

# Strafrechtlicher Know-how-Schutz in Deutschland und Russland

Regionalstammtisch der DRJV NRW/Düsseldorf  
Düsseldorf, 19. Mai 2015



WESSING & PARTNER

# Einleitung: Emails nach Hause, USB-Sticks mit Daten für die neue Firma

- 51 Milliarden Euro Schaden jährlich durch Datendiebstahl in Deutschland (Umfrage Bitkom 2015).
- Die Mehrzahl der Angriffe auf das „intellektuelle Kapital“ von Wirtschaftsunternehmen kommt von innen und wird durch ausscheidende Mitarbeiter verübt.
- Besonders betroffen: Mittelständische Unternehmen des Maschinenbaus (Jahrzehnte alte Konstruktionen und Erfahrungen, auch deshalb oft kein Patentschutz).
- Ein Konzept für den Schutz seiner Daten sollte jedes Unternehmen haben. Nicht jedes Risiko des Diebstahls von Geheimnissen lässt sich jedoch über Kontrolle ausschließen.

## „Die Wechselwilligen“

Die mittelständische Meyer GmbH produziert Fenster und ist am russischen Markt interessiert. Seit einigen Jahren besitzt sie daher eine russische Tochter, die OOO Meyer.

Der Geschäftsführer R, Staatsangehöriger der RF, verlässt diese nach kurzer Zeit wieder und geht zum Konkurrenten X. Ungefähr zeitgleich verlässt der Prokurist D (Deutscher) die deutsche Muttergesellschaft.

„Aus dem Markt“ wird bekannt, dass beide beim Konkurrenten X eine neue Abteilung gründen wollen. Nach Bekanntwerden verdächtiger Äußerungen, die auf Datendiebstahl schließen lassen, untersuchte die IT-Abteilung die dienstlichen Notebooks von R und D. Unter Verstoß gegen die Arbeitsverträge der Beiden waren fremde USB-Datenträger angeschlossen worden. Sowohl D, als auch R, hatten sich Excel-Dateien mit Konstruktionsdaten sowie detaillierte Kontaktlisten von Kunden an private Email-Adressen gesendet.

# Brainstorming

- Zivilklage gegen das Konkurrenzunternehmen X? Zu früh, da keine Beweise, auch nicht für die Auskunftsklage. Es dürfte noch nicht einmal ein schlüssiger Klagevortrag möglich sein.
- Strafanzeige? Reputationsverlust?
- Wo?
- Erfolgsaussichten:
  - Ist das Verhalten strafbar?
  - Wo kann es verfolgt werden?
  - Was ist zur Vorbereitung einer Erfolg versprechenden Strafanzeige notwendig?

# Was ist strafrechtlich geschützt?

## Russische Föderation

Коммерческая, налоговая или  
банковская тайна -

**Wirtschafts- Steuer- oder  
Bankgeheimnis,**

Art. 183 UKRF:

Legaldefinition des  
Wirtschaftsgeheimnisses durch Art.  
2 Abs. 2 des Gesetzes über das  
Wirtschaftsgeheimnis ...

## Deutschland

**Betriebs- und Geschäftsgeheimnis,**

§ 17 UWG:

Innerhalb von ca. 100 Jahren durch  
Einzelfallrechtsprechung  
ausgeformter Begriff ...

## Коммерческая тайна, Art. 2 Abs. 2 N98-ФЗ (29.07.04)

- **Informationen** beliebigen Charakters (Produktion, Technik, Ökonomie, Organisation und Anderes, auch Produktionsgeheimnisse = ноу-хау, s. Art. 1465 ZGB), darunter auch Resultate intellektuellen Schaffens,
- die kraft ihrer **Unbekanntheit** bei Dritten
- tatsächlichen oder potenziellen **kommerziellen Wert** haben
- zu denen dritte Personen **keinen legalen Zugang** haben
- für die ein **Regime des Wirtschaftsgeheimnisses** eingeführt wurde.
- Keine **Ausschlussgründe**, Art. 5 N98 ФЗ

