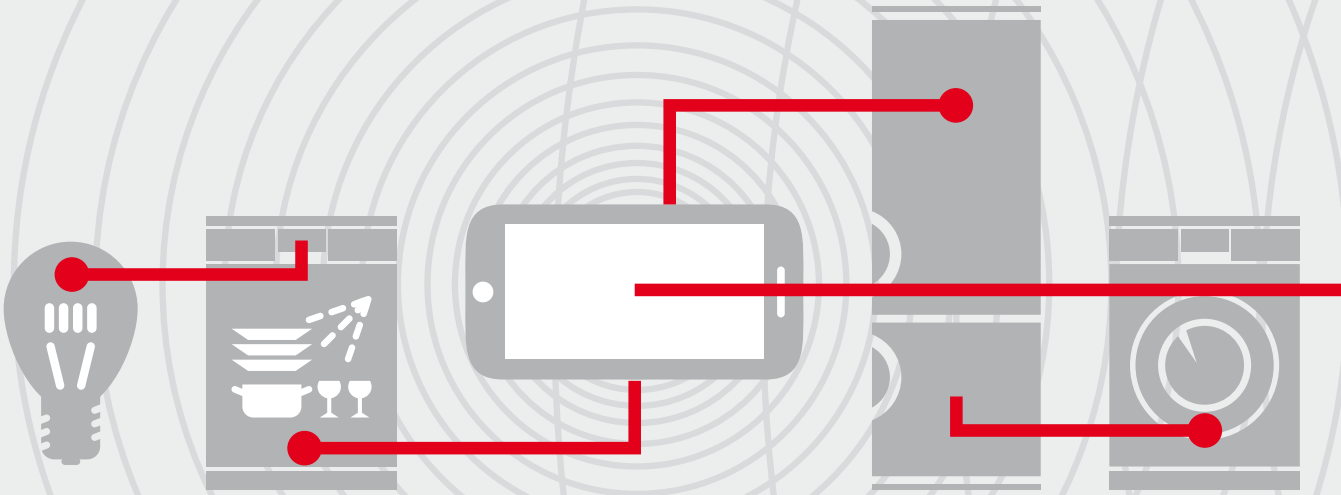
M2M und Recht:

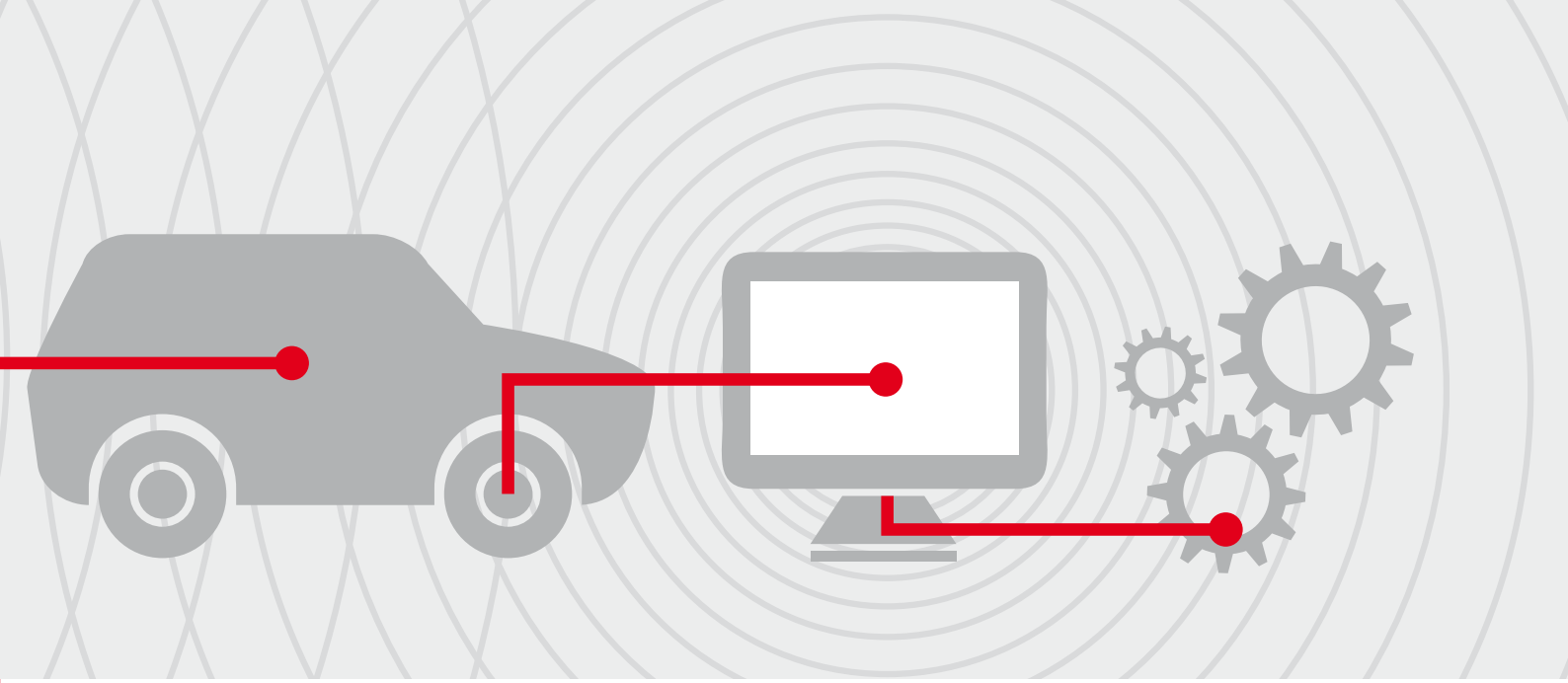
Fallstricke und Handlungsleitlinien

Dr. Bettina Horster
Dr. Sebastian Brüggemann
Dr. Jens Eckhardt
Dr. Jan-Peter Ohrtmann

Stand: Oktober 2015

Verband der Internetwirtschaft e.V.





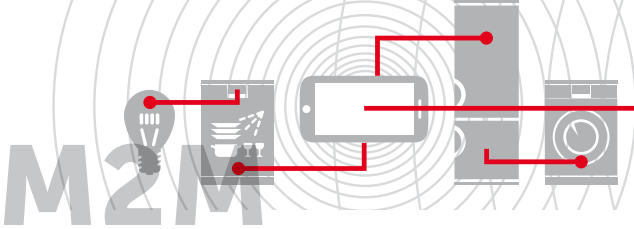
M2M und Recht:

Fallstricke und Handlungsleitlinien

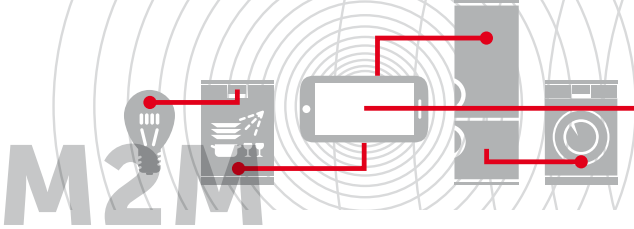
Dr. Bettina Horster
Dr. Sebastian Brüggemann
Dr. Jens Eckhardt
Dr. Jan-Peter Ohrtmann

Stand: Oktober 2015

eco – Verband der Internetwirtschaft e.V.



Inhalt



Schöne vernetzte neue Welt?

Beispiel Automobil:
Mit circa 6.000 Einzelteilen und einem zunehmend technisierten Innenleben sind Autos hoch komplexe Produkte. Um sie zukunftsfähig bauen zu können, sind Digitalisierung, Vernetzung und Standardisierung die entscheidenden Entwicklungen – und werfen zahlreiche rechtliche Fragen auf.

Automobilzulieferer TCB liefert mehreren Automobilherstellern Software für Bremssysteme. Dank M2M und Industrie 4.0 ist er in ein enges Netzwerk eingebunden, das neben den Unternehmen auch andere Zulieferer, Werkzeughersteller, Softwareunternehmen, Händler und Werkstätten umfasst. So hat er auch nach der Auslieferung noch Zugriff auf seine Systeme in den Autos und erhält beim Werkstattbesuch oder einer Internetverbindung der Fahrzeuge Informationen, denn ob Lenkung, Bremse, Motor oder Airbag – jedes System sammelt im Auto mittlerweile Daten in seinem Steuergerät. So erfährt TBC, wie schnell das Auto durchschnittlich fährt, wie viele Kilometer es zurückgelegt hat, den Zustand bestimmter Verschleißteile, Fehlermeldungen und wie stark der Fahrer gewöhnlich auf die Bremse tritt. Mit diesen Daten kann TBC seine Software besser auf die Bedürfnisse der Kunden abstimmen, und damit er noch besser Maßfertigen kann, sendet das Auto auch gleich noch Details zum häufigsten Fahrer mit: Der heißt Thorsten Müller, ist 45 Jahre alt, wiegt 80 Kilogramm und fährt oft längere Strecken, meist in den Morgenstunden und gern auch mal über dem Limit und mit zu geringem Abstand zum Vordermann. Und da TBC nicht nur in Deutschland aktiv ist, erhalten die spannenden Daten auch gleich die Entwicklungsabteilung in Japan und die Konzernzentrale in den USA. Und weil die Informationen auch die Autoversicherung von Herrn Müller sehr interessiert, kann sich TBC noch etwas nebenher verdienen.

