Datenschutz im Unternehmen

Wächter

6. Auflage 2021
ISBN 978-3-406-75402-9
C.H.BECK

begriffen als ein Baustein der Gewährleistung der Einhaltung gesetzlicher Vorgaben unter dem Aspekt der **Rechtstreue** von Unternehmen. Unter IT-Compliance versteht man die **Befolgung von Vorschriften** für die Nutzung der IT. In Art. 32 werden die Anforderungen an die Sicherheit personenbezogener Daten beschrieben. So sind unter Berücksichtigung des Stands der Technik, der Zwecke der Verarbeitung und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. IT-Compliance kann hierbei im Rahmen dieser Vorgaben zum **Nachweis der Rechtmäßigkeit** einer Datenverarbeitung dienen.

336 Kriterien der Rechtmäßigkeit der Datenverarbeitung unter dem Gesichtspunkt der IT-Compliance können wie folgt in Form von Fragen beschrieben werden: Wird die Berechtigung zur Verarbeitung personenbezogener Daten nachgewiesen? Wurden die Anwendungen, Tools und Datenbanken, die personenbezogene Daten enthalten, dem DSB gemeldet? Erfolgten Kontrollen nach Art. 32? Enthält die Anwendung Arbeitnehmerdaten und wurden die entsprechenden Datenbestände von der zuständigen Personalfunktion freigegeben? Sind **Auswertungen** vorgesehen, aus denen individuelle Mitarbeiterdaten ersichtlich sind und liegt hierzu eine Genehmigung der zuständigen Personalfunktion vor? Werden vom Management **Reports** erstellt? Welche **Schnittstellen** hat das System? Erfolgt eine technische Datenübertragung ins Ausland? Sind die Informationen entsprechend klassifiziert, zB nach vertraulich, streng vertraulich, persönlich registriert und persönlich? Sind Geschäftsgeheimnisse betroffen? Die Antworten auf diese Fragen sind dann unter dem Gesichtspunkt der Technologienutzung und ihrer möglichen Auswirkung auf die **Grundrechte** und **Grundfreiheiten** natürlicher Personen zu beantworten. Datenschutz als IT-Compliance ist damit ein originärer Ansatzpunkt der faktischen Gewährleistung von Datenschutz.

5. Fremdkontrolle der Aufsichtsbehörden

337 **a) Unabhängige externe Datenschutzkontrolle**: Datenschutz steht im Kontext der Kontrolle. Die Eigenkontrolle der Unternehmen wird ergänzt durch die Fremdkontrolle der **Aufsichtsbehörden**. Die Errichtung von Aufsichtsbehörden in den Mitgliedstaaten, die befugt sind, ihre Aufgaben und Befugnisse **unabhängig** wahrzunehmen, ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten (ErwGr. 117). Nach Art. 4 Nr. 21 ist eine ASB eine von einem Mitgliedstaat nach Art. 51 eingerichtete unabhängige staatliche Stelle. Betroffen ist eine ASB nach Art. 4 Nr. 22, weil der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitglied-

staats dieser Aufsichtsbehörde niedergelassen ist (Art. 4 Nr. 22a), diese Verarbeitung erhebliche **Auswirkungen auf Betroffene** mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann (Art. 4 Nr. 22b) oder eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde (Art. 4 Nr. 22c).

338 **b) Zentrale Aufgaben der Aufsichtsbehörden**: Für den **Unternehmensdatenschutz** haben die ASB nach Art. 57 I die Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen, die **Öffentlichkeit** für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung zu sensibilisieren und sie darüber aufzuklären. Dazu gehört auch, die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten zu sensibilisieren (Art. 57 I d). Hinzu kommt, auf Anfrage jedem Betroffenen Informationen über die Ausübung ihrer Rechte aufgrund der DSGVO zur Verfügung zu stellen. Zentral ist es, sich mit **Beschwerden** einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes nach Art. 80 zu befassen und damit den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen (Art. 57 I f). Ferner hat die ASB Untersuchungen über die Anwendung der DSGVO durchzuführen (Art. 57 I h und **Standardvertragsklauseln** iSd Art. 28 VIII (Auftragsverarbeitung) und des Art. 46 II d (Datenübermittlung) festzulegen. Hinzu kommen weitere spezifische Aufgaben der ASB wie die Erstellung und Führung einer Liste der Verarbeitungsarten, für die nach Art. 35 IV eine **Datenschutz-Folgenabschätzung** durchzuführen ist (Art. 57 I l).

