B. Datenschutzkontrolle

I. Selbst-, Eigen- und Fremdkontrolle

1. Unternehmensverantwortung im Datenschutzrecht

1.1 BDSG und ausdifferenzierter Rechtsgüterschutz: Das Schutzgut des BDSG sowie die Einhaltung gesetzlicher Vorschriften zum Datenschutz sind durch die Kontrolle der Einhaltung datenschutzgesetzlicher Handlungsvorgaben zu gewährleisten. Datenschutzkontrolle soll damit den **präventiven Schutzcharakter** des Datenschutzes unterstützen und seine wirksame Umsetzung gewährleisten. Ausgangspunkt der Kontrolle ist die **Eigenkontrolle von Unternehmen,** die das BDSG bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach § 1 II Nr. 3 i. V. m. § 2 IV beachten müssen. Unternehmen sind damit für den Datenschutz verantwortlich, wenn sie personenbezogene Daten für sich selbst erheben, verarbeiten oder nutzen oder die Verarbeitung durch andere in ihrem Auftrag vornehmen lassen (§ 3 VII). Zentrale Regelungsvorgabe für Unternehmen für die Zulässigkeit der Verarbeitung ist der **Dritter Abschnitt des BDSG,** der die Rechtsgrundlagen der Datenverarbeitung behandelt. Die Vorschrift des § 27 II definiert den **Anwendungsbereich** dieses Abschnitts. Danach sind die §§ 27 ff. – im Besonderen auch die Vorschriften der §§ 28, 29 – nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien anwendbar. Allerdings ist die Gegenausnahme, dass die §§ 27 ff. dann wieder anwendbar sind, soweit es sich um personenbezogene Daten handelt, die **offensichtlich** aus einer automatisierten Verarbeitung entnommen worden sind (Simitis-*Simitis* BDSG, § 27 Rn. 32). **262**

Für die Zulässigkeit der **Verarbeitung von Beschäftigtendaten** nach § 3 XI ist zu beachten, dass sich die Datenschutzkontrolle in Unternehmen nach § 32 II auch auf solche **Informationen über Mitarbeiter** bezieht, die nicht automatisiert verarbeitet werden bzw. auch nicht für eine beschäftigtenbezogene Datenverarbeitung erhoben wurden. Damit ergibt sich nach Einführung der Vorschrift des § 32 in 2009 die Herausforderung für Unternehmen, auch traditionelle Akten und schriftliche Aufzeichnungen in die Kontroll- und Organisationsverantwortung einzubeziehen. Es handelt sich hierbei um **Papierunterlagen und Unterlagen in Aktenordnern** (Simitis-*Seifert* BDSG, § 32 Rn. 15) zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Be- **263**

gründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung.

264 Für die Festlegung des **Umfangs der Datenschutzkontrolle** im Unternehmen ist es wichtig festzulegen, zu welchem **Zweck** die Erhebung personenbezogener Daten erfolgt (§ 28 S. 2). Für die Erfüllung eigener Geschäftszwecke betrifft die Datenschutzkontrolle die IT, während es bei der Datenerhebung für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses bereits um die Kontrolle von Bewerbungsunterlagen geht. Allerdings ist bei dieser Unterscheidung zu beachten, dass das BDSG für die Gewährleistung der Umsetzung des gesamten Gesetzes nicht nur technische Maßnahmen, sondern auch **organisatorischen Maßnahmen** einfordert. Diese Maßnahmen betreffen die gesamte Handhabung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Dazu sind die bei der Datenverarbeitung beschäftigten Personen nach § 5 auch auf das **Datengeheimnis** zu verpflichten.

