ADDITIV-GENERATIVE FERTIGUNG

IT-Sicherheitsrecht

In Kooperation mit:

3D Druck und Recht

AGENT3D
ADDITIV GENERATIVE FERTIGUNG

INHALT

Einleitung

Die **additiv-generative Fertigung (AgF)** als Industrie 4.0-Technologie stellt einen Paradigmenwechsel in der Fertigung individualisierter Produkte dar. Die Vorteile der AgF sind zahlreich: z. B. Rückverlagerung der Produktion nach Deutschland; funktionsangepasste, individualisierte Produkte, die nachfrageorientiert, zentral oder dezentral hergestellt werden können; Ressourceneffizienz und eine neue Designfreiheit.

Damit diese Vorteile nutzbar gemacht werden können und Deutschland als Leitanbieter der additiv-generativen Fertigung im Weltmarkt positioniert werden kann, müssen die rechtlichen Rahmenbedingungen stimmen. Als Zukunftstechnologie berührt die AgF viele Rechtsbereiche, wobei insbesondere das Urheber- und Patentrecht, aber auch das Vertrags- und Wettbewerbsrecht, Produkthaftungs- und Produktsicherheitsrecht sowie das Datenrecht vor neue Herausforderungen gestellt werden.

Diese Broschüre soll einen Einblick in die Forschungsergebnisse zum IT-Sicherheitsrecht geben und darstellen, welche Regelungen für Unternehmen aus dem Bereich der AgF maßgeblich sind.

Stand: November 2017

Vertrags- und Wettbewerbsrecht

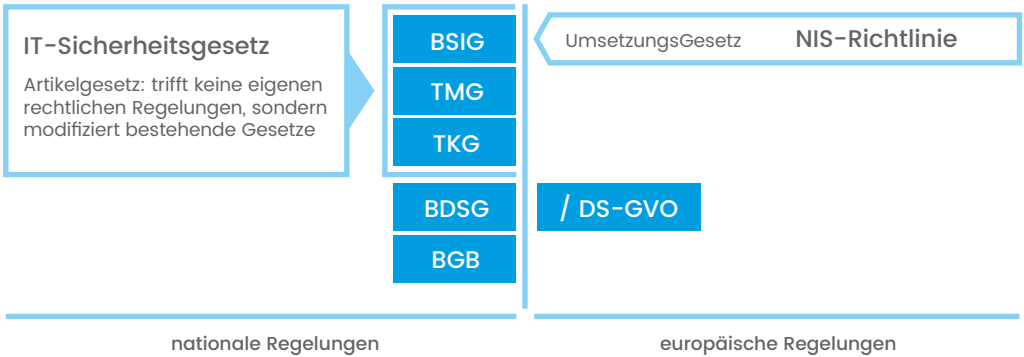
Urheber- und Patentrecht

AgF

Produkthaftung und -sicherheit

Datenschutz und IT-Sicherheit

Rechtsquellen des IT-Sicherheitsrechts



Vorschriften zur IT-Sicherheit finden sich in zahlreichen Gesetzen, wobei viele Regelungen erst im Jahr 2015 durch das IT-Sicherheitsgesetz eingeführt worden sind. Auf europäischer Ebene wurden 2016 Vorschriften zur IT-Sicherheit v. a. durch die Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Schutzniveaus von Netz- und Informationssystemen (kurz: NIS-Richtlinie) erlassen.

Spezielle Regelungen finden sich zwar auch in dem Atomgesetz (AtomG), dem Energiewirtschaftsgesetz (EnWG), für die AgF sind jedoch v. a. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG), das Bundesdatenschutzgesetz (BDSG) bzw. die Datenschutz-Grundverordnung (DS-GVO) und das Bürgerliche Gesetzbuch (BGB) maßgeblich.

Das IT-Sicherheitsrecht

Das IT-Sicherheitsrecht ist kein originäres Rechtsgebiet mit einem hauptsächlich einschlägigen Gesetzestext, wie z.B. das BGB für das Vertrags- und Deliktsrecht oder das StGB für das Strafrecht. Deshalb wird das IT-Sicherheitsrecht als Querschnittsmaterie bezeichnet.

