Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)176 E

STELLUNGNAHME ZUR ÖFFENTLICHEN ANHÖRUNG DES INNENAUSSCHUSSES DES DEUTSCHEN BUNDESTAGES AM 5. MÄRZ 2007 ZUR THEMATIK

„MODERNISIERUNG DES DATENSCHUTZES"

1. Modernisierung des Datenschutzes

Herausforderungen der Informationsgesellschaft

Die Risikoanalyse des Ersten Senats des Bundesverfassungsgerichts in seinem Urteil vom 15. Dezember 1983 – 1 BvR 209/83u.a. – stellt die gesetzgeberische Herausforderung durch moderne Informations- und Kommunikationstechnologien auch weiterhin mit der überzeugenden Schlussfolgerung eines staatlichen Gewährleistungsanspruches dar:

informationelle Selbstbestimmung als Verfassungsauftrag nach wie vor aktuell

„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. ...
Mit dem Recht aus informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß."

Arbeitspapier „Datenschutzfreundliche Technologien"

Die Datenschutzbeauftragten haben 1997 eine Arbeitsgruppe "Datenschutzfreundliche Technologien" des Arbeitskreises "Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder beauftragt der Frage nachzugehen, inwieweit datenschutzfreundliche Technologien einen Beitrag zur Bewältigung dieser Herausforderungen leisten können, deren Arbeitspapier im Folgenden immer noch einen aktuellen Einstieg in die Problematik leisten kann (www.datenschutz-mv.de/dschutz/ informat/ dsftechn/apdsftec.pdf).

Anonymität

Bereits 1983 hat das Bundesverfassungsgericht im Volkszählungsurteil – am Beispiel der Statistik – den Anspruch auf Anonymisierung anerkannt. Gemäß der bekannten Auffassung des Bundesverfassungsgerichts heißt es dort: *"Für den Schutz des Rechts auf informationelle Selbstbestimmung ist – und zwar auch schon für das Erhebungsverfahren – ... die Einhaltung des Gebots einer möglichst frühzeitigen faktischen Anonymisierung unverzichtbar, verbunden mit Vorkehrungen gegen die Deanonymisierung"* (BVerfGE 65, 1-49-).
In der Rechtsprechung zum Medienrecht ist das Recht auf Anonymität ebenfalls seit längerem als besondere Ausprägung des Persönlichkeitsrechts anerkannt, beispielsweise vom Bundesgerichtshof: *"Das Recht auf informationelle Selbstbestimmung schützt ... davor, aus dem Bereich der Anonymität in den einer persönlichen Bekanntheit gerückt zu werden"* (BGH AfP 1994, 306-307-). Auch der Rat für Forschung, Technologie und Innovation, der unter Federführung des Bundeskanzleramts und des Bundesministers für Bildung, Wissenschaft, Forschung und Technologie einen ausführlichen Bericht über Chancen, Innovationen und Herausforderungen der Informationsgesellschaft erstellt hat, hat das Thema Anonymisierung aufgegriffen. Der Rat führt in Kap. 2.5 über Datenschutz folgendes aus: *"Den Vorrang verdienen Verfahren, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern"*. Entsprechende Passagen finden sich auch in den Bundestags- und Bundesratsdrucksachen über "Deutschlands Weg in die Informationsgesellschaft" wieder (Entschließung zu der Empfehlung an den Europäischen Rat "Europa und die globale Informationsgesellschaft" und zu der Mitteilung der Kommission "Europas Weg in die Informationsgesellschaft: Ein Aktionsplan", Bundesrat, Drucksache 776/96, 10.10.1996, Bonn).

Problematische Systemelemente

Betrachtet man traditionelle informationsverarbeitende Systeme in ihrer komplexen Gesamtheit, so sind einige klassische Einzelprozesse (Systemelemente) identifizierbar, in denen üblicherweise solche Daten, die zur Identifizierung des Benutzers geeignet sind, anfallen, bearbeitet und gespeichert werden:

1. Identifizierung/Identifikation
Eine Identifizierung ist der Vorgang, der zum eindeutigen Erkennen einer Person oder eines Objektes dient (Feststellung der Identität einer Person).

2. Identitätsfeststellung
Als Identitätsfeststellung wird die Überprüfung bezeichnet, welche Personalien (Identität) einer natürlichen Person zuzuordnen sind.

3. Authentisierung
Authentisierung ist der Vorgang des Nachweises der eigenen Identität.

4. Authentifizierung
Authentifizierung ist der Vorgang der Überprüfung (Verifikation) der behaupteten Identität eines Gegenübers.

5. Autorisierung
Autorisierung bezeichnet in der Informationstechnologie die Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Diensten an Systemnutzer. Die Autorisierung erfolgt meist nach einer erfolgreichen Authentifizierung.

6. Zugriffskontrolle
Prüfung des Berechtigungsprofils relativ zu der gewünschten Aktion/ Dienstleistung des Systems

7. Protokollierung
Festhalten von Aktionen gemeinsam mit Angaben zum Benutzer zum Zwecke der Nachweisführung

8. Abrechnung
Rechnungsstellung der erbrachten und in Anspruch genommenen Systemleistungen an den Benutzer
Als Begründung für die jeweils erhobenen, anfallenden, gespeicherten und verarbeiteten personenbezogenen Daten werden überwiegend Abrechnungszwecke, verbesserte Kundenbetreuung, statistische sowie Kontrollzwecke angegeben.

Identitätsfeststellung des Benutzers nicht erforderlich

Die Feststellung der tatsächlichen Identität des Benutzers ist für die Funktionalität eines IuK-Systems grundsätzlich jedoch nicht erforderlich.
Allenfalls in bestimmten Fällen zur Autorisierung, Abrechnung und Protokollierung könnte die tatsächliche Identität des Benutzers erforderlich sein und müsste dort offen gelegt werden bzw. bekannt sein. In den übrigen Prozessen ist dies nicht notwendig.
Wenn in einem System stattfindende Aktionen nachträglich kontrolliert werden müssen, so ist eine Protokollierung erforderlich. So ist z. B. die in den

Datenschutzgesetzen des Bundes und der Länder vorgeschriebene Eingabekontrolle (z. B. Nr. 7 der Anlage zu § 9 BDSG) i. d. R. nur mit Hilfe der Protokollierung realisierbar, da die Zulässigkeit der Datenerhebung bzw. der Datenspeicherung nicht maschinell geprüft werden kann.
Bereits bei der Konzeption von IuK-Systemen sollte daher generell und für jeden einzelnen Prozess untersucht werden, ob Daten zur wahren Identität des Einzelnen zur Verfügung stehen müssen oder ob eine anonyme oder pseudonyme Gestaltung in Frage kommt.

Neue Herausforderungen erfordern Technikfolgenabschätzung

Soweit diese Feststellungen weiter Gültigkeit beanspruchen, muss sich der Gesetzgeber aber im Rahmen einer vorausschauenden Technikfolgenabschätzung mit den Herausforderungen neuer Technologien und neuer Geschäftsfelder auseinandersetzen und die Frage beantworten, ob die bisherigen Konzeptionen zukunftsfest sind.

Datenschutzkonzeption zukunftsfest?

Ein Ausgangspunkt für Überlegungen zu einem Modernisierungsbedarf des Datenschutzrechtes in Deutschland besteht in der Analyse der Zukunftsfähigkeit der hieraus entwickelten Datenschutzkonzeptionen vor dem Hintergrund der Herausforderungen der Informationsgesellschaft durch technische und technologische Entwicklungen. Dies kann und soll in der vorliegenden Stellungnahme nur schlaglichtartig erfolgen und basiert auf einem Kurzbericht des Arbeitskreises „Technische und organisatorische Datenschutzfragen", den der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern leitet, wie er zur 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorgelegt wurde.
Die folgenden Beispiele aktueller oder mittelfristig zu erwartender technischer Entwicklungen verändern unser alltägliches Leben und stellen vor allem die datenschutzrechtlichen Konzeptionen

- Trennungsgebot,
- Transparenzgebot,
- Zweckbindungsgebot,
- Datenverarbeitung auf der Grundlage einer freiwilligen Einwilligung,
- Dezentralisierung vor Zentralisierung von Datenbeständen,
- Privilegierung der privaten Verwendung,
- Personenbeziehbarkeit von Daten als personen-

bezogene Daten,
- Grundrechtsschutz durch staatliche Überwachung im Wege einer Zufallskontrolle und die
- Wertungsunterschiede zwischen der Datenverarbeitung öffentlicher und nicht-öffentlicher Stellen

grundsätzlich in Frage.

Konvergenz von Techniken und Netzen

Konvergenz bezeichnet allgemein das Zusammenstreben verschiedener Teilbereiche und deren Aufgehen in einem Ganzen neuer Qualität. Entwicklungen dieser Art können auf verschiedenen Gebieten der Technik beobachtet werden, unter anderem in der Telekommunikation. Beispielsweise führt die Einführung von Voice over IP zu einer Konvergenz zwischen Sprach- und Datennetzen. Auch das unten erwähnte Triple Play resultiert aus einer Konvergenz von Kabelfernsehnetzen, Datennetzen und klassischen Telefonnetzen. Neben den spezifischen Risiken, die von den einzelnen Diensten ausgehen, sind Wechselwirkungen und Kumulationseffekte zu befürchten (Beispiele: siehe unter IPTV und Triple Play), die eine datenschutzrechtliche Regelung zunehmend erschweren.

IPTV

IPTV ist die Übertragung von Fernsehen und Filmen über digitale Datennetze mit Hilfe des IP (Internet Protocol), auf dem auch die Datenübertragung im Internet basiert. Datenschutzrechtlich interessant sind hier so genannte Rückkanäle, mit denen die Nutzer Kontakt zu den Programmveranstaltern aufnehmen können. Über solche Rückkanäle können Nutzer beispielsweise weitere Daten vom Anbieter oder Dritten abrufen oder spielen.
Mittlerweile haben einige Anbieter in Metropolregionen IPTV auf den Markt gebracht. Eine weitere Möglichkeit, die jedoch bislang selten angeboten wird, ist die gezielte Bestellung von Filmen (Video on Demand).
Die Übertragung der Fernsehsignale erfolgt häufig nicht in offenen Netzen wie dem Internet, Rückkanäle werden jedoch in der Regel über das Internet aufgebaut. Hier werden insbesondere Daten zu den (Medien-)Konsumgewohnheiten übertragen. In Abhängigkeit davon, welche weiteren Dienste und Kommunikationsmöglichkeiten integriert sind, können auch Daten aus anderen Lebensbereichen übertragen werden. (Beispiel: In einer Fernsehsendung wird ein Auto einer bestimmten

	Marke gezeigt. Gleichzeitig kann der Zuschauer für dieses Auto eine Probefahrt beim nächstgelegenen Vertragshändler vereinbaren.) Diese können sowohl von den Anbietern selbst als auch von Dritten gesammelt und missbraucht werden („gläserner Zuschauer").
Triple Play	Unter dem Stichwort Triple Play wird das gebündelte Anbieten von Fernsehen, Telefonie (z. B. als Voice over IP) und Internetzugang verstanden. Entsprechende Angebote werden derzeit beispielsweise von Kabelnetzbetreibern unterbreitet. Neben den spezifischen Risiken, die von den einzelnen Diensten ausgehen, sind Wechselwirkungen und Kumulationseffekte zu befürchten. Insbesondere können sich Sicherheitslücken in einem Dienst auf einen anderen auswirken (z. B. von IPTV auf den Internetzugang, der ggf. zum Electronic Banking benutzt wird). Datensammlungen eines Triple-Play-Anbieters können zur Bildung umfassenderer Profile führen, als bei Anbietern von Einzeldiensten.
Spam/UBE	Spam oder UBE (unsolicited bulk e-mail) ist unerwünschte elektronische Post. Spam führt zu erheblichen Produktivitätsverlusten bei der Nutzung des Mediums E-Mail. Viele der Spam-Absender residieren im Ausland und können so kaum belangt werden, obwohl ihr Handeln in immer mehr Rechtsordnungen strafbar ist. Spam ist ein Massenphänomen. Spam gefährdet die Verfügbarkeit des E-Mail-Dienstes, weil der massenweise Eingang von Nachrichten zur Überlastung der Empfängersysteme führen kann. Um dem Spam-Aufkommen zu begegnen, setzen viele Anwender Filtermechanismen ein. Filter müssen den Kopfzeilen wie Absender und Betreff und Versandweg sowie den Inhalt der Nachrichten auswerten, um diese sinnvoll klassifizieren zu können. Dabei besteht die Gefahr, dass auch Unbefugte E-Mails lesen können. Außerdem können Nachrichten infolge einer fehlerhaften Klassifikation unterdrückt werden.
Utility Computing; Application Service Providing	Unter Utility Computing werden Techniken und Geschäftsmodelle verstanden, mit denen ein Service Provider seinen Kunden (standardisierte) IT-Dienstleistungen zur Verfügung stellt, die nach Verbrauch abgerechnet werden („IT aus der

Steckdose"). Der Begriff Application Service Providing ist nahezu synonym.
Es gibt Application Service Provider am Markt, das Geschäftsmodell ist zumindest in einigen Bereichen etabliert. Künftig wird mit einer höheren Marktdurchdringung zu rechnen sein.
Utility Computing ist praktisch immer Datenverarbeitung im Auftrag. Diese Art von Dienstleistungen dürften künftig immer stärker standardisiert werden, so dass der Auftraggeber immer weniger Informatik-Wissen für Einkauf und Betrieb dieser Leistungen benötigt. Der Application Service Provider gestaltet die Technik weitgehend selbst und könnte daran interessiert sein, dass wichtige Gestaltungselemente als Betriebsgeheimnisse angesehen werden. Dies führt dazu, dass die Auftraggeber ihrer Verantwortung bei der Auswahl und der Überwachung des Auftragnehmers immer schlechter wahrnehmen können.

Web 2.0

Bei Web 2.0 handelt es sich um einen unscharfen und umstrittenen Begriff, der neue interaktive Dienste im Internet und eine geänderte Wahrnehmung des Internet beschreiben soll. Dem Web 2.0 zugerechnete Anwendungen basieren technisch häufig auf Web-Service-APIs, Ajax (Asynchronous JavaScript and XML) und Abonnement-Diensten wie RSS. Auch die Integration von so genannter sozialer Software wie Blogs und Wikis wird als Teil des Web 2.0 angesehen. In der Wahrnehmung der Netzteilnehmer verschwindet zusehends die Trennung zwischen lokaler und zentraler Datenhaltung, lokalen und netzbasierten Anwendungen, Editoren und Nutzern sowie zwischen einzelnen Diensten. Außerdem können Anwendungen viel einfacher und mitunter ohne Programmierkenntnisse erstellt oder neu zusammengesetzt werden (siehe auch Webanwendungen). In diesem Zusammenhang postulieren einige Autoren das Ende des Software-Lebenszyklus, weil sich die neuen Anwendungen ständig im Beta-Stadium befinden. Kritiker wie Tim Berners-Lee vom W3C lehnen den Begriff Web 2.0 ab, weil niemand angeben könne, was er bedeutet.
Vom W3C wurde der verwandte Begriff „Semantic Web" (semantisches Web) geprägt: Maschinenlesbare Daten sollen nach diesem Konzept die Semantik der Web-Inhalte zum Ausdruck bringen und damit

vielfältige Möglichkeiten der Verknüpfung und Auswertung bieten.
Die erwähnten Techniken sind am Markt verfügbar. Die genannten Anwendungen führen häufig zur Veröffentlichung von Daten des Anwenders oder seines sozialen Umfeldes. Außerdem werden oft Nutzerprofile gebildet. Ob sich alle Anwender der möglichen Folgen bewusst sind, muss bezweifelt werden. Nach Medienberichten sind Anwender beispielsweise von den Folgen der Veröffentlichung von privaten Videoclips überrascht worden. Wichtig sind in diesem Zusammenhang jedoch vor allem die Folgen für Dritte. Eine weitere Auswirkung könnte darin bestehen, dass die Anwender Techniken aus diesem Bereich in ungeeigneten Umgebungen nutzen (beispielsweise unausgereifte Webanwendungen in ihrem Arbeitsumfeld zu dienstlichen Zwecken).

Standortbezogene Dienste

Standortbezogene Dienste sind über ein Netzwerk erbrachte mobile Dienste, die positions- und ggf. zeit- oder personenabhängig sind.
Am Markt verfügbar sind insbesondere standortbezogene Dienste im Bereich des GSM- oder UMTS-Mobilfunks, wie Routenplaner, Restaurant-Finder oder Positionsbestimmungen des eigenen oder eines fremden Mobiltelefons.
Dienste dieser Art können zu umfangreiche Bewegungsprofilen führen, die mit weiteren Daten über Tätigkeiten, Beziehungen oder Vorlieben des Benutzers angereichert sind. Standortbezogene Dienste können als Vorstufe des Ubiquitous Computing (siehe dort) angesehen werden.

Elektronische Ausweisdokumente; Biometrie in Ausweisen

In Ausweisdokumenten sollen in zunehmendem Maße biometrische Daten gespeichert werden. Außerdem ist offenbar geplant, auch Kryptochips und Schlüsselmaterial dort zu integrieren.
Hinsichtlich der Speicherung biometrischer Daten stellen sich zahlreiche Fragen, welche die Qualität der verwendeten Verfahren betreffen. So ist nach der Zuverlässigkeit bei der Erzeugung der Referenzdaten (Enrolment) sowie der Wiedererkennung (Parameter wie Falschzulassungsrate und Falschabweisungsrate) und nach der Langzeitstabilität zu fragen. Wichtig ist auch, ob die biometrischen Daten fälschungssicher und vertraulich gespeichert werden und wer darauf zugreifen kann (Gestaltung und Überwindungssicherheit des Zugriffsschutzes).
Werden Kryptochips samt Schlüsselmaterial in die Ausweise integriert, sind insbesondere das

Schlüsselmanagement und der Zugriffsschutz zu prüfen.

RFID

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich.
RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kredit- oder Kundenkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.
(Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken, Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 20. November 2003).
Der Arbeitskreis Technik der Konferenz hat inzwischen zum Thema eine Orientierungshilfe verabschiedet (www.datenschutz-mv.de/dschutz/informat/rfid/ohrifd.pdf).

Voice over IP

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen oft unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz. Während nämlich bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis.
Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. Dabei werden Sprach-Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und

paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.
Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Das Fernmeldegeheimnis ist selbstverständlich auch für die Internet-Telefonie zu gewährleisten. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze jedoch auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden.
Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden.
Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).
(Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in Lübeck, der BfDI erstellt zurzeit Handlungsempfehlungen zu diesem Thema und unterstützt das BSI bei der Formulierung datenschutztechnischer Anforderungen.)

SPIT

SPIT (SPam over IP Telephony) ist das massenhafte automatisierte Anrufen von VoIP-Telefonen. SPIT ist die Weiterentwicklung der automatisierten Anrufe, die bereits heute zu Werdezwecken eingesetzt werden. SPIT ist jedoch erheblich billiger als ein automatischer Anruf, weil keine spezielle Hardware erforderlich ist und weil die Verbindungskosten verschwindend gering sind.
Mit der zunehmenden Nutzung von VoIP ist auch mit dem Auftreten von SPIT zu rechnen.

Es ist mit vergleichbaren Auswirkungen wie bei Spam zu rechnen (siehe dort). Unerwünschte Anrufe, die nicht ausgefiltert werden, greifen jedoch erheblich stärker in die Privatsphäre des Betroffenen ein als unerwünschte E-Mails, da solche Anrufe zu jeder Zeit eingehen können und nach sofortiger Aufmerksamkeit und Reaktion verlangen.

Identitätsmanagement

Unter Identitätsmanagement versteht man das Verwalten von Identitäten und/oder von Identitätsdaten. Hierbei handelt es sich um zu einer (natürlichen) Person gehörende Daten (die nicht notwendigerweise für alle Datenverarbeiter auch unmittelbar personenbezogen sein müssen). Ein Identitätsmanagementsystem ist ein IT-System (einschließlich organisatorischer Komponenten), das Identitätsmanagement unterstützt. Insoweit handelt es sich bei dem Wort „Identitätsmanagement" um einen Sammelbegriff, der für eine Vielzahl von bereits bestehenden datenschutzrelevanten Techniken verwendet werden kann.
Heutzutage findet man drei hauptsächliche Ausprägungen vor, die häufig in Mischformen vorkommen:

1. Accountmanagement innerhalb einer Organisation, was Authentisierung, Autorisierung und Accounting umfasst, z. B. mit Hilfe von Verzeichnisdiensten und Single Sign-On-Lösungen;
2. Profiling von Nutzerdaten von Organisationen, z.B. mit Hilfe von Data Warehouses;
3. Nutzerkontrolliertes, kontextabhängiges Pseudonym- und Rollenmanagement, wobei sich Teilfunktionalität z. B. in E-Mail-Clients, Internet-Browsern oder Form-Fillern findet.

