# Compliance und Exportkontrolle im elektronischen Geschäftsverkehr

*Überblick über besondere Rechtsfragen des Cloud Computing*

*Von Rechtsanwalt Prof. Dr. Christoph Graf von Bernstorff, Ahlers & Vogel Bremen*

*Die AW-Prax hat sich in mehreren Beiträgen mit Grundsatzfragen des elektronischen Geschäftsverkehrs von KMU befasst und dabei auch auf spezifische Anforderungen des Cloud Computing (AW-Prax 2014, 26 ff. und 60 ff.) hingewiesen. Von besonderem Interesse ist in diesem Zusammenhang noch der Aspekt von Compliance im elektronischen Geschäftsverkehr, die im vorliegenden Beitrag behandelt wird.*

## Grundlage von Compliance

Compliance ist sehr komplex. Der Verantwortungs- und Handlungsrahmen von Geschäftsleitung und Unternehmen, der durch zivilrechtliche, öffentlichrechtliche, steuer-, zoll- und außenwirtschaftliche Pflichten bestimmt wird und aus dem sich eine Vielzahl von Rechtsrisiken ergeben, zwingt Unternehmen dazu, präventiv tätig zu werden: So müssen sie die aus ihren Geschäftsaktivitäten erwachsenden Risiken richtig erkennen, einschätzen, analysieren und sie müssen wissen, mit welchen Maßnahmen, Instrumenten und Produkten diese Risiken bewältigt werden können. Dabei kann die Geschäftsleitung von Unternehmen nicht einfach darauf vertrauen, dass sich die Organisation des Unternehmens ordnungsgemäß und regelkonform verhält, sondern es muss erkannt werden, dass Compliance Chefsache ist.

Compliance versteht sich als Weg zur *Risikovorbeugung und Schadensabwehr* für das Unternehmen, mit der

- Schadensersatzansprüche Dritter gegen das Unternehmen (*Außenhaftung*)
- wie auch Ansprüche des Unternehmens gegen die Mitglieder des Geschäftsleitungs- und des Aufsichtsorgans (*Innenhaftung*)

abgewehrt oder vermieden werden können.

Im Hinblick auf die Innenhaftung ist dies von besonderer Bedeutung, da

- in einer AG nach § 93 Abs.2 Satz 2 AktG die *Mitglieder des Vorstands* die Beweislast dafür tragen, dass sie bei ihrer Vorstandstätigkeit die

notwendige Sorgfalt beachtet haben.

- Für *GmbH-Geschäftsführer* gilt dieses Prinzip – trotz fehlender und entsprechender Regelung im GmbH-Gesetz – seit einer BGH-Entscheidung aus dem Jahr 2002 entsprechend.

Schließlich hat Compliance die Aufgabe, im Rahmen eines *Risikomanagement* Risiken frühzeitig zu erkennen und durch Überwachungsmaßnahmen möglichst ganz auszuschalten. Compliance dient daher vorrangig der Prävention, erstreckt sich aber für den Fall von Regelverstößen auch auf das Krisenmanagement im Unternehmen, das weitere Schäden verhindern soll.

- So sagt für die AG der § 91 Abs. 2 AktG ausdrücklich: „*Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.*“
- Der Governance Kodex 2013 lautet dazu in Ziffer 4.1.4.: „Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.“
- Auch hier wird – mangels entsprechender Bestimmungen für die GmbH – eine Analogie zur AG gezogen, sodass entsprechende Pflichten auch bei der GmbH-Geschäftsführung gesehen werden.

Allgemeine gesetzliche Sorgfaltspflichten in der AG finden sich in § 93 AktG: „Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die *Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters* anzuwenden.“

Diese Bestimmungen finden sich wörtlich identisch für die Geschäftsführer der GmbH in § 43 GmbHG wieder.

## Compliance-Pflichten im elektronischen Geschäftsverkehr

Schon diese beiden Normen sind Grundlage dafür, dass Vorstände und Geschäftsführer geeignete organisatorische Maßnahmen treffen müssen, um „Compliance“ zu erfüllen. Compliance ist Chefsache.

Im Rahmen der Geschäftstätigkeit über Internet oder der Verlagerung von Geschäften und Daten in eine Business Cloud enthält Compliance vor allem die nachfolgend genannten Pfichtbereiche.

*Organisationspflichten*

Die Geschäftsleitung hat Organisationspflichten, um alle die Gesellschaft gefährdenden Entwicklungen und Risiken im Zusammenhang mit der Busines Cloud zu erkennen, zu analysieren und auszuschließen.