339 **c) Zentrale Befugnisse der Aufsichtsbehörden**: In Art. 58 sind die Befugnisse der ASB beschrieben. Sie haben nach Art. 58 I **Untersuchungsbefugnisse**, nach Art. 58 II **Abhilfebefugnisse** und nach Art. 58 III **Genehmigungsbefugnisse** und **beratende Befugnisse**. Dies unterstreicht die Zielsetzung, die Durchführung des Datenschutzes zu unterstützen und Vollzugsdefizite im Datenschutz zu verbessern. Dabei kann nach Art. 58 VI jeder Mitgliedstaat durch Rechtsvorschriften vorsehen, dass eine Aufsichtsbehörde neben den in Art. 58 I, II und III genannten Befugnissen weitere Befugnisse erhält. Die Vorschrift des **§ 40 BDSG** regelt die Zuständigkeit und in Ergänzung des Art. 58 VI die Befugnisse der Aufsichtsbehörden der Länder über die nicht-öffentlichen Stellen.

340 Mit der DSGVO wurde als wesentliche Neuerung das Prinzip der einheitlichen Anlaufstelle – **One-Stop-Shop** – eingeführt (Simitis/Hornung/Spiecker gen. Döhmann/*Polenz* Art. 56 Rn. 1 ff.). Es soll dazu dienen, dass sich Unternehmen nicht mehr mit den ASB in verschiedenen Ländern auseinandersetzen müssen. Für grenzüberschreitende Datenverarbeitungen nach Art. 4 Nr. 23 – auch durch unterschiedliche Niederlassungen oder Tochtergesellschaften in der EU – ist nunmehr eine ASB zuständig. Dies ist regelmäßig diejenige am Sitz der Hauptniederlassung (Art. 4

Nr. 16). Sie ist dann nach Art. 56 I, VI federführend zuständig, **Single Contact Point** und damit einziger Ansprechpartner (Paal/Pauly/*Körffer* DSGVO Art. 56 Rn. 8). Von der Regelung zur Zuständigkeit der ASB am Sitz der Hauptniederlassung gibt es Ausnahmen. So ist die federführende Aufsichtsbehörde zB nicht zuständig, wenn es sich um rein lokale Datenverarbeitungen einer Niederlassung handelt (Art. 56 II). Dies betrifft zB die Videoüberwachung vor Ort. Konzipiert ist die Kontrolle der ASB insofern als **externe Kontrollinstanz**. Das Beispiel der lokalen Videoüberwachung an einer Lokation eines Unternehmens verdeutlicht aber auch, dass unabhängig von einer externen Kontrollinstanz die Unternehmen proaktiv tätig sein müssen, Datenschutz für ihre Organisation zu gewährleisten. Das **Prinzip der einheitlichen Anlaufstelle** soll nur dazu dienen, dass sich Unternehmen grundsätzlich nicht mit unterschiedlichen ASB auseinandersetzen müssen.

341 Das **Kohärenzverfahren** soll nach Art. 63 eine einheitliche Anwendung der DSGVO gewährleisten (Laue/Kremer Neues DatenschutzR/*Kremer* S. 362 ff.). Hierzu können nach Art. 64 Stellungnahmen abgegeben werden und es kann eine Streitbeilegung durch den **EDSA** erfolgen (Art. 64, 65). Im Wesentlichen geht es hierbei darum, ein geordnetes Verfahren für die **Zusammenarbeit zwischen den ASB** zu gewährleisten. Dieses Verfahren soll insbesondere dann angewendet werden, wenn eine ASB beabsichtigt, eine Maßnahme zu erlassen, die rechtliche Wirkungen in Bezug auf Verarbeitungsvorgänge entfalten soll, die für eine bedeutende Zahl betroffener Personen in mehreren Mitgliedstaaten erhebliche Auswirkungen haben (ErwGr. 135). Bei Vorliegen eines Einspruchs durch eine ASB trifft der EDSA nach Art. 65 Ia eine **verbindliche Entscheidung**. Die Zusammenarbeit zwischen der federführenden ASB und anderen betroffenen ASB wird so sichergestellt. Dies erfolgt, wenn eine betroffene Aufsichtsbehörde nach Art. 60 IV einen Einspruch gegen einen Beschlussentwurf der federführenden ASB eingelegt hat oder die federführende Behörde einen Einspruch als nicht maßgeblich oder nicht begründet abgelehnt hat.

