Rechtliches und Technisches Gutachten

Einhaltung datenschutzrechtlicher Anforderungen
durch das IT-Produkt

- Verfahrensregister 2.1 -

der FinanzIT GmbH, Hannover

Stand:
August 2006

Änderungs- und Versionsverwaltung des Gutachtens

Datum	Beschreibung	Kommentar
2006	Erstellung	
29.08.06	Änderungen	
31.08.06	Änderungen/Ergänzungen	

Inhaltsverzeichnis

A. Einleitung

1 Mit dem vorliegenden Gutachten beabsichtigt die FinanzIT GmbH (nachfolgend FinanzIT bezeichnet) ihr IT-Produkt „Verfahrensregister" für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) zertifizieren zu lassen.

Die Vorlage des Gutachtens beim ULD erfolgt durch den Auftraggeber.

Dem Gutachten wird der Anforderungskatalog in der Version 1.2 zu Grunde gelegt.

Mit dem Gutachten soll der Nachweis geführt werden, dass das Produkt den datenschutzrechtlichen Anforderungen zur Verleihung eines Gütesiegels für IT-Produkte erfüllt.

B. Zeitpunkt der Prüfung

2 Die Prüfung des Verfahrens fand im Juli 2006 statt.

C. Detaillierte Bezeichnung des Produktes

I. Hintergrund

3 Zur Wahrung des Rechts auf informationelle Selbstbestimmung und zur Sicherung einer ordnungsgemäßen Verarbeitung personenbezogener Daten hat der Gesetzgeber eine Meldepflicht für Verfahren automatisierter Verarbeitung personenbezogener Daten vorgesehen. Die Pflicht zur Meldung der entsprechenden Verfahren gegenüber der zuständigen Aufsichtsbehörde für den Datenschutz ergibt sich aus § 4d BDSG. Zusammen mit der im Rahmen der Umsetzung der EG-Datenschutzrichtlinie[1] (Art. 20) eingeführten Vorabkontrolle stellt die Meldepflicht für öffentliche und nichtöffentliche Stellen ein Element des Datenschutzes dar, der eine Transparenz bzgl. der Verarbeitung personenbezogener Daten herstellen soll.

4 Die Meldepflicht bezieht sich nur auf Verfahren automatisierter Verarbeitungen. Gemeint sind damit Verfahren, mit denen personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen erhoben, verarbeitet oder genutzt werden[2].

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

2 Vgl. hierzu und zum sprachlich etwas missglückten Terminus *Walz*, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Auflage 2003, § 4d Rdnr. 16

5 Welche Angaben „gemeldet" werden müssen, ergibt sich im Einzelnen aus § 4e BDSG. Demnach sind folgende Angaben gegenüber der zuständigen Aufsichtsbehörde zu machen:

6
1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

7 Dabei hat die Meldung an das Verfahrensregister vor Inbetriebnahme des meldepflichtigen Verfahrens zu erfolgen. Gleiches gilt für Änderungen.

8 Um keine übermäßigen bürokratischen Aufwand entstehen zu lassen und dem Gedanken der Selbstkontrolle von Daten verarbeitenden Stellen durch selbst bestellte behördliche oder betriebliche Datenschutzbeauftragte Rechnung zu tragen, entfällt die Meldepflicht nach § 4d Abs. 2 BDSG dann, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat. Dies bedeutet jedoch nicht, dass der eigentliche Sinn und Zweck der Meldepflicht komplett entfällt. Vielmehr muss die verantwortliche Stelle nunmehr dem betrieblichen bzw. behördlichen Beauftragten für den Datenschutz eine Übersicht der in § 4e Satz 1 genannten Angaben, also den Inhalten der Meldepflicht, zur Verfügung zu stellen (§ 4g Abs. 2 Satz 1 BDSG). Die verantwortliche Stelle muss die jeweiligen Angaben daher trotzdem zusammen- und bereitstellen.

9 Darüber hinaus sind dem Beauftragten für den Datenschutz auch Angaben über die zugriffsberechtigten Personen zur Verfügung zu stellen. Während das BDSG 77 das Zusammenstellen und Führen der Verfahrensübersicht noch als Aufgabe des betrieblichen bzw. behördlichen Datenschutzbeauftragten konstituierte, sahen das BDSG 90 sowie auch die aktuelle Fassung des BDSG vor, dass das Zusammenstellen der Verfahrensübersicht mit den entsprechenden Inhalten der Meldepflicht i.S.d. § 4e BDSG von der verantwortlichen Stelle durchzuführen ist. Dem Datenschutzbeauftragten sollen diese Informationen in einer Übersicht zur Verfügung gestellt werden, es ist nicht seine Aufgabe, diese Informationen selbst zusammen zu tragen, auch wenn dies praktisch häufig der Fall ist.

10 Genau diese Arbeitsschritte soll das Produkt der FinanzIT der verantwortlichen Stelle erleichtern und zudem auch die Arbeit des betrieblichen bzw. behördlichen Datenschutzbeauftragten erleichtern helfen. Mit der Verfahrensregister-Software der FinanzIT werden die jeweiligen Fachabteilungen bzw. verantwortlichen Personen in die Lage versetzt auf digitalem Wege die dem betrieblichen bzw. behördlichen Datenschutzbeauftragten nach § 4g Abs. 2 Satz 1 BDSG zu erteilenden Informationen zur Verfügung zu stellen und ggf. eine Freigabe des Verfahrens zu erhalten.

