



Zum Einstieg ...

eine Bestandsaufnahme.

Wie setzen Unternehmen das
Geschäftsgeheimnisschutzgesetz
in DE um?

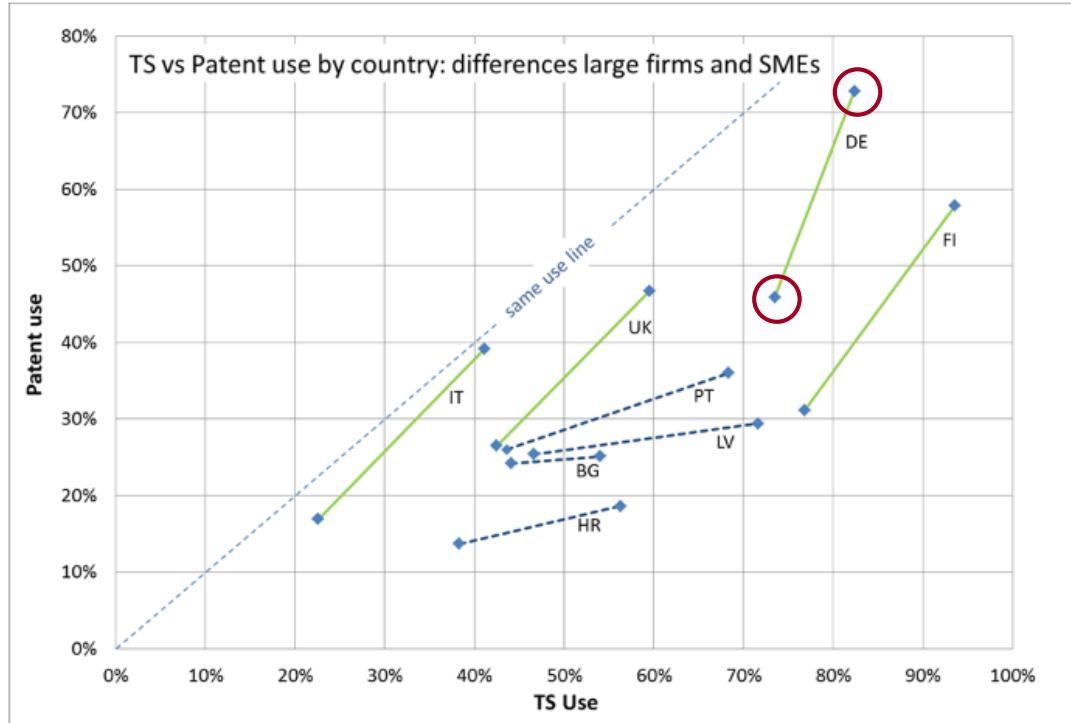
Überwiegend gar nicht.

Agenda

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



Figure 3: Trade secret vs patents use in selected Member States: differences between large firms and SMEs, 2010-2012

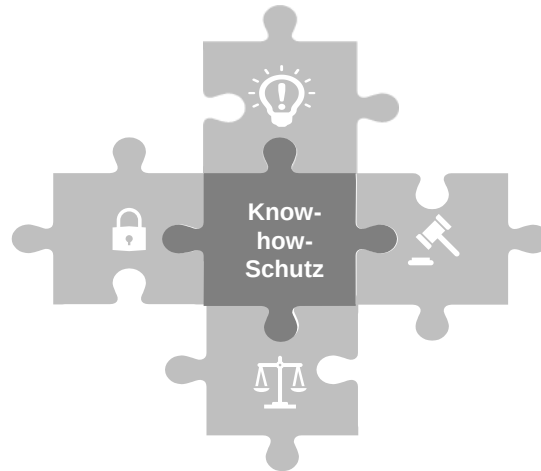


Source: Community Innovation Survey (CIS 2012) weighted totals (unweighted for IE).

