# Dr. Christian Halm

**Fachanwalt für Agrarrecht**

Fachanwalt für Versicherungsrecht

Fachanwalt für Verwaltungsrecht

Agrarmediator

## Datenschutz 27.10.2015 Berlin



Bildnachweis: Dr. Christian Halm

# Datenhoheit in der Landwirtschaft

**Frage:**

**Reichen die Rechtsgrundlagen aus, um die Datenhoheit landwirtschaftlicher Betriebe im Internetzeitalter zu sichern?**

# Wie wird geworben?

## Werbung

Telemetriesyteme , Ackerschlagdateien, und andere Datenerfassungssysteme erfassen nach und nach nahezu alle Betriebsdaten eines landwirtschaftlichen Betriebs.

Die Datenspeicherung erfolgt dabei nur zum Teil mit Wissen und Wollen des Betriebsinhabers. Die Weitergabe der Daten dürfte weitgehend ohne den Willen des Betriebsinhabers erfolgen.

Nach der Rechtsprechung des Bundesverfassungsgerichts besteht ein Recht auf informationelle Selbstbestimmung (BVerfGE 65, 1).

D.h. der Bürger hat die Möglichkeit selbst über die Erhebung und Nutzung seiner Daten zu entscheiden.

Die zunehmende Technisierung soll

- die Effizienz des Maschineneinsatzes erhöhen
- Daten für die Betriebsführung liefern

was in einem immer härteren Wettbewerb sicherlich sinnvoll ist.

Problem:

Während der Bearbeitung landwirtschaftlicher Flächen erhalten Dritte Kenntnis von betriebsspezifischen Daten.

So besteht über Sensoren die Möglichkeit der Georeferenzierung (Zuweisung raumbezogener Informationen zu einem Datensatz). Gleichzeitig besteht die Möglichkeit der Datenspeicherung.

## Daten

- Name und Adresse des Landwirts
- Standort der bewirtschaften Fläche
- Größe der bewirtschafteten Fläche
- Zeitpunkt der Einsaat
- Art der Einsaat
- Zeitpunkt und Umfang der Düngung/Pflanzenschutzmaßnahmen
- Erntezeitpunkt

## Daten

- Erntemenge und Qualität (künftig:

  Proteingehalt, Erfassung von Mykotoxinen etc.)
- Transportzeiten
- Ort der Einlagerung
- Ziel der Einlagerung
- Zeitpunkt der Vermarktung

Frage:

Inwieweit dürfen personen- und/oder flächenbezogende Daten

**Erhoben**

**Gespeichert**

**Weitergegeben**

werden?

Wer hat Interesse an den Daten:

- Der Landwirt
- Der Lohnunternehmer
- Der Landmaschinenhändler
- der  Maschinenring

- Der Landhandel
- Die Politik
- die Wirtschaft
- der Anbieter des Cloud

Welche Rolle kann der Landwirt haben:

- Maschinenbediener
- Maschineneigentümer
- Instandhalter der Maschine
- Grundstückseigentümer
- Grundstückspächter

Problem:

Das Bundesdatenschutzgesetz schützt nur personenbezogene Daten.

D.h. Betriebs- und Geschäftsdaten ohne Personenbezug sind nicht geschützt.

## Rechte nach dem BDSG:

Anspruch auf:

- Auskunft
- Berichtigung
- Löschung
- Sperrung

Ziele des Datenschutzes:

- Rechtmäßigkeit
- Einwilligung
- Zweckbindung
- Erforderlichkeit
- Datensparsamkeit

- Transparenz
- Betroffenenrechte
- Datensicherheit
- Kontrolle

Gefahren der unkontrollierten Datenerfassung:

- Zugriff auf personenbezogene Daten
- Zugriff auf flächenbezogene Daten
- Zugriff auf Daten zur Menge und Qualität der Ernte
- Zugriff auf Dauer und Intensität der Maschinennutzung

d.h.