Gemäß der Legaldefinition in § 2 Abs. 2 BSIG ist unter Sicherheit in der Informationstechnik (IT-Sicherheit) die Einhaltung bestimmter Sicherheitsstandards zu verstehen, welche die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

Dabei verlangt der Gesetzgeber nur eine relative – und keine absolute – Sicherheit, die sich an den konkreten Risikoanforderungen und den Sicherheitsstandards im Einzelfall orientiert.

Gesetz über das Bundesamt in der Informationstechnik (BSIG)

Anwendbarkeit BSIG

kritische Infrastrukturen (D/EU) (=wesentliche Dienste (EU)) § 2 Abs. 10

Sektoren

- Energie
- Informations- & Kommunikationstechnik
- Transport & Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- & Versicherungswesen
- Wasser

+

hohe Bedeutung für das Funktionieren des Allgemeinwesens

da Folge von Ausfall oder Beeinträchtigung
→ erheblicher Versorgungsengpass
→ Gefährung der öffentlichen Sicherheit

nähere Bestimmung gem § 10 Abs. 1 BSIG i.V.m. KRITIS-VOen

wenn gegeben, dann:

Pflichten gem. §§ 8a, 8b BSIG

digitale Dienste (D/EU)

§ 2 Abs. 11

Beispiele

- Cloud-Computing-Dienste
- Online-Suchmaschinen
- Online-Marktplätze

Einschränkung
Dienstanbieter darf kein Kleinst- oder kleines Unternehmen sein

Kleinstunternehmen:
< 10 Mitarbeiter und Jahresumsatz < 2 Mio. EUR

Kleines Unternehmen:
< 50 Mitarbeiter und Jahresumsatz < 10 Mio. EUR

wenn gegeben, dann:

Pflichten gem. § 8c BSIG

Anwendbarkeit in der additiv-generativen Fertigung

Sind Unternehmer aus dem Bereich der AgF Betreiber kritischer Infrastrukturen?

Um als Betreiber einer kritischen Infrastruktur zu gelten, muss das betriebene Unternehmen zu einem hohen Grad in das Gemeinwesen integriert sein, so dass durch dessen Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit drohen würden. Dies ist z.B. der Fall bei Ausfall der Strom- oder der Wasserversorgung oder der Beeinträchtigung eines Atomkraftwerks oder eines Krankenhauses. Dienstleistungen oder Gütern aus dem Bereich der additiven Fertigung kommt derzeit noch keine für das Gemeinwesen essentielle Bedeutung zu, denn die AgF-Technologien befinden sich im Vergleich zu traditionellen Fertigungsverfahren in einem Nischenbereich. Unternehmer aus dem Bereich der AgF sind derzeit i.d.R. keine Betreiber kritischer Infrastrukturen.

Sind Unternehmer aus dem Bereich der AgF Betreiber digitaler Dienste?

Versteht man als Unternehmer aus dem Bereich der AgF nur solche, die Produkte herstellen und vertreiben, und unabhängig von den auf AgF basierenden, möglichen Geschäftsmodellen, so wird man das Betreiben eines digitalen Dienstes wohl verneinen müssen. Das Geschäftsmodell CAD-Dateien zum 3D-Druck für den käuflichen Erwerb anzubieten, wobei der Vertragsschluss mit dem jeweiligen Anbieter direkt über eine Plattform erfolgen soll, ist als Online-Marktplatz i.S.d. § 2 Abs. 11 BSIG zu qualifizieren. Das Unternehmen, welches die Plattform betreibt wäre somit als digitaler Dienst mit den entsprechenden Pflichten gemäß § 8c BSIG anzusehen.

Anforderung an Anbieter digitaler Dienste

Pflichten

- Verpflichtung technisch-organisatorische Maßnahmen zu ergreifen, § 8c Abs. 1 Abs. 2 S. 1 BSIG
- Verpflichtung Sicherheitsvorfälle zu melden, § 8c Abs. 3 BSIG

