compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

Industrie 4.0 und Datenschutz

Dennis Jlussi, Rechtsanwalt in Hannover

JULI 2015

Einleitung

Die fortschreitende Integration neuester Informations- und Kommunikationstechnologien in industrielle Fertigungsprozesse – Industrie 4.0 – wirft mehr und mehr rechtliche Fragen im Zusammenhang mit Daten auf. Die rechtlich zu bewertenden Sachverhalte sind dabei nicht durchgängig im strengen Sinn völlig neu, sie erreichen aber neue Dimensionen; dies rührt hauptsächlich aus der noch konsequenteren und weiterreichenden Umsetzung datengestützter Prozesse her (Big Data – sozusagen *even bigger*). Da das Datenschutzrecht zu einem praktisch überwiegenden Teil aus rechtlichen Abwägungen besteht, können Maßnahmen, die gleichartig, jedoch intensiver sind, durchaus zu anderen rechtlichen Bewertungen führen.

Dabei stellen sich hauptsächlich Fragen in den Bereichen Arbeitnehmerdatenschutz, Kundendatenschutz und technischer Datenschutz, letzteres sowohl hinsichtlich personenbezogener als auch betrieblicher Daten.

Datenschutz und Innovation im Spannungsverhältnis

Datenschutz(-recht) und Innovation stehen in einem beinahe natürlichen Spannungsverhältnis. Gegenüber technischen Neuentwicklungen, die schnell und international sind, ist das Recht träge und national oder bestenfalls europäisch.

Die Grundlagen des heutigen Datenschutzrechts basieren auf der europäischen Datenschutzrichtlinie 95/47/EG, die im Oktober 1995 beschlossen wurde.

Selbst wenn man den vorherigen jahrelangen Beratungsprozess unberücksichtigt lässt: Die EDV-Landschaft 1995 bestand aus Windows 95, das noch standardmäßig ohne das Internetprotokoll TCP/IP und ohne Internetbrowser daherkam. Elektronische Informationen wurden zumeist auf Disketten verbreitet, CD-ROM-Laufwerke erfuhren erste Verbreitung. Von der ubiquitären Verfügbarkeit von Informationen, deren weltweiter Übermittlung praktisch in Echtzeit und den damit verbundenen Chancen und Risiken für Persönlichkeitsrechte und Unternehmensdaten haben der europäische und der nationale Gesetzgeber damals nichts geahnt.

Auch wenn das Datenschutzrecht durch kleinere Anpassungen am Gesetz, durch Sonder-Datenschutzrecht für Telemedien und elektronische Kommunikation sowie durch die Rechtsprechung bis hin zum Bundesverfassungsgericht zwischenzeitlich punktuell aufgefrischt wurde, so hat sich an der grundlegenden Erkenntnis wenig geändert: Es bedarf einiger gedanklicher Anstrengungen, um das Datenschutzrecht als Maßstab an moderne datenbasierte Produkte und Prozesse anzulegen. Dabei verbleiben jedenfalls am *Cutting Edge* immer rechtliche Risiken, die sich durch geschickte juristisch begleitete Entwicklung minimieren, aber nicht völlig ausschließen lassen.
Übrigens: Die Datenschutz-Grundverordnung, die bei Verfassung dieser Zeilen noch nicht einmal formell beschlossen war und voraussichtlich erst im Laufe des Jahres 2018 effektiv in Kraft getreten sein wird, basiert auf dem im Jahr 2011 verfassten (und vermutlich teilweise noch davor konstruierten) Entwurf der Europäischen Kommission und hängt damit der technischen Entwicklung bereits bei Inkrafttreten eine dreiviertel Dekade hinterher.

Arbeitnehmer-Datenschutz

Manche Zukunftsszenarien der *Smart Factory* sehen menschenlose Fabriken vor. Die möglichen gesellschaftlichen Auswirkungen einer eventuellen dahingehenden Entwicklung sollen nicht das Thema dieser Abhandlung sein; der Autor geht davon aus, dass auf absehbare Zeit Menschen gebraucht werden, die Maschinen zumindest überwachen und eine Verantwortung für deren reibungsloses Funktionieren tragen.

Selbst wenn die *Smart Factory* mit weniger Menschen auskommt, so folgt daraus nicht das Ende des Arbeitnehmer-Datenschutzes. Im Gegenteil: Je smarter die Fabrik ist, desto mehr Anlass gibt es, über den Schutz der verbliebenen Arbeitnehmer nachzudenken. So werden etwa Roboter, die durch Kamera- und Ultraschallsysteme Menschen erkennen, die sich in ihren Aktionsradius begeben, um Kollisionen und mithin Verletzungen zu vermeiden, Daten verarbeiten, bei denen es sich um personenbezogene Daten handelt.