„Protecting innovation through trade secrets and patents: Determinations for European Union firms“ 2017, *EUIPO*

(Großunternehmen und KMU)

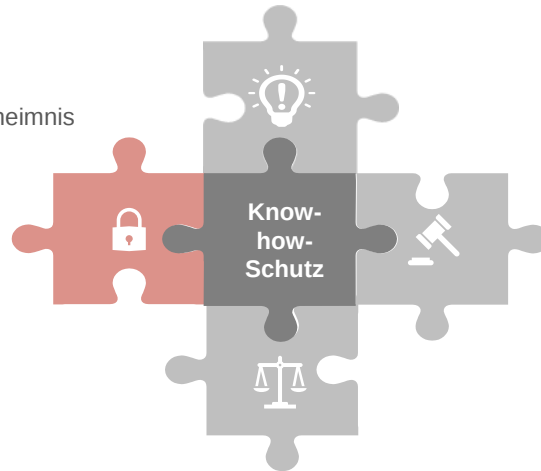
Geheimnisschutz vor dem GeschGehG



Geheimnisschutz vor 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



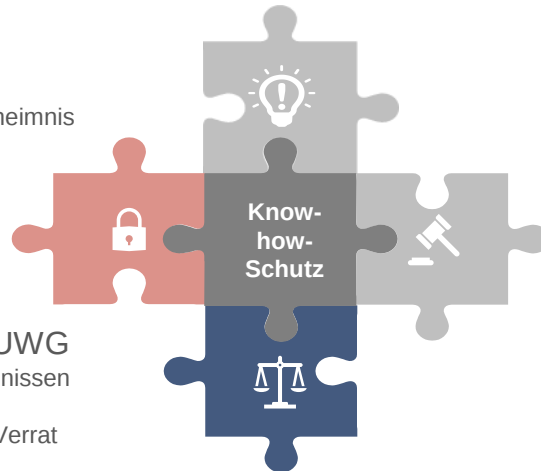
Geheimnisschutz vor dem GeschGehG

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

UWG

- § 17 – Verrat von Geschäftsgeheimnissen
- § 18 – Verwertung von Vorlagen
- § 19 – Verleiten und Erbieten zum Verrat



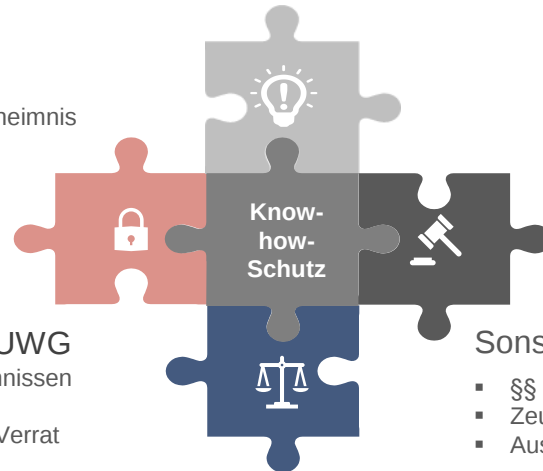
Geheimnisschutz vor dem GeschGehG

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

UWG

- § 17 – Verrat von Geschäftsgeheimnissen
- § 18 – Verwertung von Vorlagen
- § 19 – Verleiten und Erbieten zum Verrat



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)

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

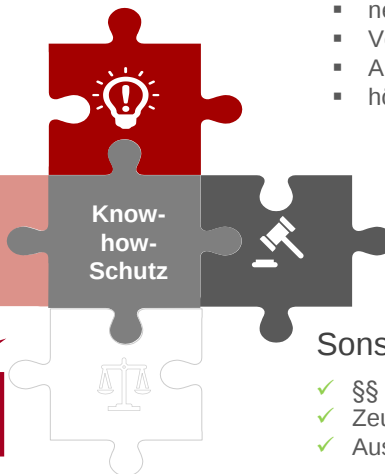
GeschGehG

- 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)

GeschGehG

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

GeschGehG

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

GeschGehG

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

GeschGehG

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

GeschGehG

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

↓
Vorliegen eines
Geschäftsgeheimnisses

↓
Information

↓
geheim

Entwicklung

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



Herstellung + Leistungserbringung

- ✓ Spezifikationen
- ✓ Anforderungen
- ✓ Fertigungsverfahren
- ✓ Testverfahren
- ✓ Vorgehensmodelle
- ✓ Kapazitäten
- ✓ Einzelkosten
- ✓ Kostenstrukturen
- ✓ Löhne, Gehälter

Einkauf

- ✓ Bezugsquellen
- ✓ Lieferanten
- ✓ Preise
- ✓ Konditionen
- ✓ Kalkulationsgrundlagen



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

- ✓ Systemarchitektur
- ✓ Eigenentwicklungen
- ✓ Sourcecode
- ✓ Algorithmen
- ✓ Inhaltsdaten
- ✓ Metadaten
- ✓ Big-Data-Analysen