Als Thorsten Müller einen Auffahrunfall hat, sendet das Auto schnell eine Meldung an die Polizei und eine Warnung an die Autos in der Umgebung. Die zahlreichen aufgezeichneten Daten dienen nun der ausführlichen Analyse: War er wieder zu schnell unterwegs, gab es ein Problem beim Pedal oder hat TBC bei der Software einen Fehler gemacht? Hätte der Fehler schon vor dem Unfall erkannt werden können und wer wäre für die Überwachung der Funktionsfähigkeit des Autos zuständig gewesen: der Autohersteller, jeder Zulieferer für sein Produkt/seine Software oder gar der Lieferant? Wer haftet nun für den entstandenen Schaden?

Wird ein Fehler am Auto gefunden, können dank M2M gezielt die anderen betroffenen Wagen in die Werkstatt beordert werden. Es lässt sich genau nachvollziehen, welche Fahrzeuge in welcher Charge davon betroffen sind. Eine riesige imageschädigende Rückrufaktion bleibt dem Hersteller erspart. Die Wagen melden gleich zurück, wann sie in der Werkstatt sein werden, sodass in der Produktion das passende Ersatzteil automatisch hergestellt und pünktlich dorthin geliefert werden kann. Das erspart der Werkstatt und dem Kunden Aufwand.

Der Hersteller kann zudem nachvollziehen, welcher Mitarbeiter an der fehlerhaften Charge gearbeitet hat. So, so: Andy Friedrich. Er hat an dem Tag nicht seine vorgeschriebenen Pausenzeiten eingehalten.

Das enge Netzwerk hat aber noch einen großen Vorteil für TBC: Der Automobilzulieferer analysiert die Daten der Konkurrenzzulieferer intensiv, um so an hilfreiches Kern-Know-how zu gelangen. Dabei entdeckt er, wie ein Mitbewerber ein konkretes Problem in der Software gelöst hat. Prima, denkt sich TBC, und kopiert illegal die Lösung für seine eigene Software, die er dem Autohersteller anbietet und prompt den Zuschlag bekommt. Während der Produktion fällt dem Konkurrenten der Diebstahl jedoch auf, eines seiner Patente wird dadurch verletzt. Sofort lässt er die gesamte Autoherstellung mit einer Unterlassungsverfügung stoppen. So geht es schließlich nicht! Und während der Klärung der Rechteverhältnisse steht die Auslieferung still …

Vorwort

Maschinen reden miteinander – auch heute schon

Liebe Leserinnen und Leser!

Digitalisierung, Internet der Dinge, Industrie 4.0, Machine-to-Machine (M2M)-Kommunikation: Sie bieten vielen Unternehmen die Chance, interessante neue Geschäftsmodelle und Services zu entwickeln. Nicht umsonst spricht man nach Mechanisierung, Elektrifizierung und Informatisierung nun von der vierten industriellen Revolution: Maschinen, Informations- und Kommunikationstechnologie sowie Prozesse werden intelligent vernetzt, um den Kunden effizientere und individuellere Lösungen anbieten zu können.

Smarte Geräte und Maschinen aller Art gehören bald zu unserem Alltag. Derzeit sind Branchenexperten zufolge bereits rund 15 Milliarden Geräte mit dem Internet verbunden. In gerade einmal fünf Jahren soll sich die Zahl mehr als verdoppeln. Ein Teil der Geräte kommuniziert auch heute schon miteinander. Die Kommunikation der Maschinen hat bereits in zahlreichen Branchen Einzug gehalten – von der Fertigungsindustrie über die Automobilbranche und Logistik bis hin zur Telemedizin. Sie eröffnet ein nahezu unendliches Spektrum an neuen Anwendungsszenarien und erlaubt dabei, in völlig neue Dimensionen vorzustoßen.

Grundlage für neue Services ist die transparente Zusammenarbeit in einem Ökosystem, das aus komplett unterschiedlichen Akteuren mit divergierenden Skills besteht. Das bringt für die einzelnen Beteiligten neue rechtliche Herausforderungen mit sich. So kann selbst ein kleines Unternehmen plötzlich gegen das Kartellrecht verstoßen. Oder weil irgendwo in der Produktionskette seine Software eingesetzt wird, muss es vielleicht für den Schaden haften, den ein Endprodukt verursacht hat. Schnell sind diese kollaborativen Netzwerke nicht mehr nur zwischen deutschen Unternehmen zu finden. Doch was gilt es beim Datenaustausch mit anderen EU – oder gar Drittländern zu beachten? Und was geschieht, wenn ein Anbieter innerhalb des Ökosystems Insolvenz anmeldet und die Prozesskette dadurch zusammenbricht?

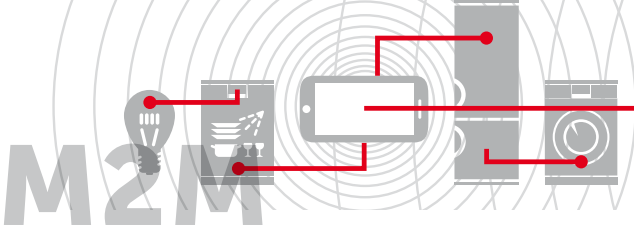
Hinzu kommen Fragen zum Datenschutz: Die Digitalisierung ermöglicht das Sammeln und Auswerten umfangreicher Daten – doch was ist hier erlaubt, insbesondere wenn sie Einblicke in das Verhalten von Beschäftigten oder Kunden liefern? Und wie unterscheiden sich personenbezogene Daten rechtlich von „Maschinendaten"?

Dieser Leitfaden möchte auf rechtliche Fallstricke im Umfeld der Digitalisierung, IoT und Industrie 4.0 aufmerksam machen und mögliche Handlungsleitlinien aufzeigen. Ziel ist es unter anderem, die Akzeptanz für diese innovative und chancenreiche Technologie zu steigern, damit sich Unsicherheit nicht innovationshemmend auswirkt.

Ich danke den Fachleuten von JUCONOMY Rechtsanwälte und PwC Legal (Düsseldorf) für ihre Unterstützung.

Spannende neue Erkenntnisse beim Lesen
wünscht Ihnen

Dr. Bettina Horster
Direktorin Mobile,
eco – Verband der Internetwirtschaft e. V.



1. Fallstricke und Handlungsleitlinien bei Unternehmensdaten

1.1 Fallstrick: Kern-Know-how nicht länger Betriebs- und Geschäftsgeheimnis

Maßgeblich für das Funktionieren von Industrie 4.0 und der Basistechnologie M2M-Kommunikation ist die enge Vernetzung der am Produktions- und Logistikprozess beteiligten Unternehmen. Zulieferer, Maschinenhersteller, IT-Dienstleister und Vertrieb müssen technisch stärker in den Produktionsbetrieb eingebunden werden und Informationen austauschen. Nur so lassen sich Abläufe weitgehend automatisieren. Durch die unternehmensübergreifende Vernetzung und Abstimmung werden interne Informationen über kollaborative Systeme an andere beteiligte Unternehmen übermittelt. Dabei werden immer mehr Daten von intelligenten Maschinen autonom erzeugt und gespeichert. Miteinander verknüpft bieten sie möglicherweise ungewollte Einblicke in die Strategien und Prozesse eines Unternehmens. Kooperationspartner könnten dies im Wettbewerb für die eigene Positionierung nutzen, ihre Angebote erweitern beziehungsweise verbessern oder schlicht die Leistung nachahmen. Auch für Dritte sind die Daten interessant, sodass ein Netzwerkpartner diese vermarkten könnte. Neben der legalen Verwendung haben Dritte vielleicht illegale Absichten damit.

Der bestehende gesetzliche Schutz reicht, etwa im Hinblick auf sensible Geschäftsstrategien, nicht aus. Das bestehende Wettbewerbsrecht (§ 17 UWG) schützt nur Betriebs- und Geschäftsgeheimnisse und ist hier eventuell nicht wirksam. Als Betriebs- und Geschäftsgeheimnisse werden in der Regel alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat. Wenn Daten aufgrund einer Zusammenarbeit zwischen Unternehmen ausgetauscht werden, besteht die Möglichkeit, dass sie nicht als Betriebs- und Geschäftsgeheimnisse gelten und daher auch grundsätzlich verwendet werden dürfen.

1.2 Handlungsleitlinie: Individuelle vertragliche Geheimhaltungsvereinbarung schließen

Um diesen Gefahren von vorneherein zu begegnen, empfiehlt sich der Abschluss von vertraglichen Geheimhaltungsvereinbarungen (Non-Disclosure Agreements beziehungsweise Confidential Disclosure Agreements), in denen die Verfügungsbefugnis über die Daten eindeutig festgeschrieben wird. Je nach Sensibilität der Daten sollten detaillierte Vereinbarungen getroffen werden, damit die erzeugten Daten nicht zweckentfremdet werden können. Die Vertragsfreiheit ermöglicht es, hier individuelle und detaillierte Regelungen im Wege der Selbstregulierung zu treffen. Die vertragliche Gestaltung stößt jedoch an ihre Grenzen, wenn beim Geschäftsmodell viele Rechtsbeziehungen spontan eingegangen werden und eine jeweilige vorherige Vertragsverhandlung zu aufwändig wäre. Hier müssen neue vertragliche Modelle und Mustervereinbarungen erarbeitet werden, die sich an einer Risikoabschätzung orientieren.