Dies nämlich sind alle „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (§ 1 Abs. 1 Bundesdatenschutzgesetz). Damit können Daten einer bestimmten Maschine in einer Fabrik, für die ein bestimmter Mitarbeiter die Verantwortung trägt, als „sachliche Verhältnisse“ personenbezogen sein, jedenfalls wenn die Daten in Abhängigkeit von der Person stehen.
Das ist für sich genommen nicht neu; die Möglichkeit, anhand von Chargennummer und Dienstplan die konkret verantwortlichen Arbeiter ausfindig zu machen, dürfte bald so alt sein wie die Industrie selbst. Neu ist aber, dass es viel mehr Daten über die konkrete Maschine gibt, dass diese Daten übermittelt werden (an andere Maschinen, auf das Produkt, zur Fernüberwachung, an Lieferanten oder Abnehmer) und dass sie im Rahmen von Big-Data-Anwendungen automatisch ausgewertet werden. Bei konsequenter Datenanalyse ergibt sich daraus u.U. eine Komplettüberwachung des Arbeitnehmers hinsichtlich Leistung, Ausschuss, Retouren usw..

Vorzugswürdig ist die Verwendung anonymisierter Daten, also solcher, bei denen die Herstellung eines Bezugs zu bestimmten Arbeitnehmern gar nicht mehr möglich ist. Dies ist nicht immer ohne Verlust der Aussagequalität möglich, aber wo es möglich ist, handelt es sich um die rechtssicherste Methode: Wirksam und endgültig anonymisierte Daten unterliegen keinerlei datenschutzrechtlichen Anforderungen mehr.

Wo keine vollständige Anonymisierung möglich ist, bietet sich zur schonenden Datenverarbeitung eine teilweise Anonymisierung an, die i.d.R. darin besteht, eine anonymisierte Kopie eines Datensatzes zu erstellen, der dann für zumindest diejenigen Analysen verwendet wird, bei denen dadurch kein Verlust der Aussagequalität einhergeht. In Ausnahmefällen, in denen sensible Daten (z.B. solche, aus denen sich Gesundheitsdaten ablesen lassen) verarbeitet werden und eine Anonymisierung nicht möglich oder nicht erwünscht ist, können die Daten pseudonymisiert und die Zuordnungstabellen getrennt aufbewahrt oder sogar bei einer *Trusted Third Party* (TTP) hinterlegt werden; also bei einem Dritten, einer Art Daten-Treuhänder, wo der Zugriff durch klare, auch zugunsten der Arbeitnehmer wirkende Regelungen an bestimmte Bedingungen geknüpft und darauf beschränkt wird. Jedenfalls muss in aller Regel ausgeschlossen sein, dass der Endkunde oder Dritte in der Liefer- oder Vertriebskette erkennen können, welche Arbeitnehmer an der Herstellung beteiligt waren.

Nicht immer sind besondere Maßnahmen zur Anonymisierung oder Pseudonymisierung notwendig; die vom Datenschutzrecht vielfach vorgesehenen Interessenabwägungen können bei weniger sensiblen Daten auch zu deren Verwendbarkeit „nur“ unter den allgemeinen datenschutzrechtlichen Bedingungen führen. Hierbei sollte der Arbeitgeber jedoch stets die Betriebskultur im Auge haben und den Betriebsrat einbinden: Während manche Belegschaftsvertreter etwa alle Daten, die Rückschlüsse auf die individuelle Leitung von Arbeitnehmern zulassen, ablehnen, halten andere die Verwendung dieser Daten (unter Umständen und Auflagen) für sinnvoll, weil ungeeignete oder besonders motivationsarme Arbeitnehmer auch für die Kollegen eine Belastung darstellen können.

§ 87 Absatz 1 Nummer 6 des Betriebsverfassungsgesetzes kommt insofern eine Schlüsselrolle zu: Danach hat der Betriebsrat ein zwingendes Mitbestimmungsrecht bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Entgegen dem Wortlaut der Norm entspricht es gefestigter höchstrichterlicher Rechtsprechung, dass für die Bestimmung zur Überwachung schon die objektive Geeignetheit ausreichend ist. Die übrigen Details der Regelung sind Gegenstand umfangreicher und nicht immer einheitlicher juristischer Kasuistik, spezielle Fragen im Hinblick auf *Smart Factories* sind jedoch noch offen. Es dürfte in aller Regel kluger Unternehmenspolitik entsprechen, auch um

des Betriebsfriedens Willen den Betriebsrat auch dann frühzeitig und kooperativ einzubeziehen und eine Betriebsvereinbarung herbeizuführen, wo die Anwendbarkeit der Vorschrift in Grenzbereichen fraglich ist.

