4 Verhältnis zum Datenschutz

Im Kontext der zu erreichenden Compliance ist auch die Einhaltung des Datenschutzes notwendig (siehe Kapitel 1). Auch im Zuge des Schutzes des Fernmeldegeheimnisses wurden zahlreiche angrenzende Bestimmungen aufgeführt, die letztlich konkrete Folgen für die Gewährleistung mehrseitiger IT-Sicherheit haben. Deshalb sind die entsprechenden Anforderungen einander abzugleichen, zumal in der Praxis oft ein grundlegender Gegensatz zwischen gesetzlichen Erfordernissen und betrieblichen Eigeninteressen konstruiert wird. Eine Konvergenz dieser Interessen kann durch den Einsatz datenschutzfreundlicher Techniken erreicht werden.

4.1 Abgleich von Datenschutz und IT-Sicherheit

Wenn es lediglich um die automatisierte Verarbeitung personenbezogener Daten geht, stimmen viele datenschutztechnisch motivierte Aspekte mit denen mehrseitiger IT-Sicherheit überein. Dies trifft vor allem auf die zu ergreifenden technischen und organisatorischen Maßnahmen zu. Auch bei der Funktion eines Datenschutzbeauftragten bzw. eines IT-Sicherheitsbeauftragten gibt es mehr Gemeinsamkeiten, als auf dem ersten Blick zu erkennen ist. Etwaige Unterschiede finden sich erst im Detail und können in erster Linie mit den verschiedenen Sichtweisen begründet werden. Gerade diese sind jedoch einer genaueren Betrachtung wert, damit das Zusammenspiel besser beurteilt werden kann.

4.1.1 Technische und organisatorische Maßnahmen

Gleich mehrere *Gesetze* schreiben die Gewährleistung angemessener technischer und organisatorischer Maßnahmen vor, die i.d.R. einen hohen Bezug zur IT-Sicherheit aufweisen:

- § 9 BDSG zum Schutz personenbezogener Daten,
- § 78a SGB X zum Schutz personenbezogener Sozialdaten,
- §§ 107 und 109 TKG zum Schutz von (nicht nur personenbezogenen) Fernmeldedaten,

- § 4 TDDSG zum Schutz von personenbezogenen Nutzerinteressen von Telediensten und
- § 18 MDStV zum Schutz von personenbezogenen Nutzerinteressen von Mediendiensten.

Zahlreiche weitere Gesetze erfordern *implizit* entsprechende Maßnahmen. So gilt z.B. der Straftatbestand des Ausspähens von Daten (§ 202a StGB) nur, wenn geschützte Daten gegen unberechtigten Zugang besonders gesichert sind. Die Verwendung technischer Aufzeichnungen als Beweismittel setzt deren erheblich erschwerte Manipulierbarkeit voraus, damit der entsprechende Straftatbestand greifen kann (§§ 268 und 269 StGB). Ein Unternehmen ist also gut beraten, auch zur Abwehr potentieller Straftaten geeignete Maßnahmen zu ergreifen, um mehrseitige IT-Sicherheit gewährleisten zu können.

Ziel der meisten technischen und organisatorischen Maßnahmen ist vor allem die Verhinderung unzulässiger Informationsverarbeitung. Dies erfordert in jedem Fall eine geeignete Implementation der Datensicherung und die entsprechende Protokollierung von Zugriffen.

Definition: Datensicherung
Maßnahmen zur Erhaltung und Sicherung des Datenverarbeitungssystems, der Daten und Datenträger vor höherer Gewalt, Fehler und Missbrauch.

Im Wesentlichen zielt die Datensicherung also auf die Ausfallsicherheit (*Safety*) ab. Die darüber hinaus ergriffenen technischen und organisatorischen Maßnahmen dienen dagegen eher der Abwehr unberechtiger Zugriffe und damit der *Security*.