Rechtsfolgen

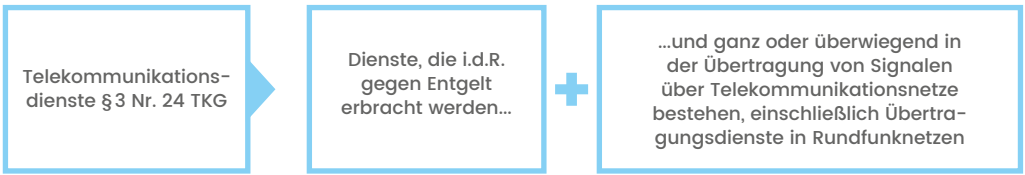
+	–
• Duldung von Überwachungsmaßnahmen durch das BSI gem. § 8c Abs. 4 • Anordnungsmöglichkeiten durch das BSI gem. § 8aq 3 S. 4 8b	• § 8c BSIG ist kein Schutzgesetz i. S. d. § 823 Abs. 2BGB

Welche Pflichten hat ein Unternehmen, wenn es einen digitalen Dienst anbietet?

Fällt ein Unternehmen unter die Legaldefinition des § 2 Abs. 11 BSIG und wird als Anbieter digitalen Dienstes qualifiziert, ist es gesetzlich verpflichtet technisch-organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der für die Bereitstellung des digitalen Dienstes genutzten Netz- und Informationssysteme zu bewältigen. Daneben besteht für die Anbieter digitaler Dienste, wie für die Betreiber kritischer Infrastrukturen, eine Meldepflicht von Sicherheitsvorfällen.


AA2835
AA2834
AA2839

Telekommunikationsgesetz (TKG)



Telekommunikationsdienste spielen für die Sicherheit im Cyberraum eine Schlüsselrolle. Das TKG richtet sich an die Anbieter von Telekommunikationsdiensten. Entsprechend der Legaldefinition des § 3 Nr. 24 TKG liegen Telekommunikationsdienste vor, wenn es sich um Dienste handelt, die in der Regel gegen Entgelt erbracht werden und ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich der Übertragung in Rundfunknetzen.

Anwendbarkeit in der additiv-generativen Fertigung

Sind Unternehmer aus dem Bereich der AgF Anbieter von Telekommunikationsdiensten?

Um als Anbieter von Telekommunikationsdiensten zu gelten, muss die Übertragung von Signalen über Telekommunikationsnetze (mit einem Schwerpunkt auf der technischen Übertragung) in das Leistungsspektrum eines Unternehmens fallen.

Unternehmen, die im Bereich der additiven Fertigungsverfahren tätig sind, decken in der Regel eine Bandbreite von Serviceleistungen ab, z.B. das Schreiben (spezieller) Software, das Design von CAD-Druckmodellen, die Herstellung des Druckgeräts, die Lieferung von Druckmaterialien, oder die Herstellung und der Vertrieb gedruckter Produkte, das Betreiben einer Plattform für CAD-Dateien etc. Es ist jedoch nicht ersichtlich, dass das schwerpunktmäßige Übertragen von Signalen in Kommunikationsnetze Teil dieses Leistungsspektrums ist.

Die im TKG normierten IT-Sicherheitsregelungen sind somit für Unternehmer aus dem Bereich der AgF nicht einschlägig.

Telemediengesetz (TMG)

Telemediendiensteanbieter

Gem. § 13 Abs. 7 werden Telemediendiensteanbieter zu IT-Sicherheitsmaßnahmen verpflichtet, soweit sie diese im Rahmen ihrer jeweiligen Verantwortlichkeit anbieten.

Pflichten

Telediensteanbieter haben sicherzustellen, dass:

- kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen, auch soweit sie durch äußere Angriffe bedingt, gesichert sind.
- Maßnahmen müssen dem Stand der Technik entsprechen

Rechtsfolge

- § 13 Abs. 7 konkretisiert vertragliche Nebenpflichten gem. § 241 Abs. 2 BGB
- § 13 Abs. 7 ist ein Schutzgesetz i.S.d. § 823 Abs. 2 BGB
  bei Verstoß gegen § 13 Abs. 7 Nr. 1 und Nr. 2a ist Bußgeld bis zu 50.000 € möglich, gem. § 16 Abs. 2, Nr. 3, Abs. 3
- § 13 Abs. 7 ist ggf. Marktverhaltensregel i.S.d. § 3 UWG

Anwendbarkeit in der additiv-generativen Fertigung

Sind Unternehmer aus dem Bereich der AgF Anbieter von Telemediendiensten?