265 Die Eigenkontrolle des Unternehmens wird ergänzt durch die **Fremdkontrolle der Aufsichtsbehörden.** Bei einer zunehmenden Durchdringung der Unternehmen mit Datenverarbeitung spielt der Umgang von Betroffenen mit ihren eigenen Daten, die Wahrnehmung ihrer Datenschutzrechte sowie die Gestaltung ihrer eigenen Maßstäbe an Datenschutz für die auf sich bezogenen Daten eine zunehmend wichtige Rolle. Dies betrifft die **Selbstkontrolle der Mitarbeiter** und ihre **persönliche Haltung** zu Anliegen des Datenschutzes. Da Mitarbeiter heute in weitem Umfang Daten generieren und auch verarbeiten, muss Datenschutzkontrolle heute integrativer **Bestandteil der Arbeitsorganisation** sein. Die Gestaltung von Datenverarbeitungssystemen muss so erfolgen, dass eine Transparenz der personenbezogenen Daten hergestellt werden kann, damit auch die entsprechenden Daten bei Wahrnehmung eines Auskunftsrechts des Betroffenen nach § 34 verfügbar sind und entsprechende **Routinen** der Berichtigung, Löschung oder Sperrung von Daten nach § 35 umgesetzt werden können. Dies sind **Datenschutz-Abgleiche** (*Wächter* Falsifikation, S. 344 ff. (345)). Dieser Punkt verdeutlicht, dass IT zur Lösung der von ihr selbst verursachten Problemstellungen beitragen kann und so ein weitgehend negativ besetzter Begriff wie **Screening** eine positive Implikation erhält. Denn durch Nutzung von Technologie wird die Rechtsanwendung verbessert.

266 Eine wichtige Herausforderung der Datenschutzkontrolle vor dem Hintergrund der Transparenz der Datenverarbeitung ist heute die Nutzung von IT bei einer **Gemeinschaftsbezogenheit von Anwendungen** sowie die Nutzung von IT als **Mittel der Kommunikation.** Dies vor dem Hintergrund, dass Mitarbeiter die genannten Medien zur Datenrecherche nutzen und solche Informationen extrahieren und abspeichern, um sie einer weiteren Verwendung zuzuführen. Um eine entsprechende Kontrolle gewährleisten zu können, sind hier die Anwendungen und Abstimmungs-

Calls in ihrer Zwecksetzung zu bestimmen. Hier nimmt die Wahrnehmung der Eigenkontrolle der Mitarbeiter in ihrer jeweiligen Jobrolle und Funktion eine überragende Stellung ein. Denn geht der Mitarbeiter als Verarbeiter, Nutzer oder Teilnehmer mit personenbezogenen Daten um, so erfolgt dies im Rahmen der Wahrnehmung von Aufgabenstellungen für den Arbeitgeber in der **Sphäre des Unternehmens.** Insofern trägt das Unternehmen das **Betriebsrisiko,** wenn die Aufgabenwahrnehmung nicht in geschlossenen Datenbanken oder innerhalb von festgelegten Unternehmensprozessen erfolgt. Das Unternehmen muss hierbei dennoch Eigenkontrolle realisieren und dies durch Schulungen der Mitarbeiter durch den DSB begleiten. Denn nach § 4g I S. 4 Nr. 2 hat der DSB die Mitarbeiter mit den jeweiligen besonderen **Erfordernissen des Datenschutzes** vertraut zu machen. Und hierzu gehören mit der zunehmenden Nutzung der IT als Arbeitsmittel Fragen der Eigen- und auch der Selbstkontrolle.