342 Neben dem Kohärenzverfahren ist auf das **Dringlichkeitsverfahren** nach Art. 66 hinzuweisen. Dies betrifft außergewöhnliche Umstände, bei denen eine betroffene ASB abweichend vom Kohärenzverfahren nach Art. 63, 64 und 65 oder dem Verfahren nach Art. 60 sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer von höchstens drei Monaten treffen kann, die in ihrem Hoheitsgebiet rechtliche Wirkung entfalten sollen (Paal/Pauly/*Körffer* DSGVO Art. 66 Rn. 2 ff., 5). Dies kann der Fall sein, wenn die ASB zu der Ansicht gelangt, dass dringender Handlungsbedarf besteht, um Rechte und **Freiheiten von Betroffenen** zu schützen. Die ASB setzt dann die anderen betroffenen ASB, den EDSA und die Kommission unverzüglich von diesen Maßnahmen und den Gründen für deren Erlass in Kenntnis. Die beschriebene unabhängige

Kontrolle sowie die beschriebenen Regeln der Zusammenarbeit der ASB sind wesentlicher Bestandteil eines **effektiven Datenschutzes**. Die unabhängige Kontrolle basiert in Europa auf Art. 8 III GRCh iVm Art. 16 II 2 AEUV. Insofern gehört Datenschutz und deren **rechtstaatliche Durchsetzung** zu den wesentlichen Grundpfeilern einer offenen demokratischen Gesellschaft. Denn so können Betroffene ihre Rechte unionsweit wahrnehmen.

II. Verzeichnis von Verarbeitungstätigkeiten

1. Aufzeichnung von Verarbeitungsvorgängen

343 Nach **Art. 30 I** sind Verantwortliche oder ihre Vertreter verpflichtet, Aufzeichnungen über ihre personenbezogene Datenverarbeitung zu führen. **Das Verarbeitungsverzeichnis** dient nach **ErwGr. 82 S. 1** dem Nachweis, dass der Verantwortliche oder der Auftragsverarbeiter die DSGVO einhält. Und nach ErwGr. 82 S. 2 dient es als Grundlage für die Kontrolle der ASB. Das Verzeichnis dient Unternehmen als administrativer Datenschutz dazu, Datenschutz in **dokumentierter Weise** umzusetzen. Die Erfassung von Verarbeitungsvorgängen trägt dazu bei, dass Unternehmen ihrer Verantwortung nach Art. 5 II nachkommen können. Damit ist das Führen des Verzeichnisses ein wesentliches Element des **Datenschutz-Managements**. Das Verzeichnis kann auch dazu dienen, Unternehmens- und Geschäftsprozesse auf einem geeigneten Niveau abzubilden. Die **Granularität der Erfassung** der Art und Weise der verarbeiteten Daten in einem strukturierten Konzept muss sich dabei an den **Risiken für Betroffene** nach Art. 24, aber auch an den Haftungsrisiken für das Unternehmen nach Art. 82 sowie den Anforderungen der Sicherheit personenbezogener Daten nach Art. 31 orientieren.

344 Das Verzeichnis kann neben einem **Privacy Assessment** dazu genutzt werden, die Rechtmäßigkeit der Datenverarbeitung nach Art. 24 I sowie das Ergebnis von Datenschutz-Folgenabschätzungen nach Art. 35 VII zu dokumentieren. In global agierenden Unternehmen eignen sich dazu Privacy Assessments, die vom Application Owner und **Privacy Officer** geprüft und freigegeben werden. Bei Änderungen der Schnittstellen von Anwendungen bzw. Tools, der Übermittlung von Daten, der verarbeiteten Daten oder der **Funktionalitäten der IT** ist eine erneute Prüfung erforderlich, ob die Verarbeitung noch rechtskonform ist. Insofern dient das Verzeichnis als Grundlage weiterer Datenschutzpflichten (*S/B* Dokumentation-*DSK*, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30, Dok. G 2.4.62, S. 2). Und dies im Sinne eines Systemdatenschutzes.

