Begriffe – Definitionen und Erklärungen

Rüdiger Dierstein, S.M.
Weichselbaum 13
82234 Oberpfaffenhofen

1. Grundbegriffe der Datenverarbeitung

Die Definitionen der Grundbegriffe sind den Normen nach DIN 44 300 in der Fassung vom November 1988 entnommen (vgl. dazu auch ISO 2382). In dieser Norm wird der Begriff *Information* im Sinne der Umgangssprache in folgender Weise verwendet:

Information	Kenntnisse über Sachverhalte und Vorgänge

Dieser Begriff ist zu unterscheiden vom Informationsbegriff der Informationstheorie nach C. Shannon (siehe DIN 44 301 sowie auch DIN 44 330).

DIN 44300 unterscheidet sorgfältig zwischen den Begriffen Zeichen, Daten und Information. Zeichen werden erst dadurch zu Daten und damit zu Informationsträgern, dass ihnen eine **Bedeutung zugeordnet** wird, d.h. dass sie **interpretiert** werden. Information ist damit etwas, das sowohl durch die interpretierende Nutzung aus Zeichen gewonnen wird, das aber umgekehrt auch die Interpretation von Zeichen, d.h. die Zuordnung von Bedeutung zu Zeichen beeinflusst (Problem des Kontextes).

DIN 44300 sagt nichts darüber aus,

- **wer** den Zeichen die Bedeutung unterlegt (Mensch oder Maschine),
- **wie** das geschieht, und
- **woher** die Bedeutung genommen wird.

1.1 Daten und Nachrichten

Benennung	Definition (DIN 44 300)
Zeichenvorrat *character set*	Eine zur Darstellung von Information vereinbarte endliche Menge von Objekten
Zeichen *character*	Ein Element (als Typ) aus einer zur Darstellung von Information vereinbarten endlichen Menge von Objekten (Zeichenvorrat, character set), auch jedes Abbild (als Exemplar) eines solchen Elements Anmerkung: Zeichen ist nicht gleichbedeutend mit Symbol*. Zeichen werden beispielsweise durch Schriftzeichen*, Lochkombinationen oder Impulsfolgen wiedergegeben. Beispiel: Das dreistellige Wort* SEE ist aus zwei Zeichen (als Typ) aufgebaut; das Zeichen E tritt zweimal auf (als Exemplar).
binär *binary*	Die Eigenschaft, jeweils einen von zwei Werten oder Zuständen annehmen zu können Anmerkung: Der Ausdruck logisch anstelle von binär ist als missverständlich zu vermeiden. Binär ist nicht gleichbedeutend mit dual.
Binärzeichen, Bit *binary character, bit*	Jedes der Zeichen* aus dem Zeichenvorrat* von zwei Zeichen. Anmerkung: Als Binärzeichen können beliebige Zeichen benutzt werden, z.B. O und L; wenn keine Verwechslung mit Ziffern* zu befürchten ist, auch 0 und 1; Wortpaare wie Ja und Nein, Wahr und Falsch, 12V und 2V können Paare von Binärzeichen sein. Grammatischer Hinweis: das Bit, die Bits.
bit *bit*	Sondereinheit für die von Null verschiedene Anzahl von Binärentscheidungen Anmerkung: Alle logarithmisch definierten Größen der Informationstheorie (siehe DIN 44 301), wie Entscheidungsgehalt, Informationsgehalt, Redundanz usw., erhält man in bit, wenn der Logarithmus zur Basis 2 genommen wird (1 bit, 2 bit, ...). Beispiel: Zur Unterscheidung von 2^n Zuständen (n ist eine ganze positive

	Zahl) sind $\mathrm{lb}\, 2^n = n$ bit, d.h. *n* Binärentscheidungen erforderlich; diese können mit *n* bits, d.h. mit *n* Binärzeichen* dargestellt werden.
Wort *word*	Eine endliche Folge von Zeichen*, die in einem bestimmten Zusammenhang als eine Einheit betrachtet wird Anmerkung: Im Grenzfall kann ein Wort leer sein.
Byte *byte*	n-Bit-Zeichen*, bei dem n. fest vorgegeben ist Anmerkung: n ist in einem gegebenen Zusammenhang durch Konstruktion festgelegt. n ist meistens 8; dann wird Byte auch Oktett genannt.
Symbol *symbol*	Ein Zeichen* oder ein nicht leeres Wort*, zusammen mit der dem Zeichen oder dem Wort in bestimmter Situation zugeordneten Bedeutung
Alphabet *alphabet*	Ein linear geordneter Zeichenvorrat* Anmerkung: Die Definition enthält als Sonderfall das aus Buchstaben* bestehende Alphabet einer natürlichen Sprache.
Nachricht *message*	Gebilde aus Zeichen* oder kontinuierliche Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Information darstellen und die zum Zwecke der Weitergabe als zusammengehörig angesehen und deshalb als Einheit betrachtet werden
Daten *data*	Gebilde aus Zeichen* oder kontinuierliche Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Information darstellen, vorrangig zum Zwecke der Verarbeitung und als deren Ergebnis Anmerkung: Verarbeitung umfasst die Durchführung mathematischer, umformender, übertragender und speichernder Operationen. Der wesentliche Unterschied zwischen Daten und Nachricht* liegt in ihrer Zweckbestimmung.
Signal *signal*	Die Darstellung von Nachrichten* oder Daten* mit physikalischen Mitteln
Code *code*	Eine Vorschrift für die eindeutige Zuordnung (Codierung) der Zeichen* eines Zeichenvorrats (Urmenge) zu denjenigen eines anderen Zeichenvorrats (Bildmenge) Anmerkung: Die Zuordnung braucht nicht umkehrbar eindeutig zu sein.
Binärcode *binary code*	Ein Code*, bei dem jedes Zeichen* der Bildmenge ein Wort* aus Binärzeichen* (Binärwort, *binary word*) ist. Besteht dieses Wort aus *n* Binärzeichen, so heißt es auch n-Bit-Zeichen Anmerkung: Es gibt Binärcodes, bei denen die Binärwörter der Bildmenge unterschiedliche Länge haben.
Fehlererkennungscode *error detecting code*	Ein Code*, dessen Gesetzmäßigkeiten es erlauben, Zeichen* der Bildmenge, denen kein Zeichen der Urmenge zugeordnet ist, als unzulässig zu erkennen Anmerkung: Solche Codes gehören zu den redundanten Codes. Es ist möglich, dass durch Störungen aus einem Zeichen ein anderes entsteht, das diesen Gesetzmäßigkeiten genügt und deshalb nicht als verfälscht erkannt wird.
Fehlerkorrekturcode *error correcting code*	Ein Fehlererkennungscode* mit zusätzlichen Regeln, die es erlauben, bei einem Teil der als unzulässig erkannten Zeichen* den Fehler zu korrigieren