Eine besondere **Facette der Kontrolle** – außerhalb der Datenschutz- **267**
kontrolle nach BDSG – ist, dass der **Betriebsrat** die Einhaltung der zugunsten der Arbeitnehmer geltenden Gesetze nach § 80 I Nr. BetrVG **überwacht.** Dieses Recht betrifft allerdings nur die beschäftigtenbezogene Datenverarbeitung, die unterstützend zur Durchführung des Arbeitsverhältnisses erfolgt oder als Mittel der Mitarbeiterüberwachung Auswirkungen auf das Arbeitsverhältnis des Mitarbeiters hat oder sein Persönlichkeitsrecht beeinträchtigen kann. Im Beschäftigtendatenschutz nach § 32 spielt die Einhaltung von Datenschutz bei personellen Maßnahmen nach § 99 II Nr. 1 BetrVG eine zunehmend wichtige Rolle. Denn der Betriebsrat muss jetzt genauer prüfen, ob **personelle Einzelmaßnahmen** in Übereinstimmung mit dem Arbeitnehmerdatenschutz erfolgen. Personelle Einzelmaßnahmen i. S. v. § 99 BetrVG sind die Einstellung, Eingruppierung, Umgruppierung und Versetzung. Datenschutz betrifft hierbei aber nicht nur die Umsetzung dieser Maßnahmen selbst, sondern auch den diesbezüglich rechtmäßigen Umgang mit beschäftigtenbezogenen Daten. Demgegenüber hat allerdings auch der Betriebsrat als unselbständiger **Teil der verantwortlichen Stelle** (*Fitting* BetrVG, § 83 Rn. 23) die Verpflichtung, die erhöhten Restriktionen des § 32 selbst einzuhalten. Die Verarbeitung von Daten durch den Betriebsrat unterliegt damit auch der Eigenkontrolle des Unternehmens.

1.2 Verfassungsrechtliche Fundierung der Kontrolle: Datenschutzkon- **268**
trolle ist unter dem Gesichtspunkt einer **verfahrensmäßigen Sicherstellung** des Datenschutzes zu betrachten (Simitis-*Dammann* BDSG, § 1 Rn. 113 ff.). Das **Recht auf informationelle Selbstbestimmung** definiert hierbei aus Sicht des Betroffenen seine Befugnis, grundsätzlich selbst darüber zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebensverhältnisse offenbart. Ergänzt wird diese Betrachtung durch die Verpflichtung der verantwortlichen Stellen, diese idealtypisch

definierte Rechtsposition durch Maßnahmen der Kontrolle zu unterstützen. Zu berücksichtigen ist für den Unternehmensdatenschutz, dass das Recht auf informationelle Selbstbestimmung allerdings nicht schrankenlos gewährleistet werden muss (BVerfGE 65, 43f.). Kernpunkt der verfassungsrechtlichen Fundierung der Datenschutzkontrolle ist es, dass darauf zu achten ist, dass der Umgang mit personenbezogenen Daten eines Betroffenen nach § 1 I i.V.m. § 3 in jedem Einzelfall an einer am **Verhältnismäßigkeitsgrundsatz** orientierten Güterabwägung stattfindet. Diesem Anspruch muss die Datenschutzkontrolle nachkommen.

269 Ein **legitimer Zweck** der Datenverarbeitung ist nach dem Gesagten nicht ausreichend, um den Kontrollanforderungen des Datenschutzrechts nachzukommen. Die Datenverarbeitung muss zum Schutz von Betroffenen erforderlich, angemessen und verhältnismäßig sein. Dies bedeutet, dass die Maßnahme für die Erreichung des Zwecks geeignet sein muss und es darf kein milderes Mittel mit gleicher Eignung zur Verfügung stehen. **Verhältnismäßig** im engeren Sinn ist eine solche Maßnahme nur dann, wenn die Nachteile, die für den Betroffenen mit der Maßnahme verbunden sind, nicht außer Verhältnis zu den Vorteilen stehen. Diese Betrachtung aus der **Schutzperspektive des Betroffenen** ist zu ergänzen aus der **Interessenperspektive des Unternehmens.** Datenschutzkontrolle steht damit zwischen dem Recht auf informationelle Selbstbestimmung des Einzelnen und der wirtschaftlichen **Betätigungsfreiheit von Unternehmen.**