Unternehmen als Verantwortliche haben danach **Aufzeichnungspflichten** nach Art. 30. Nach Art. 30 I 1 unterliegt jeder Verantwortliche und ggf. sein Vertreter der Pflicht, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen, die ihrer Zuständigkeit unterliegen. Nach Art. 30 II hat auch jeder **Auftragsverarbeiter** und ggf. sein Vertreter ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen. Ein **Vertreter** nach Art. 4 Nr. 17 ist hierbei eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß **Art. 27** bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt (Paal/Pauly/*Ernst* DSGVO Art. 4 Rn. 122). Aufgabe des Verzeichnisses der Verarbeitungstätigkeiten ist eine schriftliche Dokumentation der wesentlichen Informationen **aller** Verarbeitungstätigkeiten. **345**

Die nach Art. 30 I und II definierten Pflichten gelten nach Art. 30 V nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein **Risiko für die Rechte** und Freiheiten der betroffenen Personen beinhaltet, die Verarbeitung nicht nur **gelegentlich** erfolgt oder nicht die Verarbeitung von **sensitive Daten** nach Art. 9 I bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten iSd Art. 10 einschließt (Kühling/Buchner/*Hartung* Art. 30 Rn. 34 ff.). Zu den erheblichen Risiken für Betroffene gehört zB auch die **Videoüberwachung**. Nach Art. 30 I ist die **Unternehmensleitung** und nicht der **DSB** für das Verfahrensverzeichnis verantwortlich. Dabei sind in den Unternehmen nicht nur Verzeichnisse über aktuelle Verfahren zu führen, sondern es ist auch die **Datenverarbeitungshistorie** vorzuhalten. Insofern ist Art. 30 in engem Zusammenhang mit der **Rechenschaftspflicht** des Verantwortlichen nach Art. 5 II zu betrachten. **346**

In Art. 30 I 2 werden die **Mindestinhalte** für den Dokumentationszweck des Verzeichnisses beschrieben. Dabei ist das Verzeichnis nach Art. 30 III schriftlich zu führen und es ist der **ASB** nach Art. 30 IV auf Anfrage zur Verfügung zu stellen. Das Verzeichnis muss sämtliche nachfolgend beschriebene Angaben enthalten. Den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie des DSB. Hinzu kommt die Beschreibung der Zwecke der Verarbeitung, der **Kategorien** betroffener Personen, personenbezogener Daten und der Empfänger, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder **noch offengelegt werden**, einschließlich der Empfänger in Drittländern. Dies verdeutlicht, dass in der vorzuhaltenden Dokumentation die spezifische **Dynamik der IT** und Innovationsaufgabe der IT bei Industrie 4.0, KI und Robotik im Unternehmen reflektiert sein sollte. Und **347**

dies beinhaltet auch, dass eine **Transparenz** der unternehmensinternen IT hergestellt wird, so dass auch beantwortet werden kann, welche **Datenübermittlungen** geplant sind. Idealerweise sollten heute auch IT-Nutzungen zur Transformation des Unternehmens dokumentiert werden. Wenn möglich sollten auch die **Speicherdauer** personenbezogener Daten für die verschiedenen Anwendungsfelder der IT im Unternehmen in das Verzeichnisaufgenommen werden. Ebenso eine Beschreibung der Maßnahmen zur Datensicherheit.

348 Nach den gesetzlichen Vorgaben sind je nach **der Intensität der Datenverarbeitung** im Unternehmen die jeweiligen Zwecke aussagekräftig zu beschreiben. Als Maßstab für die **Klarheit der Beschreibungen** kann Art. 13 I c und Art. 14 I c herangezogen werden, da ebenso wie bei der Information von betroffenen Personen das Verzeichnis der **Transparenz** der personenbezogenen Datenverarbeitung dienen soll. Insofern verdeutlicht die Vorschrift des Art. 30 in besonderer Weise, dass moderner Datenschutz nach der DSGVO ein risikoorientierter **Systemdatenschutz** ist. Hierbei ist in besonderer Weise auf die Transparenz der Verarbeitung **sensitiver Daten** zu achten. Die Bezeichnung der Kategorien sollte so konkret und spezifisch sein, dass eine **Rechtmäßigkeitskontrolle** im Hinblick auf den jeweiligen Verfahrenszweck erfolgen kann. Hierbei ist im Unternehmen in jedem Fall zwischen Kunden, Geschäftspartnern und Mitarbeitern zu trennen.