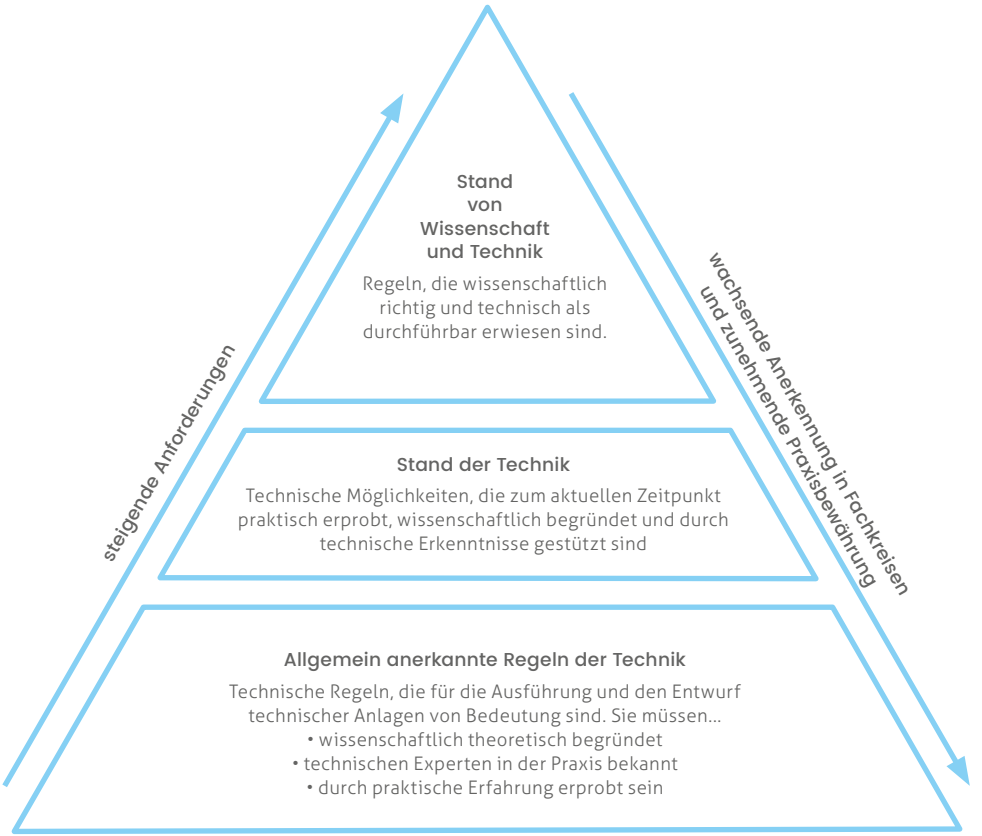
Die Legaldefinition des § 2 Nr. 1 TMG erfasst auch Betreiber einer Website zum Vergleich professioneller 3D-Druckdienste. A priori ist jeder Betreiber einer Website ein Telemediendiensteanbieter gem. § 2 Nr. 1 TMG.

Die Kernleistung der AgF – die Herstellung von Produkten im Wege additiv-generativer Fertigungsverfahren – stellen keinen Telemediendienst dar. Die vielfältigen Geschäftsmodelle im Bereich der additiven Fertigung, wie das Betreiben einer Plattform für CAD-Dateien oder das Dienstleistungsangebot der Bereitstellung von CAD-Dateien auf einer Plattform, sind ebenso als Telemediendienste anzusehen wie das Vertreiben von Druckdienstleitungen oder gedruckter Produkte über einen Webshop bzw. die eigene Website.

Welche Rechtspflichten bestehen für Anbieter von Telemediendiensten?

Das IT-Sicherheitsgesetz hat § 13 Abs. 7 in das TMG eingefügt, der Telemediendiensteanbietern auferlegt technische und organisatorische Maßnahmen nach dem Stand der Technik zu ergreifen. Um dieser Anforderung gerecht zu werden, sollte von den Betroffenen ein individuelles Informationsmanagementsicherheitssystem (ISMS) erstellt werden. Dieses besitzt den Vorteil im Schadensfall eine strukturierte, nachvollziehbare und dokumentierte Umsetzung von IT-Sicherheitsmaßnahmen nachzuweisen.