Die Regelungen zum Geheimnisschutz sollten mit dem potenziellen Vertragspartner diskutiert und gemeinsam individuell passende Regelungen gesucht werden. Bei der Diskussion solcher Vertragsregelungen lässt sich auch erkennen, welche Vorstellung der Vertragspartner von der Geschäftsbeziehung hat.

1.3 Handlungsleitlinie: Weitergabe an Dritte und missbräuchliche Eigennutzung verbieten

Eine wesentliche Begrenzung der Schutzwirkung von Geheimhaltungsvereinbarungen besteht darin, dass sie ihrem „klassischen" Inhalt nach, dem Vertragspartner nur verbieten, die geschützten Inhalte einem Dritten mitzuteilen. Nicht ausgeschlossen wird hierdurch, dass der Vertragspartner das Wissen selbst nutzt. Um diesem Effekt ebenfalls zu begegnen, bedarf es neben der Geheimhaltungsvereinbarung der Regelung, dass der Vertragspartner die gezogenen Erkenntnisse nicht für sein eigenes Angebot nutzt – insbesondere nicht, um als neuer Wettbewerber in den Markt einzutreten. Diese Regelung muss jedoch so gestaltet sein, dass sie nicht wegen ihres wettbewerbsbeschränkenden Charakters unwirksam ist.

1.4 Handlungsleitlinie: Kontrollrecht und Beweislast regeln

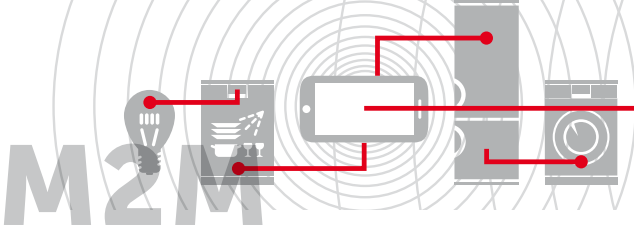
„Vertrauen ist gut, Kontrolle ist besser". Daher sollte festgelegt werden, wie das Einhalten dieser Vertragsregelungen überprüft wird. Denn ein Verstoß, der nicht auffallen kann, wird eher gewagt. Hierfür kommen insbesondere zwei Instrumente in Betracht: Kontrollrechte und Beweislastregelungen – bestenfalls beide gleichzeitig. Ein Kontrollrecht schafft die Überprüfungsmöglichkeit. Ausgeübt wird es typischerweise durch einen zur Verschwiegenheit verpflichteten sachverständigen Dritten, was nicht stets der Wirtschaftsprüfer sein muss. Eine Regelung, wonach der verpflichtete Vertragspartner beweisen muss, dass er nicht gegen die Pflicht zur Geheimhaltung im vorstehend weiten Sinn verstoßen hat, schafft klare Verhältnisse. Denn der Entlastungsbeweis ist eher zu führen, als der Nachweis eines Verstoßes. Dadurch ist auch das Risiko erhöht, „erwischt" zu werden, was zur Einhaltung der Beschränkung motiviert.

1.5 Handlungsleitlinie: Vertragsstrafe und/oder Schadensersatz festlegen

Diese Regelungen sollten noch durch eine Vertragsstrafenregelung und/oder einen pauschalierten Schadensersatz flankiert werden, der einerseits so hoch ist, dass der Verstoß wirtschaftlich uninteressant ist und gleichzeitig den typischerweise zu erwartenden Schaden abdeckt. Allerdings steht die Rechtsprechung solchen Regelungen sehr kritisch gegenüber und hat ihnen, insbesondere wenn sie nicht individuell verhandelt werden, enge Grenzen gesetzt.

Checkliste für eine vertragliche Geheimhaltungsvereinbarung zum Schutz der Unternehmensdaten

- Inhaberschaft der Daten und Nutzungsberechtigung klar regeln
- Risiko bewerten als Grundlage für die nachfolgenden Überlegungen
- Weitergabe der Daten an Dritte ausschließen
- Nutzung von Daten durch den Kooperationspartner für eigene Zwecke, insbesondere für Wettbewerbsangebote, ausschließen
- Rechtliche Grenzen der vorstehenden Ausschlüsse beachten, damit die Regelungen nicht wegen unzulässiger Wettbewerbsbeschränkung unwirksam sind
- Kontrollrechte und Beweislast zur praktischen Prüfung der vorstehenden Ausschlüsse regeln
- Vertragsstrafen und/oder Schadenspauschale im Fall von Verstößen definieren



2. Rechte des geistigen Eigentums und Softwarelizenzen

2.1 Fallstrick: Prozessvernetzung legt geistiges Eigentum offen

Damit Maschinen untereinander kommunizieren, müssen ihre Schnittstellen, Software und technischen Standards aufeinander abgestimmt werden. Die gemeinsame Datennutzung von Unternehmen umfasst daher in aller Regel über das vorstehend beschriebene Interesse am Schutz von Unternehmensdaten auch Rechte des geistigen Eigentums (Intellectual Property Rights) wie Patente, Gebrauchsmuster und Urheberrechte (beispielsweise Software und Datenbanken).

2.2 Handlungsleitlinie: Eigene Rechte schützen

Um geistiges Eigentum zu schützen, gilt es, entsprechende vertragliche Regelungen zu treffen. Darin sollten etwa Nutzungsrechte präzise eingeräumt und Vertragsstrafen berücksichtigt werden. Durch die jeweils einschlägigen Schutzrechte (insbesondere Urheber-, Patent- und Gebrauchsmusterrecht) stehen Unternehmen, anders als beim zuvor beschriebenen Schutz der Unternehmensdaten, deutlich mehr Möglichkeiten zum Schutz und zur Durchsetzung ihrer Interessen zur Verfügung.

2.3 Fallstrick: Schwaches Glied unterbricht Produktionskette

Intelligente Maschinen benötigen Software, die in den meisten Fällen von Drittanbietern stammt. Je mehr Unternehmen und Dienste mit ihren Maschinen, ihrer Logistik und nicht zuletzt ihrer Software in die Produktionsabläufe eingebunden sind, desto größer ist das Risiko einer lizenzrechtlichen Kettenreaktion: Fällt ein Baustein weg, kann dies zum Ausfall der gesamten Produktion führen. Insbesondere die Verwendung von Fremdkomponenten in einer Software kann hier schnell zum Problem werden. Hier genügt mitunter eine Unterlassungsverfügung im Wege des einstweiligen Rechtsschutzes und die gesamte Produktion steht still, bis die Rechtslage gerichtlich oder einvernehmlich geklärt oder eine technische Ersatzlösung gefunden und installiert ist.

Das Risiko der Insolvenz eines IT-Dienstleisters wird aber auch in anderen Bereichen relevant, wenn es beispielsweise um die Verfügbarkeit von unternehmens- und/oder produktionsrelevanten Daten geht, die sich in der Cloud oder bei einem externen Provider befinden.

2.4 Handlungsleitlinie: Business Continuity mit Lizenzvereinbarungen sicherstellen

Bei der Gestaltung von Lizenzverträgen rückt das Bedürfnis der Industrie nach Sicherstellung der Business Continuity in den Vordergrund. Im Rahmen von Lizenzvereinbarungen empfiehlt es sich, präzise Regelungen zu den Nutzungsrechten sowie zu Haftungsvoraussetzungen und -umfang aufzunehmen. Eine Haftungsfreistellungsklausel für den Fall, dass die lizenzierte Software Rechte Dritter verletzt, entspricht gängigen Standards. Sie erfasst aber nicht immer Schäden eines etwaigen Produktionsausfalls beispielsweise aufgrund von Unterlassungsansprüchen. Hier ist es umso wichtiger, im Rahmen der Vertragsverhandlungen Einblick in die Software und ihre Komponenten zu nehmen. Bei der Vereinbarung von Lizenzaudits ist es noch wichtiger als sonst, dass diese so ausgestaltet sind, dass die Produktionsabläufe möglichst nicht oder nur geringfügig beeinflusst werden.

In Bezug auf Wartungs- und Pflegeverträge ist, wie im Übrigen bei allen in die Produktionsabläufe eingebundenen IT-Diensten, im Rahmen der Service Level Agreements (SLA) darauf zu achten, die maximalen Ausfallzeiten möglichst eng zu definieren. Das gilt sowohl für die zugesicherte Verfügbarkeit als auch die geplanten Ausfallzeiten zur Durchführung von Updates und der Wartung der Systeme. Insbesondere Softwarehersteller und IT-Dienstleister werden sich auf diese veränderten Gegebenheiten einstellen müssen. Neben individuellen Update- und Wartungskonzepten, um Produktionsausfälle zu vermeiden oder zu minimieren, bedarf es zudem weiterer Absicherungen für den Fall von Rechtsverletzungen.

2.5 Handlungsleitlinie: Insolvenzrisiko minimieren

Ähnliches gilt für Unterbrechungen innerhalb der Lizenzkette zwischen Softwarehersteller und Unternehmen, beispielsweise wenn der Softwarehersteller oder ein zwischengeschalteter Lizenzgeber Insolvenz anmeldet. Zwar hat die höchstrichterliche Rechtsprechung im Falle der Insolvenz eines Zwischenhändlers entschieden, dass die vergebenen Unterlizenzen unabhängig hiervon weiter gelten, egal, ob sie dauerhaft erworben oder nur gemietet wurden. In welchen Fällen und unter welchen Voraussetzungen dieser so genannte Sukzessionsschutz greift, ist aber nach wie vor nicht abschließend geklärt. Auch dieses Risiko geht zu Lasten des produzierenden Unternehmens und sollte daher durch den Abschluss einer Versicherung abgedeckt werden.

