Aktuelles Recht für die Praxis

Datenschutz im Unternehmen

Bearbeitet von
Von Dr. Michael Wächter

5. Auflage 2017. Buch. XX, 483 S. Kartoniert
ISBN 978 3 406 71525 9
Format (B x L): 14,1 x 22,4 cm

schlossen wird. Dies zB nicht für Sub-Tools für vereinbarte Anwendungen oder für Anwendungen für wenige Mitarbeiter. Nach der DSGVO können zu den Tools, die nicht vereinbart werden, im Besonderen solche gehören, die **ohne Risiken** für Mitarbeiter sind. Maßstab für die Risikoeinschätzung ist Art. 24. Für die grundsätzliche Fragestellung der Definition einer Verhaltens- und Leistungskontrolle könnte der Maßstab des **Profiling** nach Art. 4 Nr. 4 dienen. Es könnte vereinbart werden, dass erst ab Bejahung eines Profiling oder dem Vorliegen einer **automatisierten Entscheidung** nach Art. 22 eine Betriebsvereinbarung abgeschlossen wird. Dies könnte für datenbasierte Unternehmen interessengerecht sein, die im Rahmen der **Industrie 4.0** auf eine digitale Produktionssteuerung und nicht primär auf menschliches Verhalten abstellen. Ferner sollte praxisgerecht definiert werden, mit welcher Abstraktion die **Zweckbestimmung** von Datenverarbeitungen festgelegt wird. Auch muss eine Festlegung erfolgen, in welchen Fällen eine **Zweckänderung** der Datenverarbeitung vorliegt.

Neben einer Basis-Betriebsvereinbarung sollten Einzelvereinbarungen **306**
abgeschlossen werden, die mit den Grundgedanken der abgeschlossenen Basis-Betriebsvereinbarung übereinstimmen. Betriebsvereinbarungen sind damit ein Werkzeug, **Zulässigkeitsanforderungen** betriebsindividuell zu regeln. Nach Art. 6 iVm Art. 5 sind dabei nicht nur Anwendungen und Unternehmensprozesse zu betrachten, sondern es ist Datenschutz auch auf der Ebene der einzelnen Daten zu gewährleisten. Dieses Regelungserfordernis auf Basis jedes einzelnen Betroffenen betrifft insofern **Arbeitnehmerdaten** ebenso wie Kunden- und Lieferantendaten. Hierzu sind Anwendungen zu nutzen, die dafür Sorge tragen, dass Daten immer akkurat, komplett und nicht doppelt vorliegen. Nach der DSGVO geht es heute um die Herstellung und Aufrechterhaltung von **Datenqualität**. Dabei ist eine Vorgehensweise, die Datenverarbeitung rechtmäßig zu gestalten, nach Art. 5 I b die **Festlegung legitimer Zwecke**. Diese sind in den Betriebsvereinbarungen explizit zu benennen und zu beschreiben. Ein problematischer Punkt ist bei der weiteren Verarbeitung der Daten die Zusammenführung von **Daten zu anderen Zwecken** sowie auch das Vorhandensein von Schnittstellen zu anderen Systemen. Denn die Daten können dann von anderen Systemen kombiniert und einer neuen multifunktionalen Nutzung zugeführt werden, die nicht definiert wurde.

Ein Beispiel für eine Einzelbetriebsvereinbarung ist eine Vereinbarung **307**
für den Vertriebsbereich zu Kundendatenbanken für Vertriebsgebiete der Mitarbeiter. Weitere Beispiele sind Vereinbarungen zu Skill-Analysen, Marketing- und Schulungs-Aktivitäten. Die dazu im Unternehmen abgeschlossenen Betriebsvereinbarungen können dann als ein **flexibles Baukastensystem** genutzt werden. Ergeben sich dann Nutzungen von Tools außerhalb der vereinbarten Zweckbestimmungen oder ändert sich die Zweckbestimmung einzelner Tools gravierend, so muss ein Nachtrag für

die betroffene Betriebsvereinbarung verhandelt werden. Alternativ könnte auch eine neue Zuordnung zu einem anderen Themengebiet (Cluster) erfolgen oder es kann auch bei einer vollständig neuen Thematik ein neues Cluster geschaffen werden. Vorteil einer solchen dynamischen Handhabung von Betriebsvereinbarungen ist es, dass Unternehmen auf diese Weise immer eine korrekte Themenzuordnung und damit eine **rechtmäßige Datenerhebung** gewährleisten.

