Your World First

Know-how-Schutz und IT-Sicherheit in der Vernetzung und Digitalisierung

Stefan Schreiber
Rechtsanwalt

"Gewusst was beim Gewusst wie"
– Schutzgegenstand "Know how"

Schutzgegenstand "Know-how" – Beispiele

- Daten, Information, Wissen

- fachlich, geschäftliches Wissen jeder Art: Geschäftsabläufe, Geschäftsvorfälle, interne Unternehmenskennzahlen, Informationen über Kunden und sonstige Geschäftspartner sowie über das Personal, Businesspläne, Markt- und Verkaufsstrategien, Fusionspläne, Marktforschungsergebnisse, etc.

Schutzgegenstand "Know-how" – Immaterialgüterrechtlicher und lauterkeitsrechtlicher Schutz

- Teile des Know-hows durch Immaterialgüterrechte geschützt
  - Patente, Urheberrecht (Software)
  - Schutz nicht immer erwünscht
  - umfasst nicht gesamtes Know-how

- Kein Ausschließlichkeitsrecht an sonstigem Know-how
  - keine gegenständlichen (Schutzobjekt), inhaltlichen (Schöpfungshöhe) oder formellen Voraussetzungen (Registerverfahren) gegeben
  - Abgrenzung zu Erfahrungswissen des Arbeitnehmers kaum möglich
  - Abgrenzung zu Nachahmungsfreiheit kaum möglich

- Sinn und Zweck des Schutzes: Förderung von Innovation und Zusammenarbeit in der Wirtschaft

Schutzgegenstand "Know-how" – UWG: Betriebs- und Geschäftsgeheimnisse

Jede im Zusammenhang mit dem Betrieb oder der Geschäftstätigkeit eines Unternehmens stehende,

nicht offenkundige Tatsache,

deren Geheimhaltung im objektiven wirtschaftlichen Interesse

wie auch im subjektiven Willen des Unternehmens fundiert ist.

Schutzgegenstand "Know-how" – Die EU Know-how-Richtlinie: Geschäftsgeheimnis

- Geschäftsgeheimnis als Oberbegriff von Know-how und Geschäftsinformation
- Definition in Art. 2 Abs. 1 RL:

*"**Informationen**, die alle nachstehenden Kriterien erfüllen:*

- *sie sind in dem Sinne **geheim**, dass sie weder in ihrer Gesamtheit noch in der genauen Anordnung oder Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich;*
- *sie sind von **kommerziellem Wert**, weil sie geheim sind;*
- *sie sind **Gegenstand von** den Umständen **entsprechenden angemessenen Geheimhaltungsmaßnahmen** durch die Person, die die rechtmäßige Kontrolle über die Information besitzt"*

Die EU Know-how-Richtlinie – Begriff des Geschäftsgeheimnisses

Wesentliche Änderung zur aktuellen Rechtslage:

Objektive "den Umständen entsprechend angemessene Geheimhaltungsmaßnahmen“ (RL)

Subjektiver "Geheimhaltungswille" (UWG)

Die EU Know-how-Richtlinie – Erlaubte und verbotene Handlungen

Erlaubte Handlungen

- Erlaubter Erwerb nach Art. 3 RL
  - unabhängig gefunden
  - mittels einer Vorgehensweise, die "mit einer seriösen Geschäftspraxis" vereinbar ist
  - NEU: mittels Reverse Engineering
  - kein Schutz, wenn offenkundig
- Nutzung aufgrund erlaubten Erwerbs
- Whistleblowing Art. 5 RL

Verbotene Handlungen Art. 4 RL

- rechtswidriger Erwerb des Geschäftsgeheimnisses Abs. 2
- Nutzung aufgrund rechtswidrigen Erwerbs Abs. 3 Nr. 1
- Nutzung über den vertraglich vereinbarten Umfang hinaus Abs. 3 Nr. 3
- Offenbarung Abs. 3 Nr. 2
- Kettenerwerb Abs. 4
- Vertrieb rechtswidrig hergestellter Produkte Abs. 5

Die EU Know-how-Richtlinie – Reverse Engineering

"Beobachtung, Untersuchung, Rückbau oder Testen eines Produktes oder Gegenstandes" (Art. 3 Abs. 1 lit. b RL)

