

IHK-Vollversammlung

Datenschutz als Standortvorteil

Karsten Neumann

Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

Rostock, den 28. November 2005

Agenda

- **Der Landesbeauftragte für den Datenschutz**
- **Personenbezogene Daten**
- **Ausgewählte Pflichten nach dem Bundesdatenschutzgesetz**
- **Internationale Aspekte**
- **Datensicherheit**
- **Datenschutzaudit**

Aufgaben (§§ 30, 32, 33, 33a DSG M-V)

- Bearbeitung von Petitionen
- Beratung von Behörden und Unternehmen
- Beratung bei der Erarbeitung von Gesetzentwürfen
- Kontrolle der Einhaltung gesetzlicher Vorschriften
- Information der Öffentlichkeit
- Zusammenarbeit mit anderen Datenschutzinstitutionen
- Beobachtung der Entwicklung der IuK-Technik

Rechtsstellung (§ 29 DSG M-V)

- Wahl durch das Parlament (sechs Jahre Amtszeit)
- 2/3-Mehrheit für Abwahl notwendig
- Organisatorische Anbindung bei der Landtagspräsidentin
- unabhängig und weisungsfrei (keine Fach- oder Rechtsaufsicht, Ausnahme: Rechtsaufsicht der Landesregierung für die Tätigkeit als Aufsichtsbehörde; Dienstaufsicht der Landtagspräsidentin)
- Oberste Dienstbehörde i. S. v. § 96 StPO u. oberste Aufsichtsbehörde i. S. v. § 99 VwGO (Entscheidung über Aktenvorlage)

Aktuelle Tätigkeitsschwerpunkte

- **Datenschutz aus einer Hand**
- **Verstärktes Beratungsangebot**
- **Datenschutz als Wettbewerbsvorteil**
(z. B. Datenschutzaudit)

Formen der Zusammenarbeit

- Konferenz der Datenschutzbeauftragten des Bundes und der Länder und deren Arbeitskreise
- Zusammenarbeit mit Aufsichtsbehörden (z. B. Düsseldorfer Kreis)
- ERFA-Kreis für betriebliche DSB in MV
- Zusammenarbeit mit anderen Datenschutzinstitutionen (z. B. im „Virtuellen Datenschutzbüro“ www.datenschutz.de)

Öffentlichkeitsarbeit

- Tätigkeitsbericht (alle zwei Jahre)
- Informationsmaterial
- Sammlung „Gesetze und Verordnungen“
- Informations- u. Beratungsveranstaltungen
- Eigenes Internetangebot
(www.datenschutz-mv.de)

Der Landesbeauftragte für den Datenschutz



Personenbezogene Daten (§ 3 Abs. 1)



Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)

Name, Alter, Anschrift, Familienstand, Einkommens- und Vermögensverhältnisse, Bankverbindungsdaten, Steuer-, Kfz- und Versicherungsnummer, Zensuren, Telefon-, Fax- und IP-Nummer, Vorstrafen, momentaner Aufenthalt, Genetische Daten, Licht- und Röntgenbilder

Datengeheimnis anno 1776

„Wir verbieten bei unserer königlichen Ungnade allen und jedem nachzuforschen, wie viel ein anderer auf seinem Folio zu Gute habe, auch soll niemand von den Bank-Schreibern sich unterstehen, solches zu offenbaren:

Weder durch Worte, Zeichen oder Schrift – bei Verlust ihrer Bedienungen, und bei den Strafen, die Meineidige zu erwarten haben.

Zu dem Ende sollen sie bei Antretung ihres Amtes besonderes schwören, dass sie alle Geschäfte, die sie als Bedienstete der Bank unter Händen haben werden, als das größte Geheimnis mit in die Grube nehmen werden.“

Erlass Friedrichs des Großen 1776

Datenvermeidung und Datensparsamkeit (§ 3a BDSG)

- **„Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.“**
- **„Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“**

Organisatorische und technische Verfahrensvorkehrungen nach dem BDSG (Überblick)

- **(Betrieblicher) Beauftragter für den Datenschutz (§§ 4f, 4g)**
- **Meldepflicht für Verfahren automatisierter Verarbeitungen (§ 4d Abs. 1 bis 4, § 4e)**
- **Vorabkontrolle bei besonderen Datenschutzrisiken (§ 4d Abs. 5, 6)**
- **Technische und organisatorische Maßnahmen (§ 9 mit Anlage)**

Internationale Aspekte

- EG-Datenschutzrichtlinie: Mit der Umsetzung der Richtlinie in das Bundesdatenschutzgesetz von 2001 und das Landesdatenschutzgesetz von 2002 sind insbesondere Datenübermittlungen ins EU-Ausland unter den gleichen Voraussetzungen möglich wie innerhalb Deutschlands.
- Basel II: Positiver Faktor bei der Bewertung der Kreditwürdigkeit eines Unternehmens ist nach dem sog. Basel-II-Abkommen ein hohes Datenschutzniveau (im Rahmen des „Riskmanagements“).