308 Werden Arbeitnehmerdaten aus einem Tool des Unternehmens erhoben, welches zwar vereinbart wurde, ohne dass aber die Datenerhebung mit der Zweckbestimmung der Betriebsvereinbarung übereinstimmt, ist die Datenerhebung nicht rechtmäßig. Insofern ist auch genau abzuwägen, welche Systeme und Tools im Rahmen einer Betriebsvereinbarung vereinbart werden. Ergeben sich keine eindeutigen gesetzlichen oder vertraglichen Zulässigkeitsregelungen, sind bei den Betroffenen **Einwilligungen** einzuholen. Werden Betriebsvereinbarungen für die Zulässigkeiten von Datenverarbeitungen abgeschlossen, so stellt sich die Frage, wer die **Rechte der Mitarbeiter** innerhalb der Unternehmensorganisation gewährleistet. Es kann sich deshalb anbieten, die einzelnen Betroffenenrechte wie auch die Zuständigkeit für die Gewährleistung von Betroffenenrechten aufzuspalten. Auf diese Weise kann auch sichergestellt werden, dass sich des Themas jeweils autorisierte Mitarbeiter annehmen, die auch über die entsprechende Handlungsbefugnis verfügen.

309 Eine Aufspaltung von Arbeitnehmerrechten in Betriebsvereinbarungen könnte wie folgt aussehen: Ein Teil könnte in der Basis-Datenschutzvereinbarung und ein Teil in den einzelnen Betriebsvereinbarungen zu speziellen Themen geregelt werden. Dabei sollte eine Unterscheidung danach getroffenen werden, ob es sich bei den Daten um klassische **Arbeitnehmerdaten der Personalabteilung** handelt oder um solche Mitarbeiterdaten, die den entsprechenden Geschäftsbereichen zuzuordnen sind. Dabei ist zu beachten, dass die Implementierung von **klassischen Personaldaten** und die Betreuung von Personalprozessen originär der Personalabteilung zugeordnet werden sollten. Die Personalabteilung verfügt über die aktuellen Personaldaten, um auch den gesetzlichen Verpflichtungen des Arbeitgebers nachkommen zu können. Die Personalabteilung könnte jedem Mitarbeiter auch einmal jährlich zu Beginn des Kalenderjahres ein **Datenblatt** mit seinen aktuellen Personaldaten zur Verfügung stellen. Gleichzeitig verbunden mit der Aufforderung an die Mitarbeiter, dass sie die Richtigkeit der erfassten Personaldaten bestätigen.

310 Informationspflichten, Auskunftsrechte, Berichtigungsrechte, Löschungsrechte, Rechte auf Einschränkung der Datenverarbeitung könnten als zentrale Rechte in der Basis-Betriebsvereinbarung geregelt werden. Dagegen sollten Rechte auf **Widerspruch** und **Datenübertragbarkeit** in den spezifischen Betriebsvereinbarungen geregelt werden, weil es sich

hierbei um spezielle Rechte handelt. Beim Widerspruch nach Art. 21 handelt es sich um Verarbeitungen nach Art. 6 f sowie um solche, welche ein **Profiling** auf Basis des Art. 6f beinhalten. Insofern schützt Art. 21 den Einzelnen vor Verarbeitungen, die nicht seinem Willen entsprechen. Ein Sonderfall ist hier auch Art. 21 II iVm Art. 21 III, welcher den Widerspruch bei **Direktwerbung** betrifft. Hinzu kommt das Recht auf Datenübertragbarkeit nach Art. 20, welches dem Betroffenen eine bessere Kontrolle über die Daten geben soll, die er dem Unternehmen bereitgestellt hat. Dies gilt für Daten, welche im Rahmen einer Einwilligung zur Verfügung gestellt wurden oder für solche Daten, die zur Erfüllung eines Vertrages erforderlich sind (ErwGr. 68).