Kunden-Datenschutz

Kundendaten stellen für die produzierenden Unternehmen einen wichtigen wirtschaftlichen Wert da. Manche Hersteller haben ihren Vertrieb deswegen auf das sogenannte Agenturmodell umgestellt (und viele mehr denken darüber nach), bei dem die Händler nur noch Handelsvertreter des Produzenten sind, um einfacher an mehr Kundendaten zu gelangen. Mehr, schnellerer und direkter Kundenkontakt ist für viele moderne Prozesse essentiell, etwa im *Lean Development*.

In zunehmendem Maße werden außerdem Produkte nach (End-)Kundenspezifikation hergestellt, die Individualisierung von Gütern verschafft den Herstellern einen Wettbewerbsvorsprung und eröffnet vielfach erst den Zugang zum Premiumsegment des jeweiligen Marktes. Automobile, Möbel, Bekleidung und vorgefertigte Bauteile für Einfamilienhäuser sind dafür nur die prominentesten Beispiele.

Datenschutzrechtlich relevant sind an sich nur die Daten natürlicher Personen. Das ist allerdings nicht auf Verbraucher beschränkt, auch am B2B-Geschäft sind mit Einzelkaufleuten und den Gesellschaftern von Personengesellschaften natürliche Personen beteiligt; die dabei auftretenden Fragen und Varianten sind vielfältig, aber die Formulierung abstrakter Vorgehensweisen wird sich an den restriktiv zu handhabenden Fällen zu orientieren haben, so dass letztlich in der Regel von der Geltung des gleichen Datenschutzniveaus wie für Endverbraucher ausgegangen werden sollte. Außerdem wird von einem Hersteller gegenüber seinen gewerblichen Kunden häufig ein ähnliches Schutzniveau schon um der geschäftlichen Diskretion Willen erwartet.

Wenn die Produkte in der *Smart Factory* selbst Daten zur Individualisierung tragen und mit den Maschinen kommunizieren, so sollten in aller Regel die direkten persönlichen Daten (Name, Adresse usw.) des Kunden nicht auch dort gespeichert sein, sondern z.B. eine pseudonyme Kennziffer verwendet werden. Diese Daten sollten nur an diejenigen Stellen weitergegeben werden, bei denen dies zur Vertragserfüllung notwendig ist, und diese Stellen sind zur Einhaltung des Datenschutzrechts zu verpflichten; dazu gehören effektive Kontrollrechte, die nicht nur auf geduldigem Papier bestehen dürfen.

Auch hier ist ein höheres Schutzniveau erforderlich, wenn es sich um sensible Daten handelt, z.B. Gesundheitsdaten bei der Produktion von Medizinprodukten. Insoweit bietet sich eine erweiterte Pseudonymisierung an, erforderlichenfalls auch mit einer *Trusted Third Party*.

Datensicherheit

Der technische Datenschutz – also die Gewährleistung von Datensicherheit – erfüllt mehrere Zwecke. Einerseits sind seine Grundlagen in § 9 des Bundesdatenschutzgesetzes (nebst Anlage) festgehalten, denn der rechtliche Schutz von Persönlichkeitsrechten würde leerlaufen, wenn die Daten nicht technisch gegen Missbrauch geschützt würden. Andererseits dient Datensicherheit aber auch unternehmenseigenen Zielen, nämlich der Bewahrung von Geschäftsgeheimnissen und Know-How und der Abwehr von Spionage und Sabotage.

Die geschäftlichen Risiken von Fehlern und Versäumnissen im Bereich der Datensicherheit sind vielfältig. Unternehmen wie Microsoft, Sony, Target, StudiVZ und viele andere können ein Lied davon singen. Wenn die Versäumnisse öffentlich werden, droht ein Reputationsverlust auf der Abnehmer-, aber möglicherweise auch auf der Zuliefererseite. Goodwill wird gegenüber dem am öffentlichen Pranger stehenden Unternehmen eher ausbleiben. Es droht auch ein Wertverlust der Marke, was insbesondere bei Unternehmen, die diese in der Bilanz aktiviert haben, problematisch sein kann. Als rechtliche Risiken kommen Bußgelder und Schadensersatz hinzu; nach den allgemeinen Regelungen führen Versäumnisse u.U. auch zur persönlichen Haftung der zuständigen Führungskräfte.