Dem Insolvenzrisiko des Softwareherstellers oder Zwischenhändlers lässt sich rechtlich mit einer Hinterlegungsvereinbarung bezüglich des Quellcodes begegnen. Auf diese Weise können zumindest der Zugriff auf die Software, die weitere Benutzung und mögliche Wartung sowie Weiterentwicklungen faktisch abgesichert werden. Rechtlich gilt es dann, schnellstmöglich eine Einigung mit dem neuen beziehungsweise eigentlichen Lizenzinhaber anzustreben.

3. Neue Verantwortlichkeiten und Haftungsfragen

3.1 Fallstrick: IT-Sicherheit wird noch komplexer

Der Austausch möglicherweise sensibler Daten birgt auch eine weitere Gefahr. Was ist etwa, wenn bei einem der verschiedenen Beteiligten ein nicht ausreichendes IT-Sicherheitsniveau herrscht? Daten könnten dann möglicherweise von Dritten ausgespäht und weitergegeben werden.

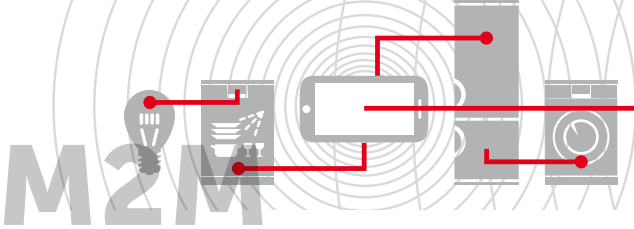
Zudem ändern sich die Anforderungen an die einzelnen Komponenten der IT-Infrastruktur, wenn sie in ein größeres Netzwerk eingebunden werden. Die Bedeutung jeder einzelnen Komponente nimmt zu, denn jede Einheit ist für die Funktionsfähigkeit des gesamten Netzwerks bedeutsam. Letztendlich hängt auch der WLAN-fähige Rauchmelder im selben Netz wie die produktionsrelevanten Maschinen und Steuerungseinheiten. Selbst der Netzwerkdrucker im Büro wird so zur kritischen Infrastruktur.

3.2 Handlungsleitlinie: Abgestuftes, sektorenspezifisches Sicherheitskonzept einführen

Statt vereinzelter technisch-organisatorischer Sicherheitsmaßnahmen empfiehlt sich, ein abgestuftes, sektorenspezifisches Sicherheitskonzept einzuführen, das sich an der Produktionsrelevanz des jeweiligen Sektors orientiert. Mit IT-Dienstleistern sollten Security Level Agreements geschlossen werden. Ein besonderes Augenmerk sollte dabei auf den Schnittstellen liegen, zu denen nicht zuletzt auch die Mitarbeiter zählen. Technische Sicherheitsmaßnahmen sollten daher stets durch Unternehmensrichtlinien, Verschwiegenheitsklauseln und ähnliche Maßnahmen ergänzt werden.

3.3 Fallstrick: Haftung bei Schäden

Doch wer zahlt für entstandene Schäden? Aufgrund der zunehmenden Komplexität wird es immer schwieriger, die Ursache und damit die rechtliche Verantwortlichkeit für einen eventuellen Schadensfall festzustellen. Bei der Haftung gegenüber Dritten ist die Verantwortlichkeit des Unternehmers durch das Produkthaftungsgesetz (ProdHaftG) und das allgemeine Deliktsrecht bestimmt.



Der Einsatz vielfältiger, möglicherweise unterschiedlich bedeutsamer, Komponenten innerhalb von unternehmens- und länderübergreifenden Netzwerken bringt aber möglicherweise das Bedürfnis mit sich, einzelne Beteiligte von der (Mit-)Haftung oder von möglichen Regressforderungen im Innenverhältnis auszuschließen, denn die komplexen Strukturen von M2M-Lösungen machen es unter Umständen schwierig, einzelne Tatbeiträge zuzuordnen und nachzuvollziehen.

3.4 Handlungsleitlinie: Verantwortlichkeiten und Haftung für einzelne Tatbeiträge festlegen

Unklarheiten bei der Risikoverteilung sollten im Rahmen der Vertragsverhandlungen durch entsprechend gestaltete Haftungsklauseln beseitigt werden. Dabei sollten Verantwortlichkeiten in Bezug auf einzelne Tatbeiträge und die sich daraus ergebende Haftung vorab vertraglich festgelegt werden. Ein Bedürfnis nach derartigen Vereinbarungen entsteht möglicherweise auch im Hinblick auf die Versicherbarkeit und die je nach Risiko unterschiedlichen Prämienkonditionen. Damit Versicherungskosten nicht ausufern, kann es für alle Beteiligten notwendig sein, einzelne Verantwortlichkeiten festzulegen.

Der vertraglichen Haftungsbeschränkung sind jedoch insbesondere im Hinblick auf deliktisches Verhalten enge Grenzen gesetzt. Ohnehin wirken derartige Konstruktionen stets nur im Innenverhältnis zwischen den beteiligten Vertragspartnern, nicht aber gegenüber und vor allem zu Lasten Dritter (Außenverhältnis). Eine vertragliche Haftungsfreistellungsvereinbarung führt im Außenverhältnis nicht dazu, dass dem Geschädigten kein Anspruch gegen den derart Freigestellten zustünde, sondern begründet lediglich einen Anspruch gegenüber dem Vertragspartner, hier in die Bresche zu springen. Im Falle der Insolvenz des Vertragspartners bleibt aber auch der Freigestellte auf den Kosten sitzen.

Letztendlich müssen sich Unternehmen jedoch der Grenzen dieser Möglichkeiten und der verbleibenden Restrisiken bewusst sein. Dem lässt sich nur durch den Abschluss einer Versicherung begegnen.

3.5 Fallstrick: Softwarehersteller haften für physisches Endprodukt

Softwarehersteller werden bei Industrie 4.0 stärker in den Produktionsprozess einbezogen. Das bedeutet für sie aber zusätzliche Haftungsrisiken, die sich auch auf die Produktion sowie das produzierte Endprodukt erstrecken können. Sind Schäden im Rahmen der Produktion auf eine fehlerhafte Programmierung der Software zurückzuführen, trifft den Softwarehersteller neben den vertraglich übernommenen Haftungsrisiken auch das ureigene Produkthaftungsrisiko.

Inwieweit er auch für Schäden an den Produktionsmaschinen oder dem Endprodukt (Mangelfolgeschäden) einzustehen hat, hängt davon ab, ob der Schaden auf einen Fehler der Software zurückzuführen ist, den der Hersteller zu vertreten hat, oder ob andere Umstände, wie etwa Bedienfehler, den Schaden (mit-)verursacht haben. Haben die Parteien keine anderweitigen Vereinbarungen getroffen, haftet der Softwarehersteller der Höhe nach unbegrenzt. Das gilt auch für die sogenannten „Weiterfressermängel", bei denen beispielsweise Programmierfehler der Firmware einen Schaden an der Platine oder gar der Maschine verursachen, in die sie integriert ist.

3.6 Handlungsleitlinie: Softwarehersteller müssen Haftungsumfang präzise verhandeln

Softwarehersteller sollten im Rahmen von Vertragsverhandlungen über eine möglichst genaue Bestimmung des Verwendungszwecks das wirtschaftliche Haftungsrisiko identifizieren und die Haftungsklauseln entsprechend ausgestalten. Dabei müssen sie die Versicherungsmöglichkeiten und den vom Kunden verlangten Versicherungsumfang berücksichtigen.

3.7 Fallstrick: Produzierende Unternehmen haften gegenüber Kunden und Dritten – auch über die Produktauslieferung hinaus

Produkthaftungspflichten treffen natürlich auch das produzierende Unternehmen selbst. Die rechtliche Verantwortlichkeit für sein Produkt und etwaige hierdurch verursachte Schäden endet keineswegs mit der Auslieferung an den Kunden. Sie besteht nicht nur fort, sondern gilt – im Falle der deliktischen Produkthaftung – nicht nur gegenüber dem Kunden sondern auch gegenüber Dritten. Es genügt bereits, wenn das Unternehmen gegen seine Verkehrssicherungspflichten verstößt und ein fehlerhaftes Produkt in Umlauf gebracht hat, wodurch ein Schaden entstanden ist. Es haftet in voller Höhe für den entstandenen Schaden und etwaige Begleitschäden, ohne Obergrenze. Nicht umsonst rufen Automobilhersteller mehr Autos zurück als sie produzieren: Selbst kleinste Produktionsfehler können hohe Sicherheitsrisiken für Leib und Leben der Kunden und anderer Straßenverkehrsteilnehmer bedeuten. Und die Geschädigten müssen lediglich beweisen, dass der Schaden auf einen Mangel des Produkts zurückzuführen ist, da sie in der Regel keinen Einblick in die Produktionsprozesse haben. Gelingt ihnen das, ist es Sache des Herstellers zu beweisen, dass er den Mangel nicht zu verantworten hat.