Viele Identitätsmanagementsysteme oder Teilkomponenten sind bereits auf dem Markt. Der Grad der Selbstbestimmung und Transparenz für den Nutzer unterscheidet sich stark in den verschiedenen Systemen. Parallel zu den Fortschritten, die Profiling-Techniken machen, und deren zunehmender Verbreitung zeigt sich in anderen Bereichen des Identitätsmanagements ein Trend weg von rein zentralisierten Speicher- und Managementkonzepten hin zu einem verstärkten Einbeziehen des Nutzers. Es gibt datenminimierende Techniken wie die „anonymen Credentials", bei denen Nutzer ihre erworbenen Berechtigungen in Form von Zertifikaten unter verschiedenen Pseudonymen nachweisen können, ohne dass dies verkettbar wäre.

	An vielen Stellen und bei vielen Beteiligten können beim Identitätsmanagement Daten anfallen, deren Verkettbarkeit zueinander und zu Personen im Einzelfall zu untersuchen ist. Auch der Nutzer selbst kann grundsätzlich große Teile seiner Kommunikation mitspeichern und verfügt damit in der Regel nicht nur über eine gute Übersicht seines eigenen digitalen Lebens, sondern diese Daten betreffen häufig auch seine Kommunikationspartner und damit Daten von anderen Personen und Organisationen.
Verbindung von Videoüberwachung, Biometrie, RFID	Videoüberwachung, biometrischen Identifikationsverfahren und RFID sind bereits oder werden demnächst massenweise verfügbar. Damit rückt auch die Vernetzung dieser Techniken in greifbare Nähe. Dies könnte zu einer Bildung von sehr aussagekräftigen Bewegungsprofilen von Menschen führen. Es erscheint möglich, sowohl große Personengruppen (z. B. Kunden oder Benutzer einer bestimmten Institution) als auch Einzelpersonen gezielt zu überwachen.
Ubiquitous Computing/ Pervasive Computing/Ambient Intelligence/ Smart Dust	Ubiquitous Computing (ubiquitäre/allgegenwärtige Computertechnik, Abk. UbiComp) bezeichnet die Allgegenwärtigkeit von Informationsverarbeitung im Alltag von Menschen in verschiedenen Lebensbereichen. Computer werden in die Umgebung eingebettet und bilden ein mobiles Netz, dessen Teile sich ständig ändern können und das sich selbst organisiert bzw. konfiguriert. Mit diesem Begriff verwandt sind Pervasive Computing (alles/den gesamten Alltag durchdringende Computertechnik), Ambient Intelligence (Umgebungsintelligenz) und Smart Dust (intelligenter Staub = extrem miniaturisierte Computer, die beispielsweise mit Sensoren ausgestattet sind). Erste Entwicklungen sind am Markt verfügbar. Hierzu zählen beispielsweise RFID-Tags. Bei UbiComp lässt sich immer schwerer eine Daten verarbeitende Stelle sinnvoll festlegen bzw. ermitteln. Auch der Begriff der Datenübermittlung passt innerhalb einer UbiComp-Umgebung kaum noch. Demgegenüber können sich in UbiComp-Netzwerken je nach Gestaltung unterschiedliche, ggf. sensible Lebensgewohnheiten widerspiegeln oder durch Profilbildung ermittelt werden.
Quantenkryptographie	Durch Nutzung von Effekten aus der Quantenphysik hoffen Forscher, eine Klasse von Computern schaffen zu können, die bestimmte Aufgaben wesentlich

effizienter löst als die jetzt verfügbaren Rechner. Mit solchen Geräten könnten insbesondere heute übliche kryptographische Verfahren gebrochen werden. So ist bereits ein Algorithmus bekannt, mit dem das Problem der Faktorisierung mit geringem Aufwand gelöst und so Kryptoverfahren wie RSA gebrochen werden können (so genannter Shor-Algorithmus).
Quanteneffekte lassen sich aber auch zu neuen Formen geheimer Kommunikation nutzen, bei denen der Empfänger von Nachrichten jeden Abhörversuch bemerkt (zum Beispiel beim so genannten BB84-Protokoll).
Quantencomputer sind derzeit als Labormuster sehr geringer Leistung verfügbar. Quanteneffekte konnten bereits erfolgreich zur Geheimhaltung von Nachrichten genutzt werden; hierzu gibt es Labormuster bzw. Prototypen.
Quantencomputer stellen künftig ein enormes Risiko für die Vertraulichkeit, Integrität und Zurechenbarkeit von Daten dar, die mit heutigen kryptographischen Methoden gesichert werden. Quantenkryptographie stellt hier einen Ausweg dar. Mittels Quantenkryptographie gesicherte Nachrichten lassen sich auch von solchen Stellen nicht unbemerkt abhören, denen dies gesetzlich zugestanden ist.

Nanotechnologie

Nanotechnologie ist die populäre Umschreibung für Forschung in Physik, Chemie und Maschinenbau, die sich mit der Trennung, dem Zusammenbau und der Verformung von Werkstoffen auf der Ebene einzelner Atome und Moleküle beschäftigt. Die Eigenschaften solcher Werkstoffe werden viel stärker durch die Oberflächeneigenschaften und durch quantenmechanische Effekte bestimmt als bei herkömmlichen Materialien.
Auf diesem Gebiet wird derzeit vor allem Grundlagenforschung betrieben. Es gibt vereinzelte Anwendungen etwa bei der Veredelung von Oberflächen und in der medizinischen Diagnostik und Therapie. Viele Auswirkungen der Nanotechnologie sind jedoch noch nicht ausreichend verstanden, so die Auswirkungen von Nanopartikeln auf die menschliche Gesundheit.
Die Nanotechnologie könnte zur Miniaturisierung, Leistungssteigerung und Verbilligung von Informations- und Kommunikationstechnik beitragen. Sie könnte auch die Entwicklung von Quantencomputern und Smart Dust beschleunigen. Dies kann sich mittelbar über die jeweiligen

Basistechniken auf den Datenschutz auswirken. Wegen des frühen Entwicklungsstandes der Nanotechnologie können Aussagen zu möglichen Folgen vorerst nur vage sein.

Rechtlicher Modernisierungsbedarf - eine Ethische Diskussion

Im gleichen Maße, wie der wirtschaftliche Wert personenbezogener Informationen steigt, scheint die gesellschaftliche Wertschätzung der Privatheit zu sinken. Im Schatten der sicherheitspolitisch determinierten politischen Diskussion eines angeblichen verfassungsmäßigen Rechtes auf „Sicherheit" werden die bürgerlichen Freiheiten und insbesondere das Recht auf informationelle Selbstbestimmung zunehmend und – entgegen ständiger Beteuerungen dauerhaft – nicht nur im Bereich öffentlicher Datenverarbeitung eingeschränkt, sondern damit Individualität und Privatheit auch im nicht-öffentlichen Bereich delegitimiert. Das „klassische" Abwehrkonzept gegen staatliche Überwachung weicht zunehmend der Gefahr für die private Gestaltungsfreiheit durch die informationstechnische Vernetzung aller Lebensbereiche. Informationstechnik ist die bestimmende Infrastruktur für das öffentliche, das berufliche und immer mehr auch das private Umfeld der Menschen. Über diese Infrastruktur hat der Einzelne immer weniger Kontrolle, selbst ein kompletter Entzug ist real ohne gravierende Einschnitte in die Lebenswirklichkeit undenkbar geworden.

Datenschutz nach „Prinzip Zufall"

Diese fehlende Kontrollmöglichkeit können die Aufsichtsbehörden gegenwärtig nicht kompensieren, sondern üben ihren gesetzlichen Auftrag nach dem „Prinzip Zufall" aus. Das Konzept der Transparenz zur Eröffnung einer Ausweichmöglichkeit erfüllt seine Funktion dann nicht mehr, wenn es keine Ausweichmöglichkeit mehr gibt. Die Einholung freiwilliger Einwilligungen wird zur wirkungslosen Bürokratie, wo die Nicht-Erteilung der Einwilligung zu erheblichen Nachteilen führt. Die Gefährdung für personenbezogene Daten durch zentrale Datenbestände ist keine besondere mehr, wenn die Vernetzung vieler kleiner Datenbestände durch den Einsatz von Recherchetechniken zum selben oder besseren Ergebnissen führt. Die Trennung zwischen öffentlichen und nicht-öffentlichen Bereich verliert ihren Schutzcharakter, wenn öffentliche Stellen auf die Datensammlungen von Privaten ungehindert

zugreifen können und umgekehrt.

Jede Modernisierung ist nur eine Zwischenstation

„Für wie immer verstandene Modernisierungsversuche gilt nichts anderes als für alle bisherigen und künftigen Datenschutzregelungen. Sie entstehen im Vorzeichen einer sich ständig wandelnden Technologie und können deshalb nur so lange auf die Verwendung personenbezogenen Daten Einfluss nehmen wie die mit ihr verbundenen sozialen und ökonomischen Folgen relativ konstant bleiben. Modernisierungen sind, anders und schärfer ausgedrückt, nicht mehr als Zwischenstationen eines unverändert offenen Regelungsprozesses."
(Simitis in BDSG, Einl., Rn 106, 6. Aufl.)

Datenschutz als Grundrechtsgewährung

Maßstab in diesen Regelungsprozess muss die in der Entscheidung des Bundesverfassungsgerichtes konkretisierte Wertung des Grundgesetzes bleiben, dass die Selbstbestimmungsmöglichkeit des Einzelnen Funktionsbedingung für die Demokratie ist und bleibt. Dieses Selbstbestimmungsmöglichkeit zu erhalten erfordert einerseits Zurückhaltung des Gesetzgebers bei der Anpassung der Datenschutz-vorschriften an vermeintliche Sicherheitsinteressen, Globalisierungszwänge oder Innovationshemmnisse, andererseits effektive und unabhängige Aufsichtsbehörden in Verbindung mit gefährdungsadäquaten Sanktionsmöglichkeiten, schadensadäquaten Straftatbeständen und Ersatzpflichten auch für Nicht-Vermögensschäden bei Verletzungen dieses Rechtes durch öffentlichen oder nicht-öffentliche Stellen.

2. Datenschutz-Audit	Die Auditierung von Produkten auf freiwilliger Basis ist ein erster Schritt zur Durchsetzung technischer Standards, die datenschutzgerechte Technologien zum Durchbruch verhelfen können. Aus den bisher als freiwillig konzipierten Produktauditierungen könnten technische Zulassungsverfahren entwickelt werden, die wie die Straßenverkehrszulassung neuer Fahrzeuge oder die Zulassung von Medikamenten die Unbedenklichkeit von IT-Produkten und –Verfahren gewährleisten.
Auditierung in Länderkompetenz	Der Vollzug des BDSG unterliegt gemäß Art. 83 GG der Länderkompetenz, womit auf die Aufsichtsbehörden nach BDSG die Aufgabe zukommt, eine einheitliche Ausgestaltung der Auditierungen fachlich kompetent und (wirtschafts-)politisch unabhängig i. S. der EG-Datenschutzrichtlinie sicherzustellen. Diese Unabhängigkeit ist neben der fachlichen Kompetenz, die personelle Ressourcen voraussetzt, die Grundvoraussetzung für eine Akzeptanz einer Auditierung.
Verfahren durch die Aufsichtsbehörden	Sie gewinnt für Hersteller und Anwender ihren entscheidenden Wert durch die sich hieraus ergebene Sicherheit auf Seiten beider Vertragspartner, dass die Datenschutzgerechtigkeit des zu verwendenden Produktes durch die gegebenenfalls prüfende Datenschutzaufsichtsbehörde festgestellt und bestätigt wurde.
Unabhängigkeit der Aufsichtsbehörden Grundvoraussetzung	Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedsstaaten von Stellen überwacht wird, die ihre Aufsichtaufgaben in völliger Unabhängigkeit wahrnehmen. Die Unabhängigkeit ist eine Grundvoraussetzung für die Akzeptanz eines Auditierungsverfahrens. In vielen deutschen Bundesländern ist demgegenüber die Datenschutzaufsicht über die Privatwirtschaft (so genannte nicht-öffentliche Stellen) immer noch in den jeweiligen Innenministerien angesiedelt und damit in den hierarchischen Weisungsstrang des Ministeriums eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle verstößt nach Feststellung der Europäischen Kommission gegen europäisches Recht und ist Gegenstand eines

Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland. In Mecklenburg-Vorpommern ist die Funktion der Aufsichtsbehörde gemäß § 33 a Landesdatenschutzgesetz (DSG M-V) 2004 dem Landesbeauftragten für den Datenschutz übertragen worden.

Koordinierung durch den Düsseldorfer Kreis gegenwärtige nicht leistbar

Als Koordinierungsgremium der Aufsichtsbehörden verfügt der sog. Düsseldorfer Kreis in Folge der geringen personellen Ausstattung der zuständigen Bereiche in den Innenministerien gegenwärtig weder über die personellen noch die fachlichen Ressourcen im IT-Bereich, um eine bundesweit koordinierte Auditierung sicherstellen zu können.

Audit auf landesrechtlicher Grundlage

Das DSG M-V regelt seit 2002 in § 5 Absatz 2:
„(2) Informationstechnische Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Prüfverfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Rechtsverordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens."
Der Landesgesetzgeber hat die Voraussetzungen dafür geschaffen, dass Hersteller und Vertriebsfirmen ihre IT-Produkte (Hardware, Software und Verfahren), die grundsätzlich auch für den Einsatz in der öffentlichen Verwaltung geeignet sind, auf ihre Datenschutzfreundlichkeit prüfen und im Erfolgsfalle mit einem Gütesiegel versehen lassen können. Dieses Datenschutzauditverfahren muss durch eine Rechtsverordnung geregelt werden.
Diese steht auch in Mecklenburg-Vorpommern seit 2002 immer noch aus. Hierfür wird seit In-Kraft-Treten der Regelung angeführt, dass auf die Umsetzung der bundesgesetzlichen Regelung gewartet werden soll, da nur eine bundesweite Verwendbarkeit des Audits sinnvoll sei.
Der Erlass einer solchen Verordnung würde nicht nur einen entscheidenden Qualitätsschritt für den präventiven Datenschutz im IT-Sektor bedeuten. Für die im Lande entwickelten IT-Produkte würde diese formelle Qualitätsbestätigung durch Auditierung zugleich auch einen nicht unbeträchtlichen Marketing- und Absatzfaktor darstellen. Hersteller und Vertriebsfirmen von IT-Produkten hätten bei einer Auditierung in Mecklenburg-Vorpommern Standortvorteile, denn nach § 5 Abs. 2 Satz 1 DSG M-V sind öffentliche Stellen des Landes

grundsätzlich verpflichtet, vorrangig auditierte Produkte einzusetzen.

Auditierte Produkte im öffentlichen Bereich

Dementsprechend ist die gesamte Landes- und Kommunalverwaltung gehalten, bei Ausschreibungen zunehmend das Kriterium der Auditierung in die Anforderungskataloge aufzunehmen. Das Datenschutz-Gütesiegel wirkt im Ausschreibungsverfahren dann als Nachweis der datenschutzrechtlichen Zulässigkeit des Produktes. Es entlastet Verwaltung und Unternehmen von der ansonsten bei jeder Ausschreibung erforderlichen Einzelfallprüfung der Geeignetheit des Produktes für den geplanten Einsatz.

Vergaberechtlich zulässige Berücksichtigung

Eine solche Regelung begegnet auch keinen durchgreifenden vergaberechtlichen Bedenken, wenn die Verfahrensausgestaltung der Vergaben eine Gleichbehandlung auditierter Produkte mit solchen, die in vergleichbarer Weise ihre Eignung nachweisen, sicherstellt.
Eine Zertifizierung kann somit nur als Bevorzugung von Bietern in dem Sinne wirken, als bei ihnen die Vorlage von besonderen Eignungsnachweisen obsolet wird.
Wie bei der Ausschreibung mit Hilfe sog. "Leitprodukte" kann ein auditiertes Produkt mit dem Zusatz "oder gleichwertig" gefordert werden (vgl. § 8 Nr. 3 Abs. 5 VOL/A). Erforderlich ist aber, dass die Produkteigenschaften und Qualitätsanforderungen des auditierten Produkts allen Bietern bekannt sind oder sein können. Es ist ratsam, die Kriterien einer für das ausgeschriebene Produkt möglichen Auditierung in der Ausschreibung anzugeben.
Zu Gunsten der Anbieter auditierter Produkte kann – wie bei bieterbezogenen Anforderungen - darauf verzichtet werden, die Vorlage weiterer Nachweise (Gutachten, Prüfzeugnisse o. ä.) zu verlangen. Auf diese Weise werden einerseits Auditierungen bevorzugt, andererseits behalten andere Bieter die Chance zu belegen, dass ihre (bislang noch) nicht auditierten Produkte (mindestens) gleiche Anforderungen erfüllen wie die auditierten.

Marketinginstrument

Neben den Wettbewerbsvorteilen im Bereich der öffentlichen Verwaltung würde sich die Auditierung auch in der Privatwirtschaft positiv auf die Vermarktung des Produktes auswirken. Hersteller und Vertriebsfirmen könnten die Qualität ihres Produktes durch das Zertifikat in Werbung und Marketing

absatzsteigernd hervorheben. Privaten Kaufinteressenten würde ein Produkt angeboten, das sich durch ein amtliches, datensicherheitstechnisch und datenschutzrechtlich relevantes „Prüfsiegel" gegenüber Konkurrenzprodukten positiv abhebt. Kunden und Abnehmer könnten diese Datenschutzeigenschaften – gerade beim IT-Einsatz in sensiblen Bereichen – in ihre Kaufentscheidung einbeziehen.

Entlastung öffentlicher Vergabestellen

In der öffentlichen Verwaltung würde die Einführung eines Datenschutzaudits gleichzeitig die Arbeit der Vergabestellen entlasten, weil wesentliche technische Komponenten, deren Datenschutzniveau der Anwender oft nur schwer beurteilen kann, bereits vorab sachverständig geprüft sind. Hierin liegt der entscheidende Vorteil für die Aufsichtsbehörden in Prüfverfahren. Sie kann die Prüfung auf die Fragen der rechtlich zulässigen Anwendung der Technik beschränken. Die Prüfung der technischen Sicherheit des Produktes könnte entfallen, die hinsichtlich der datenschutzrechtlichen Zulässigkeit der konkreten Anwendungen erleichtert. Das Prüfverfahren im Rahmen der Vergabe würde beschleunigt und qualitativ verbessert.

E-Goverment nur mit Audit

In allen E-Goverment-Verfahren wird eine umfassende datenschutzrechtliche Prüfung erforderlich sein, die alle technischen Aspekte bereits in der Konzipierung mit einschließt. Ein Auditierungsverfahren würde hierfür den geeigneten rechtlichen und technischen Rahmen bieten.

Rechtsklarheit für Entwickler

Eine Auditierung trägt zu Rechtsklarheit in Verwaltung und Wirtschaft bei, da sie gleichzeitig ein einheitlich anzuwendender Verfahrensmaßstab nach transparenten, nachprüfbaren Kriterien ist. Diese helfen den Entwicklern in den Unternehmen bereits im Konzeptstadium von Produkten.

Kostenreduzierung

Die Anhebung des Datensicherheitsniveaus wirkt sich darüber hinaus auf die Betriebssicherheit der eingesetzten Systeme aus. Fehlerhafte und redundante Anwendungen werden verringert beziehungsweise ausgeschlossen. Bearbeitungszeiten werden verkürzt – die Gesamtkosten reduziert. Die frühzeitige Berücksichtigung datenschutzrechtlicher Anforderungen verhindert nachträglichen Entwicklungs- und Kostenaufwand.

Entlastung der Aufsichtbehörden

Im Rahmen einer tiefgehenden Kontrolle technischer Einrichtungen durch die Aufsichtsbehörden wird regelmäßig ein Großteil der technischen Parameter geprüft, die auch im Rahmen einer Auditierung zu prüfen sein würden. Ein Audit-Verfahren muss mithin sicherstellen, dass alle Aufsichtsbehörden einheitliche Maßstäbe anlegen und die Ergebnisse gegenseitige anerkennen.

Wirksamkeitssteigerung von Prüfungen

Das Auditierungsverfahren für ein Produkt führt in dem Unternehmen zu einem Kompetenzzuwachs, der sich in den künftigen Produkten wieder finden wird. Zugleich wird das Produkt selbst zum Werbeträger für Datenschutz und bedient so eine wachsende Nachfrage.