- Voraussetzung: Produkt legal erworben oder öffentlich verfügbar
- vgl. § 69e UrhG als Spezialregelung

Aber: *"Das Reverse Engineering bei einem rechtmäßig erworbenen Produkt sollte als ein rechtlich zulässiges Mittel zum Erwerb von Informationen angesehen werden,* ***es sei denn, dass vertraglich etwas anderes vereinbart wurde****"* **(**Erwägungsgrund 16 S. 3)

à **To do**: ggf. entsprechende Klauseln vorsehen (inter partes)

„Vorsicht ist die Mutter der Porzellankiste“
– Schutz vor Verletzung

Die EU Know-how-Richtlinie – "Angemessene Geheimhaltungsmaßnahmen"

- keine nähergehenden Ausführungen durch die Richtlinie

  à ungewiss, wie Gesetzgeber Situation genau gestalten wird

- Entwicklung und Umsetzung von Schutzkonzepten durch die Inhaber erforderlich

  à nicht ausreichend, Geheimnisse ausschließlich gegen Außenstehende zu schützen

  à physische Zugangsregelungen und vertragliche Sicherungsmechanismen

"Angemessene Geheimhaltungsmaßnahmen" – Schutzmöglichkeiten und -strategien

Know-How Schutz		
Faktische Schutzmöglichkeiten	Rechtlicher Schutz	
	Arbeitsrechtlich	Vertraglich mit Geschäftspartnern/ Lieferanten etc.

"Angemessene Geheimhaltungsmaßnahmen" – Faktisch-technische Möglichkeiten

- Klassifizierung des Know-hows in Schutzklassen und Sicherheitsstufen
  - Need-to-know-Prinzip
  - Vertraulichkeitsvermerke
- arbeitsteilige Prozesse, Festlegung eindeutiger Zuständigkeiten
- IT-Lösungen
  - z. B. Firewall, Zugangsbeschränkungen
- Förderung von Verschwiegenheit und Loyalität der Arbeitnehmer

"Angemessene Geheimhaltungsmaßnahmen" – Vertragliche Regelungen

- Ist eine Offenlegung von Know-how überhaupt erforderlich?
- Vertragsgegenstand
- Art und Weise der Offenlegung
- Dokumentation der Offenlegung
- Geheimhaltungs- und Nichtverwendungsabreden
- Vertragsstrafe
- Auskunfts- und Prüfungsrechte
- Pflichten bei Beendigung des Vertrags
- NEU: Reverse Engineering

"Angemessene Geheimhaltungsmaßnahmen" – Arbeitsrechtlicher Know-how-Schutz

- Bindung der Know-how-Träger, beispielsweise:
  - (nachvertragliche) Wettbewerbsverbote
    à Karenzentschädigung
  - (nachvertragliche) Abwerbeverbote
  - Koppelung mit Vertragsstrafenregelungen
  - Ausdrückliche (nachvertragliche) Geheimhaltungsvereinbarungen
- Generelle Regelungen im Betrieb:
  - IT-Richtlinien, Social Media Guidelines
  - Schulung und Sensibilisierung der Arbeitnehmer
  - Kontrolle

„Wenn das Kind in den Brunnen gefallen ist“
– Verfolgung von Rechtsverletzungen

Die EU Know-how-Richtlinie – Verbesserter Rechtsschutz

- Materiell-rechtlich durch weitere Ansprüche

  - insbesondere Unterlassungs- und Schadensersatzansprüche
  - NEU: immaterieller Schadensersatz Art. 14 Abs. 2 RL; vgl. § 97 Abs. 2 S. 4 UrhG
  - daneben Ansprüche wie Vernichtungs- und Rückrufansprüche, vgl. Enforcement Richtlinie
  - Verjährung: Höchstfrist 6 Jahre, Mindestfrist und Regelungen zu Fristbeginn nicht festgelegt
  - Bestimmungen zu vorläufigen und vorbeugenden Maßnahmen

- Prozessrechtlich durch Schutz des Geheimnisses im Prozess

Know-how des Verletzten im Prozess – Gegenwärtige Situation: Offenlegung oder (und) Niederlage?