*Problematik ausländischer Dienstleister*

Erfolgt eine Unterstützung durch *US-amerikanische Cloud-Dienstleister,* kann es erforderlich sein, Urkundenbeweise noch vor Prozessbeginn an den Prozessgegner auszuhändigen (pre-trial discovery). Daher gehört es zu Compliance gerechtem Verhalten, dass mit Cloud-Anbietern vertragliche Vereinbarungen darüber getroffen werden, innerhalb welcher (kurzen) Frist Datenmaterial zur Verfügung gestellt werden muss.

*Steuerrechtliche Pflichten*

Die Nutzung eines Cloud-Anbieters im Ausland ist problematisch, wenn steuerrechtliche relevante Daten (auch im Rahmen beispielsweise einer Zollabwicklung) in einer Cloud ver- oder bearbeitet werden sollen.

So fordert § 146 Abs. 2 der Abgabenordnung (AO), dass „Bücher und sonstige erforderliche Aufzeichnungen im Inland zu führen und aufzubewahren“ sind. Wer also beispielsweise seine Zollabwicklung über ein Internetportal eines Dienstanbieters („in einer Cloud“) vornimmt, muss einen inländischen Diensteanbieter nutzen. Ausnahmsweise lässt allerdings § 146 Abs. 2 a AO zu, dass die zuständige Finanzbehörde auf schriftlichen Antrag des Steuerpflichtigen bewilligen kann, dass die elektronischen Aufzeichnungen in einem anderen EU-Land bearbeitet und aufbewahrt werden.

Selbst die Verlagerung der elektronischen Buchführung in das übrige Ausland wäre grundsätzlich möglich, wie sich aus § 146 Abs. 2 Satz 5 AO ergibt, doch kann die zuständige Finanzbehörde dies nur bewilligen, wenn die Besteuerung hierdurch nicht beeinträchtigt wird – dies dürfte daher den Weg in Nicht-EU-Ausland letztlich doch versperren.

So sollte sich auch dieser Aspekt im Cloud-Vertrag wiederfinden: Betrifft die Cloud-Dienstleistung (auch) steuerrechtlich relevante Daten, soll die Cloud-Dienstleistung nur im Inland oder nur innerhalb der EU erbracht werden dürfen.

Auch bei steuerrechtlich relevanten Daten gilt, was schon zur pre-trail discovery gesagt wurde: Der Steuerpflichtige ist nach § 147 Abs. 5 und 6 AO verantwortlich dafür, dass notwendige Daten *unverzüglich* an die Finanzbehörde herausgegeben werden können.

*Handelsrechtliche Buchführungspflicht*

Für Kaufleute gilt nach § 238 HGB hinsichtlich ihrer steuerrechtlichen Buchführungspflicht Folgendes:

(1) „Jeder Kaufmann ist verpflichtet, Bücher zu führen und in diesen seine Handelsgeschäfte und die Lage seines Vermögens nach den Grundsätzen ordnungsmäßiger Buchführung ersichtlich zu machen. Die Buchführung muss so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann. Die Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung verfolgen lassen.

(2) Der Kaufmann ist verpflichtet, eine mit der Urschrift übereinstimmende Wiedergabe der abgesandten Handelsbriefe (Kopie, Abdruck, Abschrift oder sonstige Wiedergabe des Wortlauts auf einem Schrift-, Bild- oder anderen Datenträger) zurückzubehalten.“

Nach § 257 Abs. 4 Nr. 4 HGB müssen Bücher und Belege zehn Jahre aufbewahrt werden. Die Aufbewahrung ist, wie sich aus § 257 Abs. 3 HGB ergibt, auch elektronisch möglich. Wenn Daten in eine Business Cloud ausgelagert werden, bedürfen sie daher eines Archivierungssystems, dass diese 10-Jahres-Regel erfüllt und erforderliche Daten jederzeit verfügbar und innerhalb angemessener Frist lesbar macht. Da-

mit ist klar, dass der Cloud-Vertrag auch hierzu einer Regelung bedarf.

## Exportkontrolle

Das Auslagern von Daten in eine Cloud wird meist aus Sicht der datenschutzrechtlichen Herausforderungen diskutiert. Kaum beachtet wird dagegen der Umstand, dass beim Cloud Computing auch die Grundregeln des Exportkontrollrechts zu beachten sind. Dieses muss nämlich nicht nur beachtet werden, wenn

- der *Export von Gütern* ins Ausland erfolgt,
- sondern auch, wenn ein grenzüberschreitender *Transfer von Daten* geschieht. Hierbei ist es unerheblich, ob Daten ins Ausland ausgelagert werden oder ob vom Ausland aus auf Daten zugegriffen wird.