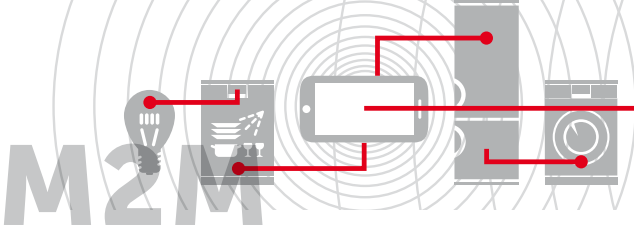
Technisch komplexe Produkte setzen zumeist entsprechend komplexe Produktionssysteme voraus. Modulare Produktionsstrukturen sind bereits heute weitestgehend technisiert – das Risikomanagement dagegen nicht gleichermaßen. Hier besteht Nachholbedarf. Industrie 4.0 beziehungsweise M2M-Kommunikation bietet eine Lösung in Form weitestgehend automatisierter, softwaregestützter Qualitätsmanagementsysteme. Solche Systeme sind in der Lage, innerhalb der einzelnen Produktionsschritte und durch Datenanalysen in Echtzeit, Fehler frühzeitig zu erkennen, zu dokumentieren und gegebenenfalls sogar zu beheben – bevor das Produkt an den Kunden geliefert wird. Gleichzeitig lassen sich auf diese Weise auch die negativen Auswirkungen auf die Produktionsabläufe möglichst gering halten.

3.8 Handlungsleitlinie: Produzierende Unternehmen reduzieren Haftungsrisiko durch automatisierte, softwaregestützte Qualitätsmanagementsysteme

Produzierende Unternehmen können ihr eigenes Haftungsrisiko durch den Einsatz automatisierter, softwaregestützter Qualitätsmanagementsysteme reduzieren beziehungsweise durch entsprechende Vertragsgestaltung teilweise auf die Systembetreiber verlagern. Allerdings werden diese kaum die unbeschränkte Haftung übernehmen und vor allem die Schnittstellen, beispielweise bei der Bedienung des Systems, bieten ein erhebliches Konfliktpotenzial. Da die Systeme alles umfangreich dokumentieren, lässt sich die eigene Verantwortung im Prozessfall unter Umständen leichter widerlegen.

Das produzierende Unternehmen muss die Interessen abwägen, wie stark es sich angesichts der Beschränkungen in vertraglichem Haftungsumfang und faktischer Haftungsmasse auf den Betreiber des Qualitätsmanagementsystems verlassen will. Organisatorische Schnittstellen zum produzierenden Unternehmen werden sich jedenfalls nicht vermeiden lassen (beispielsweise Implementierung, Bedienung der Software, manuelle Kontrollen etc.). Völlig aus der Haftung entlassen wird das produzierende Unternehmen jedoch nicht, wie die vorangegangenen Ausführungen gezeigt haben.

Sicherlich wird mit zunehmender (künstlicher) Intelligenz auch über eine eigenständige Verantwortlichkeit von Maschinen nachgedacht werden müssen. Dabei ist es aus (haftungs-) rechtlicher Sicht jedoch unwahrscheinlich, dass es hierdurch zu einer Haftungsfreistellung des Herstellers kommen wird, da der Geschädigte, mangels Durchsetzbarkeit seines Anspruchs, faktisch rechtlos gestellt würde. Letztendlich liegt die Ursache derartiger Fehler stets in der ursprünglichen Programmierung begründet.



3.9 Fallstrick: Produktbeobachtungspflichten weit über die Auslieferung hinaus

Industrie 4.0 ist keineswegs auf die unterschiedlichen Produktionssysteme innerhalb der Smart Factory beschränkt. Das zu fertigende Endprodukt kann über die einzelnen Produktionsstadien hinweg weit über die Auslieferung hinaus beobachtet werden. Gerade bei softwaregestützten Produkten werden auf diese Art und Weise Updates installiert, Wartungsarbeiten durchgeführt, aber auch der Zustand des Geräts dokumentiert und weitere Daten etwa über das Nutzungsverhalten des Kunden erhoben. Dies betrifft alle mit dem Internet verbundenen Geräte und dank „Internet of Things" sind das immer mehr in unserem alltäglichen Leben. Der Auslesezyklus kann dabei variieren und hängt etwa davon ab, ob ein Gerät über eine (ständige) Internetverbindung verfügt oder eine Datenübermittlung nur turnusmäßig im Rahmen der Wartung zustande kommt.

Die Nutzer der Produkte können bei Fehlern frühzeitig gewarnt und gezielt individuelle Maßnahmen eingeleitet werden. Umfangreiche öffentliche Rückrufaktionen lassen sich vermeiden. Der Hersteller kann zudem genau sehen, welche Funktionen wie häufig verwendet werden, wie sich der Verschleiß einzelner Teile entwickelt und wo regelmäßig Überbelastungen entstehen. Diese Erkenntnisse kann er bei der künftigen Produktentwicklung berücksichtigen, Verschwendungen und Verbesserungsmöglichkeiten leichter erkennen und die Fehlerquote verringern.

Auf der anderen Seite bleibt diese Entwicklung jedoch auch für den Pflichtenumfang des Herstellers nicht ohne Folgen. Sendet das Produkt auch nach der Auslieferung Statusupdates an den Hersteller, werden abstrakte Produktbeobachtungspflichten auf einmal sehr konkret.

Die Rechtsprechung sieht die Produzenten in der Pflicht, ihre Produkte dauerhaft auf mögliche Gefahren für den Kunden und dessen Eigentum hin zu überwachen. Dies gilt auch für das Zusammenwirken mit (Zubehör-) Produkten anderer Hersteller und nicht immer ist hierfür ein konkreter Anlass erforderlich. So verlangte der Bundesgerichtshof von einem Motorradhersteller und dessen Vertriebsgesellschaft, ein Produkt auch im Hinblick auf Gefährdungen durch die Kombination mit gängigen Zubehörteilen zu überwachen. In dem vom Gericht entschiedenen Fall, beeinträchtigte die Lenkverkleidung eines Zubehörherstellers das Fahrverhalten des Motorrads und führte letztendlich zu einem tödlichen Unfall. Bei Hinweisen auf eine mögliche Gefährdung, muss der Hersteller handeln. Die Bandbreite des Zumutbaren reicht von Hinweisen über medienwirksame Warnungen bis hin zu Rückrufaktionen.

3.10 Handlungsleitlinie: Produktbeobachtung automatisieren und konzeptionell verankern

Hersteller sind gefordert, neue Konzepte zur Produktüberwachung zu entwickeln, zu automatisieren und in den Produktionsprozess zu integrieren. Sicher ist, dass die Rechtsprechung über kurz oder lang auf die veränderten technischen Gegebenheiten reagieren und die Anforderungen für die Hersteller verschärfen wird. Auf der anderen Seite können durch die Beobachtung und Analyse Produktfehler genau einer bestimmten Charge oder Lieferung zugeordnet werden, sodass umfassende und imageschädigende Rückrufaktionen durch eine individuelle Ansprache vermieden werden können. Zudem dürften die Kosten der Produktbeobachtung durch eine weitgehende Automatisierung weiter sinken. Insbesondere im Hinblick auf mögliche Imageschäden sollten Hersteller bei der Planung und Umsetzung derartiger Konzepte allerdings von vorneherein darauf achten, dass diese den Anforderungen des geltenden Datenschutzrechts entsprechen (Privacy by Design) wie im Kapitel 5 näher beschrieben wird.

4. Personenbezogene Daten

4.1 Fallstrick: Personenbezogene Daten kontra „Maschinendaten“

Werden personenbezogene Daten erhoben, verarbeitet oder übertragen, müssen die Vorgaben des Datenschutzrechts beachtet werden. Personenbezogene Daten sind in § 3 Abs. 1 BDSG als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) definiert. Jede Erhebung und Verwendung personenbezogener Daten ist nur aufgrund des Gesetzes zulässig oder wenn die Betroffenen einwilligen. Wer die Daten erhebt, muss die Zulässigkeit beweisen können und grundsätzlich gilt die Regel, Daten möglichst sparsam zu erheben/zu verwenden. Einmal rechtmäßig erhobene personenbezogene Daten sind nicht vogelfrei, sondern jede Verwendung zu einem anderen Zweck muss wieder einer Prüfung standhalten.

Das Datenschutzrecht zwingt zur Transparenz gegenüber dem Betroffenen. Er soll jederzeit eindeutig verstehen können und wissen, wer wann was mit seinen Daten zu welchem Zweck macht. Das gilt gleichermaßen für die Einwilligung wie für die gesetzlichen Zulässigkeitsregelungen.

Darüber hinaus sollte auch bedacht werden, dass Transparenz die Grundlage von Vertrauen und Akzeptanz ist. Gerade neue Entwicklungen können bei Kunden auf Ablehnung stoßen, wenn sie diesen aufgrund fehlender Informationen misstrauen. Einmal entstandenes Misstrauen auszuräumen, ist kostenintensiver als ein gut geplantes transparentes Handeln.