11 Für die Vergabe eines Gütesiegels für IT-Produkte durch ULD sind (neben den Regelungen des BDSG) vor allem auch die Vorschriften des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (LDSG-SH) zu beachten. Das LDSG-SH enthält in § 7 LDSG-SH eine Regelung zur Meldepflicht und zum Führen eines Verfahrensverzeichnis, das weitestgehend den Regelungen des BDSG entspricht. Die Unterschiede sind eher marginal. Das LDSG-SH geht ebenfalls davon aus, dass die verantwortliche Stelle das Verfahrensverzeichnis erstellt. Allerdings sieht § 10 LDSG-SH vor, dass der behördliche Datenschutzbeauftragte das Verfahrensverzeichnis führt und zur Einsicht bereit hält. Dies ist jedoch nicht so zu verstehen, dass er auch für die Erstellung verantwortlich ist[3]. Er ist lediglich für die Zusammenstellung der Verfahrensverzeichnisse in einer Übersicht erforderlich, die ggf. für die Einsichtnahme Dritter bereit zu halten ist. Im Ergebnis sind daher die Regelungen im LDSG-SH zu denen im BDSG im Wesentlichen inhaltsgleich. Es bestehen leichte Differenzen in den zu treffenden Angaben i.S.d. § 4e Nr 1 bis 9 BDSG bzw. § 7 Abs. 1 Nr. 1 bis 8 LDSG-SH. Diese sind jedoch nicht inhaltlich bedeutender Natur. Vorab kann hier gleich erwähnt werden, dass das Produkt der FinanzIT sich an den Inhalten

3 Vgl. ULD, Hinweise zur Anwendung des Schleswig-Holsteinischen Gesetzes zum Schutze personenbezogener Informationen, Anm. zu § 10 Abs. 4

der Meldepflicht i.S.d. § 4e BDSG orientiert, da das Produkt in mehreren Bundesländern Nord- und Ostdeutschland zum Einsatz kommt. Einzig inhaltlich relevanter Unterschied ist, dass § 7 Abs. 1 Nr. 7 LDSG-SH vorsieht, dass die datenschutzrechtliche Beurteilung des behördlichen Datenschutzbeauftragten zum Verfahrensverzeichnis zu nehmen, soweit eine solche vorliegt, was nach § 4e BDSG nicht vorgesehen ist. Die Tatsache, dass dies beim Prüfprodukt nicht ausdrücklich vorgesehen ist, ist jedoch als unschädlich anzusehen, da § 7 Abs. 1 Nr. 7 LDSG-SH keine absolute Pflichtvorschrift ist und zudem eine datenschutzrechliche Bewertung auch anderweitig zum Verfahrensverzeichnis des Datenschutzbeauftragten genommen werden kann.

II. Produktbeschreibung

12 Das IT-Produkt „Verfahrensregister" stellt die Möglichkeit zur Verfügung, Prozesse zu dokumentieren, bei denen personenbezogene Daten gespeichert werden können. Es dient dem behördlichen bzw. betrieblichen Datenschutzbeauftragten als Grundlage für Prüfung der Zulässigkeit der Erfassung, Verarbeitung und Nutzung personenbezogener Daten. Daher müssen die Angaben so detailliert sein, dass dem Datenschutzbeauftragten ein Einstieg in die Prüfung ermöglicht wird und er aufgrund der Beschreibung beurteilen kann, ob eine Vorabkontrolle gemäß § 4d Abs. 5 und 6 BDSG erforderlich ist oder nicht.

13 Es handelt sich in dieser Form nicht um ein „öffentliches Verfahrensregister", das für die „Auskunft an jedermann" gemäß. § 4g Abs. 2 Satz 2 BDSG verwendet werden sollte, da evtl. Geheimhaltungsvorschriften verletzt werden würden. Für die „Auskunft an jedermann" sind die Angaben zusammen zu fassen.

14 Da die Kunden der FinanzIT die Sparkassen in Nord- und Ostdeutschland sind, dient das „Verfahrensregister" somit der Unterstützung der jeweils behördlichen[4] Datenschutzbeauftragten in den Sparkassen zur Übersicht über die Verfahren, die von der FinanzIT (und ggf. zukünftig auch von anderen Kooperationspartnern) zur Verfügung gestellt werden.

4 In der Regel sind Sparkassen als Körperschaften öffentlichen Rechts organisiert. Diese sind i.d.R. als öffentliche Stellen i.S.d. BDSG anzusehen. Abhängig von der Organisations- und Rechtform ist aber grundsätzlich auch denkbar, dass Sparkassen nichtöffentliche Stellen darstellen. In diesem Falle wären nicht behördliche, sondern betriebliche Datenschutzbeauftragte zu bestellen.

1. Technischer Hintergrund

15 Das „Verfahrensregister" der FinanzIT ist als „Lotus Notes[5]-Datenbank" realisiert worden.

16 Lotus-Notes-Datenbanken sind im Gegensatz zu relationalen Datenbanken Dokumentenbasierte Datenbanken. Das heisst Daten und Gestaltungselemente werden in Form von Dokumenten abgelegt, wobei jedes Dokument eine eindeutige ID trägt. Ein Dokument kann mehrere Felder (*items*) unterschiedlicher Typen (zum Beispiel Text oder Zahl) haben. Der Inhalt ist von der Anzeige entkoppelt. Zum Anzeigen und Ändern von Dateninhalten der Dokumente werden Masken (*forms*) verwendet, die frei gestaltet werden können. In so genannten Ansichten (*views*) können Listen von Dokumenten aus dem Datenbestand gefiltert und tabellarisch angezeigt werden. Mittels selbstgeschriebener Programme (*agents*) können Aktionen ereignis- oder zeitgesteuert ausgeführt werden. Dateinamen von Lotus-Notes-