270 Bei weiteren **gesetzgeberischen Schritten** zum Datenschutz hat der Gesetzgeber darauf zu achten, dass Einschränkungen des Rechts auf informationelle Selbstbestimmung nur in **überwiegendem Allgemeininteresse** zulässig sind (Simitis-*Simitis* BDSG, § 1 Rn. 86ff.). Angesichts der Gefährdung dieses speziellen Grundrechts hat der Gesetzgeber ausreichende gesetzliche Grundlagen zu dessen Schutz zu schaffen. Aus dieser gesetzgeberischen Verpflichtung kann allerdings nicht der Schluss gezogen werden, dass dieses Grundrecht uneingeschränkt und in allen Rechtsbereichen auf gleichem Niveau zu beachten sei. Zur notwendigen Grundrechtsverwirklichung sollte der Gesetzgeber aber in allen Rechtsbereichen darauf achten, dass er dem **Gebot der Normenklarheit** nachkommt, um eine zuverlässige gesetzliche Grundlage zur Gestaltung von Datenschutz und die Anwendung von Datenschutzrecht zu gewährleisten (*T/B/P* Einführung, S. 103f., 367f.). Denn seiner Zielsetzung entsprechend soll Datenschutz hinführen zu einer zulässigen, gesicherten auf **Wiederholung** gerichteten Verarbeitung und Nutzung personenbezogener Daten. Nur so können die Anforderungen an die Datenschutzkontrolle auch zuverlässig umgesetzt werden. In Unternehmen ist heute Best Practice, dass das Zusammenspiel von **Selbst-, Eigen- und Fremdkontrolle** intensiviert wird. Ein gute Regelung des BDSG ist es deshalb, dass sich der DSB nach § 4g I S. 2 in Zweifelsfällen an die für die Datenschutz-

kontrolle der verantwortlichen Stelle zuständige Behörde wenden kann. Der DSB kann hierbei nach § 4g I S. 3 auch die Beratung der Behörde nach § 38 I S. 2 in Anspruch nehmen.

Abschließend ist darauf hinzuweisen, dass im Unternehmensdaten- **271**
schutz das Thema der **Grundrechtsverbürgung** anders zu betrachten ist als die Abwehr von staatlichen Eingriffen in die informationelle Selbstbestimmung des einzelnen Bürgers. Denn Demokratie und Privatrechtsgesellschaft sind essenziell auf freie Information und Kommunikation angewiesen, welche Art. 5 I bzw. Art. 2 I GG garantieren. Die kommunikative Komponente der Berufsfreiheit – die unternehmerische Betätigungsfreiheit – nach Art. 12 I GG und des Eigentumsschutzes nach Art. 14 I GG können als Sondergrundrechte speziell zur Wahrnehmung von Arbeitgeberinteressen ins Feld geführt werden. Der Eigentümer kann typischerweise frei über sein **Eigentum** verfügen (*M/M* Grundrecht, S. 195). Art. 14 I GG wird allerdings nur dann zu berücksichtigen sein, wenn beim Arbeitgeber in den konkreten Bestand an Rechten und Gütern eingegriffen wird. Wird das Unternehmen in seiner Funktion als Arbeitgeber gesetzlich beschränkt, Arbeitnehmerdaten zu erheben oder zu verarbeiten und dies zu **kontrollieren,** so fällt dies lediglich in den **Schutzbereich des Art. 12 I GG,** wonach aber Eingriffe in die Freiheit der Ausübung unternehmerischer Betätigung bereits aus „vernünftigen Erwägungen des Gemeinwohls" verfassungsrechtlich gerechtfertigt sind. Da die Erfüllung eines Grundrechts wie z. B. dasjenige der informationellen Selbstbestimmung oft ein Stück Nichterfüllung anderer Grundrechte bedeutet, bleibt das erfüllte Grundrecht als verfassungsrechtlicher Grund für die Rechtfertigung solcher Nichterfüllungen bedeutsam.