Wer die Daten hat, hat einen

**Wissens- und Wettbewerbsvorteil**

Beispiel:

Maschine zum Kürzen von Hühnerschnäbeln

## 17.09.2015 Hannover

John Deere stellt drei neue selbstfahrende Feldhäcksler der Serie 8000 vor. Diese Maschinen sind mit modernster Futtererntetechnik ausgestattet.

Alle Modelle können außerdem mit HarvestLab ausgestattet werden, einem modernen Erntegutanalyse- und Dokumentationssystem, das über Inhaltsstoffbestimmung für verbesserte Futterqualität sorgt.

# 24.09.2015 **Smarter Wein mit Sensoren und Clouddiensten**

Berlin/Nürnberg - Das Internet der Dinge macht auch vor Weinbergen nicht mehr Halt. Winzer können künftig mit Hilfe von neuer Technologie, Sensoren und der Cloud das Wohl ihrer Reben überwachen.

Der Chipkonzern Intel hat dafür zusammen mit dem Nürnberger Technologieunternehmen MyOmega die Lösung «TracoVino» vorgestellt. Damit werden auf dem Weinberg die exakten Klimadaten erfasst, damit die Winzer stets überblicken können, welche Temperatur auf dem Gebiet herrscht. Die Winzer können auch sehen, wie es um die Luft- und Bodenfeuchtigkeit bestellt ist und wie stark die Sonne scheint.

Das Basisgerät mit dem Namen «MyNeXt Generation» (oder kurz «MYNXG») verbindet Sensornetzwerke, Smartphones, Netzwerkelemente des Mobilfunks und die Cloud. Optional misst das Gerät auch Blattfeuchte sowie den PH-Wert und andere Nährstoffe im Boden.

Praktischer Nutzen auch für Dritte:

- Möglichkeit der Spekulation durch gesicherte Prognosen zur Ernte
- Einfluss auf Agrar- und Nahrungsmittelpreise,
- Gezielte Steuerung von Investitionen

z.B. Landkauf und Beteiligung im Zeiten der Krise

Problem:

Welchen Einfluss hat der Landwirt, wenn der Maschinenhersteller oder der Programmierer die Daten einfach ohne Zustimmung sendet.

Welche Folgen hat es, wenn die Industrie im Rahmen der Qualitätssicherung die lückenlose Dokumentation verlangt.

## Möglichkeiten des Landwirts:

Kein Kauf von Landmaschinen, die Daten an den Dritte (zentrale Server) weiterleiten

Keinen Auftrag an Dienstleister, die solche Technik einsetzten.

Verzicht auf die Nutzung der Cloud oder

Versendung von verschlüsselten Daten.

# Rechtsgrundlagen im Datenschutz

Welche Rechtsordnung ist anwendbar:

Internationales Recht

EU-Recht

Nationales Recht (z.B. Art. 10 GG Brief- Post und Fernmeldegeheimnis)

- Postgesetz
- BDSG
- LDSG
- Telemediengesetz (Internetdienste, Webseiten)
- Telekommunikationsgesetz (Übertragung von Daten mittels Mobilfunk)
- StGB (insbes. § 203, 206 StGB)

**§ 1 BDSG**

**Zweck und Anwendungsbereich des Gesetzes**

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Grundsätzlich gilt nach dem BDSG:

Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten ist verboten.

Ausnahme:

- Eine Rechtsvorschrift erlaubt die Datennutzung
- Der Betroffene hat eingewilligt (§ 4 BDSG)

Die Daten dürfen nur zu einem bestimmten Zweck genutzt werden (§ 28 BDSG).

Es dürfen nur Daten verarbeitet werden, die zur Erreichung des Zweckes erforderlich sind.

**§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke**

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

D.h. personenbezogene Daten dürfen verarbeitet werden, wenn sie zur Vertragserfüllung erforderlich sind.

z.B. Lohnunternehmer erfasst die Daten des Auftragsgebers zur Abrechnung seiner Leistungen.