1.2 Datenverarbeitungssysteme

Benennung	Definition (DIN 44 300)
Programmbaustein *program module*	Ein nach Aufbau oder Zusammensetzung abgrenzbares programmtechn. Gebilde Anmerkung: Ein System von Programmbausteinen kann in einem gegebenen Zusammenhang wieder als ein Programmbaustein aufgefasst werden. Dem Programmbaustein können eine oder mehrere Funktionseinheiten*. entsprechen. Siehe auch DIN 40 150.
Baueinheit *physical unit*	Ein nach Aufbau oder Zusammensetzung abgrenzbares materielles Gebilde Anmerkung: Ein System von Baueinheiten kann in einem gegebenen Zusammenhang wieder als eine Baueinheit aufgefasst werden. Der Baueinheit können eine oder mehrere Funktionseinheiten* entsprechen.
Funktionseinheit *functional unit*	Ein nach Aufgabe oder Wirkung abgrenzbares Gebilde Anmerkung: Ein System von Funktionseinheiten kann in einem gegebenen Zusammenhang wieder als eine Funktionseinheit aufgefasst werden. Der Funktionseinheit können eine oder mehrere Baueinheiten* oder Programmbausteine* oder beides entsprechen.
Prozess *process*	Bei einem Rechensystem* die Gesamtheit der Vorgänge, die an der jeweiligen Ausführung eines Programms* oder eines sinnvoll abgegrenzten Programmteils beteiligt sind und von einer Instanz* gesteuert werden Anmerkung: Für die Abgrenzung eines Programmteils sind Aufgabenteilung oder Bedingungen aus der Prozessumgebung oder die ausführende Instanz bestimmend
Instanz	Eine Funktionseinheit*, die ▪ Aufträge* erteilt oder erhält ▪ erhaltene Aufträge* ablehnt oder annimmt und ▪ angenommene Aufträge* ganz oder teilweise selbst ausführt, weitergibt oder bei Unausführbarkeit zurückgibt Anmerkung: Siehe Erläuterungen DIN 66 200 Teil 1.
Kanal *channel*	Eine Funktionseinheit*, die der Übergabe von Nachrichten* oder Daten* zwischen Instanzen* dient (aus DIN 66 200 Teil 1/10.78)
Schnittstelle *interface*	Gedachter oder tatsächlicher Übergang an der Grenze zwischen zwei gleichartigen Einheiten, wie Funktionseinheiten*, Baueinheiten* oder Programmbausteinen*, mit den vereinbarten Regeln für die Übergabe von Daten* oder Signalen* Anmerkung: Siehe auch DIN 44 302.
Rechenanlage, **Datenverarbeitungsanlage,** *computer*	Die Gesamtheit der Baueinheiten*, aus denen ein Rechensystem* aufgebaut ist
digitale Rechenanlage, digitale Datenverarbeitungsanlage *digital computer*	Die Gesamtheit der Baueinheiten*, aus denen ein 'digitales Rechensystem'* aufgebaut ist
Rechensystem, Datenverarbeitungssystem *computer system, data processing system*	Eine Funktionseinheit* zur Verarbeitung und Aufbewahrung von Daten*. Verarbeitung umfasst die Durchführung mathematischer, umformender, übertragender und speichernder Operationen Anmerkung: Siehe auch Rechenanlage*; zum Systembegriff siehe DIN 19 226.
digitales Rechensystem, digitales Datenverarbeitungssystem *digital computer system, digital data processing system*	Ein Rechensystem*, das, als Funktionseinheit* betrachtet, ein Schaltwerk* ist Anmerkung: Ein digitales Rechensystem kann also nur 'digitale Daten'* verarbeiten. Analog-Digital-Umsetzer* oder Digital-Analog-Umsetzer* können angegliedert werden, um 'analoge Daten'* einzugeben bzw. auszugeben. Zum Systembegriff siehe DIN 19 226.

2. Systeme der Informationstechnik (IT-Systeme)

Die Definitionen und Festlegungen zum Begriff *System* in diesem Abschnitt sind vor allem darauf ausgerichtet, Struktur und Eigenschaften *informationsverarbeitender Systeme* zu erfassen. Die Definitionen für *System* und *System der Informationstechnik* sind fast wortgleich mit den Definitionen für Datenverarbeitungssysteme in der DIN 44300 (vgl. dazu ([dst86, dst90]).

Die Bedeutung dieser Begriffe kann auch auf beliebige Systeme anderer Art ausgedehnt und verallgemeinert werden. Solche Erweiterungen werden aber hier nicht als Maßstab für die Brauchbarkeit der Festlegungen herangezogen. Sofern ein beliebiges System neben seinen informationsverarbeitenden auch Komponenten mit anderen Funktionen enthält, werden deren Eigenschaften und Strukturen bei der Erfassung des Bedeutungsfeldes der Begriffe hier nicht berücksichtigt.

In der Praxis ist es sinnvoll, anstelle der bisher gebräuchlichen Begriffe Datenverarbeitungssystem (DV-System), Kommunikationssystem oder Informationsverarbeitungssystem (IV-System) den umfassenderen Begriff *informationstechnisches System* oder besser noch – wenn auch länger –

System der Informationstechnik (IT-System)

zu verwenden. Damit wird der technischen Entwicklung Rechnung getragen, in deren Folge Datenverarbeitung und Kommunikation inzwischen zu einem untrennbaren Ganzen zusammengewachsen sind. Der Begriff IT-System ist deshalb stets in umfassenderem Sinne zu verstehen und darf nicht von vornherein auf den Spezialfall des *Computers*, also der programmgesteuerten, speicherprogrammierten digitalen *Rechen**anlage*** (DIN 44300) eingeschränkt oder gar noch weiter auf irgendeine seiner Komponenten verengt werden. Eine umfassendere Auslegung des Begriffs IT-System ist letztlich nur eine konsequente, weiter gefasste Interpretation der Definition des *Datenverarbeitungs**systems*** der DIN 44300 (vgl. Abschnitt 1.2).

2.1 Systeme und deren Elemente

Benennung	Definition
System *system*	Eine Sammlung (oder eine Menge) von Elementen, die in einer bestimmten Umgebung oder in einem bestimmten Kontext eine Einheit bilden oder als Einheit aufgefasst werden (→ Funktionseinheit) Anmerkung: Ein System besteht aus ▪ ***Gegenständen*** Subjekten oder Objekten ▪ ***Relationen*** zwischen Gegenständen ▪ ***Aktionen*** die von Subjekten ausgehen oder auf Objekte ausgeübt werden können.
Gegenstand *item*	Element, das entweder an einer Aktion des Systems beteiligt ist oder Bestandteil einer Relation ist. Gegenstände können entweder Subjekte oder Objekte sein.
Subjekt *subject*	***Aktiver*** Gegenstand (Akteur), der Aktionen auslöst oder veranlasst.
Objekt *object*	***Passiver*** Gegenstand, auf den Aktionen ausgeübt werden Anmerkung: Die Eigenschaft eines Gegenstandes, Subjekt oder Objekt zu sein, ist in der Regel zeitabhängig. In einer Folge von Aktionen kann ein Subjekt zum Objekt werden und umgekehrt. (Beispiel: Ein Unterprogramm, dass von einem anderen Programm aufgerufen wurde, war Objekt und wird in dem Augenblick zum Subjekt, indem es selbst ein anderes (Unter)-Programm aufruft. Für Relationen ist der Unterschied Subjekt-Objekt im Allgemeinen bedeutungslos.
Aktion *action*	Funktion oder Prozess, den ein System auszuführen in der Lage ist. Im Hinblick auf das System und seine Umgebung wird unterschieden zwischen ***internen Aktionen*** wenn ausschließlich Gegenstände des Systems selbst an ihnen beteiligt sind; ***externen Aktionen*** wenn sie von einem Subjekt aus der Umgebung des Systems, also von außerhalb, auf ein Objekt im System ausgeübt werden ***(Eingabeaktion)***, oder von einem Subjekt im System auf einen Gegenstand in dessen Umgebung ***(Ausgabeaktion)***. Externe Aktionen laufen stets über eine oder mehrere Schnittstellen* des Systems.

Relation *relation*	Gedachter oder tatsächlicher Bezug zwischen Gegenständen, der Untermengen oder Unterstrukturen im System erzeugt
System der Informationstechnik, IT-System *it-system*	Jedes Gebilde, das Daten verarbeiten kann und in einem gegebenen Kontext (in einer bestimmten Umgebung) als Funktionseinheit* betrachtet wird

IT-System kann nach dieser umfassenderen Definition ein Computer sein oder ein Systemteil (Hard- oder Software oder beides). Das bekannteste, weitestverbreitete Gebilde, das als Funktions**einheit** im Sinne dieser Definition mit Daten umgehen kann, ist jedoch **der Mensch.**

Anmerkung:
Selbstverständlich gibt es Informationsverarbeitung in der Biosphäre auch außerhalb des Menschen; das wird mit dieser Aussage nicht angezweifelt. Es geht bei diesen Erläuterungen und Definitionen zum Begriff ***System*** jedoch – im Zusammenhang mit der Informationsverarbeitung durch und für Menschen – vor allem um den Unterschied zwischen Mensch und Maschine und um die Wechselwirkung zwischen beiden.

Nach der Definition kann auch jeder größere Komplex von Elementen als IT-System bezeichnet werden, sofern er unter gegebenen Randbedingungen als *Funktionseinheit* betrachtet werden soll. Typische Beispiele für solche komplexeren IT-Systeme sind z.B. Rechenzentren mit Hardware, Software, Menschen, Gebäuden und Infrastruktur, oder Netze mit allen ihren Komponenten.