2.2.1 Steuerung durch Datenschutzkontrolle: Zielsetzung der Imple- **311**
mentierung der Zulässigkeiten im Unternehmen ist es, den Anforderungen der DSGVO und anderen Gesetzen über den Datenschutz zur Datenschutzkontrolle gerecht zu werden. Datenschutzkontrolle erfordert für Unternehmen insofern **klare Zuständigkeiten** und **klare Handlungsgrundlagen**. Eine Konzeption zur Abgrenzung gesetzlicher Zulässigkeiten, Legitimationsgrundlagen anhand von Betriebsvereinbarungen sowie durch individuelle Einwilligungen ermöglicht es hierbei, die Zuständigkeiten und Verantwortungen innerhalb des Unternehmens arbeitsteilig zuzuordnen. Die gegenseitigen Schnittstellen von DSB, Rechtsabteilung, Personalabteilung, Geschäftsbereichen, Prozessverantwortlichen, Verantwortlichen für Datensicherheit, der Geschäftsleitung und den Aufsichtsbehörden können so klar abgegrenzt werden. Auf diese Weise könnten die Themen der **Transparenz der Verarbeitung**, der Datenübermittlung innerhalb einer Unternehmensgruppe, der Zweckbindung und -änderung, der Löschfristen – als tägliche Fragestelllungen im Unternehmen – in ein schlüssiges Konzept gebracht werden. Hinzu kommen Spezialthemen mit Schnittstelle zu Unternehmensexternen wie zB spezifische Datenübermittlungen an Dritte, Datenübermittlungen in Drittländer, Mitteilungspflichten im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder auch der Einschränkung der Verarbeitung sowie auch der Handhabung von Datenverletzungen. Dies letztlich auch, um datenschutzrechtlichen Dokumentations- und **Rechenschaftspflichten** nachzukommen und **Haftungsrisiken** zu minimieren.

Aufgrund der Komplexität der unterschiedlichen Geschäftsmodelle **312**
und Arbeitsorganisationen muss Datenschutz primär durch Unternehmen selbst gewährleistet werden. Unternehmen sind in der Verantwortung für eine **effiziente Eigenkontrolle.** Die Eigenkontrolle der Unternehmen spielt insofern die zentrale Rolle zur Implementierung von Datenschutz, wobei mit der Selbstkontrolle der Betroffenen eine immer wichtiger werdende Facette der Datenschutzkontrolle hinzukommt. Dies im Besonderen auch unter dem Gesichtspunkt der **Aktualität** und **Richtigkeit** der Daten (Art. 5 I d). Im Rahmen der informationellen Selbstbestim-

mung müssen Betroffene – Arbeitnehmer und Kunden im Verhältnis B2C – ihre Teilhabe an den Zulässigkeiten der Datenverarbeitung wahrnehmen. Es kommt hinzu, dass Unternehmen im Verhältnis B2B – dh im Rechtsverhältnis zu anderen Unternehmen – auch darauf angewiesen sind, dass diese Unternehmen ebenfalls Datenschutzgesetze einhalten. Auch geschäftliche Daten unterliegen der Anforderung der Richtigkeit, Aktualität und Erforderlichkeit der Daten. Zu betrachten ist vor diesem Hintergrund die **Dreisäulen-Theorie der Datenschutzkontrolle.** Unterstützend und begleitend zur Eigenkontrolle (Säule 1) hat der Gesetzgeber die Kontrolle durch die Betroffenen – die Selbstkontrolle (Säule 2) – und durch eigene Aufsichtsbehörden für den Datenschutz – die Fremdkontrolle (Säule 3) – vorgesehen.

313 Erforderlich ist vor diesem Hintergrund eine **verfahrensrechtliche Gestaltung von Datenschutz.** Bei jeder Erweiterung oder Änderung des Umfangs von Dateien sind die Dateiverantwortlichen gehalten, erneut die Zulässigkeiten zu überprüfen. Neben Zulässigkeitsprüfungen nach Art. 6 iVm Art. 5 steht Kontrolle heute auch in einem engen Kontext zu lizenzrechtlichen Fragestellungen. Die **lizenzrechtliche Komponente des Datenschutzrechts** betrifft hierbei die Sicherstellung der ordnungsgemäßen Datenverarbeitung. Der Schutz von **Data Processing Assets** erfasst hierbei auch Fragestellungen des Schutzes von Lizenzmaterial. Die Eigenkontrolle des Datenschutzes betrifft dabei die Nutzung überlassener Software sowie Fragestellungen der Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, bei welchen auch ein Zugriff auf personenbezogene Daten stattfindet.

