Datenmanagement im Unternehmen

Ulrich Herfurth, Rechtsanwalt in Hannover und Brüssel

Oktober 2018

Die Digitalisierung im Unternehmen bedeutet zum einen die Organisation betrieblicher Abläufe in strukturierten Prozessen, die digital, automatisch und vernetzt ausgeführt werden. Zum anderen entwickeln sich aus der Gewinnung und den Nutzungsmöglichkeiten von Daten ganz neue Geschäftschancen und Geschäftsmodelle.[1]

Digitalisierung ist also sowohl eine operative Aufgabe (*Digitization*) als auch eine strategische Herausforderung und Chance (*Digitalization*). Dies gilt gerade auch für den Mittelstand und kleinere Unternehmen.

Die rechtlichen Fragen zum Umgang mit Daten ziehen sich durch alle Unternehmensbereiche: Unternehmensstruktur, Finanzen, Betrieb, Personal, Markt und Kunden, Produktion und Entwicklung.

Strukturierte Daten sind daher ein geschütztes Gut, Rohstoff, Vermögen und wertvoller Schatz eines Unternehmens. Die Digitalisierung im Unternehmen erfordert nun Maßnahmen in mehreren Handlungsfeldern, die eng ineinandergreifen. Diese kann man in den Bereich Geschäftsentwicklung und dann in die vier großen Bereiche im Betrieb gliedern: Datenschutz, Datensicherheit, Dateneigentum und Daten Compliance.

Entwicklung von digitalen Geschäftsmodellen

Neue Geschäftsmodelle basieren inzwischen weitgehend auf digitalen Strukturen. Ihr Reiz liegt in der Möglichkeit der Skalierung, also der Chance auf eine exponentielle Steigerung des Geschäftsvolumens ohne einen vergleichbaren Anstieg des Aufwands. Digitale Plattformen für Handel und Dienstleistungen sind dafür die besten Beispiele.

Rechtlich geht es dabei oft um vielschichtige Fragen: Wer darf digitale Informationen nutzen, welche gesetzlichen Bedingungen sind dazu einzuhalten, welche persönlichen Daten unterliegen dem Datenschutz und welche Schutzrechte sind zu beachten? So kollidierte das Unternehmen *Uber* in Deutschland mit dem Personenbeförderungsgesetz und in Kalifornien werden die selbständigen Fahrer nun wie Angestellte angesehen. Aber auch Urheberrecht und Patente können die freie Nutzung von Technologie einschränken.

Datensicherheit schützt Unternehmen und Betrieb

Die Datensicherheit gegenüber Unfällen, Angriffen und unbefugten Zugriffen gehört zu den größten Herausforderungen und ist oft noch ein Hindernis für die Digitalisierung von Prozessen im Unternehmen.
Datensicherheit, zugleich als IT-Sicherheit, ist zunächst eine Frage von technischen und organisatorischen Maßnahmen. Aus rechtlicher Sicht muss das Unternehmen aber ebenfalls geeignete Maßnahmen

[1] Der Beitrag ist ebenfalls erschienen im RKW Magazin 3-2018

treffen, Kontrollen ausüben und Sicherungen vorsehen. Zunächst einmal geht es um die Definition von IT-Sicherheitspflichten des Managements. Dazu gibt das Basisschutzkonzept des BSI (*Bundesamt für Sicherheit in der Informationstechnologie*) eine gute Grundlage. Zusätzlich hilft die Norm 27001, sie ist allerdings etwas aufwändig zu erfüllen. Für den Betrieb empfehlen sich Unternehmensregeln zur Datensicherheit, zum Beispiel Sicherheits- und Schutzkonzepte bei der Benutzung des IT-Systems und privater Geräte für den Betrieb. Immerhin sind Smartphones und USB-Sticks ein beliebtes Einfallstor für Schadsoftware.

Setzt das Unternehmen Dienstleister ein, sollte es sich die Sicherheitsbestimmungen und Garantien in den Verträgen genau ansehen. Wie weit haften der Provider, der Software Service-Anbieter oder das Outsourcing-Unternehmen für Datenverluste und Betriebsausfälle?

Schließlich können finanzielle Risiken zum Teil abgesichert werden, die Hardware mit der IT-Versicherung, Software mit einer Zusatzpolice und Risiken aus dem Zugriff Unbefugter durch eine Cyberpolice.