Exkurs: Stand der Technik



Wann entsprechen technische und organisatorische Maßnahmen dem Stand der Technik?

Der Stand der Technik ist ein unbestimmter Rechtsbegriff, der von den allgemein anerkannten Regeln der Technik und dem Stand von Wissenschaft und Technik abzugrenzen ist. Der Begriff „Stand der Technik" bestimmt den Grad der einzuhaltenden IT-Sicherheitsmaßnahmen und kann vom Gesetzgeber für bestimmte Bereiche, wie z.B. im Immissionsschutzrecht, präzisiert werden.

In Anlehnung an die Legaldefinition gem. § 3 Abs. 6 BImSchG versteht der Gesetzgeber laut Gesetzesbegründung den Stand der Technik im Bereich des § 8a BSIG folgendermaßen:

„Stand der Technik [...] ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt."

Gilt die gesetzgeberische Definition des Standes der Technik für § 8 Abs. 1 S. 2 BSIG auch im TMG?

Auf die gesetzgeberische Definition des Standes der Technik hinsichtlich der IT-Sicherheit ist auch im Rahmen des TMG abzustellen. Das IT-SicherheitsG hat als Artikelgesetz sowohl § 8a BSIG als auch § 13 Abs. 7 TMG eingeführt. Es ist abwegig anzunehmen, dass der Gesetzgeber von verschiedenen Begriffsdefinitionen ausging und dennoch in verschiedenen Normen zur IT-Sicherheit, innerhalb desselben Rahmengesetzes, den exakt gleichen Begriff verwendet. Des Weiteren sind die Merkmale der Definition des Gesetzgebers zu § 8a Abs. 1 S. 2 BSIG mit den Schutzzielen des § 13 Abs. 7 TMG kongruent, was ebenfalls für die Übertragbarkeit der Definition spricht.

Welcher Unterschied besteht bei verbindlichen IT-Sicherheitsstandards nach dem BSIG und dem TMG?

Der Unterschied zwischen § 13 Abs. 7 TMG und § 8a BSIG liegt nicht in der Begriffsdefinition des Standes der Technik, sondern im Grad der Verbindlichkeit dieses Sicherheitsstandards. Telemediendiensteanbieter müssen gem. § 13 Abs. 7 S. 2 TMG und Betreiber digitaler Dienste haben gem. § 8c Abs. 2 S. 1 BSIG den Stand der Technik zu berücksichtigen, wohingegen Betreiber Kritischer Infrastrukturen gem. § 8a Abs. 1 S. 2 BSIG den Stand der Technik einhalten sollen. Betreibern kritischer Infrastrukturen wird mithin mehr abverlangt, was aufgrund deren hoher Integration und Bedeutung für das Gemeinwesen auch sachgerecht ist.

Bundesdatenschutzgesetz (BDSG)/ Datenschutz-Grundverordnung (DS-GVO)

bis 24. Mai 2018

BDSG

ab 25. Mai 2018

DS-GVO

§ 9 BDSG

Anwendbarkeit

- personeller Anwendungsbereich: Verantwortliche Stelle, § 3 Abs. 7, und Auftragsdatenverarbeiter, § 11
- sachlicher Anwendungsbereich: Erhebung, Verarbeitung, Nutzung personenbezogener Daten

Pflichten

Ergreifen technischer und organisatorischer Maßnahmen, um die Ausführung der Vorschriften des BDSG, insb. Anlage zu § 9 S. 1, zu gewährleisten:
- Maßnahmen müssen der Gefährdungslage entsprechen
- Wahrung des Verhältnismäßigkeitsgrundsatzes

Rechtsfolgen

- Schadenersatzpflicht gem. § 7 S. 1
- Unterlassungs- oder Schadensersatzansprüche
- Anordnungen der Aufsichtsbehörde gem. § 38 Abs. 5

Art. 32 DS-GVO

Anwendbarkeit

- personeller Anwendungsbereich: Verantwortlicher, und Auftragsdatenverarbeiter, Art. 32 Abs. 1; nicht Hersteller von Hard- oder Software
- sachlicher Anwendungsbereich: Verarbeitung personenbezogener Daten, Art. 2 Abs. 1