## Betriebs- und Geschäftsgeheimnis

- **Unternehmensbezug** der Information
- **Nichtoffenkundigkeit**
- **Berechtigtes Interesse** an Geheimhaltung
- **Geheimhaltungswille**
  - ---
- Keine gesetzlichen **Ausschlussgründe**

# RF: Regime der Geheimhaltung – Art. 10 N 98-Φ3

- 1) Bestimmung des Kreises der betroffenen Informationen
- 2) Beschränkung des Zugangs durch eine Zugriffs-/Benutzungsordnung und Kontrolle der Befolgung dieser Ordnung
- 3) Registrierung der Personen, die Zugang zu den Informationen erhalten haben bzw. denen diese zur Verfügung gestellt/übergeben werden
- 4) Regelung der Verwendung der Informationen auf der Basis des Arbeitsvertrags (Arbeitnehmer) bzw. Vertrag (Geschäftspartner)
- 5) Schriftzug:



## Exkurs (1): Urteil Gagarinskij Sud Moskau vom 10.06.13

Sachverhalt: Ein Mitarbeiter ist ausgeschieden. Er hat sich von der Arbeit Emails mit Anhängen „nach Hause“ geschickt. Die Informationen hatte er sich – ohne dienstliche Veranlassung - vom Rechner eines Kollegen mit dessen Passwort verschafft. Es wurde nachgewiesen, dass er die Informationen an einen Konkurrenten verkaufte. Schaden: 2 Mio. USD

Verteidigungsstrategie: Die Dateien seien nicht als Wirtschaftsgeheimnis markiert gewesen und dem Mitarbeiter sei nicht bewusst gewesen, dass es sich um Wirtschaftsgeheimnisse handelt.

Das Gericht stellt fest: Verletzung von Art. 183 Abs. 1, 2 UKRF.

Rechtsfolge: Besserungsarbeit von 1 Jahr (Art. 183 Abs. 1) sowie 1 Jahr 9 Monaten (Art. 183 Abs. 2), „Gesamtstrafe“: 1 J 9 Mon.



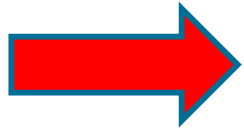
## Exkurs (2): Urteil Gagarinskij Sud Moskau vom 10.06.13

Zur Strafzumessung: Freiheitsbeschränkende Rechtsfolgen wegen Geheimnisverrat sind in Deutschland vergleichsweise selten. Hier: Noch nicht einmal Qualifikationstatbestand erfüllt, keine Vorstrafen.

Vergleich mit der deutschen Praxis: Verfahren werden oft gegen Geldauflage eingestellt, § 153a StPO.

**Aber:** Auf Grund des Schadens in Millionenhöhe wäre durchaus auch in Deutschland an eine nicht bewährungsfähige Freiheitsstrafe zu denken, vergleiche BGH (Steuerhinterziehung in Millionenhöhe), Urteil vom 02.12.08 (Aktenzeichen 1 StR 416/08).

## Exkurs (3): Urteil des Gagarinskij Sud Moskau v. 10.06.13



Gagarinskij Sud: Können Informationen ohne „Gryph“  
Wirtschaftsgeheimnis sein?

Ja:

- Im Unternehmen gab es ein **Regime** im Sinne des Art. 10 des Gesetzes **über das Wirtschaftsgeheimnis**:
  - Der **Zugang zu Computern** anderer Mitarbeiter ohne deren Zustimmung war ausgeschlossen,
  - Es waren **Anweisungen zur Behandlung von Wirtschaftsgeheimnissen** und **Regeln für die Verwendung** entsprechender Informationen erteilt worden,
  - Es gab eine **Expertenkommission zur Kontrolle** der Einhaltung der Regeln, die bei Notwendigkeit Entscheidungen traf und ausgehende Dokumente auch mit dem Gryph „Wirtschaftsgeheimnis“ versah,
- Dass die Emails keinen Gryph trugen, sei folglich unschädlich. Es handele sich um **rein interne Informationen**, die entwendet wurden und nicht dazu bestimmt waren, das Unternehmen zu verlassen.