Europaweiter Datenschutz

Datenschutz ist als Schutz von Personendaten zu verstehen. Die neue Europäische Datenschutzgrundverordnung (DSGVO) verlangt nun seit dem 25. Mai 2018, dass Unternehmen sich an weitere und strenger sanktionierte Regelungen halten und die Daten ihrer Mitarbeiter, Kunden und anderer Personen rechtlich korrekt behandeln.

Datenschutz muss technisch und organisatorisch aufgebaut sein, zudem in Form von Informationen und Schulungen der Mitarbeiter. Aus rechtlicher Sicht muss das Unternehmen dazu geeignete Maßnahmen treffen, Kontrollen ausüben und Sicherungen vorsehen.

Dies beginnt mit der Vorbereitung und einem Check zur Einhaltung der EU-Datenschutzgrundverordnung. Die ersten Maßnahmen haben die meisten Unternehmen erledigt, nämlich eine Datenschutzerklärung auf ihrer Website und für ihre Kunden, oft auch kombiniert mit einer Einwilligung in die Nutzung der Kundendaten für eigene Werbung, Newsletter usw.

Hinzu kommt nun ein Verarbeitungsverzeichnis, in dem das Unternehmen darstellt, wohin seine Daten fließen und wie sie weiter behandelt werden, zum Beispiel gelöscht.

Etwas anspruchsvoller sind dann Unternehmensrichtlinien zum Datenschutz und Verfahren zu Datenschutzkonzepten.

Natürlich müssen die Mitarbeiter zu Datenschutzanforderungen geschult werden, am besten mit einem didaktisch strukturierten Plan.

In bestimmten Fällen benötigt das Unternehmen auch eine Datenschutzfolgenabschätzung, eine Strategie zur Störfallvermeidung und zum Störfallmanagement und einen Datenschutzbeauftragten.

Bei externer Datenverarbeitung verlangt das Gesetz sichere Auftragsdatenverarbeitungsverträge.

Und bei der Weitergabe von Personendaten in Drittländer außerhalb der EU die Einhaltung bestimmter Regeln und Standards, zum Beispiel auch an Tochterunternehmen in den USA. Das Gesetz verlangt im Übrigen, dass die Personendaten sicher sind, also gegen Zugriffe von außen geschützt.

Eigentum an Daten?

Betriebliche Daten, die im laufenden Prozess anfallen und erfasst werden (Maschinendaten), stellen für das Unternehmen und andere Interessierte oft eine Quelle interessanter Erkenntnisse dar. Sie haben für Unternehmen einen besonderen Wert. Allerdings gibt es im rechtlichen Sinn kein Eigentum an maschinengenerierten Daten, abgesehen von Betriebsgeheimnissen in besonderen Fällen.

Der Umgang mit Daten und deren Überlassung an Geschäftspartner muss daher individuell geregelt werden: aus rechtlicher Sicht muss das Unternehmen mit *Data Use Agreements* geeignete Maßnahmen treffen, Kontrollen ausüben und Sicherungen vorsehen. Dazu gehören zunächst die Analyse und Definition von Datenströmen (Kunden, Lieferanten, Partner),

die Analyse zu Schutzrechten für Geistiges Eigentum und eine Schutzstrategie für überlassene Daten. Dies lässt sich am besten mit Datennutzungsvereinbarungen und Lizenzen mit Partnern umsetzen, teilweise auch mit Datennutzungsklauseln in AGB oder in Apps.

Mindestens sollte ein Unternehmen Vertraulichkeitsvereinbarungen mit seinen Nutzern treffen. Im Grunde empfiehlt sich, dass die Geschäftspartner überlassene Daten nur zum Zweck des gemeinsamen Geschäfts nutzen dürfen, nicht aber unentgeltlich, um daraus weitere Erkenntnisse zu ermitteln und wirtschaftlich zu verwerten. Besonders deutlich wird dies in der Wartung von Maschinen und Anlagen: Hersteller, Betrieb und Wartungsunternehmen haben gleichermaßen ein Interesse an der Auswertung und Verwertung der Maschinendaten.

Daten-Compliance für Rechtssicherheit

Der Umgang mit Daten und IT unterliegt nicht nur privatrechtlichen Interessen und Verträgen, sondern muss auch die staatlichen Vorgaben beachten und Anforderungen erfüllen. Das Unternehmen muss daher geeignete Maßnahmen treffen, Kontrollen ausüben und Sicherungen vorsehen. Die wichtigsten Anforderungen liegen bereits im Datenschutz begründet.
Daneben gibt es diverse Informationspflichten, zum Beispiel im Impressum auf der Website und im Online-Handel.
Und bei dem Transfer von Daten in das Ausland muss ein Unternehmen Kontrollpflichten beachten, wenn es sich dabei um Technologie im Sinn der Außenwirtschaftsverordnung handelt.