*Cloud-Daten und Exportkontrolle*

Daher erfasst das Exportkontrollrecht vom Grundsatz her auch das Cloud Computing, wenn ein Unternehmen Daten an einen Cloud-Anbieter im Ausland auslagert oder seinen Mitarbeitern an internationalen Standorten von dort aus den Zugriff auf Daten gestattet.

Es kann auch unbemerkt zu Datenexporten kommen, ohne dass ein solcher im exportkontrollrechtlichen Sinn beabsichtigt war. Das könnte schon dann der Fall sein, wenn das Cloud-Computing-Netzwerk in einem Drittland gespeicherte sensible Daten dem Zugriff ausländischer Mitarbeiter des Cloud Anbieters aussetzt.

Umgehen ließe sich diese Problematik nur, wenn alle in Clouds transferierten, dort gespeicherten und über Clouds veränderten und aus Clouds exportierte veränderte oder unveränderte Daten jeder Art *verschlüsselt* würden und die Entschlüsselungstechnik nur solchen Adressaten zugänglich gemacht wird, die exportkontrollrechtlich überprüft sind, als unbedenklich eingestuft wurden und sich einer umfänglichen Sicherheitscompliance unterworfen haben.

Das Auslagern von Daten beim Cloud Computing kann daher im Einzelfall eine Genehmigung erfordern oder sogar ganz verboten sein. Ob Beschränkungen gelten und zu beachten sind, richtet sich nach dem Inhalt der Daten oder dem Empfängerland.

Enthalten die Daten Informationen zur Herstellung von sensiblen Gütern, ist ihr Export genehmigungspflichtig. Sensible Daten sind dabei nicht nur Daten aus der Rüstungsindustrie, sondern viele auch harmlos wirkende Daten, die auch militärisch nutzbar sein könnten (dual use Daten). Die aus der Exportkontrolle von Gütern bekannten Beispiel hierfür sind die Bereiche Telekommunikation, Elektrotechnik, Chemie und Schiffstechnik.

Ist Zielort von Daten ein Embargoland, sind schon allein aus diesem Grund die Datenverlagerung beziehungsweise der Datenexport nach dort untersagt. Da Daten von allen Unternehmen in eine Cloud verlagern werden könnten – also nicht nur von Exporteuren -, sollte es sich jeder Unternehmer, der eine Datenauslagerung in eine ausländische Cloud beabsichtigt, grundsätzlich prüfen, ob das Exportkontrollrecht Anwendung findet oder nicht, um hohe Sanktionen (Bußgelder oder Freiheitsstrafen) zu vermeiden. In Zweifelsfällen kann auch das BAFA befragt werden.

| **Risikofelder und erforderliche Maßnahmen im Cloud Computing aus Sicht der Exportkontrolle** | |
|---|---|
| Risikofelder | Die Cloud-Infrastruktur befindet sich in verschiedenen Staaten mit unterschiedlichen Datenschutz- und Sicherheitsniveau.<br><br>Datenauslagerung aus der Cloud führt dazu, dass Staaten mit der Cloud-Infrastruktur in Berührung kommen, die aus Sicht der Exportkontrollkriterien nicht mit sensiblen Daten in Berührung kommen dürften.<br><br>Öffentliche Clouds sind jedermann zugänglich und daher aus Sicherheitsüberlegungen kritisch zu betrachten. Private Clouds mit geschütztem Zugang können dagegen eine Verpflichtung zur Wahrung von Exportkontrollrechtsbestimmungen übernehmen. |
| Risiko-maßnahmen | Gründliche Überprüfung des Cloud-Anbieters im Hinblick auf die Einhaltung von<br>• Compliancekriterien<br>• Datenschutzbestimmungen und<br>• Exportkontrollaspekten.<br><br>Werden Exportlizenzen für den Datentransfer in die Cloud benötigt? Genügt ein Verschlüsseln der Daten vor Transfer, Ver- oder Bearbeitung von Daten in der Cloud?<br><br>Stellt der Cloud-Anbieter sicher, dass der Zugriff auf in der Cloud abgelegte Daten durch sanktionierte Staaten, Institutionen und Personen blockiert ist? Kann der Cloud-sAnbieter damit volle Datensicherheit ohne Zugriffsmöglichkeit von unberechtigten Dritten garantieren? |