# Lösung Ausgangsfall (1): Interne Untersuchung

## Empfehlung in Deutschland: Strafanzeige auf der Grundlage einer erfolgreichen internen Untersuchung

- „**Incident Management Group**“, nach Bedarf im Einzelfall gebildete Gruppe: Geschäftsführung, interne Revision, Vertreter Buchhaltung, EDV-Abteilung, Personalabteilung, externer strafrechtlicher Vertreter des Unternehmens, IT-Forensiker – vertrauliche Kommunikation muss gewährleistet sein (Verschlüsselung).
- Gibt es eine **IT-Betriebsvereinbarung** (Ausschluss der privaten Nutzung von Computern), wird diese auch angewendet – stichprobenartige Prüfungen?
- Gegebenenfalls Beteiligung des **Betriebsrates** (§ 87 Abs. 1 Nr. 1, 6 BetrVG).
- Beachtung des **Datenschutzes**: § 32 Abs. 1 S 2 BDSG: Dokumentierter Verdacht der Verletzung von Betriebsgeheimnissen?
- Achtung: Ab dem Schlussbericht der IMG kann bei Feststellung eines Tatverdachts gegen eine bestimmte Person die **Strafantragsfrist** von drei Monaten laufen.

# Lösung Ausgangsfall (2): Interne Untersuchung

## Interne Untersuchung RF

- Zugriff des Arbeitgebers auf (dienstliche) Dateien, Briefe und Dokumente des Arbeitnehmers (Spehl/Mommsen/Grützner, Unternehmensinterne Ermittlungen, Teil II, CCZ 2014, S. 2).
- Schriftliche Mitarbeiterbefragungen (Spehl/Mommsen/Grützner, Unternehmensinterne Ermittlungen, Teil II, CCZ 2014, S. 2).
- Betriebsrat (-)

## Lösung Ausgangsfall (3): Gibt es einen Straftatverdacht? Deutsches Strafrecht

### **§ 17 Abs. 1 UWG: Illegales Mitteilen eines Geheimnisses durch einen Beschäftigten während der Dauer seines Dienstverhältnisses:**

- Weder bei D, noch bei R liegt Verdacht vor: Das Mitteilen erfolgte mit hoher Wahrscheinlichkeit nach dem Ausscheiden.

### **§ 17 Abs. 2 Nr. 1 lit. b) UWG, Sichern des Geheimnisses durch Herstellen einer verkörperten Wiedergabe, u.A. zu Zwecken des Wettbewerbs:**

- In D bei Prokurist D gegeben (z. Nachteil Meyer GmbH).
- Hinsichtlich des nur in Russland handelnden Staatsbürgers der RF handelnden R ebenfalls Verdacht gegeben: Soweit Erfolg die Meyer GmbH betrifft liegt ein Tatort in D (§ 9 Abs. 1 Alt. 2 StGB). Soweit die russische Konzerntochter OOO Meyer betroffen ist: § 17 Abs. 6 UWG i.V.m. § 5 Nr. 7 StGB, Schutzprinzip.

Ebenso: **Verdacht des unbefugten Verwertens/Mitteilens nach § 17 Abs. 2 Nr. 2 UWG** nach dem Ausscheiden, bei beiden Personen gegeben.

## Lösung Ausgangsfall (4): Wer hat sich wo strafbar gemacht? Russisches Strafrecht

**Art. 183 Abs. 2 UKRF, Illegale Weitergabe oder Nutzung von Wirtschaftsgeheimnissen, die anvertraut waren oder durch die Arbeit bekannt wurden:** Hinsichtlich R wohl ja – keine Beschränkung auf während des Arbeitsverhältnisses begangene Taten (ebenso der von Pawel Owtscharenko wiedergegebene Fall eines Gerichts in Kamensk-Uralsk aus dem Jahr 2007, Intellekt-S (15.04.08), per Internet über [www.intellektpro.ru](http://www.intellektpro.ru) )

**Art. 183 Abs. 1 UKRF: Rechtswidriges Sammeln von Informationen, die ein Wirtschaftsgeheimnis darstellen.** Hinsichtlich GF R in Russland: Durch Entwendung mittels Kopierens sowie ungesetzliche Versendung mit Hilfe des Firmennetzwerks (vgl. auch Gagarinskij Sud Moskau, Urt. v. 10.06.13). Das bloße illegale Sammeln ist wesentlich leichter nachweisbar als das Mitteilen nach deutschem Recht!