1.3 BDSG und Metabetrachtung der Compliance: Compliance betrifft **272**
und beschreibt die Gesamtheit von Maßnahmen, welche das rechtmäßige Verhalten eines Unternehmens sicher stellt (*Thüsing* Compliance, S. 8). Für den Unternehmensdatenschutz bedeutet das, dass das BDSG – wie auch andere Vorschrift, welche Unternehmen adressieren – einzuhalten sind. Die Anwendung des BDSG erhält damit eine **Metaebene,** d. h. eine zweite Ebene, welche neben der Zielsetzung, Beeinträchtigungen des Persönlichkeitsrechts entgegen zu wirken, auch die Zielsetzung hat zu überprüfen, ob die **Rechtstreue** des Unternehmens gewahrt wird. Und hierbei kann das Unternehmen zu Kontrollen, Überprüfungen und rechtlichen Maßnahmen veranlasst sein, welche – z. B. bei der Korruptionsbekämpfung – mit strengen Regelungsvorgaben des BDSG in Konflikt geraten können. Hierbei muss sich Unternehmensdatenschutz auch mit den **systemischen Krisen** wie der Finanzkrise auseinandersetzen, welche dazu führen, dass z. B. das **Bankgeheimnis** einen geringeren Stellenwert erhält. Privatsphäre- und Persönlichkeitsschutz wird vor diesem Hintergrund dynamischer. Ebenso beschleunigt durch die Digitalisierung und Vernetzung der Welt. Im Unternehmensdatenschutz ist dieser Themenbe-

reich unter dem Gesichtspunkt von Compliance **und staatlich regulierten Informationsinhalten** und Datenzugriffen betrachten. Best Practice muss sein, anhand der sich schnell verändernden Gegebenheiten zu handeln und eine **Balance** zwischen berechtigten Transparenzanforderungen des Staates und den Interessen von Betroffenen zu finden.

273 Compliance im Datenschutz kann damit nicht mit Arbeitgeberinteressen und -pflichten im Datenschutz gleichgesetzt werden. Denn bei Compliance geht es gewissermaßen um übergeordnete **Legalitätspflichten,** die aber per se keinen Vorrang vor Rechten von Betroffenen haben. Die Rechte von Betroffenen können nach § 6 I nicht durch **Rechtsgeschäft** ausgeschlossen oder **beschränkt** werden. Dies bedeutet aber nicht, dass die Rechte nicht durch Vorgaben anderer rechtlicher Erfordernisse, welche Unternehmen zu erfüllen haben, zwar nicht im Hinblick auf den Datenschutz beschränkt werden, aber faktisch durch Rechtsvorschriften der Rechtsordnung **eingeschränkt** sind. Ein Argument aus dem BDSG unterstützt diese Rechtsansicht. Mit der Einführung des Begriffs der Erforderlichkeit in die Vorschrift des § 32 als **Korrektiv** für die Grenze der Zulässigkeit einer Datenverarbeitung wird deutlich, dass die Kontrolle und Beurteilung einer Datenverarbeitung – weg von der unternehmerischen Eigenverantwortung – tendenziell in die Hände Dritter gelegt wird. Allerdings ist Datenverarbeitung nach wie vor nicht vom Ausnahmezustand eines Korruptions- oder Datenskandals, sondern vom **Normalfall** der täglichen Datenverarbeitung her zu betrachten.

274 Der Gesichtspunkt der Compliance kann dazu genutzt werden, besser zu analysieren, in welchem Fall personenbezogene Datenverarbeitung **Zweck für eine Unternehmens- oder Personalaufgabe** ist und in welchem Fall Datenverarbeitung lediglich **Mittel zur Kommunikation** ist. Das BDSG adressiert die inhaltliche Zweckebene. Demgegenüber adressiert das TMG die Facette der Kommunikation sowie das Telekommunikationsgesetz (TKG) die Facette des Transports, d.h. der Übertragung von Daten. Hier stellt sich die Frage des Fernmeldegeheimnisses (§§ 91ff., 88 TKG). Im Anbieter-Nutzer-Verhältnis gelten die Vorschriften der §§ 11 bis 15a TMG dann nicht, soweit solche Dienste im Arbeitsverhältnis ausschließlich zu beruflichen Zwecken bereitgestellt werden. Compliance ist damit ein Analyse-Tool, die Sachverhalte und deren Anforderungen in einem größeren Kontext zu betrachten.