Pflichten

Ergreifen technischer und organisatorischer Maßnahmen, Art. 32 Abs. 1 und Abs. 2, konkretisiert durch den nichtabschließenden Mindestmaßnahmenkatalog gem. Art. 23 Abs. 1 HS. 2

Rechtsfolgen

- Schadensersatz gem. Art. 82 Abs. 1 bei materiellem oder immateriellem Schaden
- Geldbuße kann, gem. Art. 83 Abs. 4 lit. a bis zu 10 000 000 € oder bei Unternehmen 2% des Jahresumsatzes betragen

Anwendbarkeit in der additiv-generativen Fertigung

Das bisherige Bundesdatenschutzgesetz (BDSG) tritt am 24. Mai 2018 außer Kraft und wird weitgehend von der unmittelbar geltenden Datenschutz-Grundverordnung (DS-GVO) abgelöst. Sowohl das BDSG, als auch die DS-GVO, schützen nicht jegliche Art von Information, sondern das Persönlichkeitsrecht des Einzelnen, welches durch den Umgang mit personenbezogenen Daten beeinträchtigt wird. Die Datensicherheit, als Teilbereich der IT-Sicherheit, bedingt den Schutz personenbezogener Daten. Folglich finden sich im BDSG und in der DS-GVO Normen zum Schutz der Datensicherheit, respektive § 9 BDSG und dessen Anlage 1 zu § 9 BDSG und Art. 32 DS-GVO. Der Anwendungsbereich des BDSG bzw. der DS-GVO, und damit deren Pflichtenkreis, ist eröffnet, wenn Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person erhoben, verarbeitet oder genutzt werden.

Die Verwendung personenbezogener Daten bei additiv-generativer Fertigung kann vielfältig sein. Personenbezogene Daten können als Zusatzinformationen erhoben werden, z.B. die Maße eines Fußes für die Anfertigung eines individuell angepassten Sportschuhs. Die Erhebung oder Verarbeitung personenbezogener Daten kann Teil des Geschäftsmodells bilden, z.B. wenn Gesicht und Körper einer Person gescannt werden um eine Miniaturfigur dieser Person zu drucken. Personenbezogene Daten können aber auch in Form von Mitarbeiterdaten anfallen, z.B. wenn registriert wird, wann welcher Mitarbeiter wie lange an einem bestimmten Druckprojekt arbeitet.

Regelungen des allgemeinen Zivilrechts: Bürgerliches Gesetzbuch (BGB)

Haftungsregime des BGB

Vertraglich
§§ 241 ff. BGB

Anspruchsgrundlage:

Vertrag bzw. dessen
- Hauptpflichten oder
- neben / Schutzpflichten gem. § 241 Abs. 2

Stärken vertraglicher Haftung

+ vermutetes Verschulden (Beweislastumkehr)
+ reiner Vermögensschaden ersatzfähig
+ Haftung für Erfüllungsgehilfen

Deliktisch
§§ 823 ff. BGB

Anspruchsgrundlage:

Gesetz, §§ 823 ff.

Schwächen des Deliktrechts

- Verschulden des Anspruchsgegners muss nachgewiesen werden
- kein Schadensersatz für reine Vermögensschäden
- Exkulpationsmöglichkeit, § 831 Abs. 1 S. 2

Welche Haftungsmechanismen gibt es im BGB?

Das Haftungsregime des BGB kann – stark vereinfacht – in vertragliche und deliktische Haftung unterteilt werden. Aufgrund der Schwächen des Deliktsrechts ist die vertragliche Haftung für den Anspruchssteller vorzugswürdiger.

Wenn die IT-Sicherheit Bestandteil der geschuldeten Hauptleistungspflicht ist, liegt bei einer IT-Sicherheitsverletzung gleichzeitig eine Pflichtverletzung vor. Die Verletzung der IT-Sicherheit kann aber auch die Verletzung einer vertraglichen Nebenpflicht gem. § 241 Abs. 2 BGB darstellen, wonach der Vertragspartner zur Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Vertragspartners verpflichtet ist.