GeschGehG

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

Vorliegen eines
Geschäftsgeheimnisses

Information

geheim

wirtschaftlicher Wert aufgrund
der Geheimhaltung

angemessene
Geheimhaltungsmaßnahmen



Angemessene Geheimhaltungsmaßnahmen

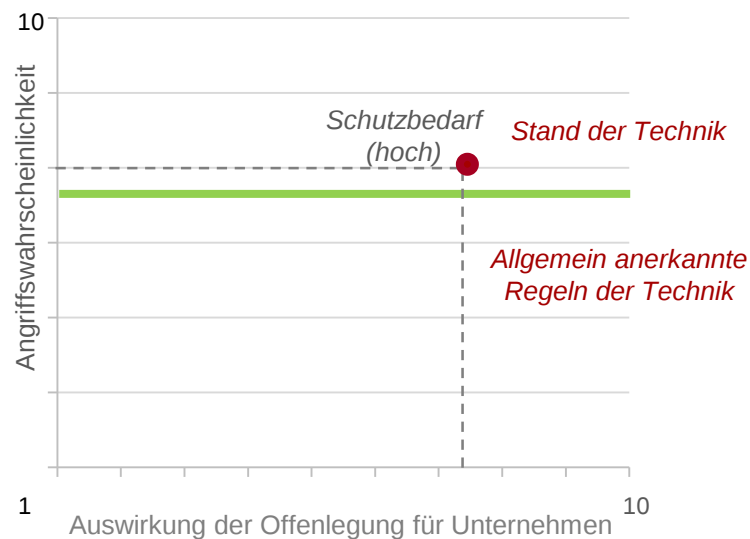
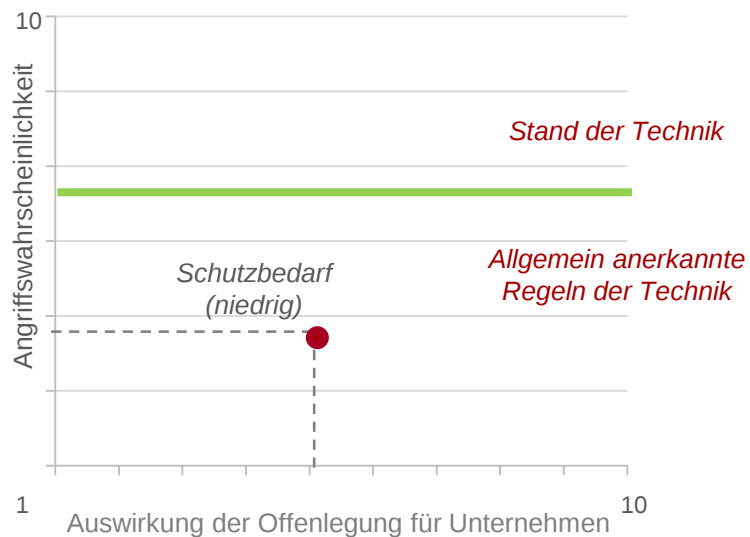
- Objekt der Maßnahme (Informationen)
- Schutzbedarf/ -niveau
- Geheimhaltungsmaßnahmen
 - technisch
 - organisatorisch
 - rechtlich
- Angemessenheit
 - Einzelfall/ individuell-konkrete Betrachtung
 - Maßstab/ Technologie-Niveau

→ erforderlich: Entwicklung eines Schutzkonzeptes

Stand der Technik?



Schutzbedarfsanalyse



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
- Orientierung an bestehende Regelungen (*Bsp.: Art. 32 DSGVO*)
- Konkretisierung durch die Rechtsprechung beachten