Die Anlage zu § 9 BDSG bestimmt folgende *Kontrollbereiche* für technische und organisatorische Maßnahmen:

- Organisationskontrolle: die innerbetriebliche *Organisation* ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird – dies gilt insbesondere für die nachfolgenden Kontrollbereiche, da dieser Bereich vor der expliziten Auflistung der anderen Bereiche gesetzt wurde;
- Zutrittskontrolle: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden – dies dient also in erster Linie dem Schutz von *Gebäuden* und Serverräumen;

- Zugangskontrolle: Die Nutzung von Datenverarbeitungssystemen durch Unbefugte ist zu verhindern – dies dient dagegen dem Schutz des jeweiligen *IT-Systems* (auch vor Angriffen);
- Zugriffskontrolle: Die zur Benutzung eines Datenverarbeitungssystems Berechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen, so dass personenbezogene Daten bei der Verarbeitung, Nutzung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können – dies betrifft die eigentlichen *Anwendungen* und *Applikationen*, mit denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden;
- Weitergabekontrolle: Bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger dürfen personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden, weshalb es überprüfbar und feststellbar sein muss, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist – dies kann deshalb vor allem als Schutz des *Netzwerks* angesehen werden;
- Eingabekontrolle: Nachträglich muss es überprüfbar und feststellbar sein, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfert worden sind – dies dient vor allem der *Zurechenbarkeit*;
- Auftragskontrolle: Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden – dies dient damit der Absicherung der *Rechtsverbindlichkeit*;
- Verfügbarkeitskontrolle: Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen – dies stellt die ausdrückliche Aufforderung zur *Ausfallsicherheit* dar;
- Datentrennungskontrolle: Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden – dies unterstützt die Gewährleistung von *Zurechenbarkeit* und *Rechtsverbindlichkeit*.

Die technischen und organisatorischen Maßnahmen nach § 9 BDSG werden auch als *Datensicherheitsmaßnahmen* bezeichnet. Die Sichtweise der angegebenen Kontrollbereiche entspricht

eher zentralen Rechenzentren, die zunehmend durch flexiblere Infrastrukturen in den Unternehmen ersetzt werden, doch existiert eine hohe Übereinstimmung zu üblichen IT-Sicherheitsmaßnahmen, wie sich aus dieser Auflistung ablesen lässt.

In mehreren Länderdatenschutzgesetzen werden daher anstelle der Kontrollbereiche inzwischen Schutzziele formuliert, die sehr nah an denen mehrseitiger IT-Sicherheit liegen. Meist wird dabei jedoch die Rechtsverbindlichkeit in Revisionsfähigkeit und Transparenz unterteilt. Auch wird vereinzelt in moderneren Landesdatenschutzgesetzen eine Risikoanalyse und ein Sicherheitskonzept vorgeschrieben. Aspekte der Datensicherheit weisen also (zunehmend) eine hohe *Schnittmenge* mit Aspekten mehrseitiger IT-Sicherheit auf:

	Verfügbarkeit	*Integrität*	*Vertraulichkeit*	*Zurechenbarkeit*	*Rechtsverbindlichkeit*
Organisationskontrolle	X	X	X	X	X
Zutrittskontrolle	X		X		
Zugangskontrolle	X	X	X		
Zugriffskontrolle	X	X	X	X	X
Weitergabekontrolle	X	X	X	X	X
Eingabekontrolle		X		X	
Auftragskontrolle					X
Verfügbarkeitskontrolle	X				
Datentrennungskontrolle		X	X	X	X

Abbildung 62: Vergleich von Kontrollbereichen und Sicherheitszielen

4.1.2 Datenschutzbeauftragter und IT-Sicherheitsbeauftragter

Die ergriffenen Datensicherheitsmaßnahmen werden sowohl vom Datenschutzbeauftragten als auch vom IT-Sicherheitsbeauftragten überprüft, sofern diese Funktionen jeweils besetzt wurden. Die Anforderungen an die Person, die die *Funktion* eines Datenschutzbeauftragten oder eines IT-Sicherheitsbeauftragten (bzw. Chief Information Security Officers) ausfüllt, sind vergleichbar und unterscheiden sich in erster Linie nur aufgrund der jeweiligen Sichtweise. Beide Funktionen werden sinnvollerweise direkt der Geschäftsführung unterstellt.