314 **2.2.2** Steuerung durch Einwilligungserklärung: Die **Einwilligung** des Betroffenen wird aufgrund der restriktiven Zulässigkeiten der DSGVO zum zentralen Steuerungsinstrument, eine rechtliche Zulässigkeit der personenbezogenen Datenverarbeitung zu erhalten. Betroffene können in die Verarbeitung ihrer Daten einwilligen. Dabei sind allerdings **Transparenzvorgaben** einzuhalten. So soll die Einwilligung nach ErwGr. 32 durch eine eindeutige Handlung erfolgen, mit der die betroffene Person **ohne Zwang** für den konkreten Fall und in Kenntnis der Sachlage unmissverständlich erklärt, dass sie mit der Verarbeitung ihrer Daten einverstanden ist. Möchte der Verantwortliche, dass der Betroffene einwilligt, so muss die Aufforderung zur Abgabe einer Einwilligungserklärung nach Art. 7 II in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erfolgen. So darf ein Vertragsschluss nicht davon abhängig gemacht werden, dass die betroffene Person eine Einwilligung in die Verarbeitung personenbezogener Daten abgibt, die nach Art. 7 IV, ErwGr. 43 für die Erfüllung des Vertrags nicht erforderlich ist. Dies betrifft das sog. Trennungsgebot (L/N/K Praxis, S. 86 ff.).

315 Nach Art. 7 III hat der Betroffene das Recht, seine Einwilligung jederzeit zu **widerrufen**. Durch den Widerruf der Einwilligung wird die

Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Darüber ist die betroffene Person vor Abgabe der Einwilligung in Kenntnis zu setzen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung möglich sein. Insofern ist im Unternehmen die jederzeitige Möglichkeit des Widerrufs betrieblich-organisatorisch umzusetzen. Der Widerruf ist damit mit dessen Geltendmachung wirksam. Der Widerruf bedarf auch keiner Begründung. Seine Geltendmachung ist damit auch nicht von der Einhaltung von Treuepflichten des Widerrufenden nach §§ 242, 241 II BGB gegenüber dem Verantwortlichen abhängig. Nach Art. 88 I, ErwGr. 155 haben die Mitgliedstaaten die Möglichkeit, Vorschriften über die Bedingungen zu erlassen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen. Nach **§ 26 II S. 4 BDSG-neu** hat der Arbeitgeber die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 III in Textform aufzuklären.

Bei der Personalarbeit sollte darauf geachtet werden, ob besondere **316**
Anforderungen an die Freiwilligkeit der Einwilligung wegen des Vorliegens einer **besonderen Datenkategorie** nach Art. 9 gegeben sind. Denn nach Art. 9 I ist die Verarbeitung **sensitiver Daten** grundsätzlich untersagt. Dazu gehören zB Daten zur ethnischen Herkunft, zu politischen Meinungen oder weltanschaulichen Überzeugungen und zur Gesundheit. Art. 9 I gilt allerdings nicht, wenn der Betroffene in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich **eingewilligt** hat. Zulässig ist die Verarbeitung dieser sensitiven Daten auch dann, wenn die Verarbeitung erforderlich ist, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem **Arbeitsrecht** und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann. Hinzu kommt die Zulässigkeit der Verarbeitung für Zwecke der Gesundheitsvorsorge oder der **Arbeitsmedizin**, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich.

Nach **§ 26 III BDSG-neu** ist die Verarbeitung sensitiver Daten iSv **317**
Art. 9 I für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. **§ 26 II BDSG-neu** gilt auch für die Einwilligung in die Verarbeitung besonderer Datenkategorien. Dabei muss sich die Einwilligung aber ausdrücklich auf diese Daten beziehen. § 22 II

BDSG-neu gilt entsprechend. Dies bedeutet, dass angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen sind. Dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und den damit verbundenen möglichen Risiken für Betroffene.

318 Ist eine Einwilligung für eine Datenverarbeitungszulässigkeit notwendig, so kann der Betroffene auf diejenigen Punkte hingewiesen werden, die eine **Überschreitung der gesetzlichen Verarbeitungszulässigkeit** nach der DSGVO oder anderen Vorschriften über den Datenschutz darstellen. Eine solche Prüfung kann im Vorfeld kann auch dazu führen, dass festgestellt wird, dass eine personenbezogene Datenverarbeitung durch die DSGVO oder eine andere Rechtsvorschrift ohne Einwilligung erlaubt ist. In einem solchen Fall sollte keine Einwilligung eingeholt werden. Insofern bedarf die Einholung einer Einwilligung aus Sicht des Unternehmens eines **Double Check,** auch um keine unnötigen Einwilligungen einzuholen. Danach bleibt festzuhalten: Die Abhängigkeit der Datenverarbeitung vom Verhalten des Betroffenen und ihre Anbindung an die **Autonomie des Betroffenen** finden ihren stärksten Ausdruck in der Einwilligungsvariante nach § 6 I iVm Art. 7. So stellt die Einwilligung des Betroffenen ein **Individualrecht** dar, welches die DSGVO ausdrücklich anerkennt. Die Einholung einer Einwilligung sollte Betroffenen deutlich machen, dass sie mit ihrer Entscheidung, ob sie zu einer Datenverarbeitung ihre Einwilligung geben, ihre Verantwortung zur **Selbstkontrolle** wahrnehmen.