Entwurf einer Rechtsverordnung für M-V

Am 6. Dezember 2005 habe ich in Warnemünde einen Workshop „Datenschutz durch Technik" durchgeführt, auf dem Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein die oben dargestellten Auswirkungen des Datenschutz-Gütesiegels eindrucksvoll dargestellt und mit Zahlen belegt haben. Des Weiteren wurden dort

- der Entwurf für eine Datenschutz-Gütesiegel-Verordnung Mecklenburg-Vorpommern (Anlage 1),
- der Anforderungskataloge für die zu akkreditierenden Sachverständigen (Anlage 2) und
- für IT-Produkte (Anlage 3) sowie

die Bedingungen für die vergaberechtliche Zulässigkeit des Verfahrens diskutiert.

Verfahrensablauf

Das Auditierungsverfahren beginnt mit der Prüfung der Produkte durch unabhängige, beim Landesbeauftragten für den Datenschutz auf der Basis eines Informations- und Pflichtenkataloges für Sachverständige und sachverständige Prüfstellen akkreditierte Sachverständige anhand des von mir veröffentlichten Kriterienkataloges. Deren Gutachten bilden die Grundlage für die Entscheidung des Landesbeauftragten für den Datenschutz über die Erteilung des Gütesiegels.

Gutachterakkreditierung

Dieses Akkreditierungverfahren wäre ein weiterer Vorteil für die Wirtschaft im Land. Fachleute aus Mecklenburg-Vorpommern könnten so ihre Qualifikation im technischen und/oder rechtlichen

Datenschutz quasi „öffentlich beglaubigt“ und zu weit geringeren Kosten als für eine öffentliche Bestellung und Vereidigung als Gutachter durch die IHK nach § 36 Gewerbeordnung nachweisen.

elektronische Gesundheitskarte als Modellprojekt

Das SGB X regelt die Auditierungsmöglichkeit in § 78c SGB X – unter der Überschrift Datenschutzaudit wie folgt:
„Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt. Die Sätze 1 und 2 gelten nicht für öffentliche Stellen der Länder mit Ausnahme der Sozialversicherungsträger und ihrer Verbände.“
Für die elektronische Gesundheitskarte nach § 291a SGB V wäre bei Umsetzung des gesetzgeberischen Auftrages die Auditierung ein wirksamer Weg zur Akzeptanzsteigerung dieses wichtigen Infrastrukturprojektes, aber nur eines der Beispiele.

Schwerin, 26. Februar 2007

KARSTEN NEUMANN

Anlagen 1 - 3

Entwurf

Landesverordnung über ein Auditverfahren zur Erteilung des Datenschutzgütesiegels im Land Mecklenburg-Vorpommern (Datenschutzgütesiegel-Landesverordnung - DSGü LVO M-V)

Vom 2006

(GVOBl. S. / GS M.-V. Gl. Nr.)

Aufgrund des § 5 Abs. 2 Satz 2 Landesdatenschutzgesetz – DSG M-V in der Fassung der Bekanntmachung vom 28. März 2002 (GVOBl. M-V S. 154), zuletzt geändert am (GVOBl. M-V S. ...) verordnet die Landesregierung:

§ 1 Auditierung von IT-Produkten

(1) Informationstechnische Produkte (IT-Produkte) erhalten auf Antrag der Hersteller- oder Vertriebsfirmen vom Landesbeauftragten für den Datenschutz das Datenschutzgütesiegel, wenn das IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht. Das Gütesiegel wird auf der Grundlage des Anforderungskatalogs des Landesbeauftragten für den Datenschutz für die Begutachtung von IT-Produkten im Rahmen des Auditverfahrens erteilt. Es wird befristet. Es kann widerrufen werden, wenn die Voraussetzungen für die Erteilung nicht mehr vorliegen.

(2) IT-Produkte im Sinne dieser Verordnung sind Hardware, Software und Verfahren, die zur Nutzung durch öffentliche Stellen des Landes Mecklenburg-Vorpommern geeignet sind.

(3) Erfolgreich auditierte IT-Produkte können durch ein Gütesiegel nach der Anlage zu dieser Verordnung gekennzeichnet werden. Die Anlage ist Bestandteil dieser Verordnung. Das Gütesiegel muss die Registrierungsnummer und die Gültigkeitsdauer enthalten. Das graphische Symbol darf die in der Anlage dargestellte Mindestgröße nicht unterschreiten.

(4) Der Landesbeauftragte für den Datenschutz führt ein Register über alle IT-Produkte mit Gütesiegel, das dort eingesehen werden kann und in geeigneter Weise veröffentlicht wird.

(5) Für IT-Produkte, die nach einem vergleichbaren Auditverfahren beim Bund oder in einem anderen Bundesland ein Gütesiegel erhalten haben, stellt der Landesbeauftragte für den

Datenschutz auf Antrag fest, ob die Voraussetzungen des § 5 Abs. 2 Satz 1 DSG M-V erfüllt sind. Für IT-Produkte nach Satz 1 ist in der Regel keine gesonderte Auditierung gemäß Absatz 1 erforderlich.

§ 2 Verfahren

(1) Voraussetzung für einen Antrag nach § 1 Abs. 1 ist die Überprüfung des IT-Produktes durch hierfür vom Landesbeauftragten für den Datenschutz anerkannte Sachverständige nach § 3. Die Sachverständigen sind von den Hersteller- oder Vertriebsfirmen zu beauftragen.

(2) Erfüllt ein IT-Produkt nach den Feststellungen des Sachverständigen die datenschutzrechtlichen Anforderungen, legt der Antragsteller das entsprechende Gutachten mit einer schriftlichen Dokumentation der Prüfung dem Landesbeauftragten für den Datenschutz mit folgenden Angaben vor:
1. Zeitpunkt der Prüfung,
2. detaillierte Bezeichnung des IT-Produktes,
3. Zweck und Einsatzbereich,
4. besondere Eigenschaften des IT-Produktes, insbesondere zur Datenvermeidung (§ 5 Abs. 1 Satz 1 DSG M-V), Datensicherheit (§§ 21 und 22 DSG M-V), Gewährleistung der Rechte der Betroffenen (§§ 24 bis 27 DSG M-V),
5. Bewertung der besonderen Eigenschaften,
6. Zusammenfassung der Prüfung zum Zweck der Veröffentlichung durch den Landesbeauftragten für den Datenschutz.

Der Landesbeauftragte für den Datenschutz kann ergänzende Angaben und die Vorlage des zu auditierenden IT-Produktes anfordern.

§ 3 Anerkennung von Sachverständigen

(1) Der Landesbeauftragte für den Datenschutz erteilt die Anerkennung zum Sachverständigen auf Antrag, wenn die erforderliche Fachkunde, Zuverlässigkeit und Unabhängigkeit nachgewiesen wird. Die Erteilung der Anerkennung erfolgt auf der Grundlage des Pflichtenkatalogs für Sachverständige des Landesbeauftragten für den Datenschutz. Sie kann fachlich beschränkt werden, wenn die Fachkunde nur für einen Teilbereich des Datenschutzes besteht. Die Voraussetzungen für die Anerkennung erfüllt in der Regel auch, wer durch eine vergleichbare Anerkennung als Sachverständiger beim Bund oder einem anderen Bundesland zugelassen wurde.

(2) Liegen die Voraussetzungen für eine Anerkennung nach Abs. 1 nicht mehr vor, widerruft der Landesbeauftragte für den Datenschutz die Anerkennung.

(3) Der Landesbeauftragte für den Datenschutz führt eine Liste der anerkannten Sachverständigen, die auch fachliche Beschränkungen der Prüfungstätigkeit ausweist. Die Liste kann beim Landesbeauftragten für den Datenschutz eingesehen und in geeigneter Weise veröffentlicht werden.

§ 4 Gebühren

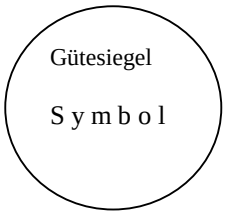
Der Landesbeauftragte für den Datenschutz kann für die ihm durch diese Verordnung übertragenen Aufgaben Gebühren nach Maßgabe einer Gebührenordnung erheben.

§ 5 In-Kraft-Treten

Diese Verordnung tritt am Tage nach ihrer Verkündung in Kraft.

Anhang:

Gütesiegel



Bei der Darstellung des Gütesiegels soll eine Größe von 24 mm Durchmesser nicht unterschritten werden. Es ist zusammen mit dem folgenden Text zu verwenden:

„Vom Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern zum Einsatz bei öffentlichen Stellen in Mecklenburg-Vorpommern empfohlen gemäß § 5 Abs. 2 DSG M-V.
Registriernummer [lfd. Nr.], [befristet bis (Datum)], weitere Informationen unter www.datenschutz-mv.de."

E N T W U R F

Stand: 17. November 2005

Informations- und Pflichtenkatalog

für Sachverständige und sachverständige Prüfstellen

A. Allgemeine Informationen für Antragsteller

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ MECKLENBURG-VORPOMMERN (LFD) ERTEILT DIE ANERKENNUNG ZUM SACHVERSTÄNDIGEN ODER ZUR SACHVERSTÄNDIGEN PRÜFSTELLE AUF ANTRAG, WENN DIE ERFORDERLICHE FACHKUNDE, ZUVERLÄSSIGKEIT UND UNABHÄNGIGKEIT NACHGEWIESEN WERDEN.

I. Anerkennung beim LfD

1. Die Anerkennung beim LfD hat den Zweck, den am Erwerb des Gütesiegels interessierten Herstellern und Vertriebsfirmen besonders sachkundige und persönlich geeignete Sachverständige sowie besonders sachkundige Prüfstellen zur Durchführung der Produktbegutachtung zur Verfügung zu stellen.

2. Die Anerkennung wird für den Zweck der Erstattung von Gutachten im Rahmen des Verfahrens zur Erlangung des Gütesiegels für IT-Produkte nach § 5 Absatz 2 Landesdatenschutzgesetz (DSG M-V) und der Datenschutzauditverordnung (DSA LVO M-V) vorgenommen.

3. Die Entscheidung über die Anerkennung erfolgt durch Verwaltungsakt. Die Anerkennung kann inhaltlich beschränkt und mit Auflagen verbunden werden. Auflagen können auch nachträglich erteilt werden.

4. Für das Verfahren zur Anerkennung von Sachverständigen und sachverständigen Prüfstellen erhebt der LfD Gebühren auf der Grundlage der Satzung über die Erhebung von Entgelten in der bei Antragstellung geltenden Fassung. Die Gebührensatzung findet ab dem Zeitpunkt der Antragstellung Anwendung. Gebühren werden auch im Fall der Ablehnung oder Rücknahme des Antrags erhoben.

5. Der LfD macht die Anerkennung des Sachverständigen oder der sachverständigen Prüfstelle durch Aufnahme in ein Register öffentlich bekannt, das sowohl konventionell als auch elektronisch geführt wird. Name, Adresse und Sachgebietsbezeichnung können gespeichert und in Listen oder auf sonstigen Datenträgern veröffentlicht und auf Anfrage jederzeit zur Verfügung gestellt werden.

II. Voraussetzungen der Anerkennung

1. Der LfD erkennt sowohl Sachverständige als natürliche Personen (dazu Teil B) als auch sachverständige Prüfstellen (dazu Teil C) an.

2. Sachverständige werden anerkannt, wenn sie die erforderliche Fachkunde, Zuverlässigkeit und Unabhängigkeit nachweisen.

3. Über die Anerkennung entscheidet der LfD nach Auswertung der eingereichten Unterlagen. Zur Überprüfung der Fachkunde kann der LfD sich vom Antragsteller bzw. vom Prüfstellenleiter Arbeitsproben vorlegen lassen, den Antragsteller bzw. Prüfstellenleiter persönlich zu einem Fachgespräch laden und weitere Erkenntnisquellen nutzen. Der LfD prüft im Fall der Vorlage von Arbeitsproben, ob die vorgelegten Unterlagen für die Bewertung der Sachkunde und Zuverlässigkeit des Antragstellers bzw. Prüfstellenleiters ausreichen.

III. Informationen für Antragsteller, die Mitglieder eines Zusammenschlusses sind

1. Beim LfD anerkannte Sachverständige können die Rechtsform, in der sie tätig sein wollen, frei wählen. Der Sachverständige muss auch als Angehöriger eines Zusammenschlusses gewährleisten, dass er seine Sachverständigenleistungen gewissenhaft, weisungsfrei, unabhängig und persönlich erbringt. Sind nicht alle Angehörige des Zusammenschlusses beim LfD anerkannt, so hat der Sachverständige darauf zu achten, die Grenzen angemessener Werbung nach dem UWG einzuhalten.

2. Ist der Sachverständige in einer rechtlich verselbstständigten Gesellschaft tätig, so wird diese selbst Partnerin des Begutachtungsvertrages.

3. Ist die persönliche Haftung des anerkannten Sachverständigen auf Grund der gewählten Rechtsform oder aus anderen Gründen ausgeschlossen, so hat der Sachverständige sicherzustellen, dass eine angemessene Haftpflichtversicherung für Ansprüche gegen die Beteiligten des Zusammenschlusses oder den Zusammenschluss als solchen abgeschlossen und aufrechterhalten wird. Ist die Haftung beschränkt, so soll der Sachverständige den Abschluss und die Aufrechterhaltung einer angemessenen Haftpflichtversicherung sicherstellen.

4. Ist der Sachverständige in einer Gesellschaft tätig, so dürfen Gesellschaftsvertrag und sonstige interne Organisationsregeln die Unabhängigkeit des Sachverständigen nicht gefährden. Eine Gefährdung ist in der Regel anzunehmen, wenn fachliche Weisungsbefugnisse anderer Gesellschafter, kaufmännischer Geschäftsführer oder der

Gesellschafterversammlung vereinbart wurden oder finanzielle Zuflüsse in Art oder Höhe an Umsatz oder Akquisition geknüpft wurden.

B. Anerkennung und Tätigkeit als einzelner Sachverständiger beim LfD

I. Anerkennung

1. Voraussetzungen der Anerkennung / Anforderungen für den Antragsteller nach § 3 Abs. 1 Datenschutzaudit-Landesverordnung (DSA LVO M-V)

Voraussetzung für die Anerkennung ist gemäß § 3 Abs. 1 DSA LVO M-V, dass der Antragsteller die erforderliche Fachkunde, Zuverlässigkeit und Unabhängigkeit erfüllt.

1.1 Fachkunde

1.1.1 Erforderlichkeit einer Doppelqualifikation

Die hohen Anforderungen an die berufliche Bildung der Sachverständigen erwachsen aus der interdisziplinären Verflechtung technischen und rechtlichen Wissens auf dem Feld des Datenschutzes und der Datensicherheit.

Bei der Begutachtung von Produkten sind stets sowohl rechtliche als auch technische Aspekte zu prüfen. Infolgedessen stellt der LfD sicher, dass bei der gutachterlichen Prüfung Sachver-stand aus den Bereichen Technik und Recht gleichermaßen bereitsteht.

Der danach erforderliche doppelte fachliche Sachverstand bei der Gutachtenerstellung kann auf unterschiedlichen Wegen durch den Gutachter oder die Gutachter bereitgestellt werden. Erforderlich und angemessen sind Erwerb und Nachweis einer Doppelqualifikation in rechtlicher und technischer Hinsicht, wenn eine Einzelperson eine unbeschränkte Anerkennung beantragt.

Antragsteller, die entweder rechtlich oder technisch über die erforderliche Fachkunde verfügen, können mit der entsprechenden fachlichen Beschränkung anerkannt werden. Der für die Gutachtenerstellung erforderliche doppelte fachliche Sachverstand ist in diesem Fall durch die Gutachter sicherzustellen, indem Gutachter, deren fachliche Anerkennungen sich ergänzen, sich zur Erstellung von Gemeinschaftsgutachten zusammenfinden.

1.1.2 Voraussetzungen der Fachkunde

Die rechtliche und technische Fachkunde kann in unterschiedlicher Form nachgewiesen werden. Die Qualifikationen beider Richtungen können formalisiert erworben und nachgewiesen werden; möglich ist aber auch der Nachweis von teilweise oder gänzlich außerhalb formalisierter Ausbildungsgänge erworbenen gleichwertigen Kenntnissen.

1.1.2.1 Erwerb technischer Kenntnisse

(1) Regelanerkennung:

Im Regelfall ist die technische Fachkunde nachzuweisen durch ein Hochschulstudium sowie praktische Erfahrungen.

(a) Hochschulausbildung

Die Hochschulausbildung erfordert

- den Abschluss eines Studiums auf dem Gebiet der Informatik oder Wirtschaftsinformatik an einer Hochschule im Sinne des § 1 HRG oder einen gleichwertigen ausländischen Abschluss oder

- den Abschluss eines Hochschulstudiums auf einem anderen Gebiet mit informationstechnischen Inhalten, die den Umfang eines durchschnittlichen Nebenfachstudiums der Informatik nicht unterschreiten, oder einen gleichwertigen ausländischen Abschluss. Ein Nebenfachstudium der Informatik, das lediglich elementare Inhalte umfasst, ist nicht ausreichend. Die informationstechnischen Studieninhalte müssen in diesem Fall gegenüber dem LfD belegt werden.

(b) Praktische Erfahrung

Darüber hinaus muss eine mindestens dreijährige berufliche Tätigkeit mit dem Schwerpunkt „Datenschutzbezogene Sicherheitsprobleme im IT-Sektor" nachgewiesen werden. Die berufliche Tätigkeit muss beratende, begutachtende oder prüfende Anteile umfassen. Eine ausschließliche Tätigkeit im Bereich IT-Sicherheit ist nicht ausreichend.

(2) Erste Ausnahmevorschrift

Die Fachkunde kann auch durch eine formale Ausbildung und sekundäre Qualifikation in IT-Ausbildungsgängen in Verbindung mit praktischen Erfahrungen nachgewiesen werden.

(a) Aus- und Weiterbildung im kaufmännisch-technischen Bereich

Die Fachkunde kann auch durch Qualifikation als Fachwirt oder Meister eines einschlägigen IT-Berufes, als IT-Professional oder durch eine Fachschulausbildung in IT-Ausbildungsgängen nachgewiesen werden.

(b) Praktische Erfahrungen

Darüber hinaus muss der Antragsteller praktische Erfahrungen im Bereich „Datenschutzbezogene Sicherheitsprobleme im IT-Sektor" von mindestens 3 Jahren in leitender oder eigenverantwortlicher Tätigkeit oder als Selbstständiger nachweisen. Die berufliche Tätigkeit muss beratende, begutachtende oder prüfende Anteile umfassen. Eine ausschließliche Tätigkeit im Bereich IT-Sicherheit ist nicht ausreichend.

(3) Zweite Ausnahmevorschrift

Die Fachkunde kann auch durch hervorragende fachliche Leistungen in einer mindestens fünfjährigen Tätigkeit im Bereich „Datenschutzbezogene Sicherheitsprobleme im IT-Sektor" nachgewiesen werden. Die berufliche Tätigkeit muss beratende, begutachtende oder prüfende Anteile umfassen. Eine ausschließliche Tätigkeit im Bereich IT-Sicherheit ist nicht ausreichend.

1.1.2.2 Erwerb rechtlicher Kenntnisse

(1) Regelanerkennung

Im Regelfall ist die rechtliche Fachkunde nachzuweisen durch ein abgeschlossenes Hochschulstudium der Rechtswissenschaft an einer Hochschule im Sinne des § 1 HRG oder einen vergleichbaren ausländischen Abschluss und eine mindestens dreijährige berufliche Tätigkeit mit dem Schwerpunkt Datenschutzrecht.

(2) Erste Ausnahmevorschrift

Die Fachkunde kann auch nachgewiesen werden durch

- den Abschluss eines anderen als unter (1) genannten Hochschulstudiums mit rechtswissenschaftlichen Inhalten, die den Umfang eines Nebenfachstudiums der Rechtswissenschaft nicht unterschreiten, oder einen gleichwertigen ausländischen Abschluss oder
- eine Qualifikation als Fachwirt oder eine Fachschulausbildung im Bereich der Rechtswissenschaft.

Die rechtswissenschaftlichen Studieninhalte müssen in diesen Fällen gegenüber dem LfD belegt werden.

In diesem Fall muss der Antragsteller eine mindestens dreijährige berufliche Tätigkeit mit dem Schwerpunkt Datenschutzrecht nachweisen, die durch den Antragsteller entweder eigenverantwortlich oder in leitender Stellung bzw. als Selbstständiger ausgeübt wurde.

(3) Zweite Ausnahmevorschrift

Die rechtliche Fachkunde kann auch durch hervorragende fachliche Leistungen in einer mindestens fünfjährigen Tätigkeit mit dem Schwerpunkt Datenschutzrecht nachgewiesen werden. Die berufliche Tätigkeit muss beratende, begutachtende oder prüfende Anteile umfassen.