Die Bestellung eines *Datenschutzbeauftragten* ist im Gegensatz zur Bestellung eines IT-Sicherheitsbeauftragten gesetztlich vorgeschrieben: Bei Unternehmen ("nicht-öffentliche Stellen") ist ein Datenschutzbeauftragter zu bestellen, sobald mindestens zehn beschäftigte Personen (bis Ende 2006 waren es noch mindestens fünf beschäftigte Arbeitnehmer, so dass nunmehr auch leitendes Personal mitgezählt wird) ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind bzw. mindestens zwanzig Personen mit der manuellen Erhebung, Verarbeitung oder Nutzung (§ 4f Abs. 1 BDSG). Unter der automatisierten Verarbeitung wird die Erhebung, Verarbeitung oder Nutzung unter Einsatz von Datenverarbeitungsanlagen verstanden. Der Datenschutzbeauftragte wirkt auf die Einhaltung datenschutzrechtlicher Vorschriften hin und besitzt hierzu ein umfassendes Kontrollrecht.

Die gesetzlich bestimmten *Anforderungen* an den Datenschutzbeauftragten sind die nötige Fachkunde (in Abhängigkeit des Schutzgrades der automatisiert verarbeiteten personenbezogenen Daten) und die Zuverlässigkeit. Was unter der erforderlichen Fachkunde zu verstehen ist, ist durch Gerichtsentscheide näher bestimmt worden und soll für den nachfolgenden Vergleich die Richtschnur bilden.

Unter dem Aspekt der *Zuverlässigkeit* werden gemeinhin beim Datenschutzbeauftragten die Fähigkeit zur Verschwiegenheit, die Vermeidung von Interessenkonflikten und die charakterliche Eignung verstanden. In den juristischen Kommentaren wird beispielsweise eine Interessenkollission mit der Funktion als Datenschutzbeauftragter bei Mitarbeitern der IT-Administration oder Mitgliedern der Geschäftsleitung gesehen.

Beim IT-Sicherheitsbeauftragten gibt es dagegen noch wenig *Erfahrungswerte* an ein entsprechendes Berufsbild, zumal dieser

nicht zwingend in den Unternehmen einzusetzen ist. Bisher wurden nur in größeren Unternehmen sowie in Unternehmen, die mit sicherheitskritischen oder besonders sensiblen Daten arbeiten, IT-Sicherheitsbeauftragte eingesetzt.

Ein *Datenschutzbeauftragter* muss nach einem Urteil des Landgerichts Ulm folgende Kenntnisse und Fähigkeiten vorweisen:

- Anwendung rechtlicher Vorschriften aus dem Bereich des Datenschutzes, um zur Erfüllung der Sorgfaltspflicht und Compliance beitragen zu können;
- Kenntnisse der betrieblichen Organisation, da die Einhaltung datenschutzrechtlicher Vorschriften in der innerbetrieblichen Organisation durchzusetzen sind;
- Ausgewiesenheit in der Informationstechnik ("Computerexperte"), da der Umgang mit automatisierten Verarbeitungen personenbezogener Daten den Schwerpunkt der beruflichen Tätigkeit ausmacht;
- didaktische Fähigkeiten, um Schulungen zur Steigerung des datenschutzrechtlichen Bewusstseins halten zu können;
- psychologisches Einfühlungsvermögen und Konfliktmanagement, weil der Datenschutzbeauftragte geschickt den Betroffeneninteressen nachgehen muss und dabei oft zwischen IT-Administration und Geschäftsführung vermitteln muss;
- Organisationstalent, um den erforderlichen Prozess zur Umsetzung datenschutzrechtlicher Anforderungen managen zu können.

Ein *IT-Sicherheitsbeauftragter* muss vergleichbare Kenntnisse und Fähigkeiten vorweisen:

- Anwendung rechtlicher Vorschriften aus dem Bereich der IT-Sicherheit, um zur Erfüllung der Sorgfaltspflicht und Compliance beitragen zu können;
- Kenntnisse der betrieblichen Organisation, da einige Schwachpunkte im Sicherheitskonzept in der innerbetrieblichen Organisation zu suchen sind;
- Ausgewiesenheit in der Informationstechnik ("Computerexperte"), da die Herausforderungen der Informationstechnik zu den Hauptaufgaben eines IT-Sicherheitsbeauftragten zählen;
- didaktische Fähigkeiten, um Schulungen zur Steigerung des Sicherheitsbewusstseins halten zu können;

- psychologisches Einfühlungsvermögen und Konfliktmanagement, weil der IT-Sicherheitsbeauftragte zwischen IT-Administration und Geschäftsführung sitzt und vermitteln muss;
- Organisationstalent, um den erforderlichen Prozess mehrseitiger IT-Sicherheit und des IT-Risikomanagements managen zu können.