Selbst, wenn die Sache nicht öffentlich wird (für personenbezogene Daten wegen der Mitteilungspflicht an die zuständige Datenschutzbehörde schwer vorstellbar), droht der Verlust von exklusivem Wissen und damit eines Wettbewerbsvorsprungs, sowie (bei Sabotage) die Betriebsunterbrechung.

Deswegen sind entsprechende Kriterien auch vorbeugend bei der Risikobewertung zu berücksichtigen. Seit

Basel II (unverändert in Basel III) sind IT-Risiken bei den operationellen Risiken des Kreditnehmers zu berücksichtigen („the risk of loss resulting of inadequate or failed internal processes, people and systems"). Die Banken haben sich lange schwergetan mit der Implementierung, zunehmend werden entsprechende Assessments aber vorgenommen oder Zertifizierungen verlangt (z.B. aus der ISO 27000-Reihe). Auch als Gegenstand der Abschlussprüfung (Audit) werden entsprechende Feststellungen rechtlich verlangt; insoweit sind ebenfalls verbindliche Standards erst langsam dabei, sich durchzusetzen, aber es wird daran kein Weg vorbei führen.

In Industrie-4.0-Prozessen und in der *Smart Factory* gibt es ersichtlich zusätzliche Angriffspunkte. Überall, wo Daten zusätzlich erfasst, übertragen oder gespeichert werden, besteht das potenzielle Risiko, dass ein Angreifer die Erfassung, Übermittlung oder Speicherung kompromittieren oder abgreifen könnte. Das heißt, dass innerhalb der Prozesse und Lieferketten, bei dem Austausch von Daten zwischen Maschinen, Produkten, Steuerung, Zulieferern, Vertrieb usw. an jeder Stelle die Daten gesichert werden müssen.

+++

caston.info

Beiträge zu Recht & Wirtschaft International finden Sie kostenfrei im Internet bei caston.info. Unsere Titelliste erhalten Sie auch per Mail.

IMPRESSUM

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-0 Fax 0511-30756-10
Mail info@herfurth.de, Web www.herfurth.de

Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.)

Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Marc-André Delp, M.L.E., Rechtsanwalt; Martin Heitmüller, Rechtsanwalt, Maître en Droit (FR); Günter Stuff, Steuerberater; Xiaomei Zhang, Juristin (CN), Mag. iur. (D); Dennis Jlussi, Rechtsanwalt; Sabine Reimann, Rechtsanwältin (D); Araceli Rojo Corral, Abogada (ES); Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia); Cord Meyer, Jurist und Bankkaufmann; Dr. jur. Reinhard Pohl, Rechtsanwalt (D); Elena Duwensee, Juristin (RU), Master of Law (RU).

KORRESPONDENTEN

u.a. Amsterdam, Athen, Barcelona, Brüssel, Budapest, Bukarest, Helsinki, Istanbul, Kiew, Kopenhagen, Lissabon, London, Luxemburg, Lyon, Mailand, Madrid, Moskau, Oslo, Paris, Prag, Sofia, Stockholm, Warschau, Wien, Salzburg, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, Dubai, Kairo, New Delhi, Bangkok, Singapur, Peking, Shanghai, Tokio, Sydney, Johannesburg

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50 Fax 0511 - 30756-60
Mail info@caston.info Web www.caston.info

Alle Angaben erfolgen nach bestem Wissen; die Haftung ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Wiedergabe, auch auszugsweise, nur mit Genehmigung der Herausgeber.

compact.
HERFURTH & PARTNER RECHT INTERNATIONAL.

NEUERSCHEINUNG

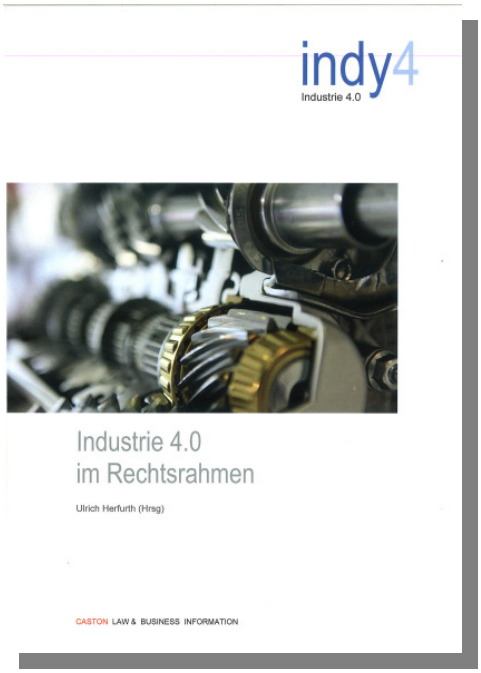
Industrie 4.0 im Rechtsrahmen
Recht für die digitale Unternehmenspraxis