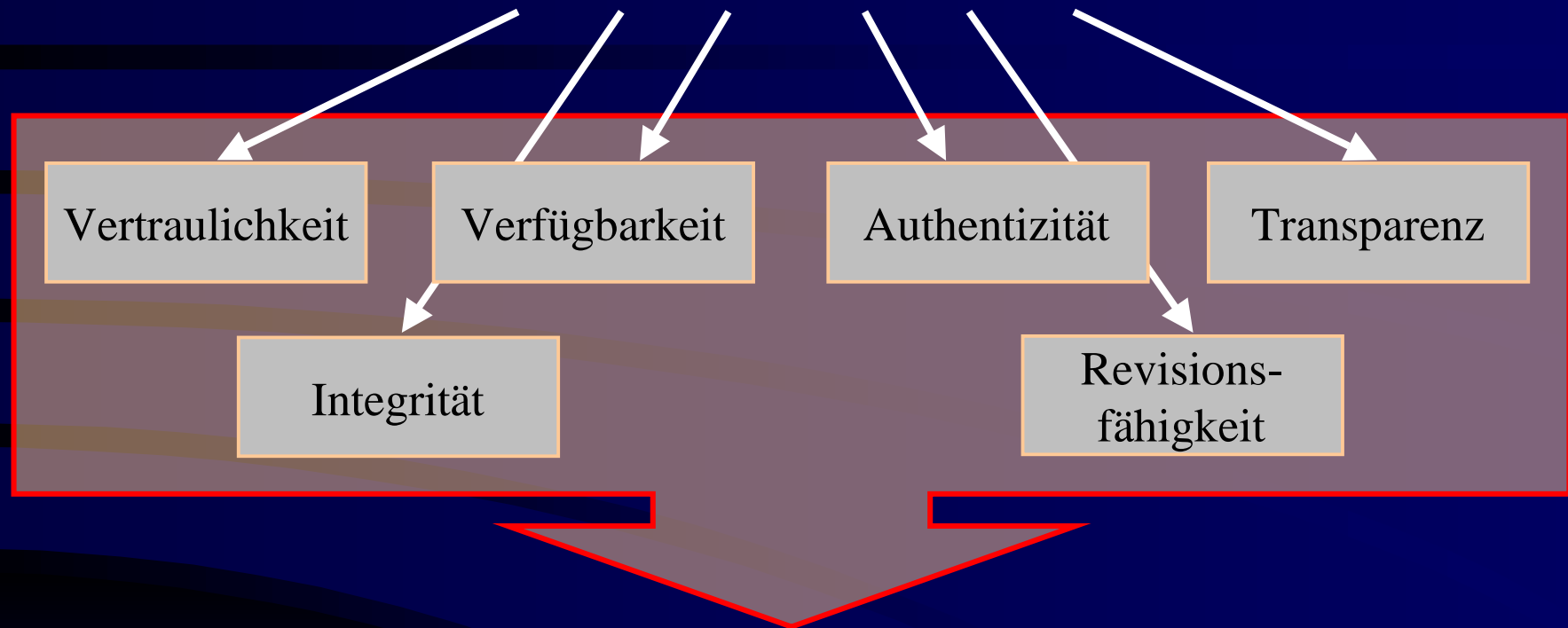
Wie groß ist das Risiko?