319 **2.2.3** Mitbestimmung durch Kollektivrecht: Die Mitbestimmung des BetrVG ist mit Einführung der DSGVO an den Mechanismen der **Datenschutzkontrolle** zu reflektieren. Zum einen betrifft die Kontrolle **Restriktionen** der personenbezogenen Datenverarbeitung nach Art. 5, 6. Und zum anderen zielt sie auf besondere Pflichten des Verantwortlichen ab. Dazu gehören die zentralen Pflichten der Risikovorsorge und der Datensicherheit nach Art. 24 und 32. Hinzu kommen Meldepflichten bei Datenschutzverstößen nach Art. 33, 34 sowie die regulatorische Vorgabe der Datenschutz-Folgenabschätzung nach Art. 35. Dies wird begleitet durch die betriebliche Mitbestimmung nach **§ 87 I Nr. 6 BetrVG**. Hierbei geht es um Maßnahmen zur Vermeidung bzw. einer angemessenen Handhabung einer **Leistungs- und Verhaltenskontrolle** von Mitarbeitern.

320 Betrachtet man die heutige intensive Nutzung der IT, so ist eine enge Verknüpfung von Datenschutzrecht und Betriebsverfassungsrecht gegeben. Insofern sollte heute das Thema der **sozialen Mitbestimmung** im Datenschutz perspektivisch als Compliance-Thema betrachtet werden. Dies nach Vorgaben des Datenschutzrechts, gleichzeitig aber unter konsequenter Betrachtung der Kompetenzregelung des § 87 I Nr. 6 BetrVG für Betriebsräte. Schwerpunkt der Betrachtung sollte danach sein, dass

der **Betriebsrat als Kooperationspartner** des Arbeitgebers nach § 80 I Nr. 1 BetrVG über die Durchführung der DSGVO und des BDSG-neu wacht und den Datenschutz im Unternehmen konstruktiv und im Rahmen der vertrauensvollen Zusammenarbeit mitgestaltet (M-G/P/S-*Kania*, § 80 BetrVG Rn. 6).

3. Selbstkontrolle der Betroffenen

3.1 Handlungsautonomie des Betroffenen: Im Datenschutzrecht hat **321**
sich die **Rolle der Arbeitnehmer** in Unternehmen – im Besonderen durch die Generierung von Daten im Rahmen von Sozialen Netzwerken und der Teilhabe an Geschäftsprozessen (*Wächter*, JurPC Web-Dok. 28/2011, Abs. 1, 61 ff.) – erheblich gewandelt. Betroffene sind heute auch **Urheber personenbezogener Informationen** und in weiten Bereichen auch aktive Teilnehmer personenbezogener Datenverarbeitung. Denn IT ist nicht mehr nur Arbeitsmittel und Werkzeug für Kommunikation, sondern in weiten Bereichen Teil der **Wertschöpfungskette** in Unternehmen. Insofern besteht bei einer Vielzahl von Tätigkeiten heute die Situation, dass die Nutzung von IT und die Verwertung von Daten zur **arbeitsvertraglichen Hauptleistungspflicht** geworden sind. Ein Beispiel ist der Vertriebsmitarbeiter, der die ihm vorliegenden Kundendaten analysiert, um dem Vertriebsbereich ein Konzept vorzustellen, auf welche Kunden das Unternehmen im Moment mit welchen Produkten und Dienstleistungen zugehen und Angebote unterbreiten sollte, um den Vertriebserfolg des Unternehmens zu gewährleisten.