1.1.2.3 Berufliche Erfahrungen

Die jeweils geforderte berufliche Praxis darf zum Zeitpunkt der Antragstellung beim LfD nicht seit mehr als drei Jahren unterbrochen sein.

1.1.2.4 Weitere fachliche Kenntnisse

Die Fachkunde erfordert neben den spezifischen rechtlichen und technischen Kenntnissen ausreichende Kenntnisse der englischen Sprache und des betrieblichen Managements, soweit diese für die Produktbegutachtung erforderlich sind.

1.1.2.5 Technische Einrichtungen

Der Sachverständige muss über die zur Ausübung der Tätigkeit als anerkannter Sachverständiger notwendigen technischen Einrichtungen verfügen können. Dies bedeutet nicht, dass er alle

technischen Einrichtungen selbst zu Eigentum erwerben muss; es reicht aus, dass ihm die erforderlichen Einrichtungen in einer Weise zur Verfügung stehen, dass der erforderliche Zugriff möglich ist.

1.1.3 Nachweis der Fachkunde

Die einzelnen Voraussetzungen der Fachkunde sind vom Antragsteller durch Nachweise zu belegen. Der LfD prüft die Fachkunde des Antragstellers anhand der Unterlagen, die dieser zum Nachweis seiner Fachkunde vorlegt. Über die Anerkennung entscheidet der LfD nach Auswertung der eingereichten Unterlagen. Zur Überprüfung der Fachkunde kann sich der LfD vom Antragsteller bzw. vom Prüfstellenleiter Arbeitsproben vorlegen lassen, den Antragsteller bzw. Prüfstellenleiter persönlich zu einem Fachgespräch laden und weitere Erkenntnisquellen nutzen. Der LfD weist darauf hin, dass vor der Vorlage der früher erstellten Arbeitsproben die Einwilligung der betroffenen Auftraggeber einzuholen ist, soweit die Gutachten deren personenbezogene Daten enthalten. Wird die Einwilligung verweigert oder aus sonstigen Gründen nicht erteilt, so sind die Arbeitsproben zu anonymisieren. Der LfD prüft im Fall der Vorlage von Arbeitsproben, ob die vorgelegten Unterlagen für die Bewertung der Sachkunde und Zuverlässigkeit des Antragstellers bzw. Prüfstellenleiters ausreichen.

1.2 Zuverlässigkeit

1.2.1 Voraussetzungen

Die erforderliche Zuverlässigkeit besitzt ein Sachverständiger, wenn er auf Grund seiner persönlichen Eigenschaften, seines Verhaltens und seiner Fähigkeiten zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist.

Für die Zuverlässigkeit bietet in der Regel derjenige keine Gewähr,

1. der ausweislich eines Bundeszentralregisterauszuges nach § 30 Absatz 5 BZRG (Führungszeugnis zur Vorlage bei einer Behörde) wegen vorsätzlich begangener Straftaten vorbestraft ist,

2. der wegen Verletzung der Vorschriften des Gewerbe- oder Arbeitsschutzrechts mit einer Geldbuße in Höhe von mehr als 500 Euro belegt worden ist,

3. dessen Bestellung zum Betriebsbeauftragten für den Datenschutz gemäß § 4 Abs. 3 Satz 4 BDSG widerrufen wurde oder dessen Abberufung nach § 38 Abs. 5 Abs. Satz 3 BDSG von der zuständigen Aufsichtsbehörde verlangt wurde,

4. der sich nicht in geordneten wirtschaftlichen Verhältnissen befindet.

1.2.2 Nachweis

Die Zuverlässigkeit ist im Antragsverfahren durch den Antragsteller gegenüber dem LfD nachzuweisen. Hierzu sind mit dem Antrag folgende Unterlagen beim LfD vorzulegen:

- ein Auszug aus dem Bundeszentralregister (Führungszeugnis zur Vorlage bei einer Behörde), den der Sachverständige gemäß § 30 Abs. 5 Bundeszentralregistergesetz (BZRG) zur unmittelbaren Vorlage beim LfD beantragt,

- die schriftliche Auskunft des zuständigen Amtsgerichts bzw. der zuständigen Amtsgerichte des Wohnsitzes bzw. der Wohnsitze der letzten 3 Jahre über Eintragungen des Antragstellers in das Schuldnerverzeichnis nach § 915 Zivilprozessordnung (ZPO),

- ein Nachweis über den Abschluss einer Haftpflichtversicherung für die Tätigkeit als Sachverständiger,

- eine Erklärung über strafrechtliche Ermittlungsverfahren,

- eine Erklärung zur Stellung als Datenschutzbeauftragter und

- eine Erklärung zu den wirtschaftlichen Verhältnissen sowie

- im Fall der beabsichtigten Beschäftigung von Hilfskräften (dazu II. 2) eine Auflistung der Mitarbeiter mit Name, Vorname, Qualifikation und Unterschrift sowie Behördenführungszeugnisse gemäß § 30 Abs. 5 BZRG für die gelisteten Mitarbeiter.

1.3 Unabhängigkeit

1.3.1 Grundsatz

Der Sachverständige darf bei der Übernahme, Vorbereitung und Durchführung eines Auftrags keiner Einflussnahme persönlicher, wirtschaftlicher oder beruflicher Natur unterliegen, die geeignet ist, ein objektives Urteil zu beeinträchtigen.

1.3.2 Anerkennung angestellter oder beamteter Antragsteller

Sachverständige, die im Angestelltenverhältnis beschäftigt werden, müssen auch nach innen, also gegenüber ihrem Arbeitgeber, fachliche Unabhängigkeit besitzen.

(1) Ein Sachverständiger, der in einem Arbeits-, Dienst- oder Beamtenverhältnis steht, erfüllt die Voraussetzungen der Unabhängigkeit, wenn er nachweist, dass

(a) er arbeits- oder dienstrechtlich abgesichert ist,

(b) die Gewähr für Unabhängigkeit und die Einhaltung der sonstigen Pflichten eines beim LfD anerkannten Sachverständigen gegeben ist,

(c) die Sachverständigentätigkeit persönlich ausgeübt werden kann,

(d) die zur Vertretung des Arbeitgebers berechtigten Organe dem mit der Leitung und Durchführung der Fachaufgaben beauftragten Sachverständigen keine fachlichen Weisungen erteilen dürfen. Der angestellte Sachverständige darf organisatorische Anweisungen des Arbeitgebers entgegennehmen.

(2) Das Einkommen eines angestellten Sachverständigen oder eines Sachverständigen in einer Sozietät darf nicht an die Ergebnisse seiner Gutachten gekoppelt werden.

1.3.3 Nachweis

Das Vorliegen der Voraussetzungen der Unabhängigkeit ist durch den Antragsteller im Antragsverfahren gegenüber dem LfD nachzuweisen. Hierzu sind dem LfD diejenigen Unterlagen vorzulegen, aus denen sich die Rechte und Pflichten des Sachverständigen gegenüber seinem Arbeitgeber, Dienstherrn oder Mitgliedern eines Zusammenschlusses ergeben.

2. Antragstellung und Registerverfahren

(1) Anträge auf Anerkennung als Sachverständiger werden an den LfD gestellt.

(2) Die anlässlich der Antragstellung erhobenen Daten werden beim LfD gespeichert:

(a) bei erfolgreicher Anerkennung während der Dauer der Anerkennung
(b) bei erfolgloser Antragstellung für die Dauer eines Jahres, beginnend mit dem Ende des Kalenderjahres, in dem der Antrag gestellt wurde.

(3) Der LfD führt über die anerkannten Gutachter ein Register in konventioneller und in elektronischer Form. In das Register werden folgende Daten der anerkannten Gutachter aufgenommen:

- Familienname
- Vorname
- akademische Grade
- Geschäftssitz

- Medien zur Kontaktaufnahme (Telefon, Fax, E-Mail)
- ggf. Beschränkungen der Fachkunde
- optional: Spezialisierungen

(4) Die Veröffentlichung ist in der Datenschutzaudit-Landesverordnung vorgeschrieben. Die Gutachter und Prüfstellen haben das Recht, gegen die konventionelle Veröffentlichung (Papierform) ihrer Daten in diesem Register Einwände gemäß § 25 Abs. 3 DSG M-V zu erheben. Anlässlich der Antragstellung gibt der LfD den Antragstellern die Möglichkeit, mit ihren Daten in das elektronische Register, das über die Homepage des LfD erreichbar ist, aufgenommen zu werden. Dazu ist die schriftliche Einwilligung der Antragsteller erforderlich. Diese Einwilligung ist für eine Anerkennung nicht erforderlich und kann widerrufen werden.

(5) Die Antragsteller können in Form von Stichworten angeben, in welchen rechtlichen und/oder technischen Bereichen sie sich für überragend qualifiziert halten. Die Angaben werden in das beim LfD sowohl konventionell als auch elektronisch geführte Register aufgenommen. Der Umfang der Angaben zu den besonderen Prüfgebieten im Register des LfD muss angemessen sein. Die Angaben dienen zur leichteren Orientierung interessierter Hersteller/Vertreiber von IT-Produkten, die eine Zertifizierung anstreben. Die Angaben werden vom LfD grundsätzlich nicht überprüft; im Register wird daher kenntlich gemacht, dass es sich bei den Angaben um Selbsterklärungen der Gutachter handelt, für deren Inhalt der LfD nicht haftet. Der LfD behält sich Plausibilitätsprüfungen im Einzelfall vor.

3. Widerruf und Erlöschen der Anerkennung

(1) Der LfD widerruft die Anerkennung, wenn die erforderliche Fachkunde, Zuverlässigkeit und Unabhängigkeit nicht mehr vorliegen. Dies ist insbesondere der Fall, wenn

(a) sich im Rahmen der Plausibilitätsprüfung eines Gutachtens durch den LfD erweist, dass das Gutachten von dem Sachverständigen unzureichend erstellt wurde,

(b) der Sachverständige sich nicht im erforderlichen Umfang auf dem Gebiet seiner Anerkennung fortbildet oder die technischen Einrichtungen, die er für die Begutachtungen einsetzt, nicht auf dem erforderlichen technischen Niveau hält,

(c) Einträge in das Schuldnerverzeichnis der Amtsgerichte oder die Eröffnung eines Insolvenzverfahrens über das Vermögen des anerkannten Sachverständigen erfolgen,

(d) ausweislich des Auszugs aus dem Bundeszentralregister eine Verurteilung wegen einer vorsätzlich begangenen Straftat erfolgt.

(2) Die Anerkennung erlischt, wenn

(a) der Sachverständige gegenüber dem LfD schriftlich erklärt, dass er nicht mehr als anerkannter Sachverständiger tätig sein will.

(b) im Falle einer befristeten Anerkennung die Zeit, für die der Sachverständige anerkannt ist, abläuft.

(c) der LfD die Anerkennung zurücknimmt oder widerruft.

II. (Informationen und Pflichten zur) Ausübung der Sachverständigentätigkeit

1. Unabhängigkeit gegenüber dem Auftraggeber

(1) Der Sachverständige darf keine Gefälligkeitsgutachten erstatten, insbesondere keine fachlichen Weisungen seiner Auftraggeber befolgen oder deren Wünschen hinsichtlich eines bestimmten Ergebnisses entsprechen. Der Sachverständige darf nicht vertraglich verpflichtet werden, bei der Erbringung seiner Leistungen Vorgaben einzuhalten, die die tatsächlichen Ermittlungen, die Bewertungen und Schlussfolgerungen derart beeinflussen, dass unvollständige oder fehlerhafte Gutachtenergebnisse verursacht werden.

(2) Der Sachverständige darf vom Auftraggeber Anweisungen zum Gutachtengegenstand und Umfang des Gutachtens entgegennehmen, da der Auftraggeber den Gegenstand einer gutachterlichen Untersuchung bestimmen kann. Der Sachverständige darf keine ergebnisbezogenen Weisungen des Auftraggebers akzeptieren.

(3) Der Sachverständige darf keine Gutachten für Verwandte, Freunde oder sonstige Personen erstatten, zu denen er in einem engen persönlichen Verhältnis steht.

(4) Der Sachverständige darf keine Gutachten über einen längeren Zeitraum ganz überwiegend für nur einen einzigen Auftraggeber erbringen. In einer solchen Konstellation ist eine Drohung mit Auftragsentzug oder Auftragsminderung geeignet, die Unabhängigkeit und Unparteilichkeit des Sachverständigen wegen der damit in Aussicht gestellten Existenzbedrohung zu beeinträchtigen.

(5) Der Sachverständige darf keine sonstigen Bindungen vertraglicher oder persönlicher Art eingehen, die seine Unabhängigkeit bei der Gutachtenerstattung in Frage stellen können.

(6) Der Sachverständige darf nicht am wirtschaftlichen Ergebnis des begutachteten Produkts beteiligt sein. Eine Beteiligung am wirtschaftlichen Ergebnis eines Produkts wird angenommen, wenn der Sachverständige eine mehr als nur unbedeutende Beteiligung an einem Hersteller- oder Vertriebsunternehmen des begutachteten Produkts hält.

(7) Der Sachverständige darf keine Vergütung für die Vermittlung von Gutachtenaufträgen zahlen, keine Sonderzahlungen entgegennehmen und keine Vergütungen annehmen, die weit über das übliche Honorar vergleichbarer Leistungen hinausgehen. Die Vereinbarung einer Provision für eine Prüfung, die zu einer Zertifizierung durch den LfD führt, ist unzulässig.

(8) Der Sachverständige muss unabhängig sein von Personen oder Institutionen, die das begutachtete Produkt geplant oder hergestellt haben oder an Vertrieb oder Instandhaltung des Produkts beteiligt waren oder sind. Unzulässig ist insbesondere

(a) dass der Sachverständige in den letzten zwei Jahren vor Abschluss des Gutachtervertrages in der Entwicklung des begutachteten Produkts tätig war oder

(b) ein paralleles gegenwärtiges Dienst- oder Werkvertragsverhältnis, also ein Nebeneinander der Tätigkeit als Sachverständiger und bei einem Hersteller oder Vertriebsunternehmen des begutachteten Produkts.

2. Zum Einsatz von Hilfskräften

(1) Der Sachverständige hat die Begutachtungsleistungen unter Anwendung der ihm zuerkannten Sachkunde in eigener Person zu erbringen.

(2) Der Sachverständige darf fachliche und sonstige Hilfskräfte nur insoweit beschäftigen, als er ihre Mitarbeit ordnungsgemäß überwachen kann. Hilfskräfte, die fachliche Leistungen zur Erstellung des Gutachtens erbringen, sind Personen, die – ob angestellt oder selbstständig –

(a) auf demselben Sachgebiet tätig sind wie der beauftragte Sachverständige,
(b) den Weisungen des Sachverständigen unterliegen und nicht beim LfD als Sachverständige anerkannt sind.

(3) Der Umfang der Tätigkeiten der Hilfskraft ist im Gutachten kenntlich zu machen.

(4) Der Sachverständige muss fachliche Hilfskräfte im Hinblick auf ihre fachliche Eignung und ihre persönliche Zuverlässigkeit sorgfältig auswählen, einweisen, anleiten, überwachen und fortbilden. Art und Umfang der Verpflichtung zur Überwachung und Anweisung im Einzelfall bestimmen sich nach dem Maß ihrer Sachkunde und Zuverlässigkeit sowie der Gegebenheiten des einzelnen Auftrags, vor allem der Schwierigkeit des zu erstellenden Gutachtens. Der LfD erwartet dabei die Sicherstellung der Zuverlässigkeit im Rahmen des dem Sachverständigen rechtlich Möglichen.

(5) Mitarbeitern, die fachliche Leistungen zur Erstellung des Gutachtens erbringen, dürfen nur solche Aufgaben übertragen werden, die der Sachverständige auf Grund seiner Fachkunde auch hätte persönlich erledigen können, andernfalls kann der Sachverständige für die Richtigkeit der Ergebnisse nicht mehr die Verantwortung übernehmen.

(6) Bedient sich der Sachverständige der Unterstützung Dritter bei der Beantwortung einer Frage, die außerhalb seines Sachgebiets liegt, ist der Dritte nicht als fachliche Hilfskraft anzusehen, da der Sachverständige aus eigener besonderer Sachkunde die Feststellungen dieses Dritten nicht würdigen und prüfen kann. Der Einsatz eines solchen Dritten ist nicht gestattet.

(7) Bei der Begutachtung dürfen nur Mitarbeiter zum Einsatz kommen, die der Sachverständige vor der Erstellung des Gutachtens beim LfD gelistet hat; dabei darf der Sachverständige nur fest angestellte Mitarbeiter listen.

(8) Die Vergabe von Unteraufträgen an Personen, die nicht per Arbeitsvertrag als Angestellte an den Sachverständigen gebunden sind, sowie an Organisationen ist ausgeschlossen.

(9) Hilfskräfte dürfen das Gutachten nicht allein oder zusammen mit dem Sachverständigen unterzeichnen. Hilfskräfte dürfen den Sachverständigen nicht, auch nicht vorübergehend, vertreten.

3. Auskunfts- und Dokumentationspflichten

(1) Der Sachverständige hat über die Produktbegutachtung schriftliche Aufzeichnungen zu machen. Die Anforderungen an die Aufzeichnungen ergeben sich zunächst aus § 2 Absatz 2 Satz 1 Nr. 1 bis 6 DSA LVO M-V; darüber hinaus müssen der Name des Auftraggebers und das Datum der Auftragserteilung ersichtlich sein.

(2) Der Sachverständige ist verpflichtet, die Aufzeichnungen über die Produktbegutachtung mindestens drei Jahre nach Ablauf des vom LfD vergebenen Gütesiegels oder der Ablehnung durch den LfD aufzubewahren. Über die Vergabe des Gütesiegels an durch ihn begutachtete Produkte sowie über eine Ablehnung wird der Sachverständige vom LfD schriftlich informiert.

(3) Der Sachverständige ist verpflichtet, die Prüfversion des Produkts mindestens drei Jahre nach Ablauf des vom LfD vergebenen Gütesiegels oder der Ablehnung durch den LfD aufzubewahren.

(4) Der Sachverständige hat auf Verlangen des LfD die aufbewahrungspflichtigen Unterlagen dem LfD in dessen Räumen vorzulegen und angemessene Zeit zu überlassen.

4. Schweigepflicht

Der Sachverständige ist zur Verschwiegenheit verpflichtet, insbesondere

(a) ist es dem Sachverständigen untersagt, bei der Ausübung seiner Tätigkeit erlangte Kenntnisse Dritten unbefugt mitzuteilen oder zum Schaden anderer oder zu seinem oder zum Nutzen anderer unbefugt zu verwerten,

(b) hat der Sachverständige seine Mitarbeiter zur Beachtung der Schweigepflicht zu verpflichten,

(c) erstreckt sich die Schweigepflicht nicht auf Anzeigen oder Auskünfte des Sachverständigen an den LfD, zu denen dieser nach den gesetzlichen und untergesetzlichen Bestimmungen verpflichtet ist,

(d) besteht die Schweigepflicht des Sachverständigen über die Beendigung des Auftragsverhältnisses hinaus; sie gilt auch für die Zeit nach Beendigung der Anerkennung.

5. Haftung des Sachverständigen

(1) Der Sachverständige darf seine Haftung für Vorsatz und grobe Fahrlässigkeit nicht ausschließen oder der Höhe nach beschränken; er soll eine Haftpflichtversicherung für sich und seine Mitarbeiter in angemessener Höhe abschließen. Die angemessene Höhe richtet sich nach dem Umfang seiner Inanspruchnahme oder dem durchschnittlichen Wert der von ihm begutachteten Objekte.

(2) Der Sachverständige kann sich insbesondere schadensersatzpflichtig machen, wenn

(a) er eine Sachverständigenleistung im Sinne des § 2 Absatz 1 DSA LVO M-V übernimmt, obwohl er weiß oder wissen musste, dass er die für diese Aufgabenstellung erforderliche besondere Sachkunde nicht besitzt,

(b) er seine Pflichten zu fachlicher Information und Fortbildung sowie seine Sorgfaltspflichten bei den tatsächlichen Feststellungen, Untersuchungen und Beratungen nicht erfüllt,

(c) er vorsätzlich oder fahrlässig bei der Erbringung der Sachverständigenleistung falsche tatsächliche Angaben macht, falsche Untersuchungsmethoden anwendet oder falsche Schlussfolgerungen zieht,

(d) er Hilfskräfte außerhalb des zulässigen Rahmens einsetzt und damit die Begutachtungsleistung nicht persönlich erbringt,

(e) seine Gedankengänge nicht nachvollziehbar und nachprüfbar darstellt oder das Gutachten nicht ausreichend begründet.