Jede Behörde, jede Verwaltung, jedes Unternehmen ist als *Funktionseinheit*, also als ein nach Aufgabe und Funktion abgrenzbares Gebilde betrachtet, ein IT-System. Genauer: jede solche Funktionseinheit enthält als Substruktur ein oder mehrere Systeme der Informationstechnik, die als Komponenten sowohl Menschen als auch nicht-menschliche Bestandteile enthalten

Beispiele für IT-Systeme

Menschen **Lebewesen** **Computer** Mainframes Arbeitsplatzsysteme, PCs Prozessrechner, Realzeitsysteme … **Subsysteme und Komponenten** Hardwarebausteine und Programme Betriebssysteme Datenbanken Anwendungssysteme …	**IT-Komplexe** Rechenzentren Rechnernetze Kommunikationsnetze Netzkomponenten … **Wirtschaftsunternehmen, Verwaltungen oder andere Teile der Gesellschaft** als informationsverarbeitende Subsysteme aus Menschen und Maschinen

2.2 Systeme und ihre Umgebung

Für die Untersuchung jedes IT-Systems (als Funktionseinheit) ist zuvor festzulegen, welche Elemente als zum System gehörend betrachtet werden sollen und welche seiner Umgebung zugeordnet werden. Für den Zusammenhang zwischen System und Umgebung gelten folgende Definitionen:

Benennung	Definition
Schnittstelle *interface*	DIN 4430: Gedachter oder tatsächlicher Übergang an der Grenze zwischen zwei gleichartigen Einheiten, wie Funktionseinheiten*, Baueinheiten* oder Programmbausteinen*, mit den vereinbarten Regeln für die Übergabe von Daten* oder Signalen* Anmerkung: Siehe auch DIN 44 302.
Externe Schnittstelle *external interface*	Eine Schnittstelle, die mindestens einen Übergang zu einem Element (einer Einheit) außerhalb des Systems enthält, also einen Übergang, der Schnittstelle zwischen System und Umgebung ist

=

Zusammenhang *connection*	Die Menge der externen Schnittstellen eines Systems oder Die Menge der gedachten oder tatsächlichen Übergänge zwischen den Elementen eines Systems und den Elementen seiner Umgebung, einschließlich der vereinbarten Regeln für die Übergabe von Daten oder Signalen
geschlossenes System, abgeschlossenes System *closed system*	Jedes System, für das die Menge der Schnittstellen die leere Menge ist Anmerkung: Das System hat keine Schnittstellen und damit keinen Zusammenhang mit seiner Umgebung. Diese Forderung ist in der Praxis i.A. nicht erfüllt. Sie ist aber als Modellvorstellung für die Untersuchung der Eigenschaften und des Verhaltens von Systemen sinnvoll.

3. Ordnungsmäßigkeit und Sicherheit

Ein wichtiger Anstoß für eine klarere, sinnvolle Festlegung des Begriffs *Sicherheit* im Zusammenhang mit IT-Systemen war die Veröffentlichung des *Orange Book* des US-amerikanischen Verteidigungsministeriums im Jahr 1985 [Orange85]. Untersuchungen in Deutschland, die schon einige Jahre früher begonnen hatten [vdBr81, Dst84], fanden ihren ersten offiziellen Niederschlag 1989 in der Veröffentlichung der *IT-Sicherheitskriterien* [BSI89] durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), – damals Zentralstelle für Sicherheit in der Informationstechnik (ZSI).

Die Begriffe *Ordnungsmäßigkeit* und *Sicherheit* müssen nicht notwendig unter dem Blickwinkel der Informations- und Kommunikationstechnik betrachtet werden. Beide Begriffe werden in anderen Fachgebieten seit langem verwendet. Beide können insbesondere mit beliebigen Systemen, beliebigen Prozessen und Sachverhalten in Verbindung gebracht werden. Die folgenden Definitionen zu Ordnungsmäßigkeit und Sicherheit lassen sich deshalb ganz oder teilweise auch auf Systeme anwenden, die nur zum Teil IT-Systeme sind, ggf. auch auf Systeme, die gar keine Komponenten der Informationstechnik enthalten.

Für manche Begriffe mag es in anderen Fachbereichen präzisere, weniger von der Umgangssprache abhängige Definitionen geben. Die Formulierungen der DIN haben aber den kaum zu unterschätzenden Vorteil, dass sie sich

- auch nach den Erfordernissen der Praxis richten,
- von einer Vielzahl von Fachleuten aus verschiedenen Fachgebieten laufend ergänzt und diskutiert werden und
- seit einer ganzen Reihe von Jahren veröffentlicht und damit weit verbreitet sind.

Das Problem der Vorbesetzung

Eine besondere Hürde in der Diskussion um die „richtige" Auslegung des Begriffs *Sicherheit* und der meisten mit ihm zusammenhängenden Terme ist die Tatsache, dass in fast allen Anwendungsgebieten diese Begriffe, vor allem das Wort Sicherheit selbst, bestimmte, den jeweiligen Anwendern längst vertraute Bedeutungen haben. Der sinnvollste Weg, diese Hürde zu überwinden ist, diese Begriffe für die Anwendung in der Informationstechnik neu zu vereinbaren – selbstverständlich weitestgehend angelehnt an die vorhandenen Definitionen – und in der Diskussion stets auf diese neuen Vereinbarungen zu verweisen. Das Gleiche gilt für die *Ordnungsmäßigkeit* und mit ihr zusammenhängende Begriffe

Um so notwendiger ist es, Bedeutungsumfang und Bedeutungsinhalt dieser Begriffe für IT-Systeme so genau wie möglich festzulegen, ohne sie jedoch dabei zu früh und unnötig einzuengen. Gedanklicher Ausgangspunkt für die Überlegungen sind die Definitionen zu den Grundbegriffen der Datenverarbeitung nach DIN44300 und 40041 (vgl. auch Abschnitt 1).

3.1 Ordnungsmäßigkeit von IT-Systemen

Die Ordnungsmäßigkeit eines Systems kann immer nur bezogen auf eine bestimmte, v*orgegebene* Ordnung behauptet und festgestellt werden. Die Ordnung selbst ist nicht im System enthalten, sondern ist die Menge von Forderungen und Randbedingungen (*set of requirements*), die von außen (Umgebung, Systemeinbettung, Umwelt) an das System gestellt werden müssen

Ein System wird als ordnungsmäßig bezeichnet, wenn es **genau** die Anforderungen erfüllt, die von der äußeren Ordnung gestellt werden, der es genügen soll. Dem entspricht folgende Definition:

Ordnungsmäßigkeit

Benennung	Definition
ordnungsmäßiges System *orderly system*	Ein System ist genau dann ordnungsmäßig, wenn es ▪ alle Aktionen korrekt ausführt, die von ihm gefordert werden, und ▪ keine Aktionen ausführt, die von ihm nicht gefordert werden Anmerkung: Die korrekte Ausführung einer Aktion schließt die *Rechtzeitigkeit* ein, d.h. die Ausführung ▪ zum geforderten Zeitpunkt ▪ im geforderten Zeitrahmen.

Die Festlegungen dieser Definition lassen sich in einen Satz zusammenfassen:

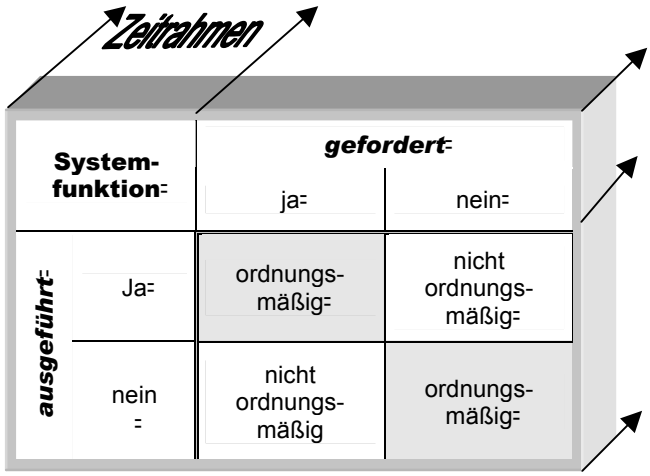
> Ein **ordnungsmäßiges System** führt **genau** diejenigen Aktionen **rechtzeitig** aus, die in der Menge der Anforderungen enthalten sind.

Diese Auslegung des Begriffs Ordnungsmäßigkeit setzt voraus, dass die Elemente des als ordnungsgemäß zu beurteilenden Systems, insbesondere dessen Funktionen (Aktionen), **vollständig und widerspruchsfrei** spezifiziert werden und dass sowohl die Spezifikationen als auch deren Implementierung nachprüfbar (verifizierbar), in letzter Konsequenz also *formal spezifizierbar und verifizierbar* sind.

Ordnungsmäßigkeit ist demnach ein *perfektes* Verhalten, das von *realen* Systemen in aller Regel nicht erfüllt wird. In der Definition der Sicherheit realer IT-Systeme ist diese Einschränkung zu berücksichtigen.