GeschGehG Schutzkonzept

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

Geheimnisschutz und Datenschutz

Exkurs

Dokumentation der „TOM“ nach Art. 32 DSGVO

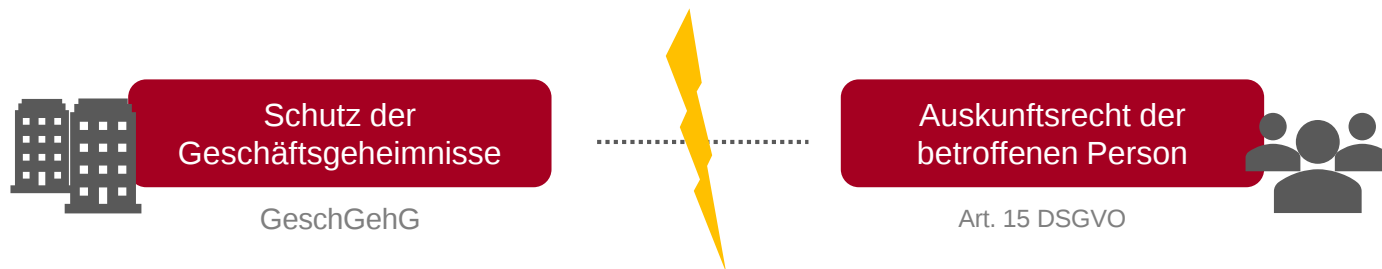
Maßnahmen	Beschreibung	Stand der Technik		Schutz- bedarf	Wirksam- keits- prüfung
		objektiv-technisch	subjektive Auswahl		

Exkurs

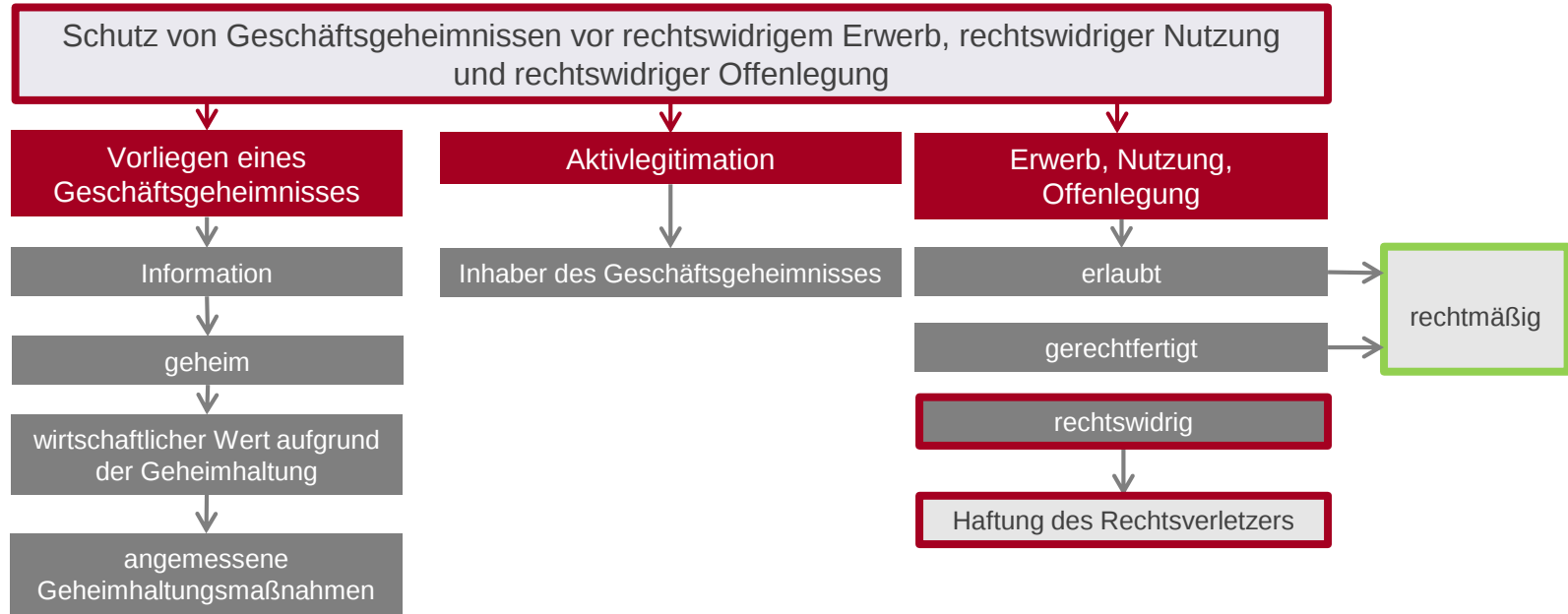
Dokumentation der „TOM“ nach Art. 32 DSGVO