Sicherlich sind die Anforderungen mehrseitiger IT-Sicherheit im Bereich der Informationstechnik umfassender als beim Datenschutzbeauftragten, denn der *IT-Sicherheitsbeauftragte* muss alle relevanten Sicherheitsstandards kennen und umsetzen können, eine Sicherheitsarchitektur selbst entwerfen können und sich etwas umfassender in Kryptographie, Betriebssicherheit, Netzwerksicherheit und Systemsicherheit auskennen. Dabei hat er auch die IT-Systeme miteinzubeziehen, die keine personenbezogenen Daten automatisiert verarbeiten.

Dafür kümmert sich der *Datenschutzbeauftragte* zusätzlich um die Datenschutzkonformität manueller Datenverarbeitung, die den IT-Sicherheitsbeauftragten eher selten interessieren. Außerdem ist der Datenschutzbeauftragte in der Ausübung seiner Fachkunde weisungsfrei, darf nicht benachteiligt werden und ist durch das Unternehmen geeignet zu unterstützen. Auf diese wichtigen Schutzrechte kann sich ein IT-Sicherheitsbeauftragter derzeit nicht berufen.

4.1.3 Sichtweisen von Datenschutz und IT-Sicherheit

Die größten Unterschiede zwischen Datenschutz und IT-Sicherheit finden sich sicherlich in der jeweils zugrunde liegenden *Sichtweise*: Während beim Datenschutz das Interesse von Betroffenen hinsichtlich der Gewährleistung ihres informationellen Selbstbestimmungsrechts vorrangig ist, ist bei IT-Sicherheit das Interesse von Systembetreibern hinsichtlich der Gewährleistung verlässlicher und beherrschbarer IT-Systeme ausschlaggebend.

Bei *mehrseitiger IT-Sicherheit* wird ein Ungleichgewicht zwar weitgehend aufgelöst und mehr Gemeinsamkeiten erreicht, doch ist hier der datenschutzrechtliche Aspekt eben nur einer unter vielen. Deshalb werden durch Maßnahmen zur IT-Sicherheit nicht nur personenbezogene Daten geschützt, sondern alle Unternehmensdaten. Beim Datenschutz ist hingegen die Inhaltsebene der Daten ausschlaggebend für die zu ergreifenden Maßnahmen, bei IT-Sicherheit dagegen die Transportebene, weil es unerheblich ist, ob die Daten einen Personenbezug aufweisen.

Das *IT-Risikomanagement* erfordert eine umfassende (auch personenbezogene) Protokollierung von Tätigkeiten und Aktionen, um insbesondere feststellen zu können, von was oder wem eine Gefährdung der eingesetzten IT-Systeme ausgeht. Ziel der Protokollierung ist damit neben der anonymisiert durchführbaren Risikoanalyse ebenfalls die durch die Sorgfaltspflicht motivierte Überwachung sicherheitsrelevanter Aktivitäten.

Beim Datenschutz ist zwar für die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle und Eingabekontrolle eine *Protokollierung* personenbezogener Daten vorgeschrieben, doch unterliegt diese einer strengen Zweckbindung, dem Grundsatz der Datensparsamkeit und der Löschungspflicht nach Ablauf der Aufbewahrungsdauer.

Anomalien lassen sich nur anhand protokollierter Werte feststellen und sind teilweise nicht so zielgenau feststellbar, wie dies beispielsweise bei der Missbrauchsanalyse hinsichtlich der Verletzung von Datenschutzbestimmungen der Fall ist. Hier werden aus Sicht der IT-Sicherheit unter Umständen längere Zeitreihenanalysen benötigt, die zwar größtenteils anonymisiert erfolgen können, doch vielleicht gerade durch die Verknüpfung mit den entsprechenden Verbindungsdaten (insbesondere der IP-Adressen) eine höhere Aussagekraft entfalten würden. Für die Festlegung der Abwehrstrategien reichen jedoch die anonymisiert ermittelten Erkenntnisse zweifellos aus.