Problem: Darlegungs- und Beweispflicht bzgl. Geschäfts-/ Betriebsgeheimnis bei Kläger

à u. U. entfällt Geheimnischarakter und damit Schutz nach UWG

Die EU Know-how-Richtlinie – Rechtsschutz

Wesentliche Änderung zur aktuellen Rechtslage:

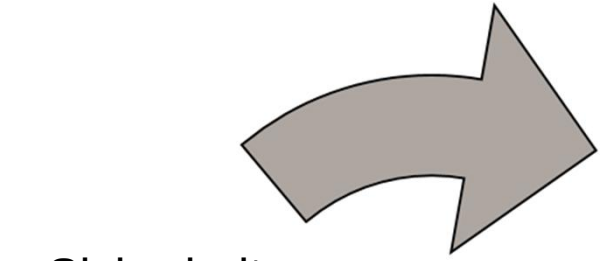
zu beweisende „den Umständen entsprechend angemessene Geheimhaltungsmaßnahmen“ (RL)

regelmäßig vermuteter "Geheimhaltungswille" (UWG)

To do: aktive Maßnahmen

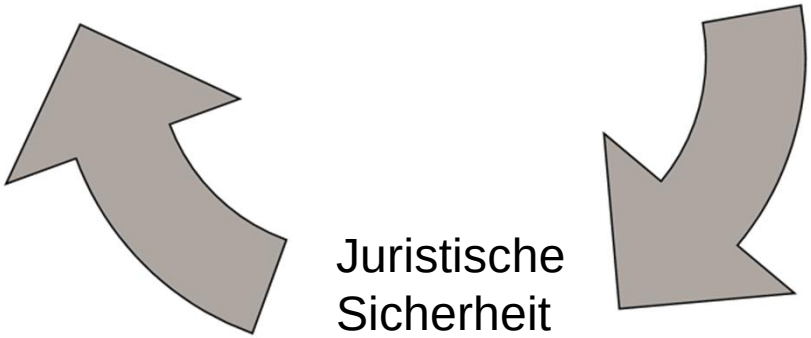
- Know-how-Schutzkonzept + Dokumentations- und Nachweispflicht
- technische Maßnahmen
- Überprüfung Know-how relevanter Vereinbarungen (intern und mit Dritten)

IT-Sicherheit und Geheimhaltungsmaßnahmen



Technische Sicherheit
(z. B. Firewall, URL-,
Content- und Spam-Filter)

Organisatorische Sicherheit
(z. B. Zuständigkeitsverteilung,
Nutzungsrichtlinien, Missbrauchs-
kontrolle, Audits, Zertifizierungen)



Juristische
Sicherheit
(z. B. Arbeitsverträge,
IT-Verträge, AGB)

Ziele der IT-Sicherheit

Hauptziele

- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Authentizität

Die häufigsten Versäumnisse

- Unzureichende IT-Sicherheitsstrategie
  - Zu geringer Stellenwert der Sicherheit
  - Vernachlässigung notwendiger Sicherheitsmaßnahmen
  - Fehlen der rechtlichen Umsetzung bei der Einführung technischer und organisatorischer Sicherheitsmaßnahmen

- Schlechte Konfiguration von IT-Systemen
  - Die Rechtevergabe wird nicht restriktiv genug gehandhabt
  - IT-Systeme sind schlecht konfiguriert

- Sorgloser Umgang mit Passwörtern und Sicherheitsmechanismen

Die häufigsten Versäumnisse

- Unsichere Vernetzung und Internetanbindung
  - Unzureichende Abschottung sensitiver Systeme gegen offene Netze
- Nichtbeachtung von Sicherheitserfordernissen
  - Sicherheitsmaßnahmen werden aus Bequemlichkeit vernachlässigt
  - Anwender und Administratoren sind mangelhaft geschult
- Schlechte Wartung von IT-Systemen
  - Verfügbare Sicherheitsupdates werden nicht eingespielt
- Benutzung privater Endgeräte im betrieblichen Einsatz

Wichtige Sicherheitsmaßnahmen

1. Systematisches Herangehen an IT-Sicherheit

- Festlegung der IT-Sicherheitsziele ß à Schutzbedarfsfeststellung
  - Welche Werte sind zu schützen (Know-how, Betriebsgeheimnisse, personenbezogene Daten, IT-Systeme)?
  - Was sind mögliche Schadensfälle?