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

Geheimnisschutz und Datenschutz



GeschGehG



GeschGehG

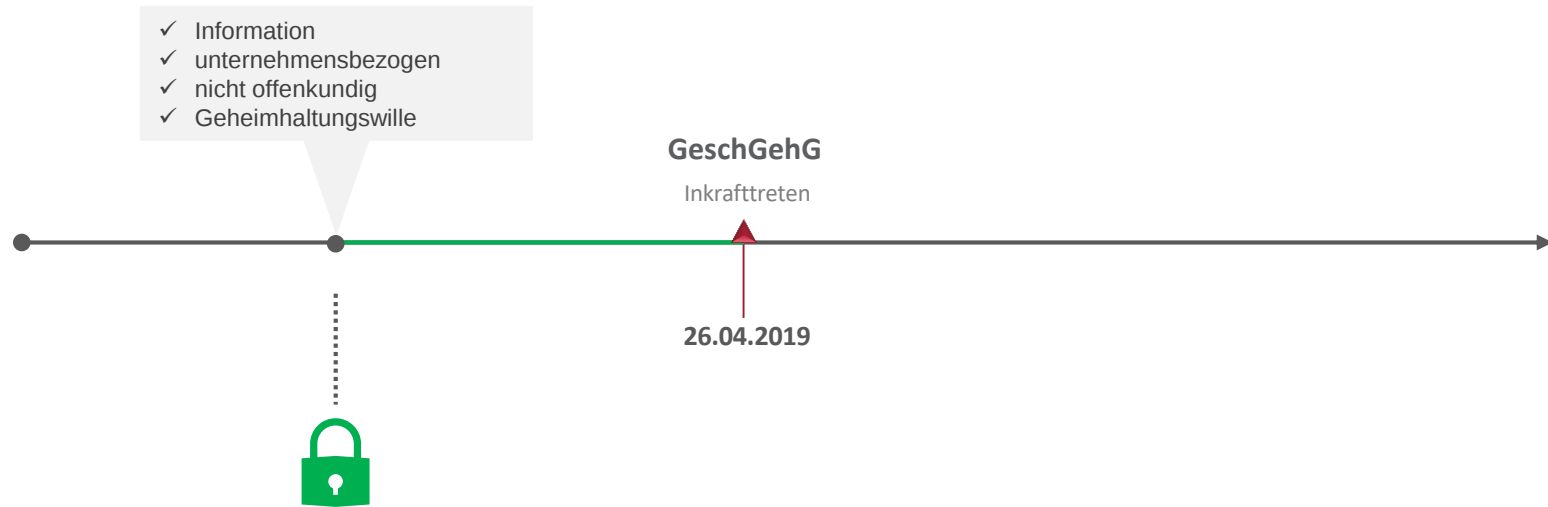
Ansprüche bei Rechtsverletzungen