275 Datenverarbeitungen des Unternehmens bzw. des Arbeitgebers sind nach BDSG im Rahmen des Konzeptes des Verbots mit Erlaubnisvorbehalt nach § 4 I prinzipiell verboten. Der **Aspekt des verkehrsgerechten Verhaltens,** welches sich innerhalb der Ordnung des Gemeinschaftslebens vollzieht, berücksichtigt das BDSG nicht. Dies, obwohl Datenverarbeitung zum alltäglichen Arbeitsmittel geworden ist. Dazu gehören **Managementsysteme** für die unterschiedlichen Unternehmensfunktionen wie auch der Umstand, dass Arbeitnehmer in ihrer Aufgabenstellung im

Unternehmen personenbezogene Daten verarbeiten. Je arbeitsteiliger und integrierter Unternehmen sind, desto mehr Arbeitnehmer gehen mit personenbezogenen Daten um. Durch die Metabetrachtung der Compliance kann insofern eine **Stimmigkeitskontrolle** der Anwendung des BDSG vorgenommen werden.

Im Unternehmensdatenschutz sind klar definierte Regeln erforderlich, **276**
welche die Betroffenen wirksam einfordern können. Zweckunbestimmte Datenerhebungen, nicht konkret zweckgebundene Datenverarbeitungen, **anlasslose Datenspeicherungen** sind Herausforderungen, die dazu erforderliche Transparenz herzustellen. Die Selbstorganisationsverpflichtung für die Zulässigkeiten der Datenverarbeitung sowie Sicherstellung der **Verfügbarkeit von Informationen** stellten eine Herausforderung der **Compliance** dar. Denn Compliance betrifft die Einhaltung und Befolgung regulatorischer Vorschriften durch Unternehmen sowie deren Mitarbeiter. Damit hat sich Datenschutz als ein zentrales Thema der Gesamtrechtsordnung etabliert. Datenschutz wird nicht als Gegenpol dynamischer Prozesse in Wirtschaft und Arbeitsleben betrachtet, sondern als Steuerungsinstrument im Rahmen der Rechtsordnung. **Trusted Information** als rechtlich geschützte Informationen und **Compliance Need** als berechtigtes Interesse sind hierbei zwei moderne Facetten. Zu den rechtlich geschützten Informationen des Unternehmens gehören z. B. Urheberrechte, Patente, aber auch Finanzdaten des Unternehmens. Zu deren Schutz ist ein geeignetes und funktionsfähigen Risiko- und Überwachungssystems einzuführen (vgl. § 91 II AktG).

Als unternehmensinternes Überwachungssystem und als Instrument **277**
zur Verbesserung von Unternehmensprozessen dienen **Internal Investigations.** Hierbei geht es um die Untersuchung, ob bei geschäftlichen Handlungen keine Verletzung von Geschäftsgrundsätzen und/oder Gesetzen vorliegt. Hierbei geht es im Besonderen auch darum, ob ein Bruch unternehmensinterner Vorgaben zum geschäftlichen Handeln keine negativen rechtlichen oder finanziellen Auswirkungen für das Unternehmen haben. In einem internen Audit geht es hierbei darum, als unethisch erkannte Geschäftspraktiken in der Zukunft zu vermeiden. Bei der Klärung von Sachverhalten im Unternehmen haben die Mitarbeiter grundsätzlich einer **Aussageverpflichtung** nach §§ 666, 675 BGB analog. Mitarbeiter, die sich auf die Geschäftsgrundsätze des Unternehmens verpflichtet haben, haben eine solche Verpflichtung auch nach § 241 II BGB, wonach sie im Rahmen ihrer arbeitsvertraglichen Pflichten auch die Rechte und Interessen ihres Arbeitgebers zu berücksichtigen haben.