- Festlegung und Bekanntmachung von Zuständigkeiten und Richtlinien
- Aufbau und Erstellung eines Sicherheitsmanagements und -konzepts

Wichtige Sicherheitsmaßnahmen

2. Technische und organisatorische Sicherheit

- Konkrete Sicherheitsmaßnahmen bei personenbezogenen Daten gemäß § 9 BDSG

*"Öffentliche und nicht öffentliche Stellen, die (…) personenbezogene Daten ergeben, verarbeiten oder nutzen, haben die **technischen und organisatorischen Maßnahmen** zu treffen, die erforderlichen sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."*

Wichtige Sicherheitsmaßnahmen

2. Technische und organisatorische Sicherheit (Anlage zu § 9 BDSG)

- Zutrittskontrolle
  - Unbefugten soll der körperliche Zugang zu Datenverarbeitungsanlagen verwehrt werden.
- Zugangskontrolle
  - Benutzung von Datenverarbeitungssystemen durch Unbefugte soll verhindert werden.
- Zugriffskontrolle
  - Ziel: Zugriff der Benutzer eines Datenverarbeitungssystems ausschließlich auf die der Zugriffsberechtigung unterliegenden Daten einzuschränken und personenbezogene Daten sollen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Wichtige Sicherheitsmaßnahmen

2. Technische und organisatorische Sicherheit (Anlage zu § 9 BDSG)

- Weitergabekontrolle
  - Verhinderung, dass Daten bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern unbefugt gelesen, kopiert oder verändert werden können und das eine Überprüfung gewährleistet werden kann, welche Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorsehen.
- Eingabekontrolle
  - Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welchem Zeitpunkt von wem in ein Datenverarbeitungssystem eingegeben worden sind.

Wichtige Sicherheitsmaßnahmen

2. Technische und organisatorische Sicherheit (Anlage zu § 9 BDSG)

- Auftragskontrolle
  - Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den jeweiligen Weisungen des Kunden verarbeitet werden.
- Verfügbarkeitskontrolle
  - Schutz der Daten vor zufälliger Zerstörung.
  - z.B. Wasserschäden, Brand, Blitzschlag und Stromausfall
- Trennungskontrolle
  - Technische Sicherstellung der zweckbestimmten Verarbeitung.

Wichtige Sicherheitsmaßnahmen

3. Juristische Sicherheit

- Gestaltung und Anpassung von Arbeitsverträgen und Betriebs- bzw. Dienstvereinbarungen
- Gestaltung von Nutzungsrichtlinien für Mitarbeiter (z. B. im Hinblick auf Internet- und E-Mail-Nutzung, Datenschutz etc.)
- Gestaltung von Geheimhaltungs- und Vertraulichkeitsvereinbarungen
- Gestaltung von Datenschutzerklärungen
- Gestaltung des rechtssicheren Auftritts im Internet

Wichtige Sicherheitsmaßnahmen

3. Juristische Sicherheit

Know-how-Schutz im Arbeitsverhältnis

- Beispiel einer vertraglichen Klausel:

"Sämtliche Arbeitsergebnisse des Arbeitnehmers für die Gesellschaft oder eines mit der Gesellschaft verbundenen Unternehmens, die in Erfüllung seiner dienstvertraglichen Pflichten oder aufgrund besonderer Weisung des Arbeitgebers (tätigkeitsbezogene Werke) oder sonst im engen inneren Bezug zu den dienstvertraglichen Pflichten (anregungsbezogene Werke) entstehen, stehen der Gesellschaft zu. Der Arbeitnehmer räumt der Gesellschaft an allen Arbeitsergebnissen umfassende, inhaltlich, zeitlich und räumlich unbegrenzte und ausschließliche Rechte ein bzw. überträgt, soweit möglich, der Gesellschaft diese Rechte. Dies bedeutet, dass die Gesellschaft zur umfassenden Nutzung und Verwertung der Rechte ausschließlich berechtigt ist. Die Gesellschaft nimmt hiermit sämtliche dieser Rechteübertragungen und –einräumungen ausdrücklich im Voraus an. "