Eine umfassende und längerfristig vorzuhaltende Protokollierung kostet zudem Geld, das für andere Sicherheitsmaßnahmen dann nicht mehr zur Verfügung steht. Dies erfordert ein präzises Protokollierungskonzept, das insbesondere die erforderlichen Beweiszwecke abdecken muss. Insofern ist die *Vorratsdatenhaltung* der Kommunikationsdaten für die Unternehmen ein ernstzunehmender Kostenfaktor, dessen Sinnhaftigkeit in der aktuellen <kes>-Sicherheitsstudie bezweifelt wird, da nur 49 % die gesetzlichen Bestimmungen zur TK-/Internet-Überwachung für angemessen beurteilen und immerhin 38 % diese für überzogen halten. Diese Vorratshaltung wird nicht durch betriebliche Sicherheitsinteressen motiviert, sondern durch staatliche.

Im Zuge der Datensicherung ist ein wesentliches Konzept aus der Sicht der IT-Sicherheit die *Redundanz* von Technik und Daten. Daten sollten also vorzugsweise gespiegelt vorliegen, um eine hinreichende Ausfallsicherheit gewährleisten zu können. Die Verfügbarkeit personenbezogener Daten (und damit auch der entsprechenden IT-Systeme, mit denen diese erhoben, verarbei-

tet oder genutzt werden) ist zwar auch ein Grundsatz im aktuellen Datenschutzrecht, doch kollidiert dieser teilweise mit dem Grundsatz der Datensparsamkeit.

Sofern es also Gegensätze zwischen Datenschutz und IT-Sicherheit gibt, lassen diese sich leicht unter dem Blickwinkel *mehrseitiger IT-Sicherheit* auflösen.

4.2 Datenschutzfreundliche Techniken

Für die Umsetzung einer verlässlichen und beherrschbaren Informationstechnik – wie bereits im zweiten Kapitel gefordert – existieren bereits einige Techniken, die sowohl den Ansprüchen mehrseitiger IT-Sicherheit als auch denen des Datenschutzes genügen.

4.2.1 Prinzipien datenschutzfreundlicher Techniken

Datenschutzfreundliche Techniken (privacy enhancing technologies) verfolgen das *Ziel*, weniger Risiken für die Privatsphäre der Betroffenen zu erreichen, indem eingesetzte Informations- und Kommunikationstechnik bei gleichzeitiger Reduzierung erforderlichen Personenbezugs genutzt werden. Durch frühzeitige Datenvermeidung setzen diese Techniken bereits im Vorfeld der Erhebung, Verarbeitung und Nutzung personenbezogener Daten an.

Datenschutzfreundliche Techniken können damit der *vorausschauenden Technikgestaltung* zugeordnet werden, und wirken sich auf den Stand der Technik aus, weshalb diese auch plakativ als "Datenschutz durch Technik" bezeichnet werden. Im Zuge datenschutzfreundlicher Techniken werden Konzepte des Systemdatenschutzes umgesetzt, der auf eine strukturelle und systemanalytische Ergänzung des individuellen Rechtsschutzes der Betroffenen aufsetzt.

Das *Prinzip der Datensparsamkeit und des Systemdatenschutzes* beinhaltet, dass sich Techniken um so leichter anwenden lassen, je weniger personenbezogene Daten von Betroffenen herausgegeben werden (müssen). Nur erforderliche Daten dürfen erhoben, verarbeitet und genutzt werden. Personenbezogene Daten sind frühzeitig zu anonymisieren oder wenigstens zu pseudonymisieren und frühestmöglich zu löschen. Die Kommunikation hat vorzugsweise verschlüsselt zu erfolgen. Typische Beispiele zur Umsetzung stellen prepaid-Chipkarten, ein Mix-Netz oder die Verwendung von Transaktionspseudonymen bei eCash-Anwendungen dar.

Das *Prinzip des Selbstdatenschutzes und der Transparenz* dagegen erfordert und unterstützt die Selbstbestimmung und -steuerung des Nutzers. Der Nutzer entscheidet selbst, wie anonym er Dienste in Anspruch nehmen will und jeder Verarbeitungsschritt wird verständlich und überprüfbar offengelegt, so dass dem Nutzer ein Identitätsmanagement ermöglicht wird. Hierzu formuliert der Nutzer eigene Schutzziele und nutzt vertrauenswürdige Institutionen (Trust Center). Ein typisches Beispiel zur Umsetzung dieses Prinzips stellt die Platform for Privacy Preferences auf www.w3org/P3P/ dar.