Werden nur „Maschinendaten“ ausgetauscht, kommt das Datenschutzrecht nicht zum Tragen. Erfolgt etwa die Standortkontrolle einer Landmaschine, liegt zwar eine Datenübermittlung vor, aber nicht zwingend von personenbezogenen Daten. Ist allerdings dabei gleichzeitig bekannt, dass eine bestimmte Person die Maschine fährt, handelt es sich bei der Übermittlung des Standorts zugleich um eine Übermittlung personenbezogener Daten – jedenfalls für den Beteiligten, der den Menschen vor Ort identifizieren kann.

Derzeit ist heftig umstritten, wann eine Information einem Menschen zugeordnet werden kann. Die (noch) herrschende Meinung besagt: wenn die datenverarbeitende Stelle das mit eigenen, nicht unverhältnismäßigen Mitteln vornehmen kann. Der so genannte absolute Ansatz bezieht auch die Kenntnisse Dritter ein und rechnet diese der datenverarbeitenden Stelle zu. Dabei kann in der Praxis fast immer der Personenbezug festgestellt werden und das Datenschutzrecht kommt demzufolge zur Anwendung. Häufig werden Daten daher anonymisiert verwendet, um die Betroffenen zu schützen, ohne die Vorgaben des Datenschutzrechts beachten zu müssen. Dies ist auch legitim.

4.2 Handlungsleitlinie: Berücksichtigung des Datenschutzrechts von Anfang an

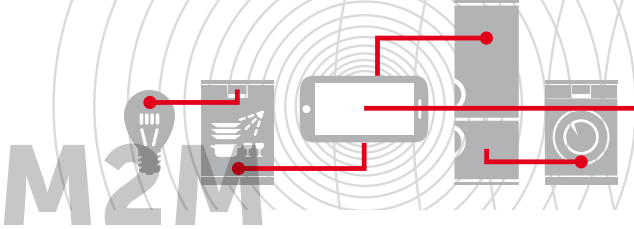
Die datenschutzrechtlichen Aspekte müssen von Anfang an bei der Planung berücksichtigt werden. Die Zulässigkeitsprüfung darf weder „auf die leichte Schulter“ genommen noch kurzfristig „nachgeschoben“ werden.

An erster Stelle steht dabei die Frage, ob personenbezogene Daten überhaupt Gegenstand des Vorgangs sind und falls ja, ob auf diese Daten beziehungsweise auf den Personenbezug der Daten durch Anonymisierung verzichtet werden kann.

Wenn personenbezogene Daten betroffen sind, dann muss hierfür eine Rechtsgrundlage gesucht und gefunden werden. Dies bedarf eventuell einer differenzierten Betrachtung und Bewertung.

4.3 Fallstrick: Datenschutz bei Beschäftigten

Der umfassende Einsatz von M2M-Lösungen erfordert ein besonderes Augenmerk auf den Datenschutz, gerade im Hinblick auf den Schutz der Beschäftigtendaten, denn die Beschäftigten werden dadurch gläsern. Standortdaten, die Qualität der Aufgabenerfüllung, aber auch Vitalfunktionen der Beschäftigten können erfasst werden, um Effizienz und Sicherheit zu erhöhen. Im Logistikbereich lassen sich dabei beispielweise aber auch Extrapausen, Umwege für private Erledigungen oder nicht abgestimmte Arbeitszeiten ermitteln, indem das Fahrzeug überwacht und zum einzelnen Mitarbeiter zurückverfolgt werden kann. Dadurch ergeben sich neue Anforderungen an die Sicherung des Beschäftigtendatenschutzes.



Das BDSG enthält für die in § 3 Abs. 11 BDSG definierten Beschäftigten zwei spezielle Regelungen in § 32 BDSG, die vorrangig vor anderen Datenschutzregelungen sind:

Spezialregelung: der Beschäftigung immanente Datenerhebung und -verwendung

Nach § 32 Abs. 1 S. 1 BDSG dürfen Arbeitgeber personenbezogene Daten von Bewerbern oder Beschäftigten erheben, verarbeiten oder nutzen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Die Zulässigkeit dieser Erhebung, Verarbeitung oder Nutzung setzt voraus, dass sie nach Art und Ausmaß der Datenerhebung und -verwendung in Anbetracht der verfolgten Zwecke angemessen ist. Die Angemessenheit ist nichts anderes als eine Interessenabwägung zwischen dem Interesse des Arbeitgebers an der Erhebung und Verwendung der Daten und des Interesses des Beschäftigten, dass keine Daten über ihn erhoben oder verwendet werden.

Entscheidende „Richtschnur" dieser Interessenabwägung ist der Beschäftigungszweck – also für welche Tätigkeit der Beschäftigte durch den Arbeitgeber eingestellt wird. Dieser setzt sich zusammen aus den gesetzlichen Vorgaben (zum Beispiel Sozialversicherungs- und Steuerrecht), arbeitsrechtlichen Kollektivvereinbarungen (Betriebs- und Tarifvereinbarungen) und natürlich der konkreten Vereinbarung im Arbeitsvertrag selbst.

Damit wird deutlich, dass die Datenverwendung dem Beschäftigungsverhältnis immanent sein – also sich typischerweise aus der Tätigkeit heraus ergeben – muss, um nach § 32 Abs. 1 S. 1 BDSG gerechtfertigt zu sein. Dies wird bei IoT oder Industrie 4.0 (bisher) üblicherweise nicht zwingend der Fall sein.

Spezialregelung: Korruptionsbekämpfung

Die zweite Spezialregelung des Beschäftigtendatenschutzes (§ 32 Abs. 1 S. 2 BDSG) regelt die Erhebung und Verwendung von Daten in Bezug auf Beschäftigte zur „Korruptionsbekämpfung" im Beschäftigtenverhältnis. Diese wird typischerweise bei IoT oder Industrie 4.0 ebenfalls nicht relevant sein.

Rückgriff auf allgemeine Regelungen im BDSG

Darüber hinaus kommt – nach überwiegender, aber nicht unumstrittener Rechtsauffassung – auch § 28 Abs. 1 S. 1 Nr. 2 und Nr. 3 BDSG in Betracht. Grundlage der Zulässigkeit ist danach eine allgemeine Abwägung des Interesses an der Erhebung und Verwendung von Beschäftigtendaten durch den Arbeitgeber gegen das Interesse der Beschäftigten am Ausschluss der Verwendung. Der Unterschied zur bereits angesprochenen Interessenabwägung besteht darin, dass die Interessen nicht dem Beschäftigungsverhältnis immanent sein müssen, sondern auch andere Interessen an der Erhebung und Verwendung der Beschäftigtendaten herangezogen werden können. Aber auch danach muss die Zulässigkeit mit Blick auf das besondere Schutzbedürfnis des Betroffenen im Beschäftigungsverhältnis restriktiv gehandhabt werden. Bei einer Interessenabwägung kann die Gewichtung in Bezug auf denselben Sachverhalt unterschiedlich erfolgen. Für IoT oder Industrie 4.0 haben sich hierzu bisher noch keine Leitlinien etabliert.

Einwilligung des Beschäftigten als Rechtsgrundlage

Daneben kommt die Einwilligung des Betroffenen in Betracht, um die Datenerhebung und -verwendung durch den Arbeitgeber zu legitimieren. Allerdings ist eine Einwilligung nur dann wirksam, wenn sie freiwillig durch den Betroffenen erteilt wird. Es besteht derzeit eine starke – wenngleich kritikwürdige – Tendenz in der Praxis, die Freiwilligkeit der Einwilligung von Beschäftigten grundsätzlich zu verneinen und diese nur dann zu bejahen, wenn dem Beschäftigten eine echte Alternative zur Bejahung der Einwilligung bleibt. Dahinter steckt die Überlegung, dass Beschäftigte aufgrund des faktischen „Machtgefälles" im Beschäftigungsverhältnis kaum frei über Ja oder Nein in Bezug auf die Datenerhebung und -verwendung entscheiden können.

Betriebsvereinbarung als Rechtsgrundlage

Als weitere Rechtsgrundlage sind im Beschäftigungsverhältnis so genannte Betriebsvereinbarungen anerkannt. Während diese in der Vergangenheit recht großzügig als Ersatz für eine individuelle Einwilligung betrachtet wurden, besteht zwischenzeitlich Zurückhaltung. Betriebsvereinbarungen sind demnach zwar geeignet, die gesetzlichen Zulässigkeitsgrenzen „ein wenig zu dehnen". Sie sind aber nicht geeignet, die Erhebung und Verwendung zulässig zu machen, welche die Grenzen der gesetzlichen Zulässigkeitsregelungen grundlegend überschreiten.

4.4 Fallstrick: Datenschutz bei Kunden

Bei IoT oder Industrie 4.0 profitiert der Kunde davon, wenn er Daten über seine Maschine sendet, weil der Hersteller so beispielsweise viele Probleme bereits im Vorfeld erkennen kann: Fehlfunktionen und teure Ausfallszeiten entstehen erst gar nicht. Meldet etwa ein Vibrationsmuster die Abnutzung an einem Maschinenfräskopf, kann der Hersteller proaktiv den Kunden kontaktieren und ihn bei der Behebung des Problems unterstützen. Anfahrtskosten und Vor-Ort-Termine werden reduziert, denn der Hersteller kann sich einfach in Echtzeit aufschalten und so Support leisten. Dabei kann er auch sehen, welche Releasestände eingespielt wurden und beim Update helfen – Over the Air und eben nicht mehr per USB-Stick. Allerdings kann der Hersteller nun auch genau sehen, wann der Kunde eine Maschine wie nutzt und ob er vielleicht etwas daran verändert/manipuliert hat.