Wichtige Sicherheitsmaßnahmen

3. Juristische Sicherheit

Richtlinien für Mitarbeiter zur E-Mail- und Internetnutzung

- Einführung einer Richtlinie zur Nutzung von **E-Mail** im Unternehmen

"Die dienstliche E-Mail-Adresse (Vorname.Name@Firma.com) darf allein zu dienstlichen Zwecken genutzt werden. Hintergrund dieser Regelung ist, dass bei erlaubter privater Nutzung ein unbeschränkter Zugriff von [Firma] auf dienstliche E-Mails aus rechtlichen Gründen nicht gestattet ist. Eine Nutzung zu privaten Zwecken ist daher nicht gestattet. Als private Nutzung der E Mail-Adresse gilt jeder Gebrauch, der keinen dienstlichen Zwecken dient, nicht dienstlich veranlasst ist oder nicht im Rahmen der arbeitsvertraglichen Aufgabenerfüllung erfolgt.

Eingehende private E-Mails sind nach Kenntnisnahme durch den Benutzer zu löschen. Der Absender der privaten E-Mail ist vom Empfänger darauf hinzuweisen, dass die dienstliche E-Mail-Adresse nur zu dienstlichen Zwecken genutzt werden darf."

Wichtige Sicherheitsmaßnahmen

3. Juristische Sicherheit

Richtlinien für Mitarbeiter zur E-Mail- und Internetnutzung

- Einführung einer Richtlinie zur Nutzung des **Internets** im Unternehmen

"Die von [Firma] angebotenen Internetdienste sind für den dienstlichen Gebrauch bestimmt. Eine private Nutzung des Internets ist in den Pausenzeiten gestattet. Dazu gehört auch die Nutzung privater E-Mail-Dienste. In jedem Fall darf die Privatnutzung die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit der IT-Systeme für dienstliche Zwecke nicht beeinträchtigen.

Bei jeder Form der Nutzung des Internets – gleich ob privat oder dienstlich – sind folgende Regeln einzuhalten: …

Nicht gestattet ist jede Nutzung, sei es durch Abruf, Verbreiten oder Verarbeitung von Daten, Texten, Äußerungen oder Abbildungen, die

- *gegen den Datenschutz, das Persönlichkeitsrecht, Urheberrecht oder Strafrecht verstoßen,*
- *in irgendeiner Form beleidigende, verleumderische, verfassungsfeindliche, rassistische, sexistische oder pornographische Inhalte aufweisen."*

Wichtige Sicherheitsmaßnahmen

3. Juristische Sicherheit

Geheimhaltungs- und Vertraulichkeitsvereinbarungen

- Umfassende Verschwiegenheitspflicht während des Arbeitsverhältnisses
- Eingeschränkte nachvertragliche Verschwiegenheitspflicht
  - BAG: auch nach Ende des Arbeitsvertrages bestehen Geheimhaltungsverpflichtungen fort
    - Ø Arbeitnehmer darf nicht als "Informationshändler" auftreten
    - Ø Arbeitnehmer darf jedoch die während der Beschäftigung redlich erworbenen Kenntnisse zu eigenem Nutzen, also für die eigene berufliche Tätigkeit, verwenden
  - BGH: Pflicht zur Geheimhaltung von Geschäfts- und Betriebsgeheimnissen endet grundsätzlich mit der Beendigung des Arbeitsverhältnisses
  - Ausnahme: Wettbewerbswidrigkeit: so z. B. unbefugte Beschaffung von schriftlichen und digitalisierten Unterlagen aus dem Arbeitsverhältnis.

Wichtige Sicherheitsmaßnahmen

3. Juristische Sicherheit

Geheimhaltungs- und Vertraulichkeitsvereinbarungen

- Wirksamkeit und rechtliche Grenzen von Geheimhaltungsvereinbarungen:

  - Unwirksamkeit von standardisierten bzw. allumfassenden Geheimhaltungsklauseln ("All-Klauseln")

  - Nur einzelne, konkret bezeichnete Geschäftsgeheimnisse dürfen vertraglich einer weitergehenden Verschwiegenheitspflicht unterstellt werden.

  - Je konkreter das Geheimnis im Vertrag bezeichnet und je bedeutender es für das Unternehmen ist, desto wahrscheinlicher ist die Rechtmäßigkeit der Klausel.