In der Grafik wird dieser Zusammenhang veranschaulicht. Die geforderten Funktionen eines Systems werden den Funktionen gegenübergestellt, die es tatsächlich ausführt.

Der Begriff Ordnungsmäßigkeit wird hier dem vielleicht geläufigeren Wort *Korrektheit* vorgezogen. In der Informatik impliziert das Wort Korrektheit in der



Arbeitsweise eines ordnungsmäßigen Systems

Regel die Möglichkeit, logisch zu beweisen, dass die Arbeitsweise eines Hardwareteils oder eines Programmbausteins fehlerfrei ist, oder dass deren Funktionsweise aus einer Menge widerspruchsfreier Axiome abgeleitet werden kann. Diese Bedeutung von Korrektheit kann im Begriff der Ordnungsmäßigkeit eines Systems oder einer Systemkomponente enthalten sein. In der Regel aber geht die Bedeutung von *Ordnungsmäßigkeit* erheblich über die bloße mathematische Korrektheit hinaus.

3.2 Verlässlichkeit – Sicherheit *der* Systeme – die technische Sicht

Ausgehend von dieser Definition der Ordnungsmäßigkeit gilt damit Aussage:

> Ein System der Informationstechnik ist ***verlässlich***, d.h. sicher aus technischer Sicht,
>
> - wenn seine Funktionsweise den vorgegebenen Anforderungen genügt. Das heißt in anderen Worten,
> - wenn die Betroffenen sich auf die **Korrektheit und Verfügbarkeit der Funktionen des Systems und der Ergebnisse** verlassen können, die mit Hilfe dieser Funktionen gewonnen wurden.

Daraus ist folgende Definition des ersten Teils des Begriffs Sicherheit, der **Verlässlichkeit,** ableitbar**.**

Diese Definition stimmt mit der Definition von *Datensicherheit* aus der DIN 44300 wörtlich überein, wenn man dort nur das Wort „***Daten***“ durch „***IT-Syste***m“ ersetzt (vgl. Abschnitt 4.).

Die Beeinträchtigung von IT-Systemen umfasst u.a. die Beeinträchtigung *der Vertraulichkeit, der Integrität und der Verfügbarkeit* von Funktionseinheiten, Funktionen und Daten, insbesondere also auch deren Verlust, Zerstörung und Verfälschung (vgl. hierzu [BSI89] und [ITSEC91]).

Verlässlichkeit

Benennung	Definition (nach DIN 44300)
IT-Sicherheit, (Verlässlichkeit) *it-.security*	Sachlage, bei der IT-Systeme unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung oder Missbrauch bewahrt sind, und zwar unter Berücksichtigung verarbeitungsfremder Risiken wie auch im Verlauf auftrags- und ordnungsgemäßer Erbringung einer Datenverarbeitungsleistung*. IT-Systeme dürfen also ▪ weder bei datenverarbeitenden Prozessen* oder auftragsbedingten Vor- und Nacharbeiten, ▪ noch in Funktionseinheiten* zur Abwicklung auftragsbedingter Arbeiten, ▪ noch durch das Handeln von an auftragsbedingten Arbeiten beteiligten Personen beeinträchtigt werden. Anmerkung: Beeinträchtigung von IT-Systemen umfasst u.a. Verlust, Zerstörung und Verfälschung.

3.3 Beherrschbarkeit – Sicherheit *vor dem* System – die Sicht der Betroffenen

Die vorhergehende Definition des Begriffs Sicherheit im Hinblick auf die Verlässlichkeit enthält keinen Hinweis darauf, dass ein aus technischer Sicht verlässlich arbeitendes IT-System sowohl das Umfeld als auch die Handlungs- und Denkweisen der mit ihm arbeitenden und von seiner sicheren Funktion abhängenden Menschen ggf. in unerwünschter Weise verändert und beeinträchtigt. Sie berücksichtigt nur mittelbar die Tatsache, dass über die bloße technische Verlässlichkeit hinaus ein System nur dann als sicher bewertet werden darf, wenn die von seiner Funktion Abhängenden es **beherrschen** können.

Das heißt, dass sie von der Funktion des Systems und von den Auswirkungen der mit seiner Hilfe gewonnen Ergebnisse nicht unzulässig beeinträchtigt werden, kurz, dass **die Betroffenen** vor dem System und dessen Auswirkungen „sicher" sind. Am einfachen Beispiel eines „sicheren Kraftfahrzeugs" leuchtet diese Forderung unmittelbar ein.

In den bisher verabschiedeten nationalen und internationalen Sicherheitskriterien ist diese **Beherrschbarkeit** als zweite, zur Verlässlichkeit komplementäre Sicht des Begriffs Sicherheit weitgehend unbeachtet geblieben, ja z.T. gar nicht (vgl. [BSI89] und [ITSEC91]) explizit berücksichtigt worden.

Voraussetzung für diese Sicht der Sicherheit ist, dass die von einem IT-System ermittelten Ergebnisse oder die von und in ihm ausgelösten Vorgänge ihrem Veranlasser *zugeordnet* und damit auch zugerechnet werden können (vgl. hierzu die [CTCP93]) und dass die Ergebnisse dieser Vorgänge Dritten gegenüber beweiskräftig sind. Erst dann gilt folgende Aussage:

> Ein System der Informationstechnik ist ***beherrschbar***, d.h. sicher aus Sicht der Betroffenen,
> - wenn seine Funktionen und deren Ergebnisse bestimmten oder bestimmbaren Veranlassern (auslösenden Instanzen) *zugerechnet* werden können, und zwar so, dass
> - die Zuordnung *revisionsfähig,* also auch Dritten gegenüber beweisbar ist.

Bestimmbare Veranlasser darf dabei nicht missverstanden werden, als müsse zu jedem Datenverarbeitungs- oder Kommunikationsvorgang eine ganz bestimmte natürliche *Person* als Veranlasser authentisch feststellbar sein. Veranlasser kann auch ein Gerät, ein Programm, irgend ein System oder eine Systemkomponente sein.

Die folgenden beiden Definitionen zeigen, dass Beherrschbarkeit als unbedingt notwendige Ergänzung des Bedeutungsumfangs von Sicherheit schon seit Langem gefordert wurde.

Beherrschbarkeit

Benennung	Definition
IT-Security (OECD /GD(92)190)	The objective of security in information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.
IT-Sicherheit *security*:	IT-Sicherheit ist eine dem Individuum und der Gesellschaft bekannte und verständliche Sachlage, bei der das mit einem IT-technischen Vorgang oder Zustand verbundene Risiko das Grenzrisiko nicht vergrößert, dass jedes Individuum für sich hieraus, früher oder später, eine Beeinträchtigung oder Verlust von Geist, Körper Seele, Freiheit, Lebensraum, Hab und Gut erfahren könnte.

In der zweiten dieser beiden Definitionen wird darüber hinaus versucht, den für alle Überlegungen zur Sicherheit zentralen Bɛgriff des **Risikos** in praktisch nutzbarer Form zu erläutern. Es ist kennzeichnend, dass in dieser Definition keine abschließende, allgemeinverbindliche Wertung dieses Begriffs versucht, sondern ausdrücklich auf die vom Einzelnen in seiner Situation von seinen Anforderungen her zu fällende Entscheidung verwiesen wird.

Die Beherrschbarkeit als zweite, komplementäre Sicht des Begriffs Sicherheit lässt sich einfach aus der Definition des *Datenschutzes* nach DIN 44300 ableiten, wenn man dort, wie bei der technischen Sicht, nur das Wort „***Daten***“ durch „***IT-Syste***m“ ersetzt (vgl. Abschnitt 4.).

Benennung	Definition (abgeleitet aus DIN 44300, *Datenschutz**)
IT-Sicherheit, (Beherrschbarkeit) *it-.security*	Sachlage, bei der IT-Systeme weder unmittelbar oder mittelbar diejenigen in ihrem Bestand oder ihrem Verhalten unzulässig beeinträchtigen, die von der Funktion oder von den Ergebnissen, die mit Hilfe der IT-Systeme gewonnen werden, betroffen sind. IT-Systeme dürfen also ▪ weder durch datenverarbeitenden Prozessen* oder auftragsbedingten Vor- und Nacharbeiten ▪ noch durch die Funktionseinheiten* zur Abwicklung auftragsbedingter Arbeiten ▪ noch über das Handeln von an auftragsbedingten Arbeiten beteiligten Personen die Betroffenen. in ihren Rechten und Handlungsmöglichkeiten unzulässig beeinträchtigen Anmerkung: Beeinträchtigung von IT-Systemen umfasst u.a. Verlust, Zerstörung und Verfälschung.