6. Werbung

(1) Auf Grund der Anerkennung ist der Sachverständige berechtigt, bei seiner gutachtlichen Tätigkeit die Bezeichnung „Beim Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern anerkannter Sachverständiger für IT-Produkte", ggf. mit dem beschränkenden Zusatz „(rechtlich)" oder „(technisch)" zu verwenden.

(2) Diese Bezeichnung darf der Sachverständige bei seiner Sachverständigentätigkeit und in dem Umfang seiner Anerkennung verwenden.

(3) Werbung des Sachverständigen für die Sachverständigentätigkeit im Rahmen der Anerkennung ist mit der Maßgabe gestattet, dass sie nach Art, Inhalt und Aufmachung der besonderen Stellung und Verantwortung eines beim LfD anerkannten Sachverständigen gerecht wird (Informationswerbung).

(4) Anerkannte Sachverständige können das Gütesiegel-Logo in der Werbung für ihre Sachverständigentätigkeit verwenden. Dabei muss sichergestellt werden, dass die Rolle des Sachverständigen im Zertifizierungsverfahren richtig dargestellt wird. Es muss der Eindruck vermieden werden, dass das Gütesiegel vom Sachverständigen selbst verliehen wird, dass die Akkreditierung des Sachverständigen beim LfD durch das Gütesiegel bestätigt wird oder dass der Sachverständige selbst das Gütesiegel verliehen bekommen hat.

III. Pflichten des anerkannten Sachverständigen gegenüber dem LfD zur Aufrechterhaltung der Anerkennung

1. Pflicht zum Erhalt der Fachkunde

(1) Der Sachverständige hat sich auf den Sachgebieten, für die er anerkannt worden ist, hinreichend fortzubilden und Möglichkeiten zum Erfahrungsaustausch wahrzunehmen.

(2) Der Sachverständige hat seine technischen Einrichtungen auf einem Stand zu halten, der die nach der DSA LVO M-V erforderlichen Prüfungen auf Datenschutz und Datensicherheit nach dem jeweiligen Stand der Technik ermöglicht. Der LfD behält sich vor, die technischen Einrichtungen des Sachverständigen nach vorheriger Terminabsprache durch eigene Vertreter in Augenschein zu nehmen.

(3) Der LfD kann im Falle unzureichender Fortbildung oder unzureichender technischer Einrichtungen dem Sachverständigen eine Frist setzen, bis zu deren Ablauf der Sachverständige für angemessene Abhilfe zu sorgen hat. Wird den Mängeln nicht fristgemäß abgeholfen, liegen die Voraussetzungen für einen Widerruf der Anerkennung vor.

2. Pflichten zur regelmäßigen Beibringung von Unterlagen

(1) Im Abstand von jeweils drei Jahren nach dem Datum der Anerkennung hat der Sachverständige dem LfD folgende Unterlagen ohne weitere Aufforderung vorzulegen:

- einen Bundeszentralregisterauszug (Führungszeugnis zur Vorlage bei einer Behörde), den der Sachverständige gemäß § 30 Absatz 5 BZRG zur unmittelbaren Vorlage beim LfD bei der zuständigen Behörde beantragt hat,

- die schriftliche Auskunft des zuständigen Amtsgerichts bzw. der zuständigen Amtsgerichte über Eintragungen des Antragstellers in das Schuldnerverzeichnis nach § 915 Absatz 1 ZPO,

- Darlegung unter Beifügung entsprechender Nachweise, welche Möglichkeiten zur Fortbildung und zum Erfahrungsaustausch im Bereich seiner Anerkennung er im abgelaufenen Zeitraum wahrgenommen hat.

(2) Der Sachverständige ist dafür verantwortlich, dass dem LfD im oben genannten zeitlichen Abstand Bundeszentralregisterauszüge der Mitarbeiter eingehen, die der Sachverständige beim LfD gelistet hat.

3. Berichts- und Anzeigepflichten des Sachverständigen

(1) Der Sachverständige hat dem LfD unverzüglich Mitteilung zu machen, wenn gegen ihn ein staatsanwaltliches Ermittlungsverfahren eröffnet wird.

(2) Der Sachverständige hat es dem LfD unverzüglich anzuzeigen, wenn in Strafverfahren gegen den Sachverständigen,

- der Erlass eines Haft- oder Unterbringungsbefehls oder die Erhebung der öffentlichen Klage erfolgt,
- der Termin zur Hauptverhandlung anberaumt wird,
- das Urteil ergeht oder das Verfahren auf sonstige Weise seinen Ausgang findet.

(3) Der Sachverständige hat es dem LfD unverzüglich mitzuteilen, wenn er

- seine weitere berufliche oder gewerbliche Tätigkeit ändert (z. B. einen neuen Arbeitsplatz annimmt oder als Beamter eine neue Tätigkeit ausübt),
- eine weitere solche Tätigkeit aufnimmt, insbesondere in ein Dienst- oder Arbeitsverhältnis eintritt oder künftig gewerblich oder freiberuflich tätig ist oder

- als angestellter Sachverständiger den Arbeitgeber wechselt.

  Durch einen solchen Wechsel kann durch die Veränderung der Arbeitsbedingungen, insbesondere bei Aufnahme einer abhängigen Beschäftigung, eine Überprüfung der Unabhängigkeit des Sachverständigen unter den veränderten Bedingungen erforderlich werden. Wechsel dieser Art können auch die Zugriffsberechtigungen auf technische Einrichtungen verändern.

(4) Der Sachverständige hat dem LfD unverzüglich Mitteilung zu machen, wenn er wegen Verletzung der Vorschriften des Gewerbe- oder Arbeitsschutzrechts mit einer Geldbuße in Höhe von mehr als 500 Euro belegt wird.

(5) Der Sachverständige hat dem LfD unverzüglich unter Darlegung des Sachverhalts Mitteilung zu machen, wenn seine Bestellung zum behördlichen oder betrieblichen Datenschutzbeauftragten widerrufen wird oder ein Abberufungsverlangen der zuständigen Aufsichtsbehörde erfolgt.

(6) Der anerkannte Sachverständige ist verpflichtet, dem LfD jeden Wohnsitzwechsel, jede Änderung der beruflichen Niederlassung, seiner Telefon- und Telefaxnummer sowie der E-Mail-Adresse unverzüglich mitzuteilen.

(7) Der Sachverständige hat dem LfD die Einleitung eines Gewerbeuntersagungsverfahrens nach § 35 GewO und die Einleitung anderer gewerberechtlicher Verfahren unverzüglich mitzuteilen.

(8) Der anerkannte Sachverständige hat eine Eintragung ins Schuldnerverzeichnis sowie Sachverhalte, die eine Eintragung ins Schuldnerverzeichnis nach sich ziehen würden, dem LfD unverzüglich mitzuteilen. Eintragungen ins Schuldnerverzeichnis erfolgen nach §§ 915 Absatz 1 ZPO, 26 Absatz 2 InsO aus folgenden Gründen:

  (a) Abgabe von eidesstattlichen Versicherungen nach § 807 ZPO und nach § 284 AO,

  (b) Gerichtliche Anordnung eines Haftbefehls nach § 901 ZPO,

  (c) Haftvollstreckungen, die sechs Monate angedauert haben,

  (d) Abweisung eines Antrags auf Eröffnung des Insolvenzverfahrens mangels Masse gemäß § 26 Absatz 2 InsO.

(9) Der anerkannte Sachverständige hat es dem LfD unverzüglich mitzuteilen, wenn über sein Vermögen oder das Vermögen einer Handelsgesellschaft, deren Geschäftsführer oder Gesellschafter er ist, die Insolvenz eröffnet wird oder über sein Vermögen die Verbraucherinsolvenz nach § 304 Absatz 1 InsO eröffnet wird.

(10) Der Sachverständige hat seinen Gutachten jeweils eine Erklärung beizufügen, in der er versichert, dass er

(a) an der Planung, Entwicklung oder Herstellung des begutachteten Produkts in den letzten zwei Jahren nicht beteiligt war.

(b) am wirtschaftlichen Ergebnis des begutachteten Produkts nicht beteiligt ist. Eine Beteiligung am wirtschaftlichen Produkt wird angenommen, wenn der Sachverständige eine mehr als nur unbedeutende Beteiligung an einem Hersteller- oder Vertriebsunternehmen des begutachteten Produkts hält.

(c) nicht ausschließlich für den Auftraggeber dieser Begutachtung als Sachverständiger tätig ist.

(d) kein paralleles Dienst- oder Werkverhältnis zum Auftraggeber unterhält.

(11) Sachverständige, die in einem öffentlich-rechtlichen Dienstverhältnis stehen, sind verpflichtet, zusammen mit jedem Gutachten eine Erklärung dahingehend abzugeben, dass der Dienstherr an Erteilung und Ausführung des Gutachtenauftrages nicht beteiligt war und keinen Einfluss genommen hat.

(12) Das Ausscheiden gelisteter Mitarbeiter ist dem LfD unverzüglich mitzuteilen.

(13) Wird der Einsatz bisher nicht gelisteter Mitarbeiter geplant, so sind dem LfD rechtzeitig die entsprechenden Nachweise zu übermitteln. Gutachten, die unter Mitwirkung nicht gelisteter Mitarbeiter erstellt wurden, werden vom LfD zurückgewiesen.

C. Anerkennung und Tätigkeit für sachverständige Prüfstellen

I. Anerkennung

1. Voraussetzungen der Anerkennung für sachverständige Prüfstellen

1.1 Zulassungsfähige Organisationsformen

(1) Der LfD anerkennt sachverständige Prüfstellen. Eine Prüfstelle wird in der Weise anerkannt, dass sie als Einheit mit eigener Rechtspersönlichkeit oder identifizierbare Einheit innerhalb einer

rechtlich verantwortlichen Organisation unter der Leitung einer natürlichen Person anerkannt wird.

(2) Handelt es sich um Prüfstellen ohne eigene Rechtspersönlichkeit, so ist erforderlich, dass die Organisation, zu der die Prüfstelle gehört, rechtlich verantwortlich gemacht werden kann.

1.2. Anforderungen an die Leitungsebene

(1) Der LfD anerkennt sachverständige Prüfstellen und stellt bei der erforderlichen Kompetenz auf den Leiter der Prüfstelle ab. Eine Prüfstelle kann nur für diejenigen Bereiche anerkannt werden, für die der Leiter der Prüfstelle die Fachkunde besitzt.

(2) Der Leiter hat seine Fachkunde im gleichen Umfang wie die einzelnen Sachverständigen zu belegen; auf die dortigen Regelungen wird daher Bezug genommen.

(3) Die Prüfstelle hat anlässlich der Anerkennung den Stellvertreter des Leiters zu benennen. Die Prüfstelle entscheidet, ob sie anlässlich ihrer Anerkennung nicht nur Fachkunde, Zuverlässigkeit und Unabhängigkeit hinsichtlich des Leiters, sondern auch in Bezug auf den Stellvertreter prüfen lässt, um im Falle eines Personalwechsels Vakanzen in der Position des Leiters zu vermeiden.

(4) Eine formale Anerkennung des Leiters als Einzelgutachter ist nicht erforderlich, wird aber auf Antrag ausgesprochen. Erfolgt neben der Anerkennung der Prüfstelle eine Anerkennung des Leitungspersonals (Leiter oder Stellvertreter) als individuelle Sachverständige, so ist diese Anerkennung nicht an ein Verbleiben des Leitungspersonals in der Prüfstelle gebunden.

(5) Der Leiter der Prüfstelle trägt für die Einhaltung der mit der Anerkennung als sachverständige Prüfstelle verbundenen Pflichten die Verantwortung.

1.3 Geordnete wirtschaftliche Verhältnisse der Prüfstelle

Der Nachweis geordneter wirtschaftlicher Verhältnisse der Prüfstelle und ggf. der Organisation, zu der die Prüfstelle gehört, erfolgt zunächst durch Selbstauskunft ihrer antragstellenden Vertreter. Der LfD behält sich das Recht vor, bei Anhaltspunkten, die die Annahme unzureichender wirtschaftlicher Solidität nahe legen, zur Sicherstellung der Unabhängigkeit die geordneten wirtschaftlichen Verhältnisse der Prüfstelle und ggf. der verantwortlichen Organisation durch Anforderung folgender Unterlagen zu überprüfen:

- bei Kapitalgesellschaften der Jahresabschluss (inklusive Bilanz, Gewinn- und Verlustrechnung, erläuterndem Anhang),

- bei sonstigen Kaufleuten der Jahresabschluss (inklusive Bilanz, Gewinn- und Verlustrechnung, nur soweit der Finanzbehörde auch vorgelegt, Anhang),
- bei freiberuflich Tätigen der Jahresabschluss, soweit der Finanzbehörde vorgelegt; ansonsten eine geordnete Aufzeichnung der Einnahmen und Ausgaben der beruflichen Tätigkeit.

1.4 Innere Unabhängigkeit der Prüfstelle

(1) Die Prüfstelle darf bei der Übernahme, Vorbereitung und Durchführung eines Auftrags keiner Einflussnahme persönlicher, wirtschaftlicher oder beruflicher Natur unterliegen, die geeignet ist, ein objektives Urteil zu beeinträchtigen. Die Prüfstelle muss dabei nicht nur nach außen – insbesondere gegenüber dem Auftraggeber – über weisungsmäßige und finanzielle Unabhängigkeit verfügen. Die Prüfstelle, die unter dem Dach einer Organisation arbeitet, muss auch nach innen, also gegenüber der Organisation, fachliche Unabhängigkeit besitzen.

(2) Wenn die Prüfstelle Teil einer Organisation ist, die auch andere Tätigkeiten als Prüfungen durchführt, müssen die Verantwortlichkeiten des maßgeblichen Personals in der Organisation, das mit der Prüftätigkeit der Prüfstelle zu tun oder darauf Einfluss hat, offen gelegt werden, um eventuelle Interessenkonflikte der Prüfstelle zu erkennen. Organisatorisch muss die Prüfstelle von anderen Teilen der Organisation, die widersprechende Interessen vertreten (Produktion, Marketing) getrennt werden.

(3) Die fachliche Unabhängigkeit der Prüfstelle und ihrer Mitarbeiter, die in einem Arbeitsverhältnis stehen, erfordert, dass

(a) arbeitsrechtlich abgesichert ist, dass die Gewähr für fachliche Unparteilichkeit und fachliche Unabhängigkeit gegeben ist,

(b) die Begutachtungen im erforderlichen Umfang ausschließlich von gelisteten Mitarbeitern unter der Verantwortung der Leitung durchgeführt werden,

(c) zur Vertretung des Arbeitgebers berechtigte Organe dem mit der Leitung und der Durchführung der Fachaufgaben beauftragten Personen keine fachlichen Weisungen erteilen dürfen. Diese Personen dürfen organisatorische Anweisungen des Arbeitgebers entgegennehmen.

(d) das Einkommen der Personals der Prüfstelle nicht an die Ergebnisse seiner Gutachten gekoppelt werden darf.

2. Antragstellung und Registerverfahren

(1) Anträge auf Anerkennung als sachverständige Prüfstelle werden an den LfD gestellt.

(2) Die anlässlich der Antragstellung erhobenen Daten werden beim LfD gespeichert:

- bei erfolgreicher Anerkennung während der Dauer der Anerkennung

- bei erfolgloser Antragstellung für die Dauer eines Jahres, beginnend mit dem Ende des Kalenderjahres, in dem der Antrag gestellt wurde.

(3) Der LfD führt über die anerkannten Gutachter und Prüfstellen ein Register in konventioneller und in elektronischer Form. In das Register werden folgende Daten der anerkannten Gutachter und Prüfstellen aufgenommen:

- Bezeichnung der Prüfstelle
- Organisation, zu der die Prüfstelle gehört (bei Prüfstellen ohne eigene Rechtspersönlichkeit)
- Leiter der Prüfstelle (Familienname, Vorname, akademische Grade)
- Stellvertretender Leiter (Familienname, Vorname, akademische Grade)
- Geschäftssitz
- Medien zur Kontaktaufnahme (Telefon, Fax, E-Mail)
- ggf. Beschränkungen der Fachkunde
- optional: Spezialisierungen

(4) Die Veröffentlichung ist in der Datenschutzaudit-Landesverordnung vorgeschrieben. Die Prüfstellen haben das Recht, gegen die konventionelle Veröffentlichung (Papierform) ihrer Daten in diesem Register Einwände gemäß § 25 Abs. 3 DSG M-V zu erheben. Anlässlich der Antragstellung gibt der LfD den Antragstellern die Möglichkeit, mit ihren Daten in das elektronische Register, das über die Homepage des LfD erreichbar ist, aufgenommen zu werden. Dazu ist die schriftliche Einwilligung der Antragsteller erforderlich. Diese Einwilligung ist für eine Anerkennung nicht erforderlich und kann widerrufen werden.

(5) Die Antragsteller können in Form von Stichworten angeben, in welchen rechtlichen und/oder technischen Bereichen sie sich für überragend qualifiziert halten. Die Angaben werden in das beim LfD sowohl konventionell als auch elektronisch geführte Register aufgenommen. Der Umfang der Angaben zu den besonderen Prüfgebieten im Register des LfD muss angemessen sein. Die Angaben dienen zur leichteren Orientierung interessierter Hersteller/Vertreiber von IT-Produkten, die eine Zertifizierung anstreben. Die Angaben werden vom LfD grundsätzlich nicht überprüft; im Register wird daher kenntlich gemacht, dass es sich bei den Angaben um Selbsterklärungen der Gutachter handelt, für deren Inhalt der LfD nicht haftet. Der LfD behält sich Plausibilitätsprüfungen im Einzelfall vor.

3. Widerruf und Erlöschen der Anerkennung

(1) Der LfD widerruft die Anerkennung, wenn die erforderliche Fachkunde, Zuverlässigkeit und

Unabhängigkeit nicht mehr vorliegen. Dies ist insbesondere der Fall, wenn

(a) sich im Rahmen der Plausibilitätsprüfung eines Gutachtens durch den LfD erweist, dass das Gutachten von der sachverständigen Prüfstelle unzureichend erstellt wurde,

(b) der Leiter sich nicht im erforderlichen Umfang auf dem Gebiet der Anerkennung der Prüfstelle fortbildet oder die technischen Einrichtungen, die die Prüfstelle für die Begutachtungen einsetzt, nicht auf dem erforderlichen technischen Niveau sind,

(c) der LfD feststellt, dass die Angaben zur Qualifikation der gelisteten Mitarbeiter nicht zutreffen oder die Prüfstelle es schuldhaft versäumt, Wechsel oder Vakanzen in der Leitung unverzüglich mitzuteilen,

(d) ausweislich des Auszugs aus dem Bundeszentralregister eine Verurteilung des Prüfstellenleiters wegen einer vorsätzlich begangenen Straftat erfolgt.

(2) Die Anerkennung erlischt, wenn

(a) der Leiter der Prüfstelle, ggf. unter Darlegung seiner Vertretungsmacht, gegenüber dem LfD schriftlich erklärt, dass die sachverständige Prüfstelle nicht mehr als solche tätig sein will.

(b) im Falle einer befristeten Anerkennung die Zeit, für die die sachverständige Prüfstelle anerkannt ist, abläuft.

(c) der LfD die Anerkennung zurücknimmt oder widerruft.

II. (Informationen und Pflichten zur) Ausübung der Tätigkeit als sachverständige Prüfstelle

1. Unabhängigkeit gegenüber dem Auftraggeber

(1) Im Einzelfall können organisatorische, wirtschaftliche, kapital- und personalmäßige Verflechtungen mit Dritten die notwendige Unabhängigkeit ausschließen. Bei der Bewertung im Einzelfall stellt der LfD auf mögliche Verflechtungen der Prüfstelle mit Dritten ab, nicht auf mögliche Verflechtungen der Organisation, zu der die Prüfstelle gehört.

(2) Die Prüfstelle darf keine Gefälligkeitsgutachten erstatten, insbesondere keine fachlichen Weisungen ihrer Auftraggeber befolgen oder deren Wünschen hinsichtlich eines bestimmten Ergebnisses entsprechen. Die Prüfstelle darf durch den Auftraggeber nicht vertraglich verpflichtet werden, bei der Erbringung ihrer Leistungen Vorgaben einzuhalten, die die tatsächlichen Ermittlungen, die Bewertungen und Schlussfolgerungen derart beeinflussen, dass unvollständige oder fehlerhafte Gutachtenergebnisse verursacht werden.