Im Rahmen der deliktischen Haftung ist § 823 Abs. 1 BGB die zentrale Norm. Zur Begründung eines Schadensersatzanspruchs muss dabei insbesondere eines der normierten Rechtsgüter verletzt sein und das Verschulden des Anspruchsgegners nachgewiesen werden.

Anwendbarkeit in der additiv-generativen Fertigung

Welche Rechtsgüter des § 823 Abs. 1 BGB könnten bei mangelnder IT-Sicherheit i.R.d. AgF verletzt werden?

In § 823 Abs. 1 BGB werden explizit die Rechtsgüter Leben, Körper, Gesundheit, Freiheit und Eigentum genannt, wobei z.B. das Allgemeine Persönlichkeitsrecht und das Recht am eingerichteten und ausgeübten Gewerbebetrieb als sonstige absolute Rechte i.R.d. § 823 Abs. 1 BGB anerkannt sind.

Das Leben, der Körper und die Gesundheit dürften bei Beeinträchtigung der IT-Sicherheit im Rahmen der AgF meist nur mittelbar betroffen sein. Probleme könnten sich zudem bei dem Kausalitätsnachweis stellen. Eine Eigentumsverletzung kann bejaht werden, falls z.B. CAD-Daten ganz oder teilweise von einem Datenträger gelöscht werden. Das Recht am eingerichteten und ausgeübten Gewerbebetrieb wird verletzt, wenn durch unzureichende IT-Sicherheitsmaßnahmen z.B. betriebliche Daten oder Know-How ausgespäht wurde.

Das Projekt AGENT-3D_Basis

Das Konsortium Agent-3D ist eine strategische Allianz für Forschung, Innovation und Wachstum führender Forschungseinrichtungen, Industrie und KMUs. Gemeinsames Ziel ist es, die additiv-generative Fertigung zur Schlüsseltechnologie der Industrie 4.0 zu entwickeln. Gefördert wird das Konsortium vom Bundesministerium für Bildung und Forschung.

Das Projekt AGENT-3D-Basis stellt eine wichtige Brückenfunktion zwischen Strategie- und Technologievorhaben dar. Dabei erarbeitet AGENT-3D_Basis wichtige Grundlagen mit interdisziplinärem Charakter, die nachfolgend in den weiteren Verbundvorhaben Anwendung finden. Fünf Themenfelder werden dabei adressiert:

- Auswirkungen sozio-ökonomischer Faktoren auf die Entwicklungschancen der AgF
- Urheber-/patentrechtlicher Schutz, Produkthaftung, wettbewerbsrechtliche Anforderungen
- Neue Wege in Konstruktion und Design
- Prozesssicherheit, Materialien und Qualitätssicherung
- Schnittstellen und Standardisierung.

Das Team der TU Berlin arbeitet seit Herbst 2015 als Teil eines interdisziplinären Forschungskonsortiums im Projektbereich AGENT-3D_Basis. Dieser erarbeitet Grundlagenerkenntnisse hinsichtlich bestehender gesellschaftlicher, politischer, volks- und betriebswirtschaftlicher sowie technologischer und rechtlicher Rahmenbedingungen. Dabei verlangt der Gesetzgeber nur eine relative – und keine absolute – Sicherheit, die sich an den konkreten Risikoanforderungen und den Sicherheitsstandards im Einzelfall orientiert.

Aktuelles: www.recht3d.tu-berlin.de und www.agent3d.de
Start: 1. Dezemeber 2015
Laufzeit: 36 Monate

Impressum

Verantwortliche:

Prof. Dr. Dr. Jürgen Ensthaler
Dr. Martin S. Haase
Jessica S. Mihalyi
Merve Oberneyer
Lehrstuhl für Wirtschafts-, Unternehmens- und Technikrecht
Technische Universität Berlin
Straße des 17. Juni 135
10623 Berlin

Redaktion:

Forschungsstelle 3D-Druck und Recht
Online unter http://www.recht3d.tu-berlin.de

Design:

Anne Gärtner, Alexander Slavny
AGENT-3D e.V.

zwanzig20
PARTNERSCHAFT FÜR INNOVATION

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Bildnachweise:
Titelseite: Marc Dietrich/stock.adobe.com
Einleitung: Philipp Manager und Frauenhofer IWU
carlosvelayos/stock.adobe.com
S. 07: Fraunhofer IWS