Die Erhebung und Verwendung von Daten der Kunden gestaltet sich etwas einfacher als bei den Beschäftigten. Die Zulässigkeitsbegrenzung ist nach dem BDSG an eine Interessenabwägung gebunden. Das Interesse an der Erhebung und Verwendung von Kundendaten wird abgewogen gegen das Interesse der Betroffenen am Ausschluss der Erhebung beziehungsweise Verwendung. Für IoT oder Industrie 4.0 haben sich hierzu bisher noch keine Leitlinien etabliert.

Kommen gesetzliche Zulässigkeitsregelungen nicht in Betracht oder decken das Geplante nicht ab, könnte eine freiwillige Einwilligung des Kunden eingefordert werden. Immerhin bringen die Datenerhebungen und -auswertungen für diesen wie eingangs beschrieben viele Vorteile mit sich. Gemäß der in Kapitel 4.1 aufgeführten Vorgaben muss dabei natürlich transparent sein, welche Daten gesammelt und von wem wofür verwendet werden etc.

Wichtig ist auch hier die Prüfung, inwiefern Daten konkret einzelnen Kunden zugeordnet werden müssen, also personenbezogen sind oder ob vielleicht eine allgemeine und anonymisierte Erhebung genügt, um etwa Produkte zu optimieren.

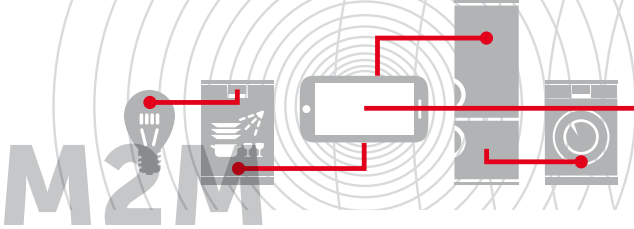
4.5 Fallstrick: Auslandsübermittlung personenbezogener Daten

Ein Datentransfer innerhalb der EU/des Europäischen Wirtschaftsraums (EWR) wird wie ein Datentransfer innerhalb Deutschlands behandelt und bedarf daher keiner gesonderten Prüfung.

Erfolgt der Datentransfer in einen so genannten Drittstaat – also außerhalb von EU/EWR – bedarf es einer weiteren datenschutzrechtlichen Prüfung. Kontrolliert den Standort einer Landmaschine, die im EU/EWR-Raum tätig ist, die Niederlassung eines Unternehmens außerhalb des EU/EWR-Raums liegt eine Datenübermittlung in einen Drittstaat vor (vorausgesetzt, dass es sich um personenbezogene Daten handelt). Bei der Datenübermittlung an Drittstaaten setzt das deutsche beziehungsweise europäische Datenschutzrecht enge Grenzen.

Bisher hat die Europäische Kommission für einige wenige Länder wie Kanada, die Schweiz oder Argentinien die generelle Feststellung getroffen, dass die Datenübermittlung dorthin zulässig ist. Für die übrigen Länder kommt es darauf an, ob bei dem datenempfangenden Unternehmen ein angemessenes Datenschutzniveau sichergestellt ist.

Für die USA existierte bis zum 06.10.2015 eine Sonderregelung, das so genannte „Safe-Harbor"-Abkommen. Nach diesem Abkommen war eine Datenübermittlung an ein dort ansässiges Unternehmen oder Teile davon zulässig, wenn sie sich verpflichten, ein dem europäischen beziehungsweise deutschen Datenschutz entsprechendes Niveau einzuhalten. Es handelte sich dabei um eine Art Selbstzertifizierung des Unternehmens mit Unterwerfung unter Sanktionen durch US-Aufsichtsinstanzen. Dieses „Safe-Harbor"-Abkommen wurde in Deutschland jedoch von den Datenschutzaufsichtsbehörden erheblich kritisiert, weil bezweifelt wurde, dass diese Verfahren tatsächlich das angestrebte Schutzniveau schaffen. Mit Urteil vom 06.10.2015



erklärte der Europäische Gerichtshof (EuGH) die Entscheidung 2000/520/EG der EU-Kommission, auf welcher dieses „Safe Harbor-Prinzip" beruhte, für unwirksam (Az. C-362/14). Das „Safe-Harbor"-Abkommen ist keine Rechtsgrundlage mehr für einen Datentransfer in die USA oder einen Zugriff auf Daten in der EU aus den USA. Es müssen alternative Gestaltungen – beispielsweise die so genannten EU-Standardverträge – gewählt werden.

4.6 Handlungsleitlinie: Datenschutzrechtliche Genehmigungen einholen

Werden personenbezogene Daten in Drittstaaten außerhalb des EU/EWR-Raums übertragen, sind Garantien und gegebenenfalls datenschutzrechtliche Genehmigungen erforderlich. In erster Linie kommen hierfür die so genannten EU-Standardverträge zur Datenübermittlung in Betracht. Der Abschluss dieser Vereinbarung zwischen dem datenübermittelnden und dem -empfangenden Unternehmen schafft ein datenschutzrechtlich angemessenes Schutzniveau bei dem datenempfangenden Unternehmen. Daneben kommen auch individuell gestaltete Verträge in Betracht, diese bedürfen jedoch der Genehmigung durch die zuständige deutsche Datenschutzaufsichtsbehörde, um den Anforderungen der §§ 4b, 4c BDSG zu genügen.

Beim Austausch von Daten innerhalb von Unternehmensgruppen können Binding Corporate Rules (BCR) die rechtmäßige Datenübermittlung vereinfachen. Diese bedürfen jedoch ebenfalls der Genehmigung durch die zuständige Datenschutzaufsichtsbehörde.

5. Kartell- und regulierungsrechtliche Aspekte

5.1 Fallstrick: Schmaler Grat zwischen enger Kooperation und kartellrechtlich relevanten Absprachen

Durch die enge Vernetzung von Software- und Maschinenherstellern, Zulieferern und Vertrieb entstehen faktische und vertragliche Beziehungsgeflechte und Abhängigkeitsverhältnisse, die über die oben genannten rechtlichen Fallstricke der gemeinsamen Datennutzung hinausgehen. Letztendlich ist es nur eine schmale Gratwanderung zwischen einer engen Kooperation und kartellrechtlich relevanten Absprachen. Aus einem intelligenten Vertriebssystem wird so über Nacht ein selektives.

Durch die (exklusive) Kooperation mit einem Hersteller eines bestimmten, branchenspezifischen Maschinentyps, steht auch kleinen Softwarefirmen die Möglichkeit offen, ihre direkten Konkurrenten (andere Softwarehersteller) vom Markt zu verdrängen oder die so gewonnene Schlüsselstellung dazu zu nutzen, den nachgelagerten Produktionsmarkt nachhaltig zu beeinflussen. Insbesondere im Bereich von IoT oder Industrie 4.0 kommt es letztendlich auf die Programmierung und Definition von Schnittstellen an. Aus dem legitimen Schutz der eigenen Urheberrechte und Patente wird so schnell die Abschottung ganzer Märkte. Eine derartige missbräuchliche Ausnutzung der eigenen marktbeherrschenden Stellung zieht neben empfindlichen Bußgeldern nicht selten auch die Pflicht zur Offenlegung der Schnittstellen zugunsten einer weitreichenden Interoperabilität und in letzter Konsequenz die Einräumung von Zwangslizenzen nach sich.

5.2 Handlungsleitlinie: Auch KMU müssen wettbewerbs- und kartellrechtliche Rahmenbedingungen für sich prüfen

Mit zunehmender Komplexität der Kooperations- und Vertragsverhältnisse im Bereich M2M und Industrie 4.0 wird es, insbesondere für Mittelständler, umso wichtiger, sich mit den auch für sie geltenden wettbewerbs- und kartellrechtlichen Rahmenbedingungen auseinanderzusetzen.

5.3 Fallstrick: Hersteller wird zum Telekommunikationsdienst

Begreift man IoT oder Industrie 4.0 als ein umfassendes (Tele-) Kommunikationskonzept, bei dem nicht nur die einzelnen Maschinen innerhalb der Produktionskette kommunizieren, sondern auch das zu fertigende Endprodukt einbezogen wird, wird der Hersteller in der Regel zugleich auch als Telekommunikationsdienst (§ 3 Nr. 24 TKG) zu qualifizieren sein. Neben bloßen regulatorischen Aspekten wie beispielsweise der Meldepflicht (§ 6 TKG) und der Aufsicht durch die Bundesnetzagentur, rücken hier vor allem sicherheits- und haftungsrechtliche Aspekte in den Vordergrund. Welche dies im Einzelnen sind, hängt dabei maßgeblich von den Umständen des jeweiligen Geschäftsmodells ab. Letztendlich stellen der vermehrte Einsatz und die fortschreitende Entwicklung der Kommunikation eine Herausforderung für das Regulierungsregime des Telekommunikationsrechts dar, auf die früher oder später auch der Gesetzgeber reagieren muss.

5.4 Handlungsleitlinie: Regelungen des Telekommunikationsrechts bedenken

Auch hier gilt es gerade für Mittelständler, sich mit den rechtlichen Rahmenbedingungen des Telekommunikationsrechts auseinanderzusetzen und das eigene Geschäftsmodell im Hinblick auf entsprechende Fallstricke zu überprüfen.