Bruce Schneier*:

„Es ist nicht die Frage, **ob** Sie angegriffen werden, sondern **wann!**“

* Entwickler von Verschlüsselungsalgorithmen und Autor von „Angewandte Kryptografie“ und „Secret&Lies-IT-Sicherheit in einer vernetzten Welt“

Sicherheitsziele



**Realisierung durch technische
und organisatorische Maßnahmen**

Einige Fakten und Zahlen

Befragung von 500 Kleinunternehmen (D, F, GB, I, NL, E)

- **Wegen fehlender oder schlecht installierter Viren-Software wurde ein Schaden von 22 Milliarden Euro pro Jahr verursacht**
- **Durchschnittliche Kosten pro betroffenen Rechner lagen bei 5000 Euro**
- **Jede fünfte befragte Firma musste die Arbeit vorübergehend einstellen**
- **Jedes dritte deutsche Unternehmen brauchte neue Hardware**
- **29 % der Unternehmen hatten wichtige Daten verloren**

Quelle: Umfrage Network Associates 2004

Polizeiliche Kriminalstatistik 2004

Stichwort Computerkriminalität:

- Anstieg der Computerkriminalität gegenüber 2003 um **12,2 %**
in Zahlen: von 59.691 auf 66.973
- Aufklärungsquote: **47 %**
- Zunahme von Computerbetrug (§ 263a StGB: Manipulation von Rechnern, Daten und Programmen): **24,6 %**
- Zunahme von Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB): **83,6 %**
- Schadenssumme durch Computerkriminalität: **> 230 Mio. €**

Bundeskriminalamt 2005

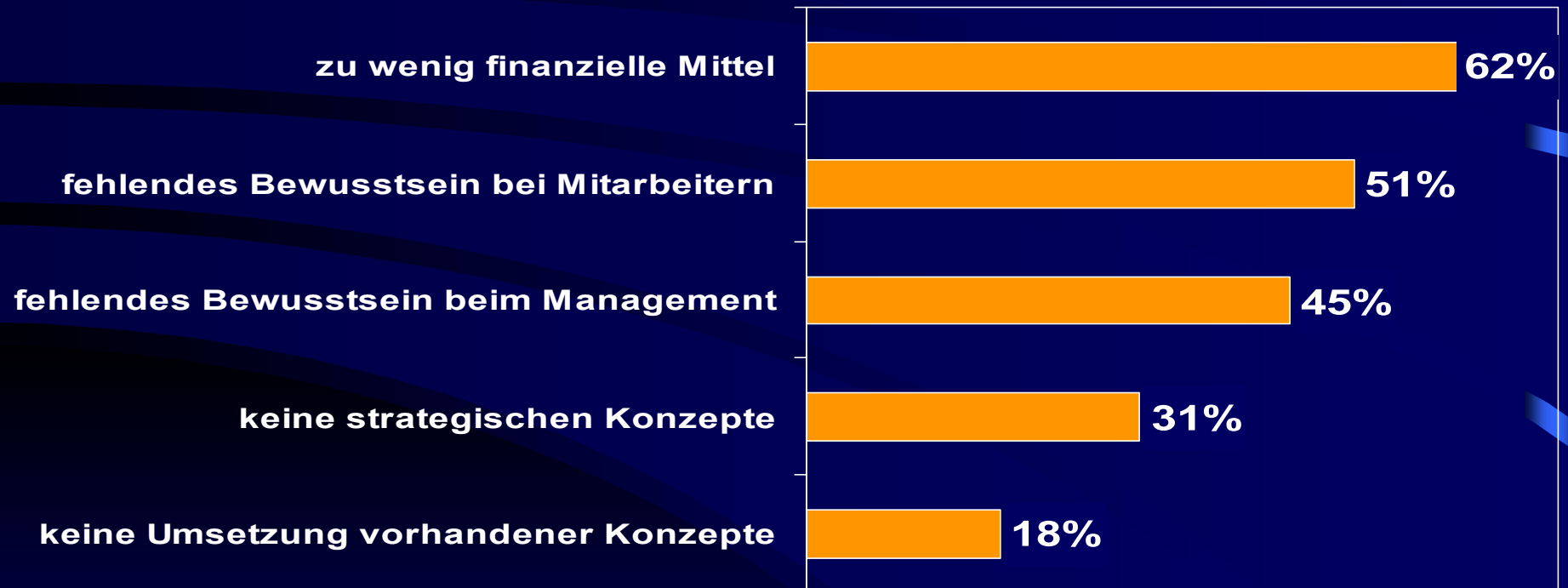
Die üblichen Schwachstellen

- **Firmenleitungen sind nicht ausreichend sensibilisiert:**
 - IT-Sicherheit ist in 70% der Firmen keine „Chiefsache“
 - die Hälfte der Firmen hat kein Sicherheitskonzept oder hat ein vorhandenes Konzept nicht umgesetzt
- **Jedes zweite Unternehmen verwendet weniger als fünf Prozent des Budgets für die Sicherheit seiner Netze**
- **Oft falsche Vorstellungen über die Bedrohungen:**
 - 58% der Sicherheitsverletzungen durch autorisierte Mitarbeiter
 - 24% der Sicherheitsverletzungen durch nichtautorisierte Mitarbeiter
 - 13% der Sicherheitsverletzungen durch Ex-Angestellte