# Lösung Ausgangsfall (5): Strafanzeige, Strafverfahren D

- **Kontaktaufnahme** zu Staatsanwaltschaft bereits vor Einreichung der Strafanzeige ist oft zweckmäßig.
- **Strafantrag** binnen drei Monaten (später besonderes öff. Interesse nötig)!
- Phase des Ermittlungsverfahrens **bis einschließlich Durchsuchung**: oftmals verhältnismäßig leicht, wenn „smoking gun“ gefunden und Verdacht gut dokumentiert wird (Abschlussbericht interne Untersuchung).
- Schwierig: **Auswertungsphase**
  - Staatsanwaltschaft hat keine Ressourcen und oftmals keine Spezialkenntnisse
  - Polizei oft ähnlich
  - Kommunikation ist Problem: Geschädigter ist „Fremdkörper“ im Verfahren, Staatsanwaltschaft will vermeiden, als parteilich im Sinne des Anzeigerstatters zu erscheinen
  - Informationsaustausch daher nur begrenzt (Beschränkungen der Akteneinsicht, trotz offensichtlicher Probleme bei Auswertung oft auch begrenzter Dialog mit Anzeigerstatter
  - Externer EDV-Sachverständiger im Auftrag der Staatsanwaltschaft kann Lösung sein

# Lösung Ausgangsfall (6): Strafanzeige, Strafverfahren D

## Ziele und mögliche Ergebnisse des Strafverfahrens:

- **Einstellungsmöglichkeiten der Staatsanwaltschaft im Blick behalten:**
  - § 170 Abs. 2 StPO, wenn die Staatsanwaltschaft nicht in der Lage ist auszuwerten,
  - § 153 StPO wegen Geringfügigkeit gegebenenfalls,
  - § 153a StPO gegen Geldauflage bei nicht vorbestraften Beschuldigten oft,
  - § 153c Abs. 1 Nr. 1 StPO, Nichtverfolgung von Auslandstaten (nur L): vorliegend nur, soweit die OOO Meyer betroffen ist, nicht dagegen soweit auch die Meyer GmbH geschädigt ist: Dann Erfolgsort Deutschland, keine Auslandstat.
  - § 154f, (Vorläufige) Einstellung des Verfahrens wegen Abwesenheit des Beschuldigten R, der als Staatsbürger der RF gem. Art. 61 Abs. 1 Verfassung der RF sowie Art. 13 Abs. 1 UKRF durch Russland nicht ausgeliefert wird.
- **Ausschöpfung des Strafrahmens**, der nicht bewährungsfähige Freiheitsstrafen umfasst, **kaum zu erwarten**. Sofern Beschuldigter akzeptiert: Strafbefehl mit **Geldstrafe** vielfach eher realistisch.



# Lösung Ausgangsfall (7): Strafanzeige, Strafverfahren D

- Möglichkeiten der **Beteiligung am Verfahren**:
- **Akteneinsicht** des Geschädigten als Nebenklageberechtigtem ist privilegiert, § 406e Abs. 1 S. 2 i.V.m. § 395 Abs. 1 Nr. 6 StPO, d.h. das berechnigte Interesse an der Einsicht wird gesetzlich vermutet.
  - In nahezu allen Fällen versucht der Beschuldigte, dem das Verfahren durch die Durchsuchung bekannt wurde, der Akteneinsicht entgegenstehende Interessen vorzutragen. Namentlich: Die Strafanzeige diene der Ausforschung von seinen eigenen Geheimnissen oder von Geheimnissen seines neuen Arbeitgebers.
- **Unterstützung der Staatsanwaltschaft** bei der Auswertung, soweit diese daran Interesse zeigt.
- Beteiligung am Verfahren als **Nebenkläger**, soweit die Sache bis zur Hauptverhandlung kommt.
- Entscheidung, ob Adhäsionsverfahren als Zivilklage im Strafprozess gem. § 403 StPO ff.: Risiko des Absehens des Gerichts von einer Entscheidung gem. § 406 Abs. 1 S. 4 StPO, wenn sich der Antrag zur Erledigung im Strafverfahren nicht eignet. Häufige Anwendung! Ggf. Kostenrisiko!