Bei einem *Mix-Netz* wird sichergestellt, dass die Existenz von Kommunikationsbeziehungen zwischen verschiedenen Instanzen nicht durch Unbefugte im Zuge einer Verkehrsflussanalyse nachvollzogen werden kann. Beim Mix-Netz wird über eine vertrauenswürdige Instanz kommuniziert, die als Proxy fungiert, dabei aber die eingehenden und ausgehenden Ursprungsadressen umkodiert, so dass nicht durch Unbefugte nachvollzogen werden kann, welche eingehende Nachricht zu welcher ausgehenden Nachricht zuzuordnen ist. Dies setzt damit asymmetrisch verschlüsselte Übertragungsdaten und eine Ansammlung mehrerer Nachrichten von verschiedenen Nutzern bzw. die Erstellung künstlich erzeugter Nachrichten bei einer Remailer-Station eines Mix-Netzes voraus, bevor die umkodierten Nachrichten weitergeleitet werden. Ein Mix-Netz arbeitet deshalb mit Zeitverzögerung.

Ein *DC-Netz* (Dining Cryptographers Network nach David Chaum) ist dagegen ein synchronisiertes Verfahren, das durch die Verwendung paarweiser, symmetrischer Verschlüsselung mittels Vernam-Chiffre die Anonymität des Senders gewährleistet.

4.3 Zusammenfassung

In der Praxis finden sich oftmals Ansätze, Datenschutz und IT-Sicherheit als grundverschieden zu betrachten, da für den erstgenannten Aspekt gesetzliche Bestimmungen existieren und der zweite Aspekt scheinbar nur durch betriebliches Eigeninteresse motiviert zu sein scheint. Ein detaillierter Abgleich ergibt jedoch mehr Gemeinsamkeiten.

4.3.1 Zusammenfassung: Abgleich von Datenschutz und IT-Sicherheit

Angemessene technische und organisatorische Maßnahmen werden zur Einhaltung der Compliance in mehreren Gesetzen gefor-

dert und sind daher durch ein Unternehmen zu ergreifen. Ziel der meisten Maßnahmen ist die Datensicherung, so dass Datenverarbeitungssysteme, Daten und Datenträger vor höherer Gewalt, Fehler und Missbrauch gesichert werden. Der Schwerpunkt liegt daher auf der Gewährleistung von Safety:

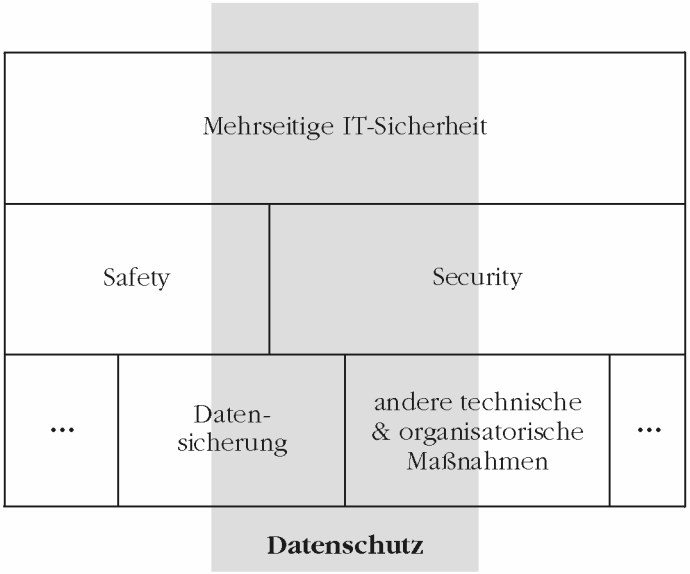

Abbildung 63: Mehrseitige IT-Sicherheit und Datenschutz

Die im BDSG formulierten Kontrollbereiche sind für die Einhaltung der Ziele mehrseitiger IT-Sicherheit geeignet, auch wenn die Sichtweise zentraler Rechenzentren bzw. Serverräume zunehmend flexibleren Infrastrukturen begegnet. In einigen Landesdatenschutzgesetzen werden daher bereits ausdrücklich die Sicherheitsziele mehrseitiger IT-Sicherheit vorgeschrieben.