**Maschinendaten:**

§ 3 BDSG erfasst nur personenbezogende Daten, d.h. Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person,

jedoch keine Maschinendaten.

Aber:

Maschinendaten können zu personenbezogenen Daten werden, wenn sich darauf Rückschlüsse etwa auf das Verhalten einer Person ziehen lassen.

Beispiel:

Sensorendaten über Beschleunigung, Geschwindigkeit, Spritverbrauch, Lage sagen auch etwas über den Fahrer und/oder Auftraggeber aus.

Dies gilt nicht, wenn die Daten nicht mit den Daten des Nutzer der Maschine verbunden werden.

**Auftragsdaten:**

Die Verarbeitung von Daten, die zur Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich sind, ist gem. § 28 Abs. 1 BDSG zulässig.

**Auftragsdurchführung:**

Die Datenverarbeitung im Rahmen der Auftragsdurchführung ist gem. § 28 Abs. 1 BDSG zulässig, nicht aber eine darüber hinausgehende Nutzung der Daten.

z.B.: Erhebung von Geoinformationen.

**Auftragsabrechnung und –abwicklung:**

Nach Erfüllung des Auftrags sind die personenbezogenen Daten zu löschen, sofern keine gesetzliche Aufbewahrungspflicht (z.B. 10 Jahre nach AO) besteht.

**Einbindung Dritter/Datenübermittlung:**

Personenbezogene Daten dürfen nur mit Einwilligung des Betroffenen oder auf einer Rechtsgrundlage übermittelt werden.

# Der Schutz des Geschäftsgeheimnisses nach dem StGB

**§ 203 Verletzung von Privatgeheimnissen**

(1)Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1.Arzt, …,

2.Berufspsychologen …,

3.Rechtsanwalt …,

…

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1.Amtsträger,

2.für den öffentlichen Dienst besonders Verpflichteten,

5.öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind.

# Gesetz gegen den unlauteren Wettbewerb (UWG)

## § 17 UWG - Verrat von Geschäfts- und Betriebsgeheimnissen

(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen,

1.sich ein Geschäfts- oder Betriebsgeheimnis durch

a)Anwendung technischer Mittel,

b)Herstellung einer verkörperten Wiedergabe des Geheimnisses oder

c)Wegnahme einer Sache, in der das Geheimnis verkörpert ist,

unbefugt verschafft oder sichert oder

2.ein Geschäfts- oder Betriebsgeheimnis, das er durch eine …Mitteiliung oder durch eine eigene oder fremde Handlung erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1.gewerbsmäßig handelt,

2.bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder

3.eine Verwertung nach Absatz 2 Nummer 2 im Ausland selbst vornimmt.

# Die Cloud

Ziel:

- Serviceplattformen für Landwirte,

  Lohnunternehmer, Maschineringe etc.

- Bessere Rückverfolgbarkeit von Agrarprodukten

-Absicherung der Daten

Aber auch den riesiger Datenpool

Vorteil:

Zugriff auf einen zentralen Server zur Steuerung der Maschinen oder zur Verwaltung der Flächen.

Nachteil:

Zentral kann für jeden einzelnen Landwirt verfolgt werden auf welche Flächen er welche Qualität erntet oder wieviel Milch produziert wird, wie viele Schweine geschlachtet wurden, wie viele Eier gelegt wurden etc..

Daraus folgt ein Insiderwissen, das z.B. die Lebensmittelindustrie gegen die Landwirtschaft ausspielen kann.

Folgen:

Das Wissen des Landwirts und des lokalen Händlers um regionale Produktivität und Produktion geht an Dritte über.

Investitionen können so gezielt gesteuert werden, um den Markt zu manipulieren.

Problem:

Landtechnikhersteller können ihre Maschinen so einrichten, dass Aufträge nur noch über die Cloud abgewickelt werden können.