# Lösung Ausgangsfall (8): Strafanzeige, Strafverfahren D

Chancen Aufklärung Gesamtkomplex über **Rechtshilfe durch Russland?**

- **Auslieferung** des R gem. Art. 2 EuALÜbk (-), s.o., wegen Art. 61 Abs. 1 Verfassung RF sowie Art. 13 Abs. 1 UKRF.
- **Weitere Rechtshilfemaßnahmen** nach den Regeln des EuRhÜbk durch die Vornahme von Untersuchungshandlungen oder die Übermittlung von Beweisstücken, Akten oder Schriftstücken ist in der Praxis meistens unwahrscheinlich.

# Lösung Ausgangsfall (9): Strafanzeige/Strafverfahren RF

## Strafanzeige gegen Geschäftsführer R in Russland empfehlenswert?

Russische Öffentlichkeit: Eindruck, dass Art. 183 UKRF faktisch nicht angewendet wird: Interfax.ru , Meldung über Beschluss vom 29.08.14: angeblich erste Entscheidung mit einer Verurteilung überhaupt.

Vgl. z.B. auch Owtscharenko, Das Strafgesetzbuch auf Wacht für das Wirtschaftsgeheimnis, Intellekt-S (15.04.08, per intellectpro.ru).

Andererseits: Rechtsfolgen können empfindlich ausfallen!

- **Apellationsbeschluss des Obersten Gerichts der Republik Tschuwaschien** vom 29.08.14: Verurteilung in I. Instanz zu 1 Jahr 6 Monate Besserungsarbeit wegen Art. 183 Abs. 2 UKRF (aufgehoben in II. Instanz wegen Verjährung),
- **Gagarinskij Sud** vom 10.06.13: 1 Jahr 9 Monate Besserungsarbeit (keine Vorstrafen),
- **Friedensrichter Kamensk-Uralsk** 2007 (kurze Beschreibung bei Owtscharenko, per Internet über [www.intellektpro.ru](http://www.intellektpro.ru) ): 6 Monate Freiheitsstrafe auf Bewährung.

# Fazit: Was ist zu tun?

## Welches Ziel: Strafe, Unterlassen künftiger Schädigung, Schadenersatz?

- **Materielle Strafvorschriften** sind vergleichbar: Das Regime des Wirtschaftsgeheimnisses in RU scheint moderner und vorhersehbarer. Die Voraussetzungen der Straftatbestände scheinen etwas leichter erfüllbar. Strafen in RU sind grundsätzlich etwas schärfer. Angemessener strafrechtlicher Schutz ist in beiden Staaten vorhanden.
- **Ergebnis der Strafverfahren D:** die verhängten Strafen in Verfahren „nur“ wegen Geheimnisverrat sind nicht drastisch, oft Einstellung gegen Geldauflage. Die Aufklärung des Sachverhalts ist jedoch bei zivilrechtlicher Geltendmachung von Schadensersatz- und Unterlassungsansprüchen oft die einzige Chance, den Anforderungen der Beweislast zu genügen. Sogar die rechtliche Möglichkeit der Aufklärung in Russland begangener Straftaten besteht, soweit die Beweismittelsituation in D das im Einzelfall zulässt (z.B. Zeugen!)
- **Ergebnis der Strafverfahren RU:** Strafen potenziell höher, Interesse der Strafverfolgungsbehörden scheinbar eher noch geringer als in Deutschland. Die wenigen bekannten Entscheidungen zeigen, dass auch in RU ein zwiespältiges Verhältnis der Strafverfolger zum Geheimnisverrat zu bestehen scheint.
- In jedem Fall gilt: Eigenes Bemühen um **interne Aufklärung** ist unersetzbare Voraussetzung für ein Ermittlungsverfahren, das nicht alsbald mangels Tatverdacht eingestellt wird.