Wichtige Sicherheitsmaßnahmen

3. Juristische Sicherheit

Geheimhaltungs- und Vertraulichkeitsvereinbarungen

"a) Der/die Arbeitnehmer/in verpflichtet sich, über Geschäfts- und Betriebsgeheimnisse der [FIRMA] Stillschweigen zu bewahren. Hierzu zählen vor allem Einzelheiten über _____ [es folgt eine abstrakte Umschreibung der geheim zu haltenden Tatsachen]. Der/die Arbeitnehmer/in wird darauf hingewiesen, dass Geheimnisverrat nach dem Gesetz über den unlauteren Wettbewerb (§ 17 UWG) strafbar ist.

b) Die Schweigepflicht erstreckt sich auch auf Angelegenheiten anderer Firmen, mit denen das Unternehmen wirtschaftlich oder organisatorisch verbunden ist.

c) Der/die Arbeitnehmer/in ist auch zur Geheimhaltung solcher Tatsachen verpflichtet, die ihm/ihr von der Geschäftsleitung ausdrücklich als vertraulich bekanntgegeben werden, oder deren Geheimhaltungsbedürftigkeit sonst für sie/ihn erkennbar ist.

Wichtige Sicherheitsmaßnahmen

"d) Der/die Arbeitnehmer/in ist nicht berechtigt, sich eigenmächtig von der Schweigepflicht freizustellen. Der Arbeitgeber wird ihn/sie ausdrücklich von der Geheimhaltungspflicht befreien, soweit dies zur Wahrung überwiegender Interessen notwendig ist.

e) Ein Verstoß gegen die Verschwiegenheitspflicht kann eine Kündigung rechtfertigen sowie Schadensersatzpflichten auslösen.

f) Die Geheimhaltungspflicht besteht auch nach Beendigung des Arbeitsverhältnisses.

g) Sollte die nachvertragliche Verschwiegenheitspflicht den/die Arbeitnehmer/in in seinem/ihrem beruflichen Fortkommen behindern, so hat der/die Arbeitnehmer/in gegen die Firma einen Anspruch auf Freistellung von dieser Pflicht.

h) Für jeden Fall eines schuldhaften Verstoßes gegen die hier vereinbarte (nachvertragliche) Verschwiegenheitspflicht verpflichtet sich der/die Arbeitnehmer/in, eine Vertragsstrafe in Höhe eines monatlichen Bruttogehalts zu zahlen. Schadensersatzansprüche des Arbeitgebers bleiben unberührt."

Wichtige Sicherheitsmaßnahmen

3. Juristische Sicherheit

Datenschutzerklärung

- Gestaltung von Datenschutzerklärungen

"Sie üben aufgrund Ihrer Aufgabenstellung eine Datenverarbeitende Tätigkeit im Sinne des Bundesdatenschutzgesetzes (BDSG) aus. Hierbei erhalten Sie Kenntnis von personenbezogenen Daten, d.h. von Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Gemäß § 5 BDSG ist es Ihnen untersagt, personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten oder zu nutzen. Gemäß § 5 BDSG verpflichten wir Sie, das Datengeheimnis zu wahren. Diese Verpflichtung besteht über das Ende der Tätigkeit in unserem Unternehmen hinaus. Wir weisen darauf hin, dass Verstöße gegen das Datengeheimnis nach § 44 in Verbindung mit § 43 Abs. 2 BDSG mit Freiheits- und Geldstrafe geahndet werden können."

Vielen Dank für Ihre Aufmerksamkeit!

Stefan Schreiber
CMS Hasche Sigle
T 0341/21672-161
F 0341/21672-134
E Stefan.Schreiber@cms-hs.com
cms.law

CMS bloggt und twittert.

Aktuelle Rechtsthemen und was eine Großkanzlei sonst bewegt unter

cmshs-bloggt.de

folgen Sie uns auf Twitter:

@CMS_HascheSigle

und holen Sie sich unsere App:

C/M/S/ Law-Now™

Law . Tax

Ihr kostenloser juristischer Online-Informationsdienst.

E-Mail-Abodienst für Fachartikel zu vielfältigen juristischen Themen.
www.cms-lawnow.com

C/M/S/ e-guides

Law . Tax

Ihre juristische Online-Bibliothek.

Profunde internationale Fachrecherche und juristisches Expertenwissen nach Maß.
eguides.cmslegal.com