3.4 Mehrseitige Sicherheit

Der Begriff mehrseitige Sicherheit (vgl. [Cha87, RPM96]) wurde geprägt, weil der Begriff ***Betroffener*** auf keinen Fall zu eng auf den eigentlichen *Benutzer* ausgelegt werden darf. IT-Sicherheit wird nicht nur von den Anwendern – den Benutzern im engeren Sinn – gefordert, sondern mit gleichem Recht auch von Entwicklern, Herstellern, Systembetreibern, von der Rechtsprechung und vielen anderen mehr, die von der Verlässlichkeit und Beherrschbarkeit der Informations- und Kommunikationssysteme in vielfältiger Weise abhängig sind. *Betroffener* kann eine Person (natürliche oder juristische) sein, eine Personengruppe, ebenso aber auch ein anderes „System” im weiteren Sinn des Begriffs IT-System.

IT-Sicherheit muss deshalb ***mehrseitig***, d.h. aus der Sicht der verschiedenen Gruppen von Betroffenen beleuchtet werden. Die Ziele und damit die Anforderungen der verschiedenen Interessentengruppen werden nur in wenigen Fällen konvergieren oder gar gleich sein. In vielen Fällen können sie sich – und werden sich auch – durchaus widersprechen. Bei der Bestimmung der semantischen Komponenten des Begriffs muss diese Mehrseitigkeit berücksichtigt werden.

3.5 Sicherheit realer IT-Systeme

Ordnungsmäßigkeit setzt stillschweigend voraus, dass Verlässlichkeit, d.h. Sicherheit im technischen Sinne, erreichbar ist, wenn alle Komponenten eines IT-Systems ordnungsgemäß, also immer korrekt funktionieren. In der Praxis ist diese Annahme immer nur näherungsweise erfüllt, weil ***reale*** IT-Systeme so gut wie immer nicht-ordnungsmäßig arbeitende Komponenten enthalten oder in nicht-ordnungsmäßiger Weise über ihre Schnittstellen von außen angesprochen werden können.

Wird der Mensch als Komponente in die Betrachtung der Sicherheit eines IT-Systems mit einbezogen, so wird die Forderung nach strikter Ordnungsmäßigkeit vollends unrealistisch. Es ist deshalb sinnvoll, die Forderung nach Verlässlichkeit an die Realität anzupassen und leicht abgewandelt zu verlangen:

- Ein reales IT-System kann aus der Sicht der Technik als sicher bezeichnet werden, wenn der Betroffene (Benutzer, Betreiber, Hersteller etc. im Sinne mehrseitiger Sicherheit) sich auf die Korrektheit und Verfügbarkeit der Funktionen des Systems und der mit seiner Hilfe gewonnen Ergebnisse auch dann **hinreichend verlassen kann**, wenn Teile des Systems nicht oder **nicht immer ordnungsmäßig arbeiten.**

Die Wendung „*so weit wie möglich“* in der Definition weist darauf hin, dass das Auftreten eines nicht-ordnungsmäßigen Verhaltens in einem Anwendungsfall hingenommen werden kann, in einem anderen nicht. Das aber setzt voraus, dass die Wahrschein-

lichkeit für das Auftreten eines nicht-ordnungsmäßigen Verhaltens in der Menge der Anforderungen berücksichtigt worden sein muss.

Genauer: in einer Sicherheitsanalyse muss ***zuvor*** festgelegt worden sein, welche *Risiken* (d.h. welche Arten des Zusammentreffens von Bedrohungen + Schwachstellen und deren zu erwartende Folgen) für ein bestimmtes IT-System in einer bestimmten Einsatzumgebung noch annehmbar sind und welche nicht (vgl. Abschnitt 3.2).

Sicherheit ist deshalb in der Praxis nie „schlechthin" feststellbar, sondern immer nur bezogen auf ein gegebenes Anforderungsprofil und damit bezogen auf eine bestimmte Anwendung und der mit ihr verbundenen Risiken.

3.6 Duale Sicherheit von IT-Systemen

Geht man von den beiden komplementären, einander ergänzenden Forderungen der Verlässlichkeit und Beherrschbarkeit als Grundlage für den Begriff Sicherheit aus, so kommt man zu folgender Definition der **dualen Sicherheit von IT-Systemen**.

Duale Sicherheit

Benennung	Definition
duale Sicherheit *dual security*	**Sicherheit der Systeme – Verlässlichkeit** (Sicherheit des Systems) Sachlage, bei der weder die Systeme noch die mit ihnen verarbeiteten Daten (Informationen) noch die Datenverarbeitung (Funktionen und Prozesse) in ihrem Bestand, ihrer Nutzung oder ihrer Verfügbarkeit unzulässig beeinträchtigt werden **Sicherheit vor dem System** – **Beherrschbarkeit** (Sicherheit der Betroffenen) Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden.
sicheres IT-System *secure it-system*	System der Informationstechnik, das den drei Grundbedrohungen, denen ein IT-System ausgesetzt sein kann, ▪ unbefugter Informationsgewinn (Verlust der Vertraulichkeit) ▪ unbefugte Modifikation von Daten (Verlust der Integrität) ▪ unbefugte Beeinträchtigung der Funktionalität (Verlust der Verfügbarkeit) in ausreichender Weise widersteht und ▪ die von seiner ordnungsgemäßen Funktion Betroffenen nicht mehr als zulässig in ihren Rechten und Handlungsmöglichkeiten beeinträchtigt..

Diese Definition impliziert für reale IT-Systeme, dass der Benutzer sich nicht nur auf die Korrektheit und Verfügbarkeit der Funktionen des Systems und der Ergebnisse **hinreichend verlassen kann**, sondern auch darauf, dass die Betroffenen durch das Vorhandensein und die Nutzung der IT-Systeme nicht mehr als zulässig in ihren Rechten und Handlungsmöglichkeiten **beeinträchtigt** werden, und zwar auch dann, wenn Teile des Systems **nicht oder nicht immer ordnungsmäßig arbeiten**.

Der in [rpm96] verwendete Begriff *mehrseitige Sicherheit* (vgl. Abschnitt 3.3) ist mit dem Begriff *duale Sicherheit* verwandt, aber nicht gleichbedeutend.

3.7 Semantische Dimensionen der Sicherheit – Fundamentalkomponenten

Im Sinne dieser Definition der dualen Sicherheit sind

- **Vertraulichkeit** (*confidentiality)*
- **Integrität** *(integrity)*
- **Verfügbarkeit** *(availability)*
- **Zurechenbarkeit** *(accountability)*
- **Revisionsfähigkeit** oder **Rechtsverbindlichkeit**

fünf **semantische Dimensionen** oder **Fundamentalkomponenten** des Begriffs Sicherheit von Systemen der Informationstechnik. Die Bedeutung der ersten vier kann eng angelehnt an die Erklärungen in [BSI89, ITSEC91] oder [CTCP93] vereinbart werden.

Revisionsfähigkeit oder **Rechtsverbindlichkeit** wird als fünfte Komponentegefordert, um die Nachweisbarkeit oder Beweisbarkeit der zurechenbaren Daten und Funktionen sicher zu stellen (umgangssprachlich: „Recht *haben*" vs „Recht *bekommen*").