Der Lebensmittelhandel verlangt im Rahmen einer Qualitätsüberwachung die Hinterlegung der Daten.

Dem Landwirt bliebt zur Zeit nur der Boykott cloudgestützer Systeme, was jedoch zu wirtschaftlichen Nachteilen führen wird.

Wer hat Interessen an den Daten:

- Flächenbewirtschafter
- Flächeneigentümer
- Maschineneigentümer
- Maschinenbediener

- Maschinenhersteller
- Maschineninstandhalter
- Netzbetreiber
- Lohnunternehmer
- Labore
- Behörden
- Arbeitgeber

- Arbeitnehmer
- Sozialversicherungsträger
- Berufsgenossenschaft
- Tarifpartner
- Auftraggeber
- Auftragnehmer
- Das Finanzamt

Welche Daten werden gesammelt:

- Arbeitszeit Bediener
- Aufenthaltsort Arbeitskraft
- Tätigkeit
- Fehlzeiten
- Ertragsdaten
- Qualitätsmerkmale

- Betriebsmittel (Art und Menge)
- Räumliche und zeitliche Bewirtschaftungsdaten
- Bodeneigenschaften
- Nutzungsauflagen (Bio)
- Geschäftsbeziehung
- Wetterdaten

Für derartige elektronische Informations- und Kommunikationsdienste gelten die Datenschutzregeln der §§ 11-15 Telemediengesetz.

Gem. § 11 TMG gilt das Gesetz für alle Datenerhebungen mit Ausnahme von Dienst- und Arbeitsverhältnissen sowie die Steuerung von Arbeits- und Geschäftsprozessen.

Der Cloudanbieter ist verpflichtet die Daten nur im Rahmen des Auftrags zu nutzen.

Eine Kontrolle ist jedoch kaum möglich.

Von Seiten der Landwirtschaft wird auf die Datenhoheit bislang kein Wert gelegt.

Beachte:

Alle Datenschutzregelung betreffen nur die personenbezogenen Daten.

Die Erfassung und Nutzung nicht personenbezogener Daten ist zulässig. Hier liegt die größere Gefahr für die Zukunft, da so das gesamte Agribusiness manipuliert werden kann.

Zur Zeit bleibt nur die Hoffnung

auf einen besseren Schutz der Daten

Das EU-Parlament hat am 14.04.2016 die Richtlinie für den Schutz von Geschäftsgeheimnissen verabschiedet.

Diese ist am 05.07.2016 in Kraft getreten.

Der deutsche Gesetzgeber muss nun bis zum 05.07.2018 das geltende Recht zu reformieren.

## Geschäftsgeheimnisse

Geschäftsgeheimnisse sind **Know-how und Geschäftsinformationen**, die (Art. 2 Abs. 1)

- geheim sind,

- von kommerziellem Wert sind, weil sie geheim sind, und

der rechtmäßige Inhaber des Geschäftsgeheimnisses durch Geheimhaltungsmaßnahmen schützt.

**Keine Geschäftsgeheimnisse** sind **Erfahrungen und Fähigkeiten**, die Mitarbeiter redlich im Rahmen ihres regulären Beschäftigungsverhältnisses erworben haben (Art. 2 Abs. 1).

# Rechtswidrige Erlangung

Die Erlangung eines Geschäftsgeheimnisses ist rechtswidrig, wenn

- der rechtmäßige Inhaber nicht zugestimmt hat und
- die Erlangung keine anständige Gepflogenheit in Gewerbe und Handel darstellt.

Eine anständige Gepflogenheit in Gewerbe und Handel liegt vor, wenn ein rechtmäßig erworbenes Produkt untersucht, zerlegt oder getestet wird, **außer der Rechtsverletzer** hat sich **vertraglich verpflichtet,** das **Geschäftsgeheimnis nicht aufzudecken.**

## Rechtswidrige Nutzung oder Offenlegung

Die Nutzung oder Offenlegung eines Geschäftsgeheimnisses ist rechtswidrig, wenn

der rechtmäßige Inhaber nicht zugestimmt hat und

der Rechtsverletzer das Geschäftsgeheimnis vorher rechtswidrig erlangt hat oder durch die Nutzung oder Offenlegung eine vertragliche oder gesetzliche Pflicht verletzt.