(3) Die Prüfstelle darf Anweisungen zum Gutachtengegenstand und Umfang des Gutachtens entgegennehmen, da der Auftraggeber den Gegenstand einer gutachterlichen Untersuchung bestimmen kann. Die Prüfstelle darf keine ergebnisbezogenen Weisungen des Auftraggebers akzeptieren.

(4) Die Prüfstelle darf keine Gutachten für Verwandte oder Freunde der Beschäftigten oder sonstige Personen erstatten, zu denen Leitung oder Mitarbeiter der Prüfstelle in einem engen persönlichen Verhältnis stehen.

(5) Die Prüfstelle darf keine Gutachten über einen längeren Zeitraum ganz überwiegend für nur einen einzigen Auftraggeber erbringen. In einer solchen Konstellation ist eine Drohung mit Auftragsentzug oder Auftragsminderung geeignet, die Unabhängigkeit und Unparteilichkeit der Prüfstelle wegen der damit in Aussicht gestellten Existenzbedrohung zu beeinträchtigen.

(6) Die Prüfstelle darf keine sonstigen Bindungen vertraglicher oder persönlicher Art eingehen, die ihre Unabhängigkeit bei der Gutachtenerstattung in Frage stellen können.

(7) Die Prüfstelle darf nicht am wirtschaftlichen Ergebnis des begutachteten Produkts beteiligt sein. Eine Beteiligung am wirtschaftlichen Ergebnis eines Produkts wird angenommen, wenn Leitung oder Mitarbeiter der Prüfstelle eine mehr als nur unbedeutende Beteiligung an einem Hersteller- oder Vertriebsunternehmen halten.

(8) Die Prüfstelle darf keine Vergütung für die Vermittlung von Gutachtenaufträgen zahlen, keine Sonderzahlungen entgegennehmen und keine Vergütungen annehmen, die weit über das übliche Honorar vergleichbarer Leistungen hinausgehen. Die Vereinbarung einer Provision für eine Prüfung, die zu einer Zertifizierung durch den LfD führt, ist unzulässig.

(9) Die Prüfstelle muss unabhängig sein von Personen oder Institutionen, die das geprüfte Produkt geplant oder hergestellt haben oder an Vertrieb oder Instandhaltung des Produkts beteiligt waren oder sind. Unzulässig ist insbesondere

   (a) dass die Prüfstelle in den letzten zwei Jahren vor Abschluss des Gutachtervertrages maßgeblich in der Entwicklung des geprüften Produkts tätig war.

   (b) ein paralleles gegenwärtiges Dienst- oder Werkvertragsverhältnis der Leitung oder eines Mitarbeiters der Prüfstelle, also ein Nebeneinander der Tätigkeit in der Prüfstelle und bei einem Hersteller oder Vertriebsunternehmen des Produkts.

2. Geordnete wirtschaftliche Verhältnisse

Der LfD kann es der Prüfstelle zur Auflage machen, im Falle laufender gewerberechtlicher Ermittlungsverfahren bis zur Einstellung oder zum Freispruch die Anerkennung ruhen zu lassen (keine Werbung, keine Annahme neuer Aufträge).

3. Der Einsatz von Hilfskräften innerhalb der Prüfstelle

(1) Die Prüfstelle darf zur Erstellung des Gutachtens Mitarbeiter als fachliche Hilfskräfte einsetzen. Ein beim LfD als Gutachter anerkannter Mitarbeiter der Prüfstelle, der bei einer beim LfD anerkannten Prüfstelle angestellt ist, ist keine fachliche Hilfskraft.

(2) Die Prüfstelle muss fachliche Hilfskräfte im Hinblick auf ihre fachliche Eignung und ihre persönliche Zuverlässigkeit sorgfältig auswählen, einweisen, anleiten, überwachen und fortbilden. Art und Umfang der Verpflichtung zur Überwachung und Anweisung im Einzelfall bestimmen sich nach dem Maß ihrer Sachkunde und Zuverlässigkeit sowie der Gegebenheiten des einzelnen Auftrags, vor allem der Schwierigkeit des zu erstellenden Gutachtens. Der LfD erwartet dabei die Sicherstellung der Zuverlässigkeit im Rahmen des der Prüfstelle rechtlich Möglichen.

(3) Mitarbeitern, die fachliche Leistungen zur Erstellung des Gutachtens erbringen, dürfen nur solche Aufgaben übertragen werden, die der Leiter der Prüfstellen auf Grund seiner Fachkunde auch hätte persönlich erledigen können, andernfalls kann der Leiter der Prüfstelle für die Richtigkeit der Ergebnisse nicht mehr die Verantwortung übernehmen.

(4) Bei der Begutachtung dürfen nur Mitarbeiter zum Einsatz kommen, die die Prüfstelle vor der Erstellung des Gutachtens beim LfD gelistet hat.

(5) Bedient sich die Prüfstelle der Unterstützung Dritter bei der Beantwortung einer Frage, die außerhalb ihres anerkannten Sachgebiets liegt, ist der Dritte nicht als fachliche Hilfskraft anzusehen, da die Prüfstelle aus eigener besonderer Sachkunde die Feststellungen dieses Dritten nicht würdigen und prüfen kann. Der Einsatz eines solchen Dritten im Rahmen der Erstellung des Gutachtens ist nicht gestattet.

(6) Der Umfang der Tätigkeit der fachlichen Hilfskräfte ist im Gutachten kenntlich zu machen.

(7) Hilfskräfte dürfen das Gutachten nicht alleine oder zusammen mit dem zeichnungsberechtigten Leiter der Prüfstelle unterzeichnen. Hilfskräfte dürfen den Leiter der Prüfstelle nicht, auch nicht vorübergehend, vertreten.

(8) Die Vergabe von Unteraufträgen an Personen, die nicht per Arbeitsvertrag als Angestellte an den Sachverständigen gebunden sind sowie an Organisationen ist ausgeschlossen.

4. Auskunfts- und Dokumentationspflichten

(1) Die sachverständige Prüfstelle hat über die Produktbegutachtung schriftliche Aufzeichnungen anzufertigen. Die Anforderungen an die Aufzeichnungen ergeben sich zunächst aus § 2 Absatz 2 Satz 1 Nr. 1 bis 6 DSA LVO M-V; darüber hinaus müssen der Name des Auftraggebers und das Datum der Auftragserteilung ersichtlich sein.

(2) Die sachverständige Prüfstelle ist verpflichtet, die Aufzeichnungen über die Begutachtung mindestens drei Jahre nach Ablauf des vom LfD vergebenen Gütesiegels oder der Ablehnung durch den LfD aufzubewahren. Über die Vergabe des Gütesiegels an durch ihn begutachtete Produkte sowie über eine Ablehnung wird der Sachverständige vom LfD schriftlich informiert.

(3) Die sachverständige Prüfstelle ist verpflichtet, die Prüfversion des Produkts mindestens drei Jahre nach Ablauf des vom LfD vergebenen Gütesiegels oder der Ablehnung durch den LfD aufzubewahren. Die Aufbewahrungsfrist für die Aufbewahrung der Aufzeichnungen und der Prüfversion beginnt mit dem Schluss des Kalenderjahres, in dem die Aufzeichnungen zu machen oder die Unterlagen entstanden sind.

(4) Die sachverständige Prüfstelle hat auf Verlangen des LfD die aufbewahrungspflichtigen Unterlagen dem LfD in dessen Räumen vorzulegen und angemessene Zeit zu überlassen.

5. Schweigepflicht

Leitung und Mitarbeiter der Prüfstelle sowie andere am Vertragsschluss und der Begutachtung beteiligte Mitarbeiter der ggf. verantwortlichen Organisation sind zur Verschwiegenheit verpflichtet. Insbesondere

(a) ist es den Beteiligten untersagt, bei der Ausübung ihrer Tätigkeit erlangte Kenntnisse Dritten unbefugt mitzuteilen oder zum Schaden anderer oder zu ihrem oder zum Nutzen anderer unbefugt zu verwerten,

(b) haben die Leitung der Prüfstelle und ggf. die verantwortliche Organisation ihre Mitarbeiter zur Beachtung der Schweigepflicht zu verpflichten,

(c) erstreckt sich die Schweigepflicht nicht auf Anzeigen oder Auskünfte der sachverständigen Prüfstelle oder der verantwortlichen Organisation an den LfD, zu denen diese nach dem „Informations- und Pflichtenkatalog für Sachverständige und sachverständige Prüfstellen" verpflichtet sind,

(d) besteht die Schweigepflicht der Beteiligten über die Beendigung des Auftragsverhältnisses hinaus; sie gilt auch für die Zeit nach Beendigung der Anerkennung.

6. Haftung

(1) Die Haftung für Vorsatz und grobe Fahrlässigkeit darf von der haftenden Einheit nicht ausgeschlossen oder der Höhe nach beschränkt werden; sie soll eine Haftpflichtversicherung für die Prüfstelle in angemessener Höhe abschließen. Die angemessene Höhe richtet sich nach dem Umfang der Inanspruchnahme oder dem durchschnittlichen Wert der von der Prüfstelle begutachteten Objekte.

(2) Die haftende Einheit kann sich insbesondere schadensersatzpflichtig machen, wenn

(a) die Prüfstelle eine Sachverständigenleistung im Sinne des § 2 Absatz 1 DSA LVO M-V übernimmt, obwohl die Leitung weiß oder wissen musste, dass die Prüfstelle die für diese Aufgabenstellung erforderliche besondere Sachkunde nicht besitzt.

(b) die Prüfstelle die Pflichten zu fachlicher Information und Fortbildung sowie die Sorgfaltspflichten bei den tatsächlichen Feststellungen, Untersuchungen und Beratungen nicht erfüllt.

(c) die Prüfstelle vorsätzlich oder fahrlässig bei der Erbringung der Sachverständigenleistung falsche tatsächliche Angaben macht, falsche Untersuchungsmethoden anwendet oder falsche Schlussfolgerungen zieht.

(d) die Begutachtung nicht durch die gelisteten Mitarbeiter persönlich erbracht und durch die Leitung verantwortet wird.

(e) die Prüfungen nicht nachvollziehbar und nachprüfbar dargestellt werden oder das Gutachten nicht ausreichend begründet wird.

7. Werbung

(1) Auf Grund der Anerkennung ist die sachverständige Prüfstelle berechtigt, bei ihrer gutachterlichen Tätigkeit die Bezeichnung „Beim Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern anerkannte sachverständige Prüfstelle für IT-Produkte", ggf. mit dem beschränkenden Zusatz „(rechtlich)" oder „(technisch)" zu verwenden.

(2) Diese Bezeichnung darf die sachverständige Prüfstelle bei ihrer Gutachtentätigkeit und in dem Umfang ihrer Anerkennung verwenden.

(3) Werbung der sachverständigen Prüfstelle für die Begutachtungstätigkeit im Rahmen der Anerkennung ist mit der Maßgabe gestattet, dass sie nach Art, Inhalt und Aufmachung der besonderen Stellung und Verantwortung einer beim LfD anerkannten sachverständigen Prüfstelle gerecht wird (Informationswerbung). Es muss deutlich werden, dass nicht die Organisation als solche, sondern die Prüfstelle beim LfD anerkannt ist.

(4) Anerkannte Prüfstellen können das Gütesiegel-Logo in der Werbung für ihre Gutachtertätigkeit verwenden. Dabei muss sichergestellt werden, dass die Rolle der Prüfstelle im Zertifizierungsverfahren nicht missverständlich dargestellt wird. Es muss der Eindruck vermieden werden, dass das Gütesiegel von der Prüfstelle selbst verliehen wird, dass die Akkreditierung der Prüfstelle beim LfD durch das Gütesiegel bestätigt wird oder dass die Prüfstelle selbst das Gütesiegel verliehen bekommen hat.

III. Pflichten der anerkannten Prüfstelle gegenüber dem LfD zur Aufrechterhaltung der Anerkennung

1. Pflicht zum Erhalt der Fachkunde

(1) Der Leiter der Prüfstelle hat sich auf den Sachgebieten, für die die Prüfstelle anerkannt worden ist, hinreichend fortzubilden und Möglichkeiten zum Erfahrungsaustausch wahrzunehmen.

(2) Der Leiter der Prüfstelle ist verantwortlich dafür, die gelisteten Mitarbeiter hinreichend fortzubilden.

(3) Die Prüfstelle hat ihre technischen Einrichtungen auf einem Stand zu halten, der die nach der DSA LVO M-V erforderlichen Prüfungen auf Datenschutz und Datensicherheit nach dem jeweiligen Stand der Technik ermöglicht. Der LfD behält sich vor, die technischen Einrichtungen der Prüfstelle nach vorheriger Terminabsprache durch eigene Vertreter in Augenschein zu nehmen.

(4) Der LfD kann im Falle unzureichender Fortbildung oder unzureichender technischer Einrichtungen der Prüfstelle eine Frist setzen, bis zu deren Ablauf die Prüfstelle für angemessene Abhilfe zu sorgen hat. Wird den Mängeln nicht fristgemäß abgeholfen, liegen die Voraussetzungen für einen Widerruf der Anerkennung vor.

2. Pflichten zur regelmäßigen Beibringung von Unterlagen

Hinsichtlich des Leiters der sachverständigen Prüfstelle wird auf die Pflichten des einzelnen Sachverständigen zur regelmäßigen Beibringung von Unterlagen Bezug genommen. Soweit sich der benannte Stellvertreter einer formalen Prüfung unterzogen hat, gelten diese Anforderungen auch für diesen.

Im Übrigen hat die sachverständige Prüfstelle dem LfD ohne besondere Aufforderungen im Abstand von jeweils drei Jahren nach dem Datum der Anerkennung Behördenführungszeugnisse der gelisteten Mitarbeiter vorzulegen.

3. Berichts- und Anzeigepflichten der sachverständigen Prüfstelle

Hinsichtlich des Leiters der Prüfstelle gelten die Berichts- und Anzeigepflichten für den einzelnen Sachverständigen, auf die Bezug genommen wird.

Für die Prüfstelle ist der LfD in den folgenden Fällen zu benachrichtigen:

(1) Der LfD ist unverzüglich zu benachrichtigen, wenn der Leiter der Prüfstelle wechselt oder eine Vakanz von mehr als drei Monaten auftritt.

(2) Das Ausscheiden gelisteter Mitarbeiter aus der Prüfstelle ist dem LfD unverzüglich mitzuteilen.

(3) Wird der Einsatz bisher nicht gelisteter Mitarbeiter geplant, so sind dem LfD rechtzeitig die entsprechenden Nachweise zu übermitteln. Gutachten, die unter Mitwirkung nicht gelisteter Mitarbeiter erstellt wurden, werden vom LfD zurückgewiesen.

(4) Die Prüfstelle hat den LfD unverzüglich zu unterrichten, wenn gegen sie selbst oder die Organisation, zu der sie gehört, ein gewerberechtliches Verfahren eingeleitet werden sollte.

(5) Tritt im Rechtsstatus, in den Besitzverhältnissen, der Stellung innerhalb eines Unternehmenskonzerns oder den Finanzierungsquellen der Prüfstelle eine Veränderung ein, so ist der LfD davon unverzüglich zu unterrichten.

(6) Ist die Prüfstelle als identifizierbare Einheit innerhalb einer Organisation anerkannt worden, so ist der LfD unverzüglich zu benachrichtigen, wenn sich

- Struktur und Verantwortungsbereiche innerhalb der Organisation verändern,

- Rechtsstatus, Besitzverhältnisse, die Stellung innerhalb eines Unternehmenskonzerns oder die Finanzierungsquellen der Organisation verändern,

- der Gesellschaftsvertrag oder die Satzung der Organisation ändern.

(7) Die Prüfstelle hat jedem einzelnen Gutachten eine Erklärung beizufügen, mit der der Leiter versichert, dass die Prüfstelle

(a) an der Planung, Entwicklung oder Herstellung des begutachteten Produkts in den letzten zwei Jahren nicht beteiligt war.

(b) am wirtschaftlichen Ergebnis des geprüften Produkts nicht beteiligt ist. Eine Beteiligung am wirtschaftlichen Produkt wird angenommen, wenn Leitung oder Mitarbeiter der Prüfstelle eine mehr als nur unbedeutende Beteiligung an einem Hersteller- oder Vertriebsunternehmen des begutachteten Produkts halten.

(c) nicht ausschließlich für den Auftraggeber dieser Begutachtung als Prüfstelle tätig ist.

(d) keinen Mitarbeiter beschäftigt, der ein paralleles Dienst- oder Werkverhältnis zum Auftraggeber unterhält.

Anforderungskatalog v 0.0 für die Begutachtung von IT-Produkten im Rahmen des Datenschutzauditverfahrens beim Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern

Anforderungskatalog v 0.0

Stand: 17.11.2005

Der Anforderungskatalog stellt beispielhaft Datenschutz- und Datensicherheitsanforderungen sowie in ihrem Zusammenhang zu berücksichtigende Fragen nach wichtigen Rechtsnormen dar. Er gibt eine Mustergliederung für das Abarbeiten von Anforderungen jeweils nach Datenart vor (siehe Prüfschema). Eine reine Prüfcheckliste kommt nicht in Betracht, da sich die Anforderungsprofile und Datenarten pro zu prüfendem IT-Produkt unterscheiden und außerdem die Sachverständigen ihre Bewertungen stets begründen müssen.

Pro Frage ist zu untersuchen,

- ob sie jeweils relevant für das IT-Produkt ist,
- ob das IT-Produkt zur Erfüllung der Datenschutzanforderung beiträgt, diese erschwert oder den Punkt unberührt lässt,
- ob eine Realisierung gemäß dem Stand der Technik erfolgt,
- ob die Erfüllung der Anforderungen keinen erheblichen Aufwand erfordert,
- welche Standardeinstellung ausgeliefert wird,
- welche Konfigurationsmöglichkeiten oder andere Freiheitsgrade bestehen und
- wie all dies dokumentiert und nutzeradäquat umgesetzt ist.

Die Relevanz der Fragen wird sich insbesondere darin unterscheiden, ob es sich um spezielle Verwaltungsverfahren und darauf zugeschnittene Produkte handelt oder ob es universeller einsetzbare IT-Produkte sind.

Dieser Text stellt im **Komplex 1** zunächst Anforderungen an die Technikgestaltung dar. Dies betrifft insbesondere Anforderungen der Datenvermeidung und der Transparenz.

Komplex 2 zählt die einschlägigen Datenschutzbestimmungen auf, um die Zulässigkeit der angestrebten Datenverarbeitung überprüfen zu können.

In **Komplex 3** wird untersucht, welche technischen und organisatorischen Maßnahmen zum Schutz der Betroffen das Produkt unterstützt.

Komplex 4 stellt Kriterien vor, um die Umsetzungen der Rechte der Betroffenen (z. B. Benachrichtigung, Auskunft, Transparenzgebote) beurteilen zu können.

Alle Komplexe müssen gleichermaßen bei der Prüfung des IT-Produktes berücksichtigt werden.

Übersicht über die einzelnen Komplexe

A. Allgemeines Anforderungsprofil

Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten

In diesem Komplex werden allgemeine und übergreifende Anforderungen an die Technikgestaltung bearbeitet. Dies betrifft insbesondere Anforderungen der Datenvermeidung und der Transparenz.

Komplex 2: Zulässigkeit der Datenverarbeitung

Die Frage der Zulässigkeit einer Datenverarbeitung beurteilt sich danach, welches Recht auf die Stellen anzuwenden ist, für die das Produkt vorgesehen ist. Bei Stellen des Landes Mecklenburg-Vorpommern ist dies grundsätzlich das Landesdatenschutzgesetz (DSG M-V), bei Wettbewerbsunternehmen u. U. das BDSG (§ 2 Abs. 5 DSG M-V). Bei Sozialleistungsträgern gilt das SGB. Die insofern geltenden Vorschriften werden ausgeführt. Daneben sind sämtliche speziellen bereichsspezifischen Regelungen zu beachten. Beispielhaft (aber nicht abschließend) seien hier als Bundesrecht

§§ 75 ff. AusländerG,

BundesstatistikG,

PersonenstandsG,

Pass- und PersonalausweisG,

Strafprozessordnung,

§§ 185 ff. StrafvollzugsG,

StraßenverkehrsG,

Teledienstedatenschutzgesetz

Telekommunikationsgesetz

oder als Landesrecht

§ 7 LHochschulG,

Mediendienste-Staatsvertrag

LMeldeG,

LArchivG,

§§ 100 ff. LBeamtenG,

LStatistikG,

Sicherheits- und OrdnungsG,

§ 4 LPresseG,

§§ 70 ff. SchulG,

genannt.

