



TaylorWessing

Fernmeldegeheimnis und Geheimnisschutz – Kenne die Regeln

29.08.2022 / Johannes Simon, LL.M. (Durham), Rechtsanwalt und Fachanwalt für Arbeitsrecht
Mareike Gehrman, Rechtsanwältin und Fachanwältin für IT-Recht

Agenda

1	Geheimnisschutz	3
2	Fernmeldegeheimnis	9
3	Ihre Ansprechpartner	14

1 | Geheimnisschutz

Begriff des Geschäftsgeheimnisses

Zum 26. April 2019 ist das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) in Kraft getreten. Dieses enthält erstmals eine gesetzliche Definition des Begriffs „Geschäftsgeheimnis“. **§ 2 Nr. 1 GeschGehG** bestimmt dabei, dass ein „Geschäftsgeheimnis“ im Sinne des Gesetzes vorliegt, wenn die Information:

- **nicht** allgemein bekannt oder ohne Weiteres zugänglich ist und
- daher von wirtschaftlichem Wert ist und
- der berechtigte Geheimnisinhaber ein schützenswertes Interesse an der Geheimhaltung hat und
- sie Gegenstand von „**den Umständen nach angemessenen Geheimhaltungsmaßnahmen**“ ist (neu!)

→ Damit entfällt die zuvor von der Rechtsprechung entwickelte Vermutungsregel, dass alle nicht offenkundigen Betriebsinterna grundsätzlich Geschäftsgeheimnisse sind.

→ Vertragliche Verschwiegenheitsklauseln bieten **ohne entsprechende angemessene Maßnahmen keinen Schutz mehr!**



Angemessene Geheimhaltungsmaßnahmen nach GeschGehG (1)

Was bedeutet „angemessene“ Geheimhaltungsmaßnahme im Sinne des GeschGehG?

- Das Gesetz verlangt „**angemessene**“, **nicht** „optimale“ Geheimhaltungsmaßnahmen
- Welche Maßnahmen „angemessen“ sind, richtet sich nach den Umständen des Einzelfalls. Berücksichtigt werden können ausweislich der Gesetzesbegründung u.a.:
 - Der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten
 - Die Bedeutung der Information für das Unternehmen
 - Die **Größe des Unternehmens** („subjektiv, dynamischer“ Maßstab)
 - Art der Kennzeichnung der Information
 - Bereits vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern

Angemessene Geheimhaltungsmaßnahmen nach GeschGehG (2)

Überblick über mögliche Geheimhaltungsmaßnahmen

- Einführung eines strikten „Need-to-know“-Prinzips im Unternehmen
(d.h. Wissensbegrenzung auf das für die Tätigkeit Notwendige)
- Physische und elektronische Zugangs- und Nutzungsbeschränkungen
 - (z.B. Zutrittsbeschränkungen und -kontrollen, Alarmanlagen, beschränkte Zugriffsrechte auf physische und elektronische Datenbanken/Ordner unter Berücksichtigung des „Need-to-know“-Prinzips, Passwortschutz, Sperrung von USB-Anschlüssen)
- Abschluss von neuen Geheimhaltungsvereinbarungen mit (Leih-)Arbeitnehmern, Sub-Unternehmern und Geschäftspartnern
 - **Achtung!** Nach der jüngsten Rechtsprechung sind sog. „Catch-All-Klauseln“ in NDAs, die Geschäftsgeheimnisse nicht näher spezifizieren, unwirksam vgl. Arbeitsgericht Aachen v. 13.1.2022 - 8 Ca 1229/20)
- Etablierung verbindlicher Regeln für Arbeitnehmer in Bezug auf den Umgang mit Geschäftsgeheimnissen
 - (z.B. Verlassen des Arbeitsplatzes nur nach Sperrung des Bildschirms, Aufbewahrung vertraulicher Unterlagen in abgeschlossenen Schränken, Verschlüsselung sensibler E-Mails, Verbot der Nutzung privater IT-Geräte für betriebliche Zwecke, Verbot der Mitnahme sensibler Unterlagen ins Home Office).
 - Bei Bestehen Betriebsrat ggf. MBR bei der Einführung Geschäftsgeheimnis-Überwachungssystem beachten (Abschluss BV)
 - Bei Aufstellung betrieblicher Verhaltensregeln zum Know-how Schutz, sog. Ordnungsverhalten (§ 87 Abs. 1 Nr. 1 BetrVG)
 - Bei Einführung technischer Schutzmaßnahmen (z.B. Registrierung von Zugriffsversuchen auf sensible Informationen) MBR aus § 87 Abs. 1 Nr. 6 BetrVG
- Regelmäßige Schulungen der Arbeitnehmer zum Thema „Geheimnisschutz“