§ 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

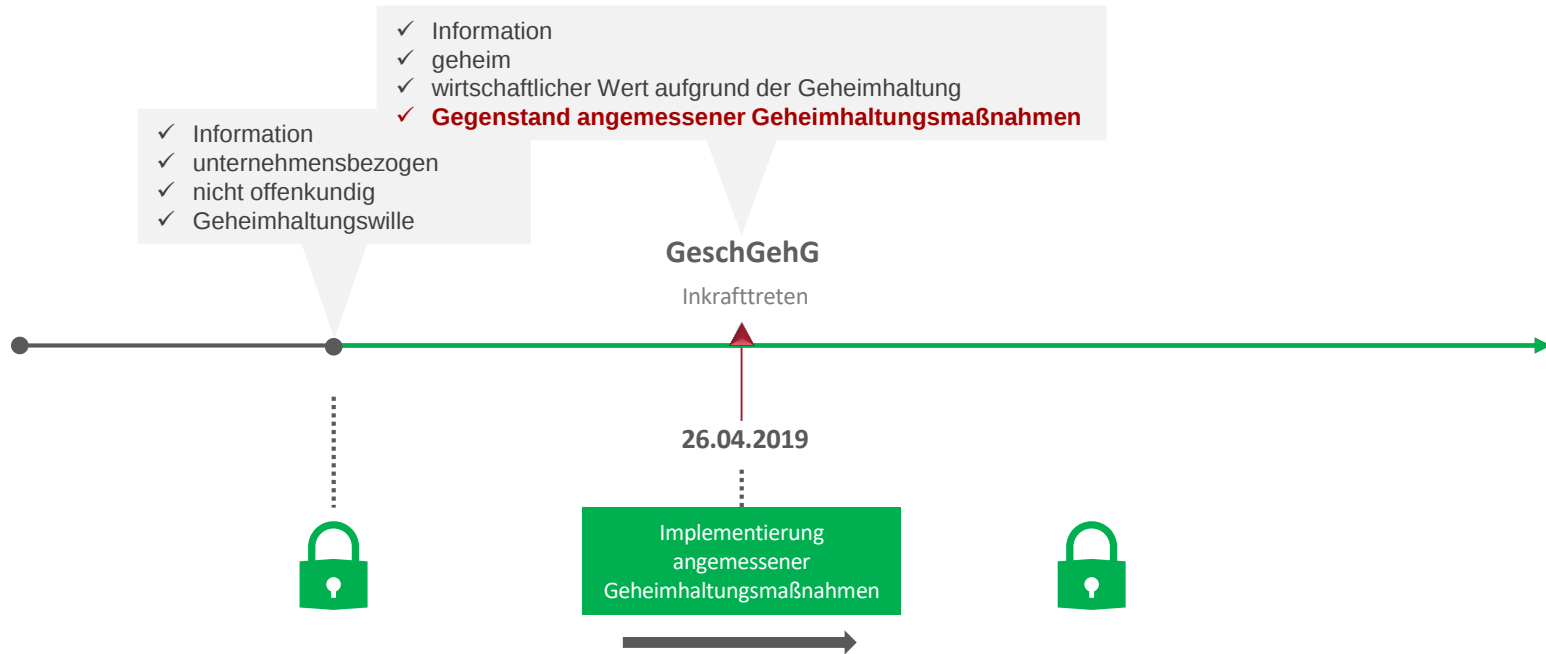
(Risiko)Management



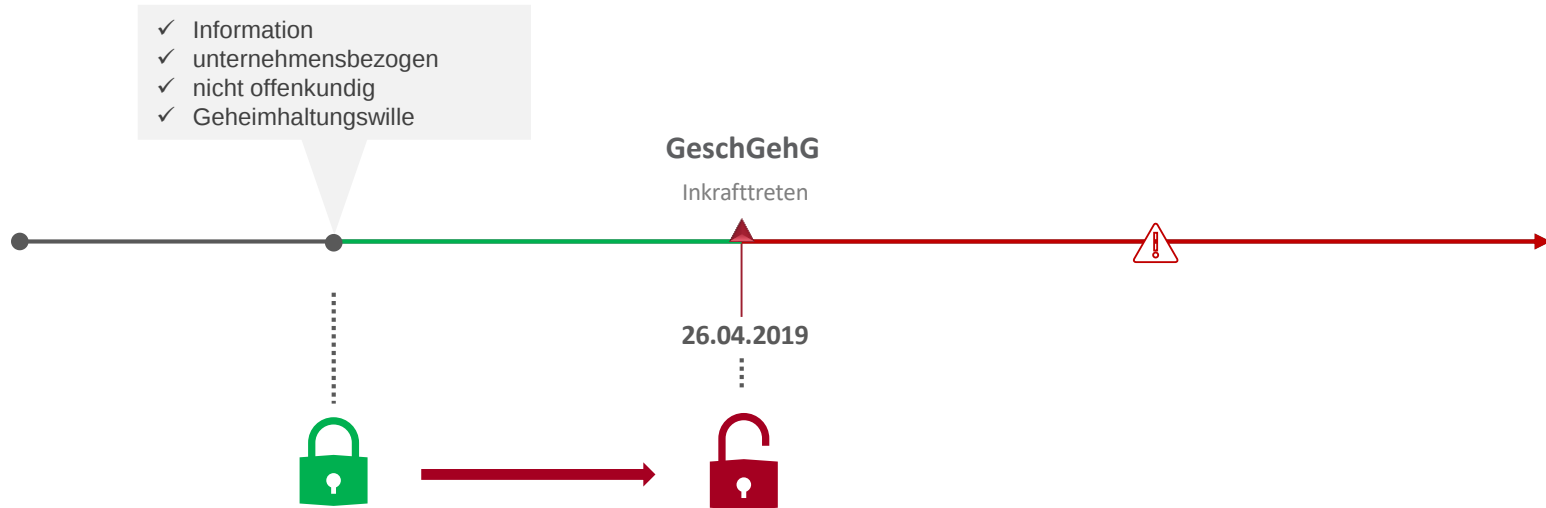
Bestehende Geschäftsgeheimnisse