Damit steht die Zulässigkeit der Datenverarbeitung nicht mehr zwi- **322**
schen den Polen der Leistungs- und Verhaltenskontrolle bei unterstützenden IT, sondern sie adressiert eine IT im Zentrum des Arbeitsverhältnisses. Denn die IT wird zum eigentlichen Wertschöpfungsfaktor und deren Nutzung wird zur **Hauptleistungspflicht des Mitarbeiters**. Dieser Befund wird dadurch verstärkt, dass bei Vertragsanbahnungen nicht mehr Unternehmen auf Unternehmen zugehen, sondern Mitarbeiter von Unternehmen auf Mitarbeiter anderer Unternehmen. Dies bedeutet eine höhere Agilität, verdeutlicht aber auch, dass Mitarbeiter eine **Selbstkontrolle** für ihre Daten wahrnehmen müssen. Und hierbei nehmen sie gleichzeitig auch eine wesentliche Rolle bei der Einhaltung der **Eigenkontrolle** von Unternehmen wahr. Selbst- und Eigenkontrolle werden zunehmend zu einer Einheit bzw. stehen in einem engen Verhältnis.

Im Rahmen der Selbstkontrolle handeln Mitarbeiter als Arbeitnehmer **323**
oder in einer Management-Funktion. In Ausnahmefällen kann auch ein Handeln als Privatperson in Betracht kommen. So kann Unternehmen daran gelegen sein, dass Mitarbeiter in öffentlichen Foren – im Besonderen in **Sozialen Netzwerken** – nicht den Anschein erwecken, im Namen

des Unternehmens zu sprechen. Im Zweifel handeln Mitarbeiter aber – unter datenschutzrechtlichen Gesichtspunkten – nicht als Privatpersonen, weil die DSGVO nach Art. 2 II c anwendbar ist. Es findet danach keine Datenverarbeitung ausschließlich zur Ausübung **persönlicher Tätigkeiten** statt. Die DSGVO soll in solchen Fällen nach ErwGr. 18 auch Anwendung finden, weil ein Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit gegeben ist (P/P-*Ernst* DSGVO Art. 2 Rn. 16). In der Zukunft könnten hierzu – wie auch zu anderen Themen – **Verhaltensregeln** nach Art. 40 II erarbeitet werden. Solche Regeln können zB die faire und transparente Verarbeitung betreffen. Ebenso Präzisierungen zu berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen oder auch zur Erhebung personenbezogener Daten. Diese Verhaltensregeln sollen keine eigene Rechtsgrundlage begründen. Sie sollen nach ErwGr. 98 aber branchenspezifische Besonderheiten oder Bedürfnisse von **kleinen und mittleren Unternehmen** berücksichtigen (*L/N/K* Praxis, S. 255 ff. (256)).

324 In einer verarbeitungsintensiven Organisation ist es nach § 241 II BGB auch Aufgabe der Mitarbeiter, die Eigenkontrolle des Unternehmens zur rechtmäßigen Datenverarbeitung zu unterstützen. Dabei ist darauf zu achten, dass dieses Thema der **Datenschutzadministration** und der Datensicherheit für das Unternehmen getrennt wird von berechtigten Arbeitnehmerinteressen. Denn diese sind wiederum eine wichtige Rechtsposition, welche durch Geschäftsinteressen und Zwänge des Marktes nicht zu negieren und auch nicht zu relativieren sind. Ein Problemfeld ist in diesem Bereich die heutige Grauzone der Herstellung einer persönlichen **Visibilität** der Mitarbeiter in Sozialen Netzwerken und im Markt im Unternehmensinteresse. Denn hierbei wird die **Identität der Mitarbeiter** in den Vordergrund gestellt und das Unternehmen erscheint lediglich als Hintergrund-Kulisse. Diese Vorgehensweise wird heute im Vertrieb deshalb favorisiert, weil die persönliche soziale Brand (Marke) eines Mitarbeiters und damit seine Individualität für eine authentische Persönlichkeit steht, die Vertrauen in die Produkte und Dienstleistungen des Unternehmens vermittelt. Damit erfolgt eine starke Überschneidung **geschäftlicher Informationen** und solchen über Mitarbeiter. Hierzu müssen in den Unternehmen Grenzlinien erarbeitet werden, die für das Geschäft der jeweiligen Branche möglich sind, aber auf der anderen Seite auch Kerntatbestände der DSGVO und anderer Gesetze über den Datenschutz sicherstellen.

325 Das Unternehmen wird damit zur Plattform der eigenen Identität. Dies in der Weise wie bei **Selfies**, bei denen das eigene Ich in Beziehung zu anderen Personen oder Sehenswürdigkeiten gesetzt wird. Das **Spielen mit der eigenen Identität** und das Präsentmachen der eigenen Person sollten allerdings nicht dazu führen, dass die Selbstkontrolle des Einzelnen eingeschränkt oder weitgehend unmöglich gemacht wird, weil dieser