Angemessene Geheimhaltungsmaßnahmen nach GeschGehG (3)

Folgen / Risiken bei unterlassener Implementierung angemessener Geheimhaltungsmaßnahmen:

- Verstoß gegen die allgemeine Schadensabwendungsspflicht (Organisationsverschulden)
- **Haftung der Geschäftsführung** aus § 43 Abs. 1 GmbHG (Wegfall Schutz D&O Versicherung?)
 - Bei Bestehen einer Vermögensbetreuungspflicht (z.B. CFO, kaufmännische Leitung) ggf. Risiko des Vorwurfs der Untreue (§ 266 StGB; Geschäftsgeheimnisse = Vermögenswerte)
- **Wertminderung** des Unternehmens (Know-how und Geschäftsgeheimnisse sind erhebliche wertbildende Faktoren)
- **Kein** zivilrechtlicher und strafrechtlicher **Rechtsschutz** nach dem GeschGehG bei Verletzung von Geschäftsgeheimnissen durch (ehemalige) Mitarbeiter
- Mögliche **Haftung gegenüber Dritten**, soweit deren Geschäftsgeheimnisse (ggf. ohne Wissen der Geschäftsführung eines Unternehmens) durch eigene Mitarbeiter verletzt werden
- **Verlust von Kundenaufträgen** wegen fehlender / unzureichender Schutzmaßnahmen



Fazit

- Neues GeschGehG birgt **Haftungsrisiken** für Organe und Führungskräfte (Geschäftsführung, kaufmännische Leitung, Personalleitung etc.)
- Ggf. kein Schutz durch D&O Versicherung gegen persönliche Haftung Organe / Führungskräfte
- Ohne angemessene Maßnahmen besteht **(derzeit) kein Schutz von Geschäftsgeheimnissen** (Risiko für Werthaltigkeit oder ggf. sogar Existenz des Unternehmens)
 - **Keine Umsetzungsfrist (vgl. LAG Düsseldorf, Urteil v. 3.6.2020 – 12 SaGa 4/20)**
- **Angriffe Dritter möglich**: das Unternehmen haftet bereits, wenn das Management hätte „wissen müssen“, das „gestohlene“ Geschäftsgeheimnisse verwendet werden; ggf. **Verlust von Aufträgen**
- Präventionsmaßnahmen – Errichtung **Überwachungssystem** – erforderlich:
 - Benennung „Team“
 - Ausarbeitung / Optimierung Schutzmaßnahmenkatalog für Überwachungssystem
 - „Ausrollen“ Überwachungssystem / Optimierungsmaßnahmen
 - Turnusmäßige Revision für Überwachungssystem



2 | Fernmeldegeheimnis

Das Fernmeldegeheimnis

Was ist das?

- Fernmeldegeheimnis schützt die Vertraulichkeit der unkörperlichen Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs

Was ist neu?