Komplex 3: Technische und organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen

In Komplex 3 werden für Datenschutzanforderungen, die sich bei zulässiger Datenverarbeitung im Wesentlichen aus den Katalogen nach BDSG und DSG M-V über technische und organisatorische Maßnahmen ergeben, beispielhaft (technische) Maßnahmen diskutiert, die zur Umsetzung dieser Anforderungen führen können. Dabei wird auch der Grad der technischen Umsetzung dieser Maßnahmen durch das Produkt problematisiert. Beachtet werden muss bei der Bewertung,

- welches Angreifermodell den getroffenen/zu treffenden Maßnahmen zugrunde liegt,
- gegen welche Angriffe Schutzmaßnahmen vom IT-Produkt selbst vorgesehen sind,
- welche zusätzlichen Maßnahmen unterstützt werden (bzw. ob es dabei Einschränkungen gibt) und schließlich,
- welche Restrisiken verbleiben.

Komplex 4: Rechte der Betroffenen

Die Gewährleistung der Betroffenenrechte wird heutzutage vielfach auf organisatorischer Ebene abgedeckt. Beim zu zertifizierenden IT-Produkt ist entscheidend, inwieweit dort technisch

- die Wahrnehmung der Rechte direkt durch die Betroffenen ermöglicht oder sogar gefördert sowie
- die organisatorische Ebene beim Betreiber zur Gewährleistung der Betroffenenrechte unterstützt wird.

Es sind jeweils zusätzlich sowohl die Aspekte der Datensparsamkeit (z. B. ist eine Abwicklung anonym oder unter Pseudonym möglich) als auch der Protokollierung der Wahrnehmung der Betroffenenrechte zu berücksichtigen.

B. Anforderungsprofil für Protokolldaten

Bewertung

Es ist zu beachten, dass innerhalb eines Produktes verschiedene Datenarten verarbeitet und zwischen einzelnen Komponenten ausgetauscht werden. Beispielhaft genannt seien hier *Betroffenendaten* (häufig auch als *Primärdaten* bezeichnet), z. B. Daten über

Einwohner in einem Einwohnermeldeamt, und *Sekundärdaten* (z. B. Protokolldaten über Dateneingaben und Datenbankzugriffe, aber auch über Konfigurationsänderungen oder Zugang zu sensiblen Räumen wie Rechenzentrum).

Für jede dieser Datenarten ist nur ein Ausschnitt des Anforderungskataloges relevant. Durch mehrfaches Überprüfen des Kataloges (einmal für jede Datenart) müssen die entsprechenden Anforderungen gefunden und die Umsetzung durch das Produkt bewertet werden.

A. Allgemeines Anforderungsprofil

Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten

1.1 Datensparsamkeit

Untersuchungsgegenstand:
Wurden die Anforderungen der Datensparsamkeit umgesetzt?

In diesem Zusammenhang wichtige Fragen:

- Kann der Betroffene anonym oder pseudonym agieren oder können seine Daten zumindest nachträglich anonymisiert oder pseudonymisiert werden?
- Ist ein vollständiger Verzicht auf personenbezogene Daten möglich? Wenn nein, warum nicht?
- Welche (Kombinationen von) personenbezogenen Daten sind wirklich erforderlich? Wovon hängt dies ab?
- Wird auf das Anlegen von temporären Datenbeständen (z. B. unnötige Protokollierung, Parallel- und Zwischenspeicherung) verzichtet bzw. sind diese Datenbestände wirksam gegen unbefugten Zugriff gesichert?
- Verzichtet der Empfänger von Daten freiwillig bzw. auf Grundlage seiner veröffentlichten Informations-/Datenschutzpolicy auf die Speicherung und Auswertung von ihm übermittelten (Teil-)Informationen, die für seine Aufgabenerfüllung nicht erforderlich sind? – Filterung auf Empfängerseite für „zuviel" übermittelte Daten.

1.2 Frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren, wenn Daten noch erforderlich, aber Personenbezug verzichtbar

Untersuchungsgegenstand:
Gibt es Methoden für frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren personenbezogener Daten?

In diesem Zusammenhang wichtige Fragen:

- Wie werden Löschen, Anonymisierung und Pseudonymisierung umgesetzt (automatisch / in welchen Abhängigkeiten)?
- Wird die Pseudonymisierung/Anonymisierung zum frühest möglichen Zeitpunkt vorgenommen?
- Wovon hängt der Zeitpunkt der Anonymisierung oder Pseudonymisierung ab?

- Sind geeignete Maßnahmen ergriffen worden, um die Zuordnungsfunktion bei einer Pseudonymisierung zu sichern? Ist die Zuordnungsfunktion geeignet, oder besteht die Gefahr, mit nur wenig Zusatzwissen einzelne Daten depseudonymisieren zu können (etwa bei einer Pseudonymisierung durch Vertauschen von Namensbuchstaben etc.)?
- Zu technischen Fragen des Löschens siehe auch Abschnitt 4.3.2.

1.3 Transparenz und Produktbeschreibung

Untersuchungsgegenstand:
Liegt eine aussagekräftige und aktuelle Produktbeschreibung vor?

In diesem Zusammenhang wichtige Fragen:

- Ist die Transparenz der Datenverarbeitung (Datenflüsse, Speicherungsorte, Übermittlungswege, Zugriffsmöglichkeiten) gegenüber
  - Anwendern (Systemadministration und Nutzer) sowie
  - Betroffenen

  gewährleistet?
- Sind die Vorkenntnisse, die zum Verstehen der Produktbeschreibung erforderlich sind (Sprache, Know-how), angemessen?
- Inwieweit ist ein leichter Zugriff auf die Produktbeschreibung und eine geeignete Auswertbarkeit gewährleistet (Inhaltsverzeichnis, Index, Volltextsuche)?
- Wird die Aktualität sichergestellt?
- Wird das zu Grunde liegende Konzept ausreichend erläutert?
- Besteht eine Einsichtsmöglichkeit in den Quelltext/das Gerät? Für wen (auch für Außenstehende oder nur für den Gutachter)?

1.4 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit ergeben?

Komplex 2: Zulässigkeit der Datenverarbeitung

2 Zulässigkeit der Datenverarbeitung

2.1 Ermächtigungsgrundlage für die Verarbeitung von Daten (für jede Phase der Datenverarbeitung gesondert)

2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten (z. B. §§ 7, 14–16 DSG M-V; §§ 28 ff. BDSG oder bereichsspezifisches Recht wie §§ 67a ff. SGB X)

Untersuchungsgegenstand:
Sind die Zulässigkeitsvoraussetzungen für die Datenverarbeitung erfüllt?

In diesem Zusammenhang wichtige Fragen:

- Gibt es einen abgeschlossenen Katalog von Daten, die verarbeitet werden sollen?

  Wenn ja: Werden die Erhebung und die Speicherung auf diese Daten beschränkt (keine Freitextfelder!)?
  Wenn nein: Beschränken sich die Daten auf das Erforderliche?
- Erfolgt eine Verarbeitung besonders sensibler Daten (§ 67 Abs. 12 SGB X, § 3 Abs. 9 BDSG), die die Zulässigkeit einschränken könnte (§ 7 Abs. 2, 3 DSG M-V, § 67a Abs. 1 S. 2, 67b Abs. 1 S. 2 SGB X, § 28 Abs. 6-9 BDSG)? Wie wird eine solche Einschränkung umgesetzt?
- Unterliegen die Daten zusätzlichen besonderen materiellen Anforderungen (z. B. berufliche Schweigepflicht, vgl. § 203 StGB), und wie werden diese bei der weiteren Verarbeitung berücksichtigt?
- Inwieweit sind Pseudonymisierung- bzw. Anonymisierungsgebote (z. B. § 34 DSG M-V) zu beachten?

2.1.2 Einwilligung des Betroffenen (§ 8 DSG M-V, § 67b Abs. 2, 3 SGB X, § 4a BDSG)

Untersuchungsgegenstand:
Wird die Wirksamkeit einer Einwilligung unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Stellt das Produkt eine Mustereinwilligungserklärung oder Hinweise zur Gestaltung der Einwilligungserklärung zur Verfügung? Ist die Formulierung einer vorgegebenen Einwilligungserklärung hinreichend bestimmt, d. h. enthält sie Angaben zu verarbeitenden Stellen, verarbeiteten Datenkategorien, den Phasen der Datenverarbeitung, insbesondere geplanten Übermittlungen und den Empfängern der Übermittlung, dem Zweck der Datenverarbeitung sowie einen Hinweis auf die Freiwilligkeit und Widerrufbarkeit der Einwilligung?
- Sind die Formerfordernisse nach § 8 Abs. 2 DSG M-V (bzw. § 67b Abs. 2 SGB X, § 4a Abs. 1 S. 3, 4 BDSG) gewahrt?
- Kann die Einwilligung frei erklärt werden, oder ist eine Leistung an die Erklärung der Einwilligung gekoppelt?
- Gibt es eine Unterstützung durch das IT-System (dabei ist zu berücksichtigen, dass i. d. R. die Einwilligung vor der ersten Speicherung vorliegen muss)?

2.1.3 Besonderheiten in den einzelnen Phasen der Datenverarbeitung

2.1.3.1 Vorschriften über die Datenerhebung (§ 9 DSG M-V, § 67a Abs. 1 SGB X, § 28 Abs. 1 BDSG, vgl. § 13 BDSG)

Untersuchungsgegenstand:
Werden die gesetzlichen Regelungen bei der Erhebung von Daten umgesetzt?

In diesem Zusammenhang wichtige Fragen:

- Erfolgt eine Dokumentation über die Herkunft der Daten?
- Erfolgt eine Unterrichtung bzw. Aufklärung des Betroffenen (§ 9 Abs. 3, 4 DSG M-V, § 67a Abs. 3, 5 SGB X) bzw. des Dritten (§ 9 Abs. 4 S. 1 DSG M-V, § 67a Abs. 4 SGB X)? In welcher Form unterstützt das Produkt dies?
- Erfolgt eine verdeckte Erhebung von Daten ohne Kenntnis des Betroffenen (z. B. bei biometrischen Verfahren)?

2.1.3.2 Vorschriften über die Übermittlung (§§ 14-17 DSG M-V, §§ 67d-78 SGB X, §§ 28, 29 BDSG)

Untersuchungsgegenstand:
Werden die Vorschriften zur Übermittlung umgesetzt?

In diesem Zusammenhang wichtige Fragen:

- Erfolgt eine Protokollierung der Übermittlungen? Sind die datenschutzrechtlichen Vorschriften für die Protokolldaten erfüllt?
- Erfolgt ein Hinweis bzw. eine Verpflichtung auf die Zweckbindung der erhaltenen Daten (vgl. §§ 15 Abs. 2 S. 3, 16 Abs. 5 S. 2 DSG M-V, § 78 Abs. 2 SGB X, § 4b Abs. 6 BDSG)?
- Kann eine Zweckbindung technisch überwacht werden, und können Daten, die nicht übermittelt werden dürfen, von der Übermittlung ausgeschlossen werden?
- Wird die Richtigkeit der Empfängeradresse verifiziert? Gibt es Filter für mögliche Adressaten bzw. Adressatenkreise, an die keinesfalls eine Übermittlung erfolgen darf (z. B. durch Sperrung von Empfängeradressen außerhalb des Hauses in einem E-Mail-System)?
- Filter für ausgehende Informationen: Gibt es Mechanismen, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. durch rückstandslose Beseitigung von personenbezogenen (Zusatz-)Daten bei möglicher Herausgabe (z. B. detaillierte Informationen über den Autor in Word-Dokumenten, automatisierte Weitergabe von Zusatzinformationen bei HTTP-Kommunikation durch Voreinstellungen im Webbrowser)?
- Gibt es Maßnahmen zur Steigerung der Sensibilität der Verarbeiter, um diese vor unbedachten/unerlaubten Übermittlungen zu schützen?

- Sind bei der Übermittlung an Dritte Maßnahmen vorgesehen, um Daten zu anonymisieren oder pseudonymisieren (siehe auch Abschnitt 1.2)?

2.1.3.3 Löschung nach Wegfall der Erfordernis (§ 13 DSG M-V)

Untersuchungsgegenstand:
Wird sichergestellt, dass Daten nach Wegfall der Erfordernis gelöscht werden oder ein Personenbezug abgetrennt wird?

In diesem Zusammenhang wichtige Fragen:

- Sind Fristen (Löschungsfristen, Wiedervorlagefristen) zu beachten? Wie wird deren Beachtung sichergestellt?
- Siehe auch Abschnitt 4.3.2 zu Löschung.

Siehe auch Abschnitt 1.2 zur Anonymisierung/Pseudonymisierung.

2.2 Einhaltung allgemeiner datenschutzrechtlicher Grundsätze und Pflichten

2.2.1 Zweckbindung (§ 10 Abs. 2 DSG M-V, § 67c Abs. 1 SGB X) und Zweckänderung (§ 10 Abs. 3 DSG M-V, § 67c Abs. 2 SGB X, § 28 Abs. 2, 3 BDSG)

Untersuchungsgegenstand:
Wie wird sichergestellt, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden bzw. dass eine Zweckänderung nur innerhalb des gesetzlichen Rahmens erfolgt?

In diesem Zusammenhang wichtige Fragen:

- Wie wird der Zweck dokumentiert, für den die personenbezogenen Daten erhoben werden?
- Gibt es eine revisionssichere Protokollierung der Verarbeitung, um Zweckänderungen nachweisen zu können?
- Wird die Zweckbindung dadurch garantiert, dass personenbezogene Daten vermieden werden oder ihre Verkettbarkeit und damit eine zweckändernde Nutzung erschwert oder verhindert wird?
- Gibt es eine Kennzeichnung von Datensätzen mit entsprechenden Zwecken sowie Zugriffsrechte, die andere Auswertungsmethoden oder eine Übermittlung einschränken?

2.2.2 Erleichterung der Umsetzung des Trennungsgebotes nach § 5 Abs. 3 DSG M-V

Untersuchungsgegenstand:
Wird das Trennungsgebot unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Wie ist das Trennungsgebot technisch umgesetzt?
- Gibt es Verfahren zur automatisierten Pseudo-/Anonymisierung (siehe auch Abschnitt 1.2)?
- Werden schutzwürdige Belange geprüft, die einer Weitergabe von untrennbar verbundenen Daten entgegenstehen?

2.2.3 Gewährleistung der Datensicherheit (§§ 21, 22 DSG M-V, Anlage zu § 9 BDSG)

Untersuchungsgegenstand:
Werden die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit durch das Produkt selbst ergriffen bzw. enthält das Produkt Hinweise zur Umsetzung der erforderlichen Maßnahmen?

Dazu Komplex 3

2.3 Datenverarbeitung im Auftrag (§ 4 DSG M-V, § 80 SGB X, § 11 BDSG)

Frage: Erfolgt eine Datenverarbeitung im Auftrag bzw. ist eine solche vorgesehen?

Untersuchungsgegenstand:
Sind die Voraussetzungen für eine Datenverarbeitung im Auftrag gegeben?

In diesem Zusammenhang wichtige Fragen:

- Ist eine Verarbeitung der Daten durch einen externen Dritten zulässig (vgl. dazu § 203 StGB, § 80 Abs. 5 SGB X)?
- Gibt es einen Vertrag oder einen Mustervertrag zur Datenverarbeitung im Auftrag?
- Entspricht der Vertrag den Anforderungen der einschlägigen Vorschriften (§ 4 Abs. 1 Satz 4 DSG M-V, § 80 SGB X, § 11 Abs. 2 BDSG)
- Wie wird die Kontrolle des Auftragnehmers durch den Auftraggeber unterstützt?
- Wie wird das Recht des Auftraggebers unterstützt, dem Auftragnehmer Weisungen zu erteilen?
- Wie sind die technischen und organisatorischen Maßnahmen umgesetzt, die die Bindung des Auftragnehmers an die Weisungen der Daten verarbeitenden Stelle sicherstellen?

2.4 Voraussetzungen besonderer technischer Verfahren

2.4.1 Handelt es sich um ein gemeinsames Verfahren oder um ein Abrufverfahren (§ 3 Abs. 8, 9, § 17 DSG M-V, § 79 SGB X, vgl. § 10 BDSG)?

Untersuchungsgegenstand:
Werden Daten in einem gemeinsamen Verfahren oder einem automatisierten Abrufverfahren an Dritte übermittelt, und sind die Voraussetzungen für die Einrichtung eines solchen Verfahrens erfüllt?

In diesem Zusammenhang wichtige Fragen:

- Ist ein automatisiertes Abrufverfahren unter den Beteiligten zulässig (vgl. insbesondere § 79 SGB X)?
- Inwieweit ist die Einrichtung des Verfahrens im Hinblick auf die schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen?
- Wie wird die Zuständigkeit der Verfahrensbeteiligten für einzelne Verfahrensteile festgelegt und die Kontrollierbarkeit der Zulässigkeit gewährleistet?
- Inwiefern sind Festlegungen von Fachaufsichtsbehörden zu Zwecken, Art der übermittelten Daten, Empfängern sowie technischen und organisatorischen Maßnahmen zu beachten (§ 10 Abs. 2 BDSG, § 79 Abs. 2 SGB X)?
- Inwiefern bestehen Unterrichtungspflichten von Aufsichtsbehörden (§ 10 Abs. 3 BDSG, § 79 Abs. 3 SGB X)?
- Wie sind die Protokollierungserfordernisse für Datenübermittlungen und Abrufe (z. B. § 10 Abs. 4 BDSG, § 79 Abs. 4 SGB X) umgesetzt?

2.4.2 Weitere besondere technische Verfahren

Untersuchungsgegenstand:
Wie wird die Beachtung zusätzlicher spezieller materiell-rechtlicher Anforderungen beim Einsatz besonderer technischer Verfahren sichergestellt?

In diesem Zusammenhang wichtige Fragen:
Sind besondere Anforderungen einschlägig, z. B.

- Zulässigkeit von mobilen personenbezogenen Datenverarbeitungssystemen (§ 36 DSG M-V, § 6c BDSG)
- Automatisierte Einzelentscheidungen (§ 12 DSG M-V, § 6a BDSG, § 67b Abs. 4 SGB X)
- Videoüberwachung und -aufzeichnung (z. B. § 37 DSG M-V, § 6b BDSG)
- Fernmessen, Fernwirken (§ 38 DSG M-V)
- Siehe auch Abschnitte 3.2.3.1(mobile Datenverarbeitungssysteme), 3.2.3.2 (Videoüberwachung), 3.2.3.3 (automatisierte Einzelentscheidungen).

2.5 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit ergeben?

Komplex 3: Technische und organisatorische Maßnahmen:

Begleitmaßnahmen zum Schutz der Betroffenen

3.1 Abstrakte Pflichten

3.1.1 § 21 DSG M-V (bzw. § 78a SGB X oder § 9 BDSG jeweils mit Anhang)

3.1.1.1 Maßnahmen, um Unbefugten den Zugang zu Datenträgern zu verwehren

Untersuchungsgegenstand:
Wird durch geeignete Maßnahmen Unbefugten der Zugang zu Datenträgern verwehrt?

In diesem Zusammenhang wichtige Fragen:

- Unterliegen die Zugangskontrollmechanismen datenschutzrechtlichen Regelungen (insb. bei Chipkarten, Token, biometrische Verfahren durch die Verarbeitung von Sekundärdaten)?
- Ist die Vergabe von Zugangsrechten adäquat und revisionssicher?

3.1.1.2 Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 21 Abs. 2 Nr. 1 DSG M-V)

Untersuchungsgegenstand:
Wurden geeignete Maßnahmen ergriffen, um zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können?

In diesem Zusammenhang wichtige Fragen:

- Sind Methoden zur Authentisierung realisiert (insb.: Ist ein Passwortschutz sicher umgesetzt, z. B. durch Einmalpasswörter (z. B. Challenge-Response), zeitabhängige Passwörter, Schutz gegen Ausspähung oder Erraten, Prüfung der Länge, Vergabe/Wechsel durch Nutzer selbst, Prüfung von Komplexitätsanforderungen, automatisierte Beschränkung des Gültigkeitszeitraumes, Einschränkung der Wiederverwendbarkeit, Sperrmöglichkeit bei Fehlversuchen)?
- Unterliegen die Zugangs- und Zugriffskontrollmechanismen datenschutzrechtlichen Regelungen (insb. bei Chipkarten, Token, biometrische Verfahren durch die Verarbeitung von Sekundärdaten)?
- Werden Systemadministrationsebene und Anwendungsebene ausreichend getrennt?
- Können und werden ausreichend detaillierte Zugriffsrechte vergeben? Sind ggf. Rollenkonzepte (etwa besondere Berechtigungen von Systemadministration und Kontrollrollen wie Leitung, Datenschutzbeauftragtem oder Revision) berücksichtigt?