Legal Scan für die Unternehmensführung

Die Summe dieser Aufgaben ist für so manches kleine und mittlere Unternehmen durchaus eine Herausforderung. Die Praxis zeigt aber, dass mit einem systematischen Vorgehen die anstehenden Fragen effizient und kostenorientiert abgearbeitet werden können.

Als ein erster Schritt bietet sich dazu die *Legal Scan Methode* an, mit der die Geschäftsleitung in checklistengestützten Interviews eine aktuelle Bestandsaufnahme der Situation im Unternehmen durchführt. Die Methode ist keine gründliche Unternehmensprüfung, sondern eine schnelle und effiziente Ermittlung der Situation. Die Ergebnisse sind durchaus subjektiv, je nach Blickwinkel der Geschäftsleitung, und werden noch umfassender, wenn sie im Team ermittelt werden.

Daran ist interessant, dass die Erkenntnisse nicht höchstpräzise sind, aber sehr schnell ein weitgehend treffendes Bild zeichnen. Die Auswertung der Interviews erfolgt in einem Scoring auf Basis eines Punktesystems und gibt dem Unternehmen zugleich erste Handlungsanweisungen. Dieses Vorgehen ist gerade für kleine und mittlere Unternehmen hilfreich.

Haftung des Managements

Die beschriebenen Aufgabenbereiche zeigen, dass die Unternehmensführung gerade im Umgang mit Daten des Unternehmens in erhebliche Verantwortung und damit auch in ein Haftungsrisiko kommt.

Die Pflichten des Geschäftsführers umfassen auch die Sorgfaltspflicht, und diese bestimmt sich nach dem Maßstab eines sorgfältigen Kaufmanns. Dabei kann er nicht jedes Risiko aus der Geschäftstätigkeit ausschließen, insbesondere wird er oft vor der Frage stehen, welche Maßnahme er ergreift oder ob er sogar nicht tätig wird. Seine Entscheidungen werden an der *Business Judgement Rule* gemessen, also wie er sein unternehmerisches Ermessen ausübt. Eine Entscheidung muss daher auf einer belastbaren Informationsgrundlage und einer sorgfältigen und nachvollziehbaren Abwägung der Vor- und Nachteile der verschiedenen möglichen Maßnahmen beruhen. So mag es sein, dass er kleinere, sehr wahrscheinliche Risiken in Kauf nimmt, um ein hohes Einzelrisiko mit sehr geringer Wahrscheinlichkeit zu vermeiden oder aber umgekehrt. Hohe, aber unwahrscheinliche Risiken sollte er allerdings gegen Prämie solidarisieren, also versichern.

Untätigkeit selbst kann durchaus auch ein Risiko darstellen, wenn sie als Versäumnis zu bewerten ist: so wäre es wohl eine Verletzung der Sorgfaltspflicht, wenn der Geschäftsführer keine geeignete Cyberversicherung abschließt, nur um die Prämie zu sparen.

Generell sind betriebliche Entscheidungen typischeweise konkreter fassbar und mit technisch-

organisatorischen oder juristischen Maßnahmen zu erfassen und einzudämmen. Demgegenüber lassen sich geschäftliche Entscheidungen oft sehr viel schwieriger bewerten.

Die Entscheidung, auf welche Weise und in welchem Umfang das Unternehmen seine Geschäftsmodelle auf digitale Modelle umstellt, ist stets eine Herausforderung für die Geschäftsführung. Erfolgt die Umstellung zu früh, kann das Unternehmen den Wechsel nicht verkraften – das neue digitale Geschäft kannibalisiert vielleicht die klassischen Bereiche schneller, als es neue Erträge abwirft.

Wenn umgekehrt das Unternehmen zu spät oder gar nicht auf digitale Modelle umstellt, der Wettbewerb dazu aber neue und überlegene Modelle, Produkte und Leistungen anbietet, wird dies Einbußen im Markt und im Extremfall sogar den Untergang des Unternehmens bedeuten. Solche Managemententscheidungen sind zwar meist nicht justitiabel, können als nicht nach dem Verschuldensprinzip zur Haftung des Geschäftsführers führen – die Karriere des Managegers wird aber für die Zukunft deutlich beeinträchtigt sein.

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); 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, Bratislava, Brüssel, Budapest, Bukarest, Helsinki, Istanbul, Kiew, Kopenhagen, Lissabon, London, Luxemburg, 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, Tokio, Sydney.

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