Industrie 4.0 ist für die meisten Unternehmen nicht mehr nur ein Schlagwort, sondern als Weg in die Digitalisierung von Produktion und Geschäftsprozessen bereits Realität.

Bei der Umsetzung der technologischen Entwicklungen entstehen allerdings zahlreiche neue rechtliche Fragen, die ein Unternehmen geklärt haben muss, um seine Ziele störungsfrei und sicher verfolgen zu können. Im Vordergrund steht die Sicherheit von Prozessen und Produkten - von größter Bedeutung ist aber auch der Umgang mit eigenen und fremden Daten und die Rechte daran. Je mehr sich ein Unternehmen digitalisiert, umso stärker verlagern sich seine Werte in diesem Bereich.

Der neue Report „Industrie 4.0 im Rechtsrahmen“ beschreibt in den verschiedenen Feldern, welche rechtlichen Rahmenbedingungen die Unternehmensprozesse steuern:

Besondere Herausforderungen entstehen aus dem Umgang mit autonomen Prozessen in der Leistungskette, im Qualitätsmanagement, in unternehmens- und in länderübergreifenden Beziehungen und Abläufen. Generierung, Besitz, Verwendung und Verwertung der großen Datenmengen werfen neue Fragen zu Schutz und Zugriffsrechten auf – und verlangen eine privatrechtliche vertragliche Gestaltung. Industrie 4.0 berührt aber auch wichtige andere Bereiche wie Personal und Arbeitsgestaltung, Wettbewerbsrecht, Finanzierung und Rechnungswesen und Beziehungen zu Providern, Plattformen und Netzen.
„Industrie 4.0 im Rechtsrahmen“ greift diese Fragen auf und gibt dazu aktuelle Lösungsansätze.



Industrie 4.0 im Rechtsrahmen
Leistungen, Daten, Strukturen

Herfurth, Ulrich (Hrsg)
Caston Edition, Hannover
ISBN 978-3-936647-03-7

Verlag:
Caston GmbH
Law & Business Information
D-30159 Hannover
Luisenstrasse 5
www.caston.info

compact.

HERFURTH & PARTNER RECHT INTERNATIONAL.

Inhalt

Querschnitt
- Rechtliche Aspekte zu Industrie 4.0

Betrieb & Systeme
- Verträge, Produktion, Lieferkette
- Netze, Telekom, Datensicherheit, Lizenzen

Technologie und Daten
- Datenschutz und Datensicherheit
- Dateneigentum
- Industrie 4.0 und das Immaterialgüterrecht
- Strafrechtsschutz für Computer und Daten

Finanzen
- Daten in Bilanz und Besteuerung

Markt und Wettbewerb
- Kartellrecht, Wettbewerbsrecht

Personal & Management
- Personal
- Geschäftsführung mit Legal Controlling

International
- Industrie 4.0 und Recht in den USA
- Industrie 4.0 und Recht in Brasilien
- Industrie 4.0 und Recht in China
- Industrie 4.0 und Recht in Russland
- Industrie 4.0 und Recht in Indien

Bestellung

Fax an 0511-307 56-10	*Stück*	*EUR/Stk*	*EUR /Ges*
▪ Industrie 4.0 in Eckpunkten, 2. Aufl. 2016-01		45,00	
▪ Industrie 4.0 im Rechtsrahmen, 1. Aufl. 2016-09		45,00	
Summe (inkl. Mwst u Versand im Inland)		XXXX	

Einige Beiträge finden sich in beiden Reports. Sie erhalten daher bei Bestellung **beider Publikationen** einen **Bonus** in Höhe von 20,00 EUR.

Name, Vorname*:

Position:

Firma*:

PLZ, Ort*:

Strasse*:

eMail*:

Unterschrift*:

*) Pflichtfelder

CASTON GmbH, Law & Business Information
Luisenstr. 5, 30159 Hannover
FON 0511 – 307 56-50 www.caston.info
FAX 0511 – 307 56-60 info@caston.info