Quelle: PricewaterhouseCoopers LLP New York

Sicherheitsstudie KES/Microsoft September 2004

Ursachen für Sicherheitsmängel:



Fehlendes IT Know-how

Prof. Dr. Dieter Engels, Bundesrechnungshof-Präsident:

- In der Privatwirtschaft erreichen zwischen 30 und 40 Prozent der IT-Projekte ihr Funktionsziel nicht.
- Es fehlt häufig an IT-Know-how, um mit IT-Firmen auf Augenhöhe zusammenarbeiten zu können.

Die unrühmlichen Beispiele:

- LKW-Maut (TollCollect)
- A2LL (Software für ALG II)
- bald auch JobCard oder Elektronische Gesundheitskarte?

Sicherheit durch

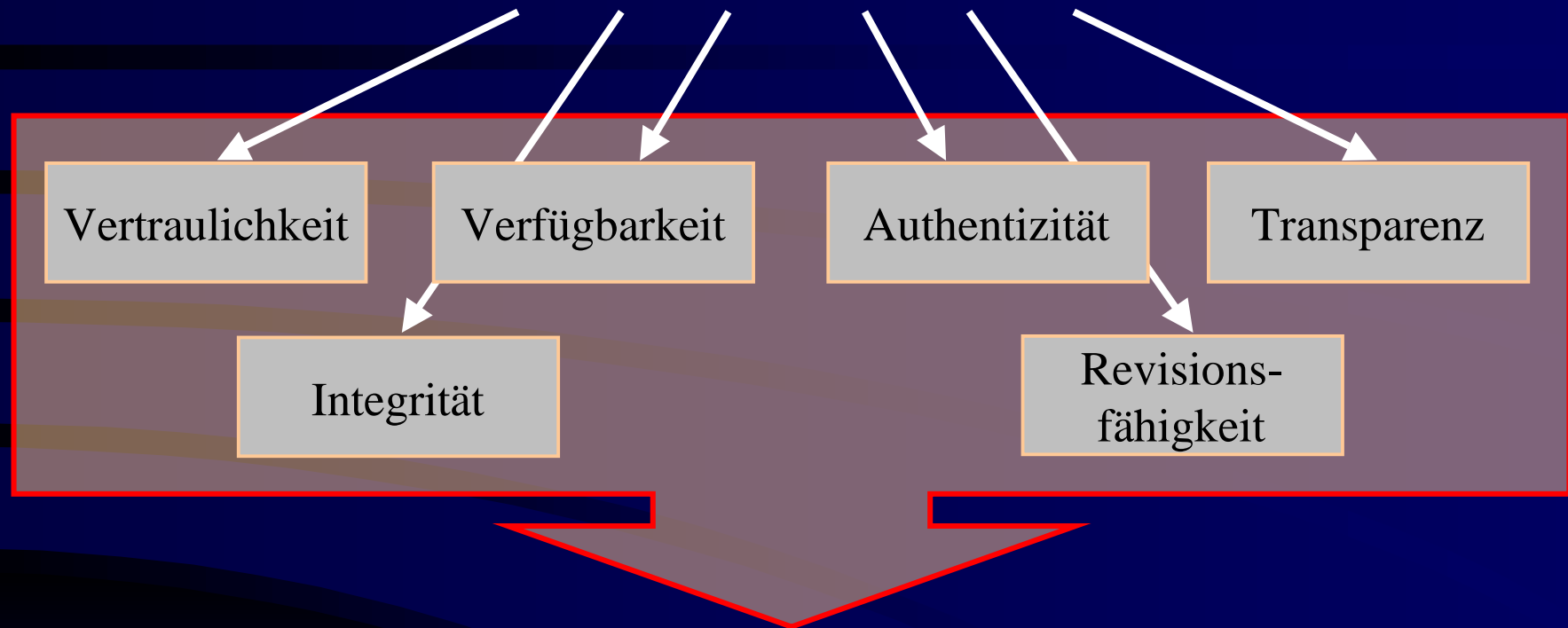
Verhinderung
krimineller Handlungen

Aufspüren von
Regelverstößen

Ergreifen von
Gegenmaßnahmen

Unternehmertum heißt Risikomanagement

Sicherheitsziele



Ganzheitliche Strategie

Datenschutzaudit (allgemeines)