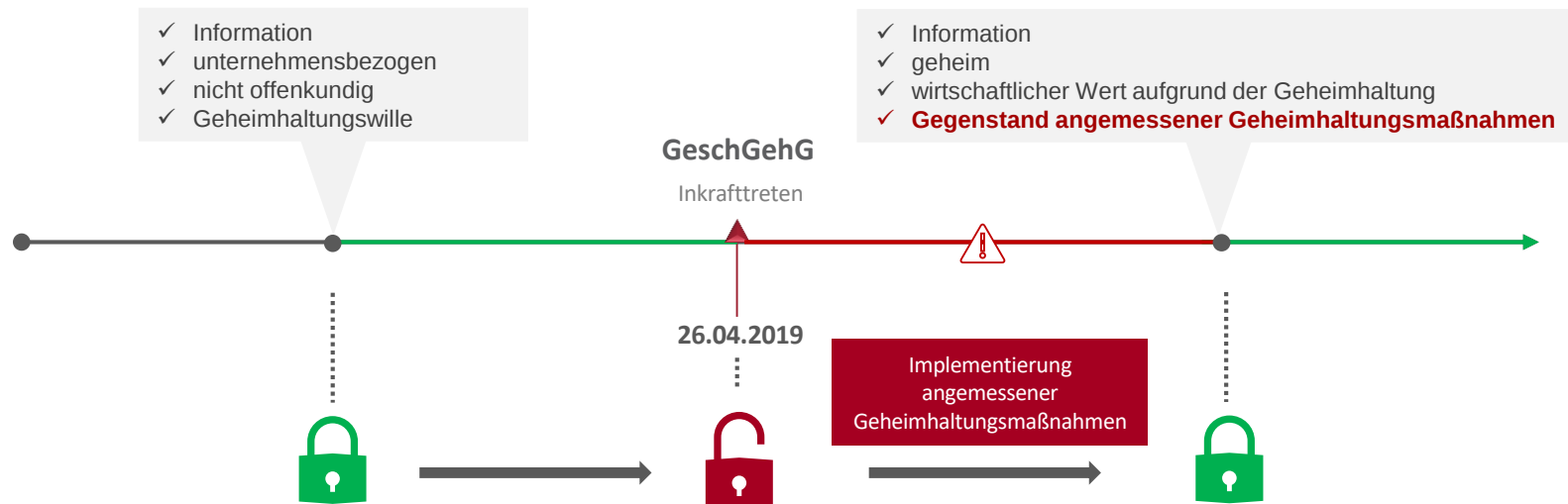
Bestehende Geschäftsgeheimnisse anfänglich geschützt



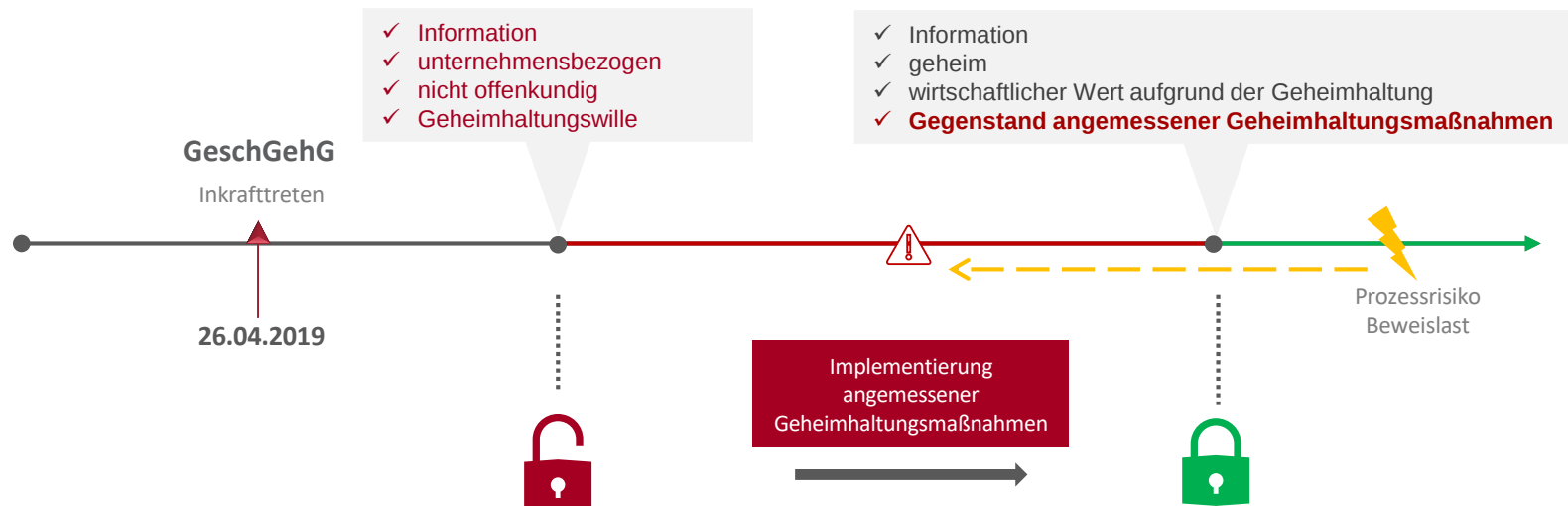
Bestehende Geschäftsgeheimnisse nicht anfänglich geschützt