349 Die Anforderungen an das Verzeichnis der Verarbeitungen können wie folgt dargestellt werden. Dabei bietet es sich für datenbasierte Unternehmen an, das **Privacy Assessment** mit dem Verzeichnis als Mittel eines Systemdatenschutzes zu verbinden.

Anwendungsfelder Privacy Assessment und Verzeichnis

- Aktueller Nachweis der Dokumentation der IT im Unternehmen für die Vergangenheit und Gegenwart mit Veränderungshistorie als Verantwortlicher
- Festlegung der Verarbeitungszwecke der IT:
  Personenbezogene Datenverarbeitung zur Unterstützung primärer Geschäftszwecke, IT zur Wertschöpfung und Datenverwendung als Geschäftsmodell, Nutzung der IT zur Kommunikation, Implementierung neuer Verwendungen im Rahmen von KI und Robotik
- Nachweis der Rechtmäßigkeit der IT: Rechtsgrundlage, Richtigkeit der Daten, Aktualität der Daten, Maßnahmen zur Gewährleistung von Betroffenenrechten
- Datenschutz durch Technik: Privacy by Design, Privacy by Default
- Datenschutzfolgenabschätzung
- Gewährleistung der Aufgabenstellung des DSB
- Gewährleistung der verfügbaren Vorlage des Verzeichnisses für die Aufsichtsbehörde
- Gewährleistung der verfügbaren Vorlage des Privacy Assessments für die Fachfunktionen und dem Betriebsrat im Unternehmen
- Gewährleistung der Verfügbarkeit von Verzeichnis und von Privacy Assessment zur Gewährleistung der Qualität der Verarbeitung und Compliance der IT

Nach Art. 30 II sind ebenfalls **Auftragsverarbeiter** zu Aufzeichnungen verpflichtet. Allerdings ergibt sich hier ein reduzierter Umfang. Dies hängt damit zusammen, dass Auftragsverarbeiter nach Art. 29 weisungsgebunden tätig werden (Plath/*Plath* BDSG-DSGVO Art. 30 Rn. 3). Das Verzeichnis Auftragsverarbeitung enthält Angaben zu Namen und Kontaktdaten des Auftragsverarbeiters. Ferner müssen im Verzeichnis die Kategorien von Verarbeitungen enthalten sein, die im Auftrag jedes Verantwortlichen durchgeführt werden. Hinzu kommen Angaben zu ggf. **durchgeführten Übermittlungen** von personenbezogenen Daten an ein Drittland, einschließlich der Angabe des betreffenden Drittlands, sowie von geeigneten Garantien für die in Art. 49 I UAbs. 2 genannten Datenübermittlungen. Abschließend sollte eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 I im Verzeichnis vorhanden sein. Zentrale Anforderung für das Verzeichnis der Auftragsverarbeiter ist allerdings, dass die Kategorien der Verarbeitungen nach Art. 30 IIb den **Verantwortlichen** zuordnet werden (Paal/Pauly/*Martini* DSGVO Art. 30 Rn. 20). **350**

Die Gesichtspunkte der Anforderungen an das Verzeichnis für Auftragsverarbeiter kann wie folgt dargestellt werden: **351**

Zielsetzungen der Angaben im Verzeichnis Auftragsverarbeiter

Inhalt des Verzeichnisses: Angaben nach Art. 30 IIa–d mit der Zielsetzung, die Tätigkeiten des IT-Providers transparent zu machen. Die Dokumentation betrifft auch die durch den Verantwortlichen erteilten Weisungen nach Art. 28 III UAbs. 2 S. 2 – Namen und Kontaktdaten nach Art. 30 IIa mit der Zielsetzung die Identifikation von Ansprechpartnern zu gewährleisten – Beschreibung der Verarbeitungen nach Art. 30 IIb, um Risiken für Betroffene durch eine Transparenz der IT zu reduzieren – Übermittlung in Drittländer nach Art. 30 IIc, um die Einhaltung des Datenschutzniveaus zu gewährleisten – Technisch-organisatorische Maßnahmen nach Art. 30 IId, um Maßnahmen zur Datensicherheit zu gewährleisten.