6. Handelsbeschränkungen

6.1 Fallstrick: Handelsbeschränkungen bei länderübergreifendem M2M-Einsatz

Im Hinblick auf den länderübergreifenden Einsatz von M2M-Lösungen muss bedacht werden, dass einzelne Komponenten, zum Beispiel bestimmte Verschlüsselungstechniken, nationalen und internationalen Handelsbeschränkungen unterliegen.

6.2 Handlungsleitlinie: Handelsbeschränkungen in Geschäftsmodelle und Prozesse einbeziehen

Weil das Interesse an sicheren Kommunikationstechniken beim Einsatz von IoT- oder Industrie-4.0-Lösungen als hoch einzuschätzen ist und im jeweiligen Interesse der Beteiligten liegt, müssen im Rahmen eines länderübergreifenden Einsatzes derartige Restriktionen berücksichtigt werden. Nationale und internationale Handelsbeschränkungen müssen in Geschäftsmodelle und Prozesse einbezogen werden.

Autoren

Dr. Bettina Horster
Vorstand Business Development bei der VIVAI Software AG, Direktorin Mobile bei eco – Verband der Internetwirtschaft

Die Diplom-Informatikerin Dr. Bettina Horster leitet bei der VIVAI Software AG den Bereich Business Development und Consulting und ist zudem für das Ressort Industrie 4.0 zuständig. Sie führte eines der ersten EU-Projekte im Bereich Industrie 4.0, das 2014 von der Initiative „Deutschland – Land der Ideen" von Bundesregierung und BDI ausgezeichnet wurde. Viele Jahre beriet sie das Bundeswirtschaftsministerium und das Wirtschaftsministerium des Landes NRW in Fragen mobiler Technologien. Seit 1996 leistet sie echte Pionierarbeit rund mobile Services. Durch diverse Studien, Veranstaltungen, wissenschaftliche Ausarbeitungen und extensive Pressearbeit hat sie die Mobile-Szene maßgeblich beeinflusst. Seit 1999 leitet sie die Kompetenzgruppe Mobile bei eco – Europas größtem Verband der Internetwirtschaft.

Dr. Sebastian Brüggemann
Rechtsanwalt, Lehrbeauftragter

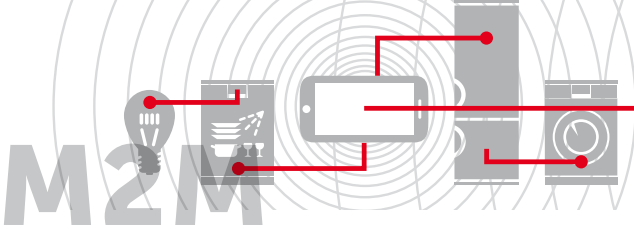
Dr. Sebastian Brüggemann, M.A., ist Rechtsanwalt und Lehrbeauftragter für Internetrecht an der Juristischen Fakultät der Eberhard Karls Universität Tübingen. Als Rechtsanwalt berät er mittelständische und internationale Unternehmen sowie Kreativschaffende in Fragen des Informationstechnologie-, Urheber-, Medien- und Datenschutzrechts. In dieser Funktion war er unter anderem für die mittelständische Sozietät SGT Rechtsanwälte (Stuttgart) sowie im Team Technologie, Medien, Telekommunikation der PwC Legal AG Rechtsanwaltsgesellschaft (Düsseldorf) tätig. Neben den Themen M2M, Internet der Dinge (IoT) und Industrie 4.0 gilt sein besonderes Interesse den aktuellen Entwicklungen der Start-up-Szene.

Dr. Jens Eckhardt
Rechtsanwalt und Fachanwalt für Informationstechnologierecht, JUCONOMY Rechtsanwälte

Dr. Jens Eckhardt ist Partner der Sozietät JUCONOMY Rechtsanwälte in Düsseldorf und seit 2001 als Rechtsanwalt in den Bereichen Informationstechnologie, Telekommunikation, Datenschutz und Marketing tätig. Seit 15 Jahren hält er auch regelmäßig Vorträge und verfasst Veröffentlichungen, insbesondere zu verschiedenen Aspekten des Datenschutzrechts, des Telekommunikationsrechts und des Marketings; unter anderem ist er Mitautor des Beck'schen TKG-Kommentars (Verlag C. H. Beck), des Kommentars Recht der elektronischen Medien (Verlag C. H. Beck) und des Beck'schen Mandatshandbuchs IT-Recht (Verlag C. H. Beck). Zudem doziert er an der Ulmer Akademie für Datenschutz und IT-Sicherheit (udis) gGmbH zum Thema Datenschutzrecht. Bei EuroCloud Deutschland_eco e. V. ist er als Vorstand im Ressort Recht & Compliance tätig und leitet die Kompetenzgruppe Recht.

Dr. Jan-Peter Ohrtmann
Rechtsanwalt, PwC Legal

Rechtsanwalt Dr. Jan-Peter Ohrtmann leitet das Team Technologie, Medien, Telekommunikation der PwC Legal AG Rechtsanwaltsgesellschaft, ist fachlicher Leiter der Datenschutzpraxis von PwC und PwC Legal und Mitglied der EU Data Privacy Steering Group der PwC Netzwerkgesellschaften. Vor seiner anwaltlichen Tätigkeit war er zwischen 2000 und 2002 in einem Start-up-Unternehmen im Bereich Online-Ticketing für den Bereich Recht verantwortlich. Seit nunmehr über zwölf Jahren berät er anwaltlich in der gesamten Bandbreite des IT-Rechts. Dr. Ohrtmann war zwischen 2004 und 2014 Lehrbeauftragter der Heinrich-Heine-Universität Düsseldorf im LL.M.-Studiengang Informationsrecht zum IT-Outsourcing und Datenschutzrecht, referiert regelmäßig zu IT-rechtlichen Themen und ist Autor verschiedener Fachbeiträge.



Rechtlicher Hinweis

1. Allgemeines

Die in diesem Leitfaden zur Verfügung gestellten Informationen dienen der allgemeinen Darstellung der rechtlichen Rahmenbedingungen für die Themen M2M und Internet of Things , stellen keine Rechtsberatung dar und können auch keine Rechtsberatung ersetzen, da eine solche immer die Kenntnis aller Einzelumstände, insbesondere des konkreten Einzelfalls voraussetzt.

2. Inhalt des Leitfadens

Die Herausgeber/Autoren übernehmen keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der bereit gestellten Informationen. Dies gilt insbesondere im Hinblick auf neueste Entwicklungen in der Rechtsprechung oder der Gesetzeslage. Haftungsansprüche gegen die Herausgeber/Autoren, die sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens der Herausgeber/Autoren kein nacheislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.

3. Verweise und Links

Bei direkten oder indirekten Verweisen auf fremde Inhalte (z. B. „Links"), die außerhalb des Verantwortungsbereichs der Herausgeber/Autoren liegen, würde eine Haftungsverpflichtung ausschließlich in dem Fall in Kraft treten, in dem die Herausgeber/Autoren von den Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar wäre, die Nutzung im Falle rechtswidriger Inhalte zu verhindern. Die Herausgeber/Autoren erklären hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der verlinkten Seiten haben die Herausgeber/Autoren keinen Einfluss. Sie distanzieren sich ausdrücklich von allen Inhalten aller verlinkten Seiten, die nach der Linksetzung verändert wur- den. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotener Informationen entstehen, haftet allein der Anbieter der Seite, auf welche verwiesen wurde, nicht diejenigen, die über Links auf die jeweilige Veröffentlichung lediglich verweisen.

4. Urheberrecht

Die in diesem Leitfaden dargestellten Inhalte wie Texte, Grafiken oder Bilder sind nach dem deutschen Urhebergesetz urheberrechtlich geschützt. Jede urheberrechtlich nicht gestattete Verwertung bedarf der vorherigen schriftlichen Zustimmung des Herausgebers. Beiträge Dritter sind als solche gekennzeichnet. Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien. Die unerlaubte Vervielfältigung oder Weitergabe einzelner Teile oder des gesamten Leitfadens ist ausdrücklich nicht gestattet. Ausgenommen ist dabei der individuelle bzw. private Gebrauch, wobei die private Nutzung kein Recht zur Weitergabe an Dritte beinhaltet. Gleiches gilt für Veröffentlichungen oder sonstige Arbeiten.

Impressum

eco – Verband der Internetwirtschaft e.V.
Lichtstraße 43h
50825 Köln

Tel: 0221 / 700048 – 0
Fax: 0221 / 700048 – 111
E-Mail: info@eco.de
Web: www.eco.de

Vorstand:
Prof. Michael Rotert (Vorsitzender),
Oliver Süme (stv.
Vorsitzender)
Klaus Landefeld
Felix Höger
Prof. Dr. Norbert Pohlmann

Vereinsregister: Amtsgericht Köln, VR 14478
Sitz des Vereins: Köln

Verband der Internetwirtschaft e.V.

eco – Verband der Internetwirtschaft e.V.
Lichtstraße 43h, 50825 Köln
fon +49(0)221/700048-0
fax +49(0)221/700048-111
info@eco.de, www.eco.de

20 JAHRE eco

WIR GESTALTEN DAS INTERNET.
GESTERN.HEUTE.ÜBER MORGEN.

eco