Benennung	Definition
Vertraulichkeit *confidentiality*	Sachlage, bei der Daten weder unbefugt zur Kenntnis genommen, erschlossen noch anderweitig verfügbar gemacht werden können (kein unbefugter Informationsgewinn)
Integrität *integrit***y**	Sachlage, bei der weder Daten noch Funktionen eines IT-Systems unbefugt und unbemerkt verändert oder benutzt werden können
Verfügbarkeit *availability*	Sachlage, bei der Daten und Funktionen eines IT-Systems genau zum geforderten Zeitpunkt und im vorgegebenen Zeitrahmen funktionsfähig bereitstehen (vgl. hierzu auch DIN 40041 und 40042)
Zurechenbarkeit *accountability*	Sachlage, bei der Abläufe und Ergebnisse eines IT-Systems korrekt einer veranlassenden Instanz zugeordnet werden können
Revisionsfähigkeit oder **Rechtsverbindlichkeit**	Sachlage, bei der Abläufe und Ergebnisse eines IT-Systems Dritten gegenüber beweiskräftig (nachweisbar) geltend gemacht werden können

4. Datenschutz und Datensicherung

4.1 DIN 44 300 (November 1988)

DIN hat 1988 in der überarbeiteten Norm 44300 für die Beschreibung von *Sicherheit* die leider drei Begriffe so übernommen, wie sie bis dahin schon viel Verwirrung gestiftet hatten, und definiert::

Benennung	Definition
Datensicherheit *data security*	Sachlage, bei der Daten* unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung oder Missbrauch bewahrt sind, und zwar unter Berücksichtigung verarbeitungsfremder Risiken wie auch im Verlauf auftrags- und ordnungsgemäßer Erbringung einer Datenverarbeitungsleistung*. Daten dürfen also ▪ weder bei datenverarbeitenden Prozessen* oder auftragsbedingten Vor- und Nacharbeiten, ▪ noch in Funktionseinheiten* zur Abwicklung auftragsbedingter Arbeiten, ▪ noch durch das Handeln von an auftragsbedingten Arbeiten beteiligten Personen beeinträchtigt werden. Anmerkung: Beeinträchtigung von Daten umfasst u.a. Verlust, Zerstörung, Verfälschung. Zum Begriff Sicherheit siehe DIN VDE 31 000 Teil 2.
Datensicherung *data security means*	Maßnahmen und Einrichtungen, die Datensicherheit* herbeiführen oder aufrechterhalten Anmerkung: Zum Begriff Sicherheit siehe DIN VDE 31 000 Teil 2.
Datenschutz *privacy protection*	Sachlage, bei der die schutzwürdigen Belange Betroffener vor Beeinträchtigung, die von der Verarbeitung der Daten* ausgeht, bewahrt sind. Betroffene können natürliche oder juristische Personen oder Personenvereinigungen sein, aber nur insoweit, als Daten über sie verarbeitet werden oder durch Verarbeitung von Daten auf ihre Identität geschlossen werden kann. Anmerkung: Die rechtliche Seite des Datenschutzes wird durch Gesetz, Rechtsverordnung oder Rechtsprechung geregelt. Es ist zu unterscheiden zwischen Datenschutz und Maßnahmen, die ihn herbeiführen. Zum Begriff Schutz siehe DIN VDE 31 000 Teil 2.

Anmerkungen:

(1) Der Begriff *Datenschutz* war durch die Definitionen in den Datenschutzgesetzen von Bund und Ländern festgeschrieben und von Vielen lange als „Schutz ***der*** Daten“ missverstanden worden. DIN hat versucht, dieses Missverständnis auszuräumen, ohne aber den Begriff selbst durch einen besser geeigneten – wie z.B. *„Schutz der Betroffenen“* - zu ersetzen(vgl. dazu die Bedeutung des besser geeigneten englischen Begriffs *privacy)*. Dabei war der Gedanke verloren gegangen, dass es sich bei Datenschutz und Datensicherheit um zwei zwar verschiedene, aber ein-

ander ergänzende Sichten des Grundbegriffs *Sicherheit* handelt

(2) In der DIN-Definition der Datensicherheit wird neben der *unzulässigen Verarbeitung* der umfassendere Begriff *unzulässige Nutzung* nicht erwähnt, der in den Einleitungen der neueren Fassungen aller deutschen Datenschutzgesetze ergänzend aufgeführt wird (vgl. dazu LDSG Hessen §1 Zif.1 in den Fassungen von 1978 und 1986).

=

4.2 Arbeitskreis „Sichere Systeme“ der GDD (1983)

Schon früh ist versucht worden, die drei grundlegenden Begriffe *Datenschutz, Datensicherheit* und *Datensicherung* als Mengendefinitionen zu formulieren. Diese Definitionen gehen auf einen Ansatz von *Vor der Brück, Jahl* u.a. [vdBr83] zurück. Der Ansatz wurde durch *Bayer* und *Dierstein* weitergeführt und ergänzt. Die endgültige Fassung wurde bis 1983 im Arbeitskreis *Sichere Systeme* (AK-DaSi) der Gesellschaft für Datenschutz und Datensicherung (GDD) erarbeitet.

Benennung	Definition
Datenschutz *privacy*	eine Menge von Anforderungen, die die Zulässigkeit und die Ausführbarkeit der Informationsgewinnung und der Zugriffe auf Daten festlegen
Datensicherung *data security*	eine Menge von Maßnahmen – einschließlich der dazu gehörenden Einrichtungen und organisatorischen Regelungen – die ergriffen werden, um den Datenschutz zu verwirklichen
Datensicherheit	ist genau dann gegeben, wenn die Datensicherung des Systems hinreichend ist, den Datenschutz zu gewährleisten.

4.3 Bundes- und Landesdatenschutzgesetze

Die Bundes- und Landesdatenschutzgesetze der Bundesrepublik Deutschland geben durchweg ***keine*** *Definition* des Begriffs *Datenschutz.* Sie beschränken sich darauf, Datenschutz anhand der Aufgabe zu erläutern, die damit gelöst werden soll.

Analog dazu lassen sich zwar aus diesen Erläuterungen auch Erklärungen für die Begriffe *Datensicherheit* und *Datensicherung* herleiten. Dies sind jedoch ebensowenig wirkliche Definitionen.

Benennung	Erläuterung
Datenschutz *privacy*	Datenschutz hat die Aufgabe, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
Datensicherheit *data security*	Datensicherheit hat die Aufgabe, (so weit wie möglich) Daten vor Beeinträchtigung zu bewahren.
Datensicherung	technische und organisatorische Maßnahmen zur Erreichung von Datensicherheit

Die Bedeutung des Begriffs Datensicherung wird vielfach noch weiter eingeengt auf die bloßen Maßnahmen des *Backup*. Das sollte tunlichst vermieden werden.

Eine einfache Erläuterung für den Begriff *IT-Sicherheit* kann hier, wie in der DIN 44300, aus dem Begriff Datensicherheit abgeleitet werden.

IT-Sicherheit *it-security*	IT-Sicherheit hat die Aufgabe, (so weit wie möglich) IT-Systeme vor Beeinträchtigung zu bewahren.

4.3.1 Bundesdatenschutzgesetz (BDSG)

Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes, Artikel 1 (Neufassung des Bundesdatenschutzgesetzes – BDSG) vom Dezember 1990.

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, durch
1. öffentliche Stellen des Bundes
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit
   a) sie Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.

(3) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen:
1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§5 und 9.
2. Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§5, 9, 39 und 40. Außerdem gelten für Dateien öffentlicher Stellen die Regelungen über die Verarbeitung und Nutzung personenbezogener Daten in Akten. Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt.

(4) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

Die Begriffsbestimmungen in den deutschen Gesetzen zum Datenschutz sind nach und nach immer weiter den Anforderungen an die Verlässlichkeit und Beherrschbarkeit der automatisierten Datenverarbeitung angepasst worden. Dabei wurde insbesondere versucht, Datenschutz und IT-Sicherheit, so weit irgend angängig, vom Stand der Technik unabhängig zu definieren oder zu beschreiben.

Novellierung des BDSG (BDSG-Arbeitsfassung zum Änderungsgesetz vom 23. Mai 2001)

Für den nächsten Novellierungsschritt (Anpassung des BDSG an die EU-Richtlinie 1995; Änderungsgesetz am 23. Mai 2001 in Kraft getreten) sind im §1 drei aufschlussreiche Änderungen vorgesehen:

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) wie früher …

(2) wie früher …

1. ...
2. ...
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht-automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) wie der frühere Absatz (4)

(4) *wie der frühere Absatz (5)*

Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zwecke des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

Absatz (2),Ziffer 3 erfasst in der erweiterten Form auch nicht automatisierte Dateien.

Der bisherige *Absatz (3)* (s. oben) soll ganz entfallen. Es hat sich gezeigt, dass temporäre Dateien, obwohl nur für den vorübergehenden, betrieblichen Gebrauch vorgesehen, sehr wohl zweckentfremdet und missbraucht werden können. Die alten *Absätze (4) und (5)* werden damit zu den neuen (3) und (4).

Der Text des neuen *Absatz (5)* nimmt auf den wachsenden internationalen Datenaustausch Bezug:

4.3.2 Saarländisches Datenschutzgesetz

Die Definition der Aufgabe des Datenschutzes im *Saarländischen Gesetz zum Schutz personenbezogener Daten* in der Fassung des Änderungsgesetzes vom 14.12.1982 und in dessen neuer Fassung vom 24.3.1993 zeigt, wie die Bedeutung des Begriffs Datenschutz sich in zehn Jahren erweitert und gewandelt hat.