Das Verzeichnis der Verarbeitungstätigkeiten ist das **Adressbuch des DSB.** Die verantwortliche Stelle wird dem DSB deshalb das Verzeichnis der Verarbeitungstätigkeiten zur Verfügung stellen. Dieses enthält die wesentlichen Informationen für den DSB, damit dieser nach Art. 39 I die Beratung des Verantwortlichen und der Beschäftigten nach der DSGVO und anderen Vorschriften über den Datenschutz durchführen kann. Dieses Verzeichnis dient als Einstieg in eine **Rechtmäßigkeitskontrolle** und dient damit einer verfahrensmäßigen Umsetzung der Grundrechte und Grundfreiheiten der Betroffenen sowie des Rechts auf informationelle Selbstbestimmung. Das Verzeichnis, dessen Pflege und Aktualisierung trägt als **administrative Maßnahmen** zur Transparenz der personenbezogenen Datenverarbeitung bei. **352**

353 Für die Unternehmenspraxis hat das Erfordernis der Löschung von Daten aufgrund der heutigen **Kultur der Datenvorratshaltung** eine große Bedeutung. Dies ist für die Unternehmensleitung und den DSB auch deshalb ein Thema, weil **Big Data** als Wertschöpfungsquelle entsprechenden Löschungserfordernissen grundsätzlich entgegenstehen. Häufig werden Daten auch **by name** benötigt, um unternehmerische Aufgabenstellungen umsetzen zu können. Das Management benötigt gerade bei komplexen Organisationsstrukturen und einem breiten Produkt- und Dienstleistungsangebot im Konzern einen Durchgriff auf Daten, um das Geschäft für Kunden **in Echtzeit** steuern zu können. Insofern ist auch die Anonymisierung und Pseudonymisierung von Mitarbeiternamen ein Diskussionspunkt, wenn Kundenbetreuungen durch namentlich zuzuordnende Mitarbeiter erfolgen. Das verdeutlicht, dass für eine Vielzahl von Anwendungen das Privacy Assessment und auch das Verzeichnis für Verarbeitungen **mit Personenbezug** – beides als administrativer Datenschutz – immer wieder auch daraufhin aktualisiert werden muss, um die Dynamik der IT im Unternehmen aufzugreifen.

354 Je nach Größe und Intensität der Datenverarbeitung sind hierzu im Unternehmen Konzepte zu erarbeiten, die dem gesetzlichen Schutzzweck der DSGVO und dem BDSG gerecht werden. Die Verarbeitung von **Beschäftigtendaten** muss bei diesem Aspekt die Rechte der Mitbestimmung einbeziehen. Bei der Masse der Dateien und Verfahren sind für den Beschäftigtendatenschutz gangbare und damit pragmatische Konzepte zu entwickeln. Beim Beschäftigungsdatenschutz bieten sich hierbei Rückkoppelungen zwischen der **Eigenkontrolle** der Unternehmen und der Interessenwahrnehmung der **Mitbestimmung** durch Abschluss von Betriebsvereinbarungen an. Abgerundet wird das Konzept der Verfahrensübersichten und der erforderlichen Betriebsvereinbarungen durch die Umsetzung von **Verpflichtungserklärungen** aller Mitarbeiter, die toolgestützt arbeiten und damit in die Unternehmens-IT eingebunden.

355 Nach einem modernen Ansatz sollten administrative Konzepte von Privacy Assessment und Verzeichnis auch dazu dienen, diese mit den **Vereinbarungen von Tools** mit der Mitbestimmung nach § 87 I Nr. 6 BetrVG konsistent zu halten. Dies entspricht einer **Systemverträglichkeit** der Rechtmäßigkeit der IT und Regelungen sozialer Angelegenheiten nach dem BetrVG. Die verschiedenen Rechtsmaterien mit ihren begrifflichen Festlegungen sind hierbei **widerspruchfrei** in der betrieblichen Realität umzusetzen. So sind zwar das DSGVO und das BetrVG unterschiedliche Rechtskreise, die Handhabung automatisierter Verfahren sollte allerdings so erfolgen, dass die Beteiligten im Unternehmen – Management, DSB, Personalabteilung, Betriebsrat und Beschäftigte – die jeweilige Lösung mittragen können.

356 In diesem Zusammenhang ist darauf zu achten, dass der Lebenszyklus der Tools dokumentiert wird. Es ist den Mitarbeitern deshalb anzu-