## Rechtswidrige Nutzung oder Offenlegung

Die **Erlangung**, Nutzung oder Offenlegung eines Geschäftsgeheimnisses ist außerdem rechtswidrig, wenn der Rechtsverletzer wusste oder hätte wissen müssen, dass die Person, die ihm das Geschäftsgeheimnis mitgeteilt hat **oder eine andere Person vor ihr**, dieses selbst rechtswidrig nutzte oder offenlegte.

## Rechtswidrige Nutzung oder Offenlegung

Die Nutzung eines Geschäftsgeheimnisses ist rechtswidrig, wenn der Rechtsverletzer Produkte, die in erheblichem Umfang auf durch eine Rechtsverletzung erlangten Geschäftsgeheimnissen basieren, herstellt, anbietet oder vermarktet oder zu diesen Zwecken importiert, exportiert oder lagert und **wusste oder hätte wissen müssen,** dass er dadurch das Geschäftsgeheimnis rechtswidrig genutzt wurde.

## Rechtmäßige Erlangung, Nutzung oder Offenlegung

Keine Rechtsverletzung liegt vor, wenn durch die Erlangung, Nutzung oder Offenlegung ein **durch EU-Gesetze, nationale Gesetze oder gerichtliche Praxis anerkanntes „Allgemeinwohl“ oder anderes „legitimes Interesse“**geschützt wird

## Rechtsschutz bei gerichtlich festgestellten Rechtsverletzungen

Die Gerichte können die Beseitigung der Rechtsverletzung anordnen, indem sie

- die (weitere) Nutzung oder Offenlegung des Geschäftsgeheimnisses verbieten,

- die **Herausgabe** an den rechtmäßigen Inhaber oder die **Vernichtung** aller oder Teile der **physischen und elektronischen Datenträger, die das Geschäftsgeheimnis enthalten**, verlangen und

## Rechtsschutz bei gerichtlich festgestellten Rechtsverletzungen

- im Falle rechtsverletzender Produkte deren Herstellung, Angebot, Vermarktung und Nutzung sowie Import, Export oder Lagerung zu diesen Zwecken verbieten sowie den Rechtsverletzer auffordern, Maßnahmen zur Beseitigung der Rechtsverletzung zu ergreifen, z.B. die Dokumente oder Datenträger, die das Geschäftsgeheimnis enthalten, an den rechtmäßigen Inhaber herauszugeben oder zu vernichten.

## Rechtsschutz bei gerichtlich festgestellten Rechtsverletzungen

Anstelle der Beseitigung der Rechtsverletzung kann **jede Partei** in Ausnahmefällen beantragen, dass der Rechtsverletzer einen „finanziellen Ausgleich“ an den rechtmäßigen Inhaber zahlt.

## Rechtsschutz bei gerichtlich festgestellten Rechtsverletzungen

Neben der Beseitigung der Rechtsverletzung bzw. dem „finanziellen Ausgleich“ muss der Rechtsverletzer dem rechtmäßigen Inhaber Schadensersatz zahlen, wenn er wusste oder hätte wissen müssen, dass er rechtswidrig handelte

## Vorläufiger Rechtsschutz

Weist ein rechtmäßiger Inhaber nach, dass ein Rechtsverletzer **mit hinreichender Sicherheit** auf seine Kosten eine Rechtsverletzung begangen hat oder zu begehen droht, können die Gerichte insbesondere die (weitere) Nutzung oder Offenlegung des Geschäftsgeheimnisses vorübergehend verbieten und rechtsverletzende Produkte beschlagnahmen.