Die gleiche Aussage gilt für die verschiedenen Fassungen des *Hessisches Datenschutzgesetzes* in seinen Fassungen von 1970 bis 1999

Fassung 1982

§ 1 Aufgabe und Gegenstand des Datenschutzes

(1) Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.

(2) **…**

Fassung 1993

§ 1 Aufgabe

(1) Aufgabe dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch die Verarbeitung personenbezogener Daten durch öffentliche Stellen in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

4.3.3 Hessisches Datenschutzgesetz

Ausgabe Oktober 1970 (in der Fassung vom 4.9.74)

§ 1 Bereich des Datenschutzes

Der Datenschutz erfasst alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten und Ergebnisse ihrer Verarbeitung im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts..

§ 2 Inhalt des Datenschutzes:

Die vom Datenschutz erfassten Unterlagen, Daten und Ergebnisse sind so zu ermitteln, weiterzuleiten und aufzubewahren, dass sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können. Dies ist durch geeignete personelle und technische Vorkehrungen sicherzustellen.

Fassung 31.1.1978

§ 1 Aufgabe und Gegenstand

(1) Aufgabe des Gesetzes ist es,

1 den Bürger durch Verhinderung des Missbrauchs bei der Verarbeitung (Speicherung, Übermittlung, Veränderung und Löschung) personenbezogener Daten zu schützen und einer Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.

2 das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Veränderung infolge der automatisierten Datenverarbeitung zu bewahren.

(2) …

Fassung November 1986

§ 1 Aufgabe

Aufgabe dieses Gesetzes ist es, die Verarbeitung personenbezogener Daten durch öffentliche Stellen zu regeln, um

1. das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind,
2. das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren.

Fassung 7. Januar 1999

§ 1 Aufgabe

(1) Aufgabe dieses Gesetzes ist es, die Verarbeitung personenbezogener Daten durch die in §3 Abs.1 genannten Stellen zu regeln, um

1. das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind,
2. das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren.

(2) Aufgabe der obersten Landesbehörden, Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts ist es, die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz jeweils für ihren Bereich sicherzustellen.

In den novellierten Fassungen der Gesetze ist Aufgabe und Ziel des Datenschutzes nach §1 nicht mehr nur die Abwehr möglicher Gefahren oder Beeinträchtigungen, sondern die Gewährleistung des grundsätzlichen Rechts des Einzelnen, über Nutzung und Verbreitung auf seine Person bezogener Daten (Informationen) *selbst* zu bestimmen – offensichtlich eine Auswirkung der Leitsätze des Volkszählungsurteils des BVerfG von 1983.

Eine *Veränderung* im verfassungsmäßigen Gefüge muss dabei nicht mehr zwangsläufig mit einer *Gefährdung* des einzelnen und seiner Rechte gekoppelt sein (vgl. Änderung der Wortwahl in Ziffer (1) Absatz 2.).

4.3.4 Richtlinie der Europäischen Union (1995)

Auch die EU gibt in den „Erwägungsgründen“ keine eigene Definition der grundlegenden Begriffe an, sondern umschreibt wiederum nur deren Aufgaben oder Ziele gemäß den Forderungen der Richtlinie.

I. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Erwägungsgründe

…

(2) Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.

…

(10) Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.

(11) Die in dieser Richtlinie enthaltenen Grundsätze zum Schutz der Rechte und Freiheiten der Personen, insbesondere der Achtung der Privatsphäre, konkretisieren und erweitern die in dem Übereinkommen des Europarats vom 28. Januar 1981 zum Schutze der Personen bei der automatischen Verarbeitung personenbezogener Daten enthaltenen Grundsätze.

…

(25) Die Schutzprinzipien finden zum einen ihren Niederschlag in den Pflichten, die den Personen, Behörden, Unternehmen, Geschäftsstellen oder anderen für die Verarbeitung verantwortlichen Stellen obliegen; diese Pflichten betreffen insbesondere die Datenqualität, die technische Sicherheit, die Meldung bei der Kontrollstelle und die Voraussetzungen, unter denen eine Verarbeitung vorgenommen werden kann. Zum anderen kommen sie zum Ausdruck in den Rechten der Personen, deren Daten Gegenstand von Verarbeitungen sind, über diese informiert zu werden, Zugang zu den Daten zu erhalten, ihre Berichtigung verlangen bzw. unter gewissen Voraussetzungen Widerspruch gegen die Verarbeitung einlegen zu können.

4.4 Information Technology Security Evaluation Criteria (ITSEC) (6/1991)

In der ersten Fassung der Europäischen Kriterien wird in der Einleitung der Begriff *„Sicherheit von Systemen der Informationstechnik (IT-Sicherheit)“* beschrieben [itsec91]. Hier ist der Begriff noch ausschließlich auf die Sichtweise *Verlässlichkeit* eingeschränkt. Erst mit den Kanadischen Kriterien [CTCP93] ist mit der Zurechenbarkeit *(accountability)* die zweite Sicht, die Sicherheit der Betroffenen, erstmalig im Ansatz in die Definition von IT-Sicherheit mit aufgenommen worden.

IT-Security

0.2 In this context, IT-security means,

- **confidentiality** – prevention of the unauthorized disclosure of information;
- **integrity** – prevention of the unauthorized modification of information;
- **availability** – prevention of the unauthorized withholding of information or resources.

0.3 An IT **system** or **product** will have its own requirements for maintenance of confidentiality, integrity and availability. In order to meet these requirements it will implement a number of technical security measures, in this document referred to as **security enforcing** functions, covering, for example, areas such as access control, auditing, and error recovery. Appropriate confidence in these functions will be needed: in this document this is referred to as **assurance**, whether it is confidence in the **correctness** of the security functions (both from the development and the operational points of view) or confidence in the **effectiveness** of those functions.

… … …

1.4 … An IT system is a specific IT installation with a particular purpose and known operational environment. An :hp1.IT product is a hardware and/or software package that can be bought off the shelf and incorporated into a variety of systems. An IT system is generally constructed from a number of hardware and software **components**. …

1.5 From the point of view of security, the main difference between systems and products lies in what is certain about their operational environment. A system is designed to meet the requirements of a specific group of **end-users** It has a real world environment which can be defined and observed in every detail; in particular the characteristics and requirements of its end-users will be known and the threats to its security are real threats which can be determined. A product must be suitable for incorporation in many systems; the product designer can only make general assumptions about the operational environment of a system of which it may become a component. It is up to the person buying and constructing the system to make sure that these assumptions are consistent with the actual environment of the system.

4.5 Volkszählungsurteil des BVerfG vom 15.12.1983 – Informationelle Selbstbestimmung

Aus den Leitsätzen des Volkszählungsurteils

(1) Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs.1 GG umfasst. ***Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.***

(2) Einschränkungen dieses Rechts auf »**informationelle Selbstbestimmung**« sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche die Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

Aus der Urteilsbegründung

- **…** Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus ***eigener Selbstbestimmung*** zu planen oder zu entscheiden. **…** Hieraus folgt: (→ Leitsatz 1)**.**

- **…** Dieses Recht auf »informationelle Selbstbestimmung« ist ***nicht schrankenlos*** gewährleistet. Der einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über »seine« Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. **…**

- Grundsätzlich muss daher der einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.

- **…** Die Verfassungsbeschwerden geben keinen Anlass zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Daten abgestellt werden. Entscheidend sind ihre ***Nutzbarkeit und Verwendungsmöglichkeit***. Diese hängen einerseits von dem ***Zweck***, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen ***Verarbeitungs- und Verknüpfungsmöglichkeiten*** ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein »belangloses« Datum mehr.

- Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht*,* ***zu welchem Zweck Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten. …***

5. Begriffe und Kenngrößen zu Zuverlässigkeit und Verfügbarkeit

Verfügbarkeit und Zuverlässigkeit sind seit jeher der *Sicherheit technischer Systeme* grundlegende Bestandteile des Bedeutungsfeldes von Sicherheit. Die meisten der in diesem Zusammenhang verwendeten Begriffe wurden sinnfällig festgelegt, so z.B. die *Zuverlässigkeit* als eine spezielle Eigenschaft (Fähigkeit) eines technischen Systems.

Man achte sorgfältig darauf, dass der Begriff ***Zuverlässigkeit*** (*reliability)* nicht mit der ***Verlässlichkeit*** *(assurance*) verwechselt wird, wie er im Zusammenhang mit den verschiedenen Kriterienkatalogen für die Bewertung der Sicherheit von IT-Systemen (BSISEC, ITSEC, CC und andere) verwendet wird.