Ein berechtigtes Interesse sind **gute Gründe,** etwas zu tun. Berechtig- **278**
tes Interesse beschreibt im Datenschutz einen Erlaubnistatbestand, etwas tun zu dürfen, was ansonsten verboten wäre. Nach § 32 wird das berechtigte Interesse des Arbeitgebers nach § 28 I Nr. 2 für Beschäftigtendaten als **Handlungsoption** grundsätzlich nicht mehr anerkannt. Die Betrach-

tung der Zulässigkeit nach § 32 ergibt sich im Wesentlichen aus der Schutzperspektive des Beschäftigten. Das ist für kritische Sachverhalte richtig. Nicht aber für legitime Zwecke, die für die Durchführung des Arbeitsverhältnisses nicht erforderlich sind. Die Erhebung von Mitarbeiterdaten für Online-Schulungen ist für die Durchführung von Beschäftigungsverhältnissen sicherlich nicht erforderlich. Für die **Aufrechterhaltung der Wettbewerbsfähigkeit** des Unternehmens ist dies aber sicherlich von zentraler Bedeutung, denn die Unternehmensperformance hängt häufig nicht unwesentlich von der Aktualität der fachlichen Kenntnisse und Fähigkeiten der Mitarbeiter ab. In diesem Kontext berechtigter Interessen des Unternehmens sind insofern auch Maßnahmen der Compliance zu betrachten.

279 **1.4** Qualitätsmanagement und Datenschutzaudit: Datenschutzkontrolle hat neben der verfassungsrechtlichen Facette und dem Gesichtspunkt der Rechtsbefolgung auch den Aspekt der Qualität. Beim Qualitätsmanagement geht es nicht nur um die Festlegung von datenschutzrechtlichen Mindeststandards, sondern darüber hinaus auch um die Erarbeitung quantifizierbarer Qualitätskriterien (*Wächter* Falsifikation, S. 343 ff.). Dies ist ein betriebswirtschaftlicher Aspekt, der das Thema Datenschutz überführt in den Bereich der **Risikovorsorge in Unternehmen.** Der Gesetzgeber hat dieses Thema mit der Vorschrift des § 9 a, dem Datenschutzaudit geregelt (Simitis-*Scholz* BDSG, § 9a Rn. 1 ff.), aber keine inhaltlichen Vorgaben zur Verbesserung von Datenschutz und Datensicherheit gemacht.

280 Zugriffsmanagement auf Daten betrifft auch die Frage des Qualitätsmanagements. Hierzu sind technische **Anforderungen für Unternehmensprozesse** fest zu legen. Die internationale DIN Norm **ISO/IEC 27001** (Information Technology) spezifiziert die Anforderungen für dokumentierte Informationssicherheits-Managementsysteme unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Die Norm beschreibt Anforderungen für die Implementierung von geeigneten Sicherheitsmechanismen, welche an die Gegebenheiten der einzelnen Organisationen angepasst werden müssen. Im Unternehmen sind danach Sicherheitsmechanismen zu etablieren, um **Assets** zu schützen und **Business Risks** zu reduzieren. Die ISO/IEC-Vorschriften dienen hierzu zur Formulierung von Anforderungen und Zielsetzungen zur Informationssicherheit und zur Beachtung von Gesetzen. Ein wichtiger Aspekt ist hierbei die Verfügbarkeit von Daten sowie die Business Continuity. Hierzu sind im Unternehmen Maßnahmen (z. B. zu Cyber Security, Intrusion Detection, Trusted Third Party Authentication) zu etablieren.

281 Bei der inhaltlichen Bestimmung der Frage der **Qualität personenbezogener Datenverarbeitung** nach § 9a kann auf die Vorschrift des Art. 6 EUDatRL zurückzugreifen werden. Dort sind die elementaren Grundsätze zur **Qualität der Daten** festgelegt. Dazu gehören die Verarbeitung