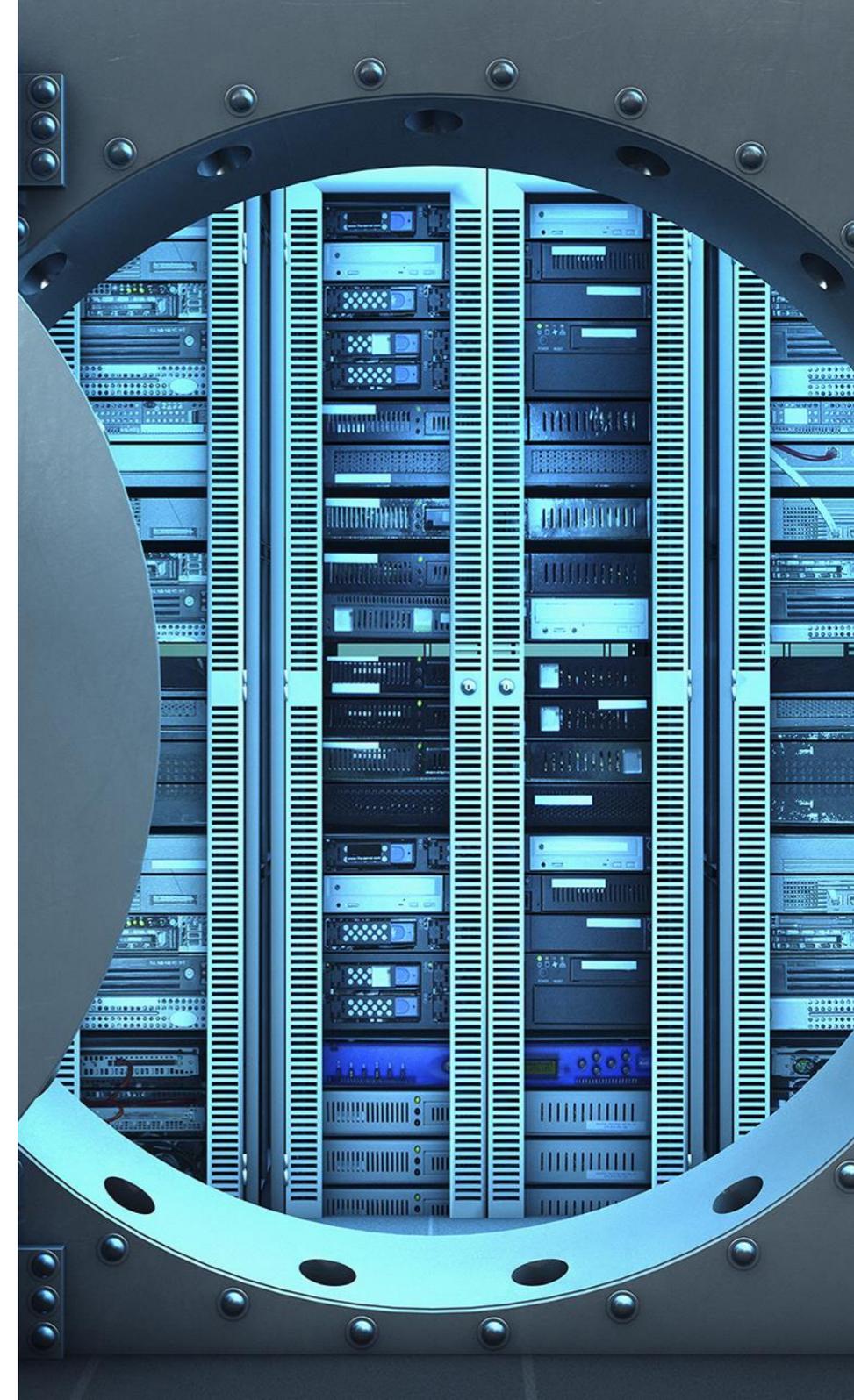
- seit 01.12.2021: Regelung in § 3 TTDSG (vormals in § 88 TKG)
- insb. erweiterter Verpflichtetenkreis

Um welche Daten geht es?

- Inhalt der Kommunikation und nähere Umstände
- Nähere Umstände: Verkehrsdaten zum Aussenden, Übermitteln und Empfangen von Telekommunikationssignalen, u.a. Zeitpunkt, Dauer, Kommunikationsteilnehmer, IP-Adresse, erfolgloser Verbindungsversuch

Sanktionen

- § 206 StGB: Verletzung des Fernmeldegeheimnisses



§ 206 StGB Verletzung des Post- und Fernmeldegeheimnisses



1. Tatbestand

a) Objektiver Tatbestand

- Tauglicher Täter
 - Inhaber oder Beschäftigter in einem Unternehmen, welches geschäftsmäßig Post- oder Telekommunikationsdienste erbringt
- Tatsache, die dem Post- oder Fernmeldegeheimnis unterliegt
 - neben Inhalt der Kommunikation, auch Identität der Teilnehmer, sowie nähere Umstände z.B. erfolglose Verbindungsversuche
- Bekanntwerden der Tatsachen
- Tathandlung: Unbefugtes Mitteilen

b) Subjektiver Tatbestand

2. Rechtswidrigkeit

3. Schuld

4. Strafverfolgung: § 303c StGB relatives Strafantragsdelikt

Praxishinweis:

- **(P)** Arbeitgeber als Erbringer geschäftsmäßiger Telekommunikationsdienste?
 - Nach wohl h.M. gilt der Tatbestand für alle Unternehmen, die ihren Mitarbeitern die Privatnutzung der Telefonie, E-Mail oder Internet gestatten (aber str., Argument: Verstoß gegen Analogieverbot)
 - Arbeitsgerichte, eher (-)
 - Datenschutzbehörden, Kommentarliteratur im TK-Bereich, eher (+)
 - Problem für die Praxis: Unklare Rechtslage!
 - Ohne eine eigene Richtlinie zur Nutzung der IT ist eine Kontrolle der E-Mails oder des EDV Arbeitsplatzes nur unter dem Risiko eigener Strafbarkeit möglich
 - Eine Einwilligung muss alle Nutzer umfassen!
 - Oder: Private Nutzung verbieten und überprüfen.

Erweiterter Verpflichtetenkreis seit Einführung des TTDSG

Fernmeldegeheimnis

Inhalt und Umstände der Telekommunikation

✓ Telefon + SMS



§ 24 Nr. 3 TKG n. F.:
OTT-Dienste =
Telekommunikation



OTT = Over-the-Top-Dienst,
z.B. Messenger oder Videotelefonie-Dienst

NEU:

- **OTT-0-Dienste** bieten Funktionen wie klassische TK-Dienste, z. B. Anrufe über das offene Internet per SkypeOut-Funktion in das öffentliche Telefonnetz (PSTN)
- **OTT-I-Dienste** ermöglichen Individual- / Gruppenkommunikation in Form von Sprache, Bildern, Videos und sonstigen Daten unter Einsatz des „Internet Protocol“ allein über das offene Internet, ohne dabei inhaltliche Angebote aufzuweisen; dazu gehören Instant-Messenger, aber auch Webmaildienste
- **OTT-II-Dienste** weisen inhaltliche Elemente auf und reichen damit von Suchmaschinen, über On-Demand-Plattformen, bis zu Informationsportalen
- „**Interpersonelle Kommunikationsdienste**“ (§ 3 Nr. 24 TKG) = OTT-0-Dienste und OTT-I-Dienste sind nun TK-Dienste (§ 3 Nr. 61 TKG n.F.) ; hingegen nicht OTT-II-Dienste
- **Fernmeldegeheimnis (§ 3 TTDSG) gilt für OTT-0-Dienste und OTT-I-Dienste**

Auswirkungen am Beispiel: Videokonferenzen

Beispiel: Videokonferenzsysteme

- Definition, § 3 Nr. 24 TKG: "**interpersoneller Telekommunikationsdienst**" ein gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Telekommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen
- Neben der DSGVO gelten die speziellen Regelungen von § 3 und §§ 9 ff. TTDSG für Arbeitgeber und Anbieter, in der Praxis wird aber oft nur eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen
- **Beispiele für Risiken:**
 - **Analyse-Tool:** Erhebung und Auswertung von Verkehrs- und Standortdaten über Videokonferenzen der Mitarbeiter (z.B. IP-Adresse, Teilnehmer, Ort, Uhrzeit oder Dauer)
→ Einhaltung insbesondere von §§ 3, 9 und 13 TTDSG prüfen, idR (-)
 - **Gruppenschaltung bei Sprachtelefonie:** Ohne Zustimmung des Gruppenmitglieds unzulässig, zwar für berufliche Anrufe möglich, aber bedarf der Zustimmung im Hinblick auf die private Nutzung (z.B. Anzeige der Rufnummer, Information über den Anruf an sich)

TaylorWessing

Ihre Ansprechpartner

Private and Confidential



Johannes Simon, LL.M. (Durham)
Partner, Düsseldorf

+49 211 8387-195
j.simon@taylorwessing.com

Beratungsschwerpunkte

- Fremdpersonal-Compliance
- Flexibler Personaleinsatz
- Know-how Schutz im Unternehmen
- Arbeitsrechtliche Restrukturierungen



Mareike Gehrman
Salary Partnerin, Düsseldorf

+49 211 8387-162
m.gehrman@taylorwessing.com

Beratungsschwerpunkte

- Datenschutz und Cybersecurity
- IT-Recht

[Europe](#) > [Middle East](#) > [Asia](#)

Taylor Wessing 2022

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at <https://deutschland.taylorwessing.com/en/regulatory>.

taylorwessing.com