- Problem: Datenschutzniveau einzelner Produkte von Anwendern schwer beurteilbar
- Lösung: Feststellung der „Datenschutzfreundlichkeit“ von Produkten durch Prüfverfahren (Produktaudit, Gütesiegel)
- Ausgestaltung des Auditverfahrens in künftiger Rechtsverordnung der Landesregierung aufgrund § 5 Abs. 2 DSGVO M-V
- Anforderungskatalog des LfD für Produktprüfung

Datenschutzaudit (Ablauf)

- Beauftragung Sachverständiger / sachverständiger Prüfstelle (beim LfD akkreditiert) durch Hersteller- oder Vertriebsfirma
- Akkreditierung beim LfD setzt Nachweis der erforderlichen Fachkunde, Zuverlässigkeit und Unabhängigkeit voraus
- Prüfung des Produkts / Übersendung der schriftlichen Dokumentation der Prüfung an den LfD
- Erteilung des Gütesiegels, wenn nach Prüfung durch LfD keine Hinderungsgründe

Datenschutzaudit (konkret)

- Gütesiegel-Kriterium: Vereinbarkeit der Produkte mit Vorschriften über Datenschutz und Datensicherheit
- Produkte: Hardware, Software, Verfahren (sofern zur Nutzung durch öffentliche Stellen geeignet)
- Produkte, die ein solches (Audit-)Verfahren erfolgreich durchlaufen haben, sollen von öffentlichen Stellen bevorzugt eingesetzt werden
- Vorteil in Vergabeverfahren /Verbesserung der allgemeinen Marktchancen

Was bedeutet das Gütesiegel nach dem Landesdatenschutzgesetz?

Bescheinigung der Vereinbarkeit eines Produktes mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren

Empfehlung des Einsatzes dieses Produktes bei den öffentlichen Stellen des Landes durch den LfD

Welche Produkte könnten ein Gütesiegel erhalten?

Informationstechnische Produkte (Hard- und Software, sowie Datenverarbeitungsverfahren).

Voraussetzung: Eignung zur Nutzung durch öffentliche Stellen

Welches könnten die Kriterien für die Vergabe von Gütesiegeln sein?

- Allgemein: Vereinbarkeit des Produkts mit den Vorschriften über Datenschutz und Datensicherheit
- Insbesondere : Aspekte der Datenvermeidung und Datensparsamkeit, Datensicherheit und Revisionsfähigkeit sowie Gewährleistung der Rechte der Betroffenen
- Anforderungskatalog des LfD für Prüfung von IT-Produkten (Regelmäßige Fortschreibung)

Wer würde die Gutachten erstellen?

- Gutachten würden von den beim LfD akkreditierten Sachverständigen / sachverständigen Prüfstellen erstellt werden
- Akkreditierung beim LfD setzt Nachweis der erforderlichen Fachkunde, Zuverlässigkeit und Unabhängigkeit voraus
- LfD würde öffentlich einsehbare Liste über akkreditierte Sachverständige und sachverständige Prüfstellen führen

Prüfungsgesichtspunkte

- Schlüssigkeit des Gutachtens
- Methodisch einwandfreie Vorgehensweise des Sachverständigen oder der sachverständigen Prüfstellen
- In Zweifelsfällen kann das zu zertifizierende Produkt in Augenschein genommen werden

Befristung von Gütesiegeln

- Gütesiegel werden befristet
- Angesichts Innovationstempo bei Informationstechnik Befristung regelmäßig auf zwei Jahre (Schleswig-Holstein)

Zweck des Gütesiegels

- Erleichterung der Auswahl von Produkten, die mit Datenschutzbestimmungen in Einklang stehen, für Behörden und Firmen
- Nutzung des Gütesiegels für Marketingzwecke im Privatkundenbereich

Wo kann ich mich über Gütesiegel informieren?

Informationen zum Gütesiegel (Schleswig-Holstein):
Unabhängiges Landeszentrum für Datenschutz

<http://www.datenschutzzentrum.de/guetesiegel/>

Der Landesbeauftragte für den Datenschutz
Johannes-Stelling-Str. 21
19053 Schwerin
Telefon:0385-59494-0
Telefax:0385-5949458
E-Mail:datenschutz@mvnet.de
Internet:www.lfd.m-v.de