## Allg. Anforderungen an das Gerichtsverfahren

Die Gerichte sollen die Geschäftsgeheimnisse, die durch das Gerichtsverfahren bekannt werden könnten, schützen. Insbesondere dürfen sie auf Antrag einer Partei oder **auf eigene Initiative**

## Allg. Anforderungen an das Gerichtsverfahren

- Personen die Einsicht in im Verfahren vorgelegte Dokumente verwehren; jedoch muss **mindestens eine Person jeder Partei und – falls im Hinblick auf das Verfahren angemessen – ihr Rechtsvertreter volle Einsicht** in die Dokumente **erhalten**;

## Allg. Anforderungen an das Gerichtsverfahren

Personen von im Verfahren stattfindenden Anhörungen ausschließen; jedoch muss **mindestens eine Person jeder Partei und – falls im Hinblick auf das Verfahren angemessen – ihr Rechtsvertreter** an der Anhörung **teilnehmen dürfen**.

## Allg. Anforderungen an das Gerichtsverfahren

Die Gerichte sollen gegen ungerechtfertigte Klagen vorgehen, die ein vermeintlich rechtmäßiger Inhaber erhebt, um einem vermeintlichen Rechtsverletzer zu schaden. Sie **können** insbesondere die Möglichkeit erhalten, Sanktionen, auch in Form von Geldbußen, gegen den vermeintlich rechtmäßigen Inhaber zu verhängen.

## Safe-Harbor-Abkommen:

Safe Harbor regelt seit dem Jahr 2000 die gewerbliche Datenübermittlung zwischen der EU und den USA. US-Unternehmen können sich dabei selbst bescheinigen, dass sie sich an die Datenschutzbestimmungen der EU halten.

Das Safe-Harbor-Abkommen zwischen der EU und den USA erlaubt es europäischen Unternehmen und den europäischen Tochtergesellschaften amerikanischer Firmen, personenbezogene Daten in die Vereinigten Staaten zu übermitteln. Der EU-Datenschutzrichtlinie von 1995 zufolge dürfen personenbezogene Daten nur dann in andere Länder übermittelt werden, wenn die Informationen dort ausreichend geschützt werden. Es ist Aufgabe der EU-Kommission, darüber zu entscheiden, ob andere Länder dieses Schutzniveau garantieren können.

Das Urteil des EuGH zu facebook könnte erhebliche Auswirkungen haben. Rund 5.500 US-Unternehmen speichern europäische Kundendaten in den Vereinigten Staaten. In seinem Schlussantrag hatte Generalanwalt Yves Bot die Meinung vertreten, dass US-amerikanische Geheimdienste wie die NSA nahezu uneingeschränkt auf Nutzerdaten zugreifen können, die Unternehmen auf dortigen Servern speichern.

Allerdings bestehe eine faktische Übergangsregelung. Der EuGH hat auch entschieden, dass nur er selbst eine Entscheidung der EU-Kommission für ungültig erklären kann. Bis also ein entsprechendes Verfahren zum EuGH kommt, bleiben die Standardvertragsklauseln weiter gültig.

Die Zeit bis dahin muss genutzt werden, um die Politik auf das Problem des Datenschutzes in der Landwirtschaft aufmerksam zu machen. Die wirtschaftliche Folgen des Datenverlustes können sich auf den gesamten Handel und die Versorgungslage in Europa nachhaltig auswirken und über Jahrzehnte gewachsene Strukturen in nur wenigen Jahren zerstören.

**Die Antwort zur Eingangsfrage:**

**Nein !**

## Kontakt

Rechtsanwalt Dr. Christian Halm

RAe Halm & Preßer

Lutherstraße 14

66538 Neunkirchen

Telefon: 06821 92100

Fax: 06821 921050

E-Mail: dr.halm@halm-presser.de

www.agrarjurist.de

## Sie können auch abwarten ...

**bis sich die Beauftragung eines spezialisierten Rechtsanwalts nicht mehr lohnt !**