- Wie wird die Vergabe dieser Rechte dokumentiert (z. B. durch eine Protokolldatei, ein externes Tool)? Wer hat Zugriff auf die Dokumentation? Wie wird die Einhaltung der Aufbewahrungsfrist der Dokumentation sichergestellt (vgl. auch Abschnitt 3.3)?
- Werden Firewalls oder Intrusion Detection & Response Systeme wirkungsvoll gegen unbefugte Zugriffe eingesetzt?
- Sind verwendete Verschlüsselungsverfahren adäquat umgesetzt (s. a. Abschnitt 3.2.1)
- Sind Maßnahmen zum Löschen/Sperren/Zerstören der Daten oder Geräte bei unbefugtem Öffnen/Eingriff (z. B. bei Chipkarten) vorgesehen?
- Werden geeignete Mechanismen eingesetzt, um eine absichtliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. Kennzeichnung der Daten für Sensibilisierung (z. B. „VS") oder Nachverfolgbarkeit (z. B. steganographische Markierung)?
- Filter für ausgehende Informationen: Gibt es Mechanismen, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. durch rückstandslose Beseitigung von personenbezogenen (Zusatz-)Daten bei möglicher Herausgabe (z. B. detaillierte Informationen über den Autor in Word-Dokumenten, automatisierte Weitergabe von Zusatzinformationen bei HTTP-Kommunikation durch Voreinstellungen im Webbrowser)? (siehe auch Abschnitt 2.2.3)
- Werden Mechanismen eingesetzt, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. durch die Reduktion des Einsichtwinkels bei Monitoren oder das Vermeiden von Abstrahlung bei Monitor, (Funk-)Tastatur, Maus usw. (Tempest)?
- Wird die rückstandslose Beseitigung personenbezogener Daten von Datenträgern/Geräte(teile)n (z. B. Festplatten, Schreibbändern, Faxbauteilen), die an Dritte weitergegeben werden können, gewährleistet oder unterstützt?
- Wurden Maßnahmen ergriffen, um die Sensibilität der Verarbeiter zu steigern (z. B. automatisierte Warnhinweise etc.)?
- Zu technischen Fragen des Löschens siehe auch Abschnitt 4.3.2.
- Zu technischen Fragen der Sicherung der Übermittlung siehe auch Abschnitt 2.2.3.
- Zu technischen Fragen der Sicherung der Integrität siehe auch Abschnitt 3.1.1.4.

3.1.1.3 Protokollierung von Datenverarbeitungsvorgängen (§§ 21 Abs. 2 Nr. 5, 22 Abs. 2 DSG M-V, § 10 Abs. 4 BDSG, § 79 Abs. 4 SGB X)

Untersuchungsgegenstand:
Werden Daten und Datenverarbeitungsvorgänge (u. a. Eingabe, Veränderung, Weitergabe, Abruf, Löschung etc.) protokolliert, wenn dies rechtlich erforderlich ist?

In diesem Zusammenhang wichtige Fragen:

- Welche der Daten werden ausschließlich automatisiert gespeichert?

- Wie lassen sich die Protokolldaten auswerten? Gibt es automatisierte Auswertungsroutinen? Nach welchen Kriterien? Welche Zugriffsrechte gibt es?
- Ist eine Vollprotokollierung erforderlich? Sind Stichproben ausreichend? Ist der Umfang der Stichprobe konfigurierbar?
- Wurden die datenschutzrechtlichen Anforderungen für die Verarbeitung der Protokolldaten geprüft? Sind ggf. spezielle Regelungen zu beachten (z. B. bei Aufzeichnung von Telefonaten, Videoüberwachung)?
- Wann werden die Protokolldaten gelöscht (zeitgesteuert statt speicherplatzgesteuert)?
- Sind gesetzliche Speicherfristen für die Protokolldatenbestände zu beachten (z. B. § 22 Abs. 4 DSG M-V), oder sind die Speicherfristen durch die Anwender festzulegen? Wie können sie in diesem Fall konfiguriert werden?
- Welche Maßnahmen wurden zum Schutz überlaufender Protokolldateien unternommen?

3.1.1.4 Weitere technische und organisatorische Maßnahmen (§ 21 Abs. 1, Abs. 2 Nr. 1-3 DSG M-V)

Untersuchungsgegenstand:
Sind durch die bisher untersuchten oder weitere Mechanismen die Sicherheitsziele wie Vertraulichkeit, Integrität und Verfügbarkeit im notwendigen Umfang gewährleistet?

In diesem Zusammenhang wichtige Fragen:

- Kommen Maßnahmen zur Sicherstellung der Integrität von Daten und Programmen (z. B. Virenschutz, Prüfsummen, digitale Signatur, Kapselung von Programm(teil)en, Deaktivieren von möglicherweise schädigenden Funktionen (z. B. ActiveX)) zur Anwendung, und sind sie adäquat umgesetzt?
- Werden ausreichende Maßnahmen zur Sicherstellung der Verfügbarkeit (z. B. Sicherheitskopien in erforderlichem Umfang mit geeigneter Lagerung, ggf. unterbrechungsfreie Stromversorgung, Zugangs-, Zutritts- und Zugriffsrechte auch für Stellvertreter) ergriffen?
- Wird die Vertraulichkeit von Datenbeständen bei Speicherung und Übermittlung ausreichend sichergestellt?
- zu technischen Fragen der Verschlüsselung siehe auch Abschnitt 3.2.1

3.1.2 Erleichterung der Vorabkontrolle (§ 19 Abs. 2 DSG M-V, vgl. § 4d Abs. 5, 6 BDSG, Art. 20 EU-DSRL)

Untersuchungsgegenstand:
Wird eine eventuell notwendige Vorabkontrolle durch das Produkt (inkl. Beschreibung) unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Werden Test und Freigabe unterstützt (z. B. durch die Mitlieferung von relevanten und umfassenden Testdaten/fällen, Hinweise zu Prüfungen, Bereitstellung von Formularen etc.)
- Werden Werkzeuge (Formulare, interaktive Tools) zur Erstellung von individuell zugeschnittenen Dokumentationen und Konzepten bereitgestellt?

3.1.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses (§ 18 DSG M-V, vgl. Meldepflicht §§ 4d, 4e BDSG)

Untersuchungsgegenstand:
Wird durch das Produkt (inkl. Beschreibung) die Erstellung von Verfahrensverzeichnissen oder die Meldung von Verfahren unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Werden Werkzeuge (Formulare, interaktive Tools) zur Erstellung von individuell zugeschnittenen Dokumentationen und Konzepten bereitgestellt?
- Werden prototypische Dokumentationen und Konzepte bereitgestellt?

3.1.4 Sonstige Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten (§ 20 DSG M-V, vgl. § 81 Abs. 4 SGB X, §§ 4e, 4f BDSG)

Untersuchungsgegenstand:
Wird der behördliche Datenschutzbeauftragte bei der Wahrnehmung seiner Pflichten unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Werden Test und Freigabe unterstützt (z. B. durch die Mitlieferung von relevanten Testdaten, Hinweise zu Prüfungen, Bereitstellung von Formularen etc.)?
- Wird die datenschutzrechtliche Kontrolle des Produktes und seines Betriebes durch geeignete Maßnahmen (z. B. Bereitstellung adäquater Dokumentation, Hilfsmittel bei der Auswertung von Protokolldaten etc.) unterstützt?

3.2 Spezifische Pflichten

3.2.1 § 22 DSG M-V, z. B. Verschlüsselung bei tragbaren Computern

Untersuchungsgegenstand:
Wird eine bestehende Pflicht zur Verschlüsselung von Datenbeständen adäquat umgesetzt?

In diesem Zusammenhang wichtige Fragen:

- Werden anerkannte und offengelegte Verschlüsselungsverfahren eingesetzt?
- Sind Schlüsselgenerierung und Schlüsselmanagement adäquat realisiert?
- Wurden ausreichende Schlüssellängen eingesetzt?
- Wurden Maßnahmen vorgesehen, falls sich die verwendeten Verfahren oder Schlüssellängen als unzulänglich herausstellen (z. B. Wechsel des Verfahrens oder seiner Komponenten, umschlüsseln etc.)

3.2.2 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens (§ 3 Abs. 4 Satz 2 Nr. 9 DSG M-V, § 67 Abs. 8a SGB X, § 3 Abs. 6a BDSG)

Untersuchungsgegenstand:
Wird eine gebotene oder geforderte Pseudonymisierung erleichtert oder unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Ist eine Pseudonymisierung von Daten für Zwecke der Forschung (§ 34 Abs. 1 DSG M-V) geboten?
- Ist eine Pseudonymisierung von Daten im Rahmen der Datenverarbeitung und Übermittlung gefordert oder geboten?
- Siehe auch Abschnitt 1.2.

3.2.3 Technische Umsetzung von Transparenz- und Beteiligungsgeboten für die Betroffenen bei besonderem Technikeinsatz

3.2.3.1 bei Chipkarten (§ 36 Abs. 2, 3 DSG M-V, § 6c BDSG)

Untersuchungsgegenstand:
Werden die besonderen Vorschriften zur Information der Betroffenen bei der Verwendung personenbezogener Speicher- und Verarbeitungsmedien umgesetzt?

In diesem Zusammenhang wichtige Fragen:

- Sind die Verarbeitungsgeräte so gestaltet, dass Verarbeitungsvorgänge sowie Art und Umfang personenbezogener Daten jederzeit erkennbar sind?

3.2.3.2 bei Videoüberwachung (§ 37 Abs. 2 S. 1 DSG M-V, § 6b Abs. 2, 4 BDSG)

Untersuchungsgegenstand:
Werden die gesetzlichen Vorgaben umgesetzt?

In diesem Zusammenhang wichtige Fragen:

- Wird die Tatsache einer Aufzeichnung den Betroffenen erkennbar gemacht?
- Wird die Einhaltung der gesetzlichen Löschungsfristen für Aufzeichnungen sichergestellt?
- Werden geeignete Sicherungsmaßnahmen zum Schutz der Aufzeichnungen ergriffen? (siehe auch Abschnitt 3.1.1.2)

3.2.3.3 bei automatisierten Einzelentscheidungen (§ 12 S. 2 Nr. 2 DSG M-V, § 6a Abs. 2 Nr. 2, Abs. 3 BDSG)

Untersuchungsgegenstand:
Werden die gesetzlichen Vorgaben umgesetzt?

In diesem Zusammenhang wichtige Fragen:

- Gibt es Rechtsgrundlagen für automatisierte Einzelentscheidungen, die sich ausschließlich auf die Ergebnisse automatisierter Verfahren stützen?
- Auf welche Weise können Betroffene ihre besonderen persönlichen Interessen geltend machen?

3.3 Sonstige Anforderungen

Untersuchungsgegenstand:
In welcher Weise werden Anwender bei der Erfüllung ihrer sonstigen, sich aus dem Landesdatenschutzgesetz ergebenden Pflichten unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Gibt es Anleitungen, um die nötigen Unterlagen zu erstellen?
- Wie werden die Erstellung des Sicherheitskonzeptes und der Risikoanalyse (nach §§ 21, 22 Abs. 5 DSG M-V) unterstützt? (siehe auch Abschnitte 3.1.2, 3.1.4)
- Wie werden Test und Freigabe (nach § 19 Abs. 1 DSG M-V) sowie deren Protokollierung und Dokumentation unterstützt? (siehe auch Abschnitte 3.1.2, 3.1.4)
- Wie wird die Erstellung der Verfahrensdokumentation (nach §§ 18, 21 Abs. 2 Nr. 6 DSG M-V) unterstützt, insbesondere die Darstellung des Verfahrenszwecks (nach § 18 Abs. 1 Nr. 2 DSG M-V, siehe auch Rechtsgrundlagen nach Abschnitt 2) sowie die sonstige Verfahrensbeschreibung (nach § 18 DSG M-V, siehe auch Abschnitte 3.1.2, 3.1.3, 3.1.4)? Wie wird dokumentiert, welchen Personen welche Nutzungsrechte an welchen informationstechnischen Geräten, Programmen und automatisierten Dateien für welche Zeiträume gewährt wurden (z. B. durch die Bereitstellung von Werkzeugen zur Dokumentation der Nutzungsrechtevergabe und Administration)? Wie werden dabei die Aufbewahrungsfrist von mindestens 5 Jahren und die Revisionssicherheit gemäß § 21 Abs. 2 Nr. 5 DSG M-V sichergestellt?
- Wie wird dokumentiert, welche Personen für welche Zeiträume befugt sind, Änderungen an der Funktionsweise von informationstechnischen Geräten, an den Programmen, an der Speicherorganisation der automatisierten Dateien und den Nutzungsrechten vorzunehmen (s. § 22 Abs. 2 DSG M-V)? Wie werden dabei die Aufbewahrungsfrist von mindestens 5 Jahren und die Revisionssicherheit gemäß § 21 Abs. 2 Nr. 5 DSG M-V sichergestellt?

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit ergeben?

Komplex 4: Rechte der Betroffenen

4.1 Aufklärung und Benachrichtigung (§§ 23, 9 Abs. 3, 4 DSG M-V, vgl. § 33 BDSG)

Untersuchungsgegenstand:
Inwieweit werden Aufklärung und Benachrichtigung von Betroffenen vom IT-Produkt geleistet oder unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Gibt es besondere Maßnahmen, um die Transparenz der Datenverarbeitung für den Betroffenen sicherzustellen?
- Können dem Betroffenen einzelne Datenverarbeitungsschritte (z. B. Übermittlungen in Form eines „Einzelnutzungsnachweises") verdeutlicht werden?

4.2 Auskunft (§ 24 DSG M-V, §§ 25, 83 SGB X, § 34 BDSG, Art. 12 EU-DSRL)

Untersuchungsgegenstand:
Wird eine Auskunft vom IT-Produkt angemessen unterstützt?

In diesem Zusammenhang wichtige Fragen:

- Gibt es eine automatisierte Auskunftsbearbeitung durch das IT-Produkt, so dass Hemmschwellen beim Betroffenen und zeitliche Verzögerungen gering sind?
- Sind alle Daten zur Auskunftserteilung leicht auffindbar; gibt es Hilfsmittel dazu?
- Werden untrennbare Verknüpfungen mit personenbezogenen Daten anderer Betroffener vermieden?
- Gibt es eine Protokollierung bei der Übermittlung personenbezogener Daten?
- In welcher Weise erfolgt eine Authentisierung des Auskunftsberechtigten?
- Erfasst die Auskunftsmöglichkeit den gesamten Auskunftsanspruch [gespeicherte Daten, Zweck und Rechtsgrundlage, Herkunft und Empfängerkreis (Auftragnehmer, Datenveränderung), Funktionsweise (logischer Aufbau)] von automatisierten Verfahren?

4.3 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung (§§ 13, 25 DSG M-V, § 84 SGB X, § 35 BDSG)

4.3.1 Berichtigung

Untersuchungsgegenstand:
In welcher Form leistet oder unterstützt das IT-Produkt die Berichtigung von Daten?

In diesem Zusammenhang wichtige Fragen:

- Gibt es automatisierte Berichtigungsbearbeitung vom IT-Produkt?
- Wie wird eine korrekte und unverzügliche Umsetzung der Berichtigung sichergestellt?
- Wie wird eine automatisierte Berichtigung qualitätsgesichert?
- Wie werden Berichtigungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet?

4.3.2 Vollständige Löschung

Untersuchungsgegenstand:
Wie ist die Löschung realisiert?

In diesem Zusammenhang wichtige Fragen:

- Wird vollständig und irreversibel gelöscht?
- Geschieht dies durch physikalisches Löschen auf allen Medien (ohne zusätzliche Kopien, etwa innerhalb einer Funktion zum Rückgängigmachen von Löschungen)?
- Ist eine Selektivität des Löschens möglich (z. B. problematisch bei CD-ROM)?
- Wird durch Überschreiben gelöscht? Ist die Umsetzung (z. B. Anzahl der Überschreibvorgänge) adäquat?
- Wie ist die Umsetzung der Löschung auf Backup-Medien realisiert?
- Wie werden Löschungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet?
- Wie werden Lösch- und Prüffristen (Wiedervorlage) realisiert oder unterstützt?
- Wie werden Löschungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet?

4.3.3 Sperrung

Untersuchungsgegenstand:
Wie wird eine Sperrung von Daten umgesetzt?

In diesem Zusammenhang wichtige Fragen:

- Gibt es eine Möglichkeit, die Datensätze so zu kennzeichnen, dass sie für die normale Verarbeitung nicht zur Verfügung stehen, aber gleichwohl gespeichert bleiben?
- Wie wird dies gewährleistet?
- Wie wird die Sperrung und ggf. Aufhebung der Sperre protokolliert (Zeitpunkt, Auftraggeber etc.)? (siehe auch Abschnitt 3.1.1.3)

4.3.4 Einwand bzw. Widerspruch gegen die Verarbeitung (§ 25 Abs. 3 DSG M-V, § 84 Abs. 1a SGB X, § 35 Abs. 5 BDSG)

Untersuchungsgegenstand:
Gibt es eine technische Unterstützung des Widerspruchsrechtes?

In diesem Zusammenhang wichtige Fragen:

- Wie werden Widersprüche an Empfänger vorangegangener Datenübermittlungen weitergeleitet?

4.3.5 Gegendarstellung (§ 35 Abs. 6 S. 2, 3 BDSG)

Untersuchungsgegenstand:
Wie wird realisiert, dass auf Verlangen des Betroffenen dessen Gegendarstellung beigefügt wird?

4.4 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit ergeben?

B. Anforderungsprofil für Protokolldaten

Für die Bewertung der Verarbeitung von Protokolldaten sind nicht immer sämtliche Anforderungen aus dem Allgemeinen Anforderungsprofil einschlägig. Im Folgenden sind die wichtigsten Anforderungen dargestellt, die bei der Bewertung der Protokolldaten zu beachten sind. Dieser Katalog ist nicht abschließend, im Einzelfall können auch weitere Anforderungen zu prüfen sein.

Komplex 1:

- **Datenvermeidung und Datensparsamkeit**

Wird der Grundsatz der Datenvermeidung und Datensparsamkeit berücksichtigt, d. h., werden Protokolldaten nur in dem erforderlichem Maß erhoben und wird – falls dieser nicht erforderlich ist – auf den Personenbezug verzichtet?

- **Transparenz**

Ist der Umfang der Protokollierung für die Betroffenen hinreichend transparent?

Komplex 2:

- Auf welcher Rechtsgrundlage sind die Erhebung und Speicherung der Protokolldaten zulässig? Sind die Voraussetzungen der Rechtsgrundlage erfüllt?

- Wird die Einhaltung der Zweckbindung für Protokolldaten (§ 10 Abs. 6 DSG M-V, § 14 Abs. 4 BDSG) durch das Produkt unterstützt?

- Gibt es gesetzliche Aufbewahrungsfristen für die Protokolldaten? Werden die Protokolldaten nach Ablauf der Frist bzw. nach Wegfall der Erfordernis gelöscht?

Komplex 3:

- Fragestellungen aus 3.1.1.3

- Sind die Protokolldaten ausreichend gegen unbefugte Zugriffe, gegen Manipulationen und gegen Verlust geschützt? Wer kann die Zugriffsbefugnisse verwalten (wichtig für die Manipulationsresistenz sowie bei gemeinsamen Verfahren und Abrufverfahren).

- Können anhand der protokollierten Daten die in § 22 Abs. 4 DSG M-V genannten Informationen über die Daten verarbeitende Person, den Zeitpunkt sowie die Art und Weise der Speicherung, Verarbeitung und Übermittlung ermittelt werden? Insbesondere: Kann bei ändernden Zugriffen ermittelt werden, welche Datenbestände vor der Änderung verfügbar waren? Kann bei lesenden Zugriffen ermittelt werden, welche Daten der Daten verarbeitenden Person angezeigt bzw. übermittelt werden ? (Dies ist nicht evident, wenn lediglich Datenbankbefehle protokolliert werden.)

- Sind ggf. unterschiedliche Speicherfristen mit folgender Löschung für verschiedenartige Protokolldaten, die aber durch ein System verarbeitet werden, technisch darstellbar (vgl. z. B. § 22 Abs. 4 DSG M-V)?

Komplex 4

- Sind die Protokolldaten im Sinne des Komplexes 4 verarbeitbar (selektive Löschung von Einzeldaten, Beauskunftung, Berichtigung, Sperrung, Einwand)? Dies betrifft zum einen die Protokolldaten der Daten verarbeitenden Person selbst (in erster Linie Mitarbeiterinnen und Mitarbeiter) als Betroffene, zum anderen die Daten der Betroffenen (Bürgerinnen und Bürger), deren (Primär-)Daten verarbeitet und als Teile der Protokolldaten erhoben, gespeichert und verarbeitet werden.