Die Funktion des Datenschutzbeauftragten wie auch des IT-Sicherheitsbeauftragten erfordert letztlich ein vergleichbares Profil. In Abhängigkeit des Schutzgrades der zu schützenden Daten und IT-Systemen sind an beide vergleichbare Anforderungen an Fachkunde und Zuverlässigkeit zu stellen. Der IT-Sicherheitsbeauftragte muss jedoch zusätzlich alle relevanten Sicherheitsstandards beherrschen und über ein fundiertes Basiswissen verfügen, um eine Sicherheitsarchitektur geeignet aufbauen zu können. Allerdings verfügt er nicht über die entsprechenden Schutzrechte wie ein Datenschutzbeauftragter.

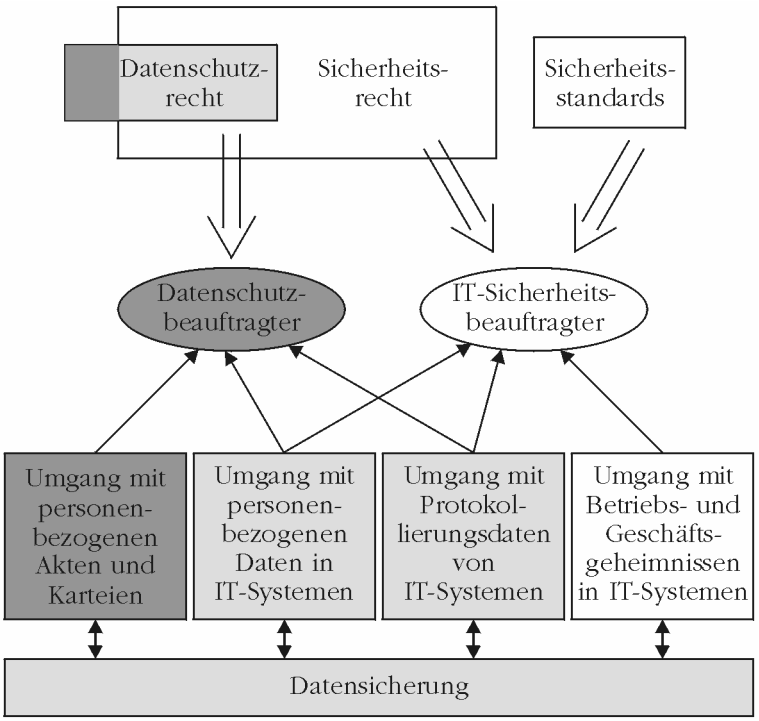

Abbildung 64: Vergleich der Beauftragten für Datenschutz und IT-Sicherheit

Die größten Unterschiede zwischen Datenschutz und IT-Sicherheit finden sich in der zugrunde liegenden Sichtweise, denn während der Datenschutz personenbezogene Daten im Interesse der Betroffenen schützt, sichert IT-Sicherheit alle Unternehmensdaten aufgrund der Interessen der Systembetreiber ab. In der Praxis überschneiden sich diese Ansätze oft, so dass lediglich hinsichtlich des zu wählenden Protokollierungskonzepts ein Klärungsbedarf besteht. Doch auch diese Gegensätze lassen sich unter der übergeordneten Sicht mehrseitiger IT-Sicherheit auflösen.

4.3.2 Zusammenfassung: Datenschutzfreundliche Techniken

Mehrseitige IT-Sicherheit und Datenschutz konvergieren beim Einsatz datenschutzfreundlicher Techniken. Diese verfolgen das Ziel der Risikoreduzierung durch frühzeitige Entfernung des Personenbezugs bei der Nutzung von Informations- und Kommunikationstechniken.

Datenschutzfreundliche Techniken werden einerseits durch das Prinzip der Datensparsamkeit und des Systemdatenschutzes geprägt, um frühzeit auf etwaigen Personenbezug verzichten zu können. Andererseits zeichnen sich datenschutzfreundliche Techniken durch das Prinzip des Selbstdatenschutzes und der Transparenz aus, die die Selbstbestimmung des Nutzers im Sinne eines Identitätsmanagements fördern.