Die Begriffe in diesem Abschnitt werden zitiert nach [Schn92]. Textteile zwischen Anführungszeichen sind Zitate aus den zugehörigen Normen, vornehmlich aus DIN 40041 (Entwurf 11/1988) und 40042.

Benennung	Definition
Zuverlässigkeit *reliability (broad sense)*	„Beschaffenheit einer Einheit bzgl. ihrer Eignung, während oder nach vorgegebenen Zeitspannen bei vorgegebenen Anwendungsbedingungen die Zuverlässigkeitsanforderungen zu erfüllen" *kürzer* Die Fähigkeit einer Betrachtungseinheit, den vereinbarten Anforderungen während einer vereinbarten Zeitdauer zu genügen.
Verfügbarkeit *(a) reliability* *(b) availability*	„Wahrscheinlichkeit, eine Einheit zu einem vorgegebenen Zeitpunkt der geforderten Anwendungsdauer in einem funktionsfähigen Zustand anzutreffen" Zum Englischen (a) bei fehlender Reparatur (b) bei Reparatur, im stationären Fall
Ausfalldauer (Störungsdauer) *down time*	Zeitspanne vom Ausfallzeitpunkt einer Betrachtungseinheit bis zur Wiederherstellung der Einsatzbereitschaft
Lebensdauer	Für die einzelne nicht instandsetzbare Betrachtungseinheit beobachtete Zeitspanne vom Beanspruchungsbeginn bis zum Ausfallzeitpunkt
Brauchbarkeitsdauer *time to failure* (TTF)	"Intervall der Anwendungsdauer, während dem die Zuverlässigkeitsforderung erfüllt wird" Mittelwert ist die MTTF.
Ausfallabstand *time between failures*	„Intervall der Anwendungsdauer zwischen zwei aufeinander folgenden Ausfällen"
Mittlerer Ausfallabstand *mean time between failures* (MTBF)	Mathematischer Erwartungswert des Ausfallabstands im stationären Betrieb

Nach der Definition in DIN 40041 kann man nicht von einer „Zuverlässigkeit schlechthin" sprechen, denn diese Eigenschaft wird immer auf den durch die Anforderungen definierten Einzelfall genauer festgelegt. In einer früheren Fassung der Definition war dies besser erkennbar. Dort hieß es:

- „Zuverlässigkeit ist die Fähigkeit einer Betrachtungseinheit, innerhalb der vorgegebenen Grenzen denjenigen durch den Verwendungszweck bedingten Anforderungen zu genügen, die an das Verhalten ihrer Eigenschaften während einer gegebenen Zeitdauer gestellt sind."

Zuverlässigkeit ist nach DIN auch *keine quantitative* Größe und damit auch keine Wahrscheinlichkeit. Die in der Zuverlässigkeitstechnik mit am häufigsten benutzte quantitative Größe ist die *Verfügbarkeit.*

Die in der Tabelle synonym verwendeten Begriffe *Betriebsdauer* und *Brauchbarkeitsdauer* sollen generell einen Zeitraum des störungsfreien Betriebs bezeichnen, also dessen Länge bedeuten. Unter *Lebensdauer* wird spezieller die Zeit bis zum ersten Ausfall des betrachteten Systems verstanden, und zwar von einem definierten Anfangszeitpunkt ab, zu dem **alle** Teilsysteme intakt sind, in Ausnahmefällen auch eine wohlbestimmte Auswahl der Teilsysteme. Im Falle eines redundanten Systems sind also Ausfälle und Reparaturen von Teilsystemen während der Lebensdauer des Systems durchaus zugelassen, nur darf durch diese (zugelassenen) Ausfälle kein Systemausfall verursacht werden.

Ein *m*-von-*n*- oder *m*-aus-*n*-System ist ein System, das funktioniert, wenn mindestens *m* seiner *n* Komponenten funktionieren

6. Veröffentlichungen

BSI89 Bundesamt für Sicherheit in der Informationstechnik (BSI) – *IT-Sicherheitskriterien – Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT) – 1.Fassung 1989*
herausgegeben im Auftrag der Bundesregierung, Bundesanzeiger Verlagsgesellschaft mbH, Bonn 1989, 107 Seiten, ISBN 3-88784-192-1

BSIEval90 Bundesamt für Sicherheit in der Informationstechnik (BSI) – *IT-Evaluationshandbuch – Handbuch für die Prüfung der Sicherheit von Systemen der Informationstechnik (IT) – 1 Fassung 1990*
herausgegeben im Auftrag der Bundesregierung, Bundesanzeiger Verlagsgesellschaft mbH, Bonn 1990, 101 Seiten, ISBN 3-88784-220-0

BDIHdb92 Bundesamt für Sicherheit in der Informationstechnik (BSI) – *IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik – Version 1.0 – März 1992*
Bonn 1992, 327 Seiten, BSI 7105

vdBr80 vor der Brück, H. -- *Die grundlegenden Eigenschaften sicherer DV-Systeme*
4. Datenschutzfachtagung DAFTA'80 der Gesellschaft für Datenschutz und Datensicherung (GDD), Datakontext-Verlag, Köln 1981, S. 131–137

[vdBr83] vor der Brück, H.; Jahl, C.; Köhler, C.; Ramsperger, N. – *Untersuchung der EDV-technischen Datenschutz- und Datensicherungsprobleme in verteilten DV-Systemen*
Bericht B-SZ 1321/01 der IABG (Industrieanlagen-Betriebsgesellschaft mbH), Ottobrunn 1983 (Forschungsbericht DV 83-0112 6 des Bundesministeriums für Forschung und Technologie)

Chau87 Chaum, D. – *Sicherheit ohne Identifizierung: Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen*
Informatik-Spektrum 10/5 (1987), p. 262–277 und Datenschutz und Datensicherung DuD/1 (1988), p. 26–41

CC97 CCEB – Common Criteria Editorial Board – *Common Criteria for Information Technology Security Evaluation (CC) – Version 1.0*
Washington, 1997

CTCP93 CSSC – *The Canadian Trusted Computer Product Evaluation Criteria – Version 3.0e*
Canadian System Security Centre, Communication Security Establishment, Government of Canada, Jan. 1993, XXV+208 S.

Dst86 Dierstein, R. – *Basic Functions of Secure Systems*
Proceedings Securicom '86 – 4ème Congrès Mondial de la Protection et de la Sécurité Informatique et des Communications, Paris 1986, S. 467–476

Dst90 Dierstein, R. – *The Concept of Secure Information Processing Systems and Their Basic Functions*
Proceedings of the IFIP SEC '90, 6th International Conference and Exhibition on Information Security, Espoo (Helsinki), Finland; Elsevier Science Publishers B.V., Amsterdam, 1991

Dst97 Dierstein, R.; – *Duale Sicherheit – IT-Sicherheit und ihre Besonderheiten*
in: Pfitzmann, A.; Müller, G. (Hrsg.) – *„Mehrseitige Sicherheit in der Kommunikationstechnik“* (Kolleg der Gottlieb-Daimler und Karl-Benz-Stiftung), Verlag Addison-Wesley-Longman, Bonn – Reading (Mass.) 1997, p.31–60, ISBN 3-8273-1116-0

DIN88 DIN – *Deutsche Norm – Informationsverarbeitung Begriffe Teile 1–9*
Deutsches Institut für Normung; Beuth Verlag GmbH, Berlin, November 1988

ITSEC91 CEC – Directorate General XIII – *Information Technology Security Evaluation Criteria (ITSEC) – Provisional Harmonised Criteria*
Office for Official Publications of the European Communities, Luxembourg, Juni 1991, 163 p., ISBN 92-826-3004-8

ITSEM93 Commission of the European Communities (CEC), Directorate General XIII – *Information Technology Security Evaluation Manual (ITSEM) – Provisional Harmonized Methodology*
Brussels 1994, 262 pages, ISBN 92-826-7087-2

Orange85 DoD – *The „Orange Book“. – Trusted Computer Systems Evaluation Criteria (TCSEC)*
US-Department of Defense (DoD) 5200.28-STD; Washington D.C., 1985

RPM96 Rannenberg, K.; Pfitzmann, A.; Müller, G. – *Sicherheit, insbesondere mehrseitige IT-Sicherheit*
it+ti Informationstechnik und technische Informatik, 38. Jahrgang 1996, Heft 4, S. 5-10, München

Schn92 Schneeweiss, W – *Zuverlässigkeitstechnik – von den Komponenten zum System*
Reihe CCG-Texte 1–2, Datakontext-Verlag, Köln 1992