Bestehende Geschäftsgeheimnisse nachträglich geschützt



Geschäftsgeheimnisse nachträglich geschützt





Checklisten

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		

Checkliste Geheimhaltungsklauseln

Betroffene Verträge	Ziele der Geheimhaltung	Ausgestaltung
NDAs	✓ Risikominderung im Zusammenhang mit der (ggf. gegenseitigen) Offenbarung von Interna ✓ Sicherstellung der Nutzung der im Laufe der Zusammenarbeit bekannt gewordenen vertraulichen Informationen nur zu den vertraglich festgelegten Zwecken ✓ Pflicht des Dritten zur Ergreifung angemessener Geheimhaltungsmaßnahmen	☐ Entweder: Bestandteil der jeweiligen Hauptverträge ☐ Oder: selbständige NDAs (v. a. im Vorfeld vor Abschluss weitergehender Leistungs- und Austauschverträge) ☐ Begrenzung (Diff. Mitarbeiter/ B2B) ▪ Umfang, Dauer der Geheimhaltungspflicht ▪ Nutzung der Erkenntnisse bei nicht erfolgtem Vertragsschluss /nach Vertragsablauf ▪ Geheimhaltungsmaßnahmen ☐ Vermeidung von „globalen“/ “general purpose“-NDAs
Forschungs- und Entwicklungsverträge		☐ Definition des Geschäftsgeheimnisses im Vertrag ▪ ggf. Konkretisierung der Geheimnisse ▪ Spannungsfeld: Bestimmtheit ↔ Schutzinteresse ☐ Geheimhaltungsklausel ☐ Vertragsstrafe
Kooperationsverträge		
Subunternehmerverträge		
Lizenzverträge		
Verträge mit freien Mitarbeitern		
Arbeitsverträge		☐ ggf. nachvertragliches Nutzungs-/ Wettbewerbsverbot (u. U. mit Karenzentschädigung)

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 Problem sein, dass sensible Daten nicht mehr bei US-Unternehmen gespeichert werden dürfen. „Richtig frei“ sind Daten eher jenseits des Atlantik.

hk2.eu/newsletter

Datenschutzbeauftragter

HK2
Comtection

START DSGVO DATENSCHUTZBEAUFTRAGTER CONSULTING TEAM BLOG

HK2 COMTECTION

IT's.BB **BvD^{e.V.}**
MITGLIED

DATENSCHUTZRECHT

Datenschutz ist Pflicht und Chance zugleich. Wir unterstützen Ihr Unternehmen bei der Bewältigung datenschutzrechtlicher Anforderungen. Mit einem Datenschutzbeauftragten der HK2 Comtection erfüllen Sie die gesetzliche Pflicht zur Bestellung eines Beauftragten für den Datenschutz nach Art. 37 DSGVO, § 38 BDSG.

Zudem bieten wir nach ihren individuellen Vorgaben:

IT-SICHERHEIT

Maßnahmen zur IT-Sicherheit sind zum Schutz von Unternehmenswerten, Know-How, personenbezogenen Daten und Umsatz erforderlich. Ohne Lösungen zur IT-Sicherheit gibt es kein wirksames Risikomanagement. Es ist gesetzliche Pflicht der Geschäftsleitung, angemessene Sicherheitsvorkehrungen zu treffen. Die DSGVO verschärft die Anforderungen an den technischen Datenschutz deutlich.

Wir begleiten Sie bei der Umsetzung, Prüfung und Beauftragung von extern.

www.comtection.de



www.geheimnisschutz.eu

www.hk2.eu

www.comtection.de

HK2
Rechtsanwälte

Kontakt

Karsten U. Bartels LL.M.

Rechtsanwalt

bartels@hk2.eu

HK2 Rechtsanwälte

Hausvogteiplatz 11 A

10117 Berlin

Telefon: +49 30 2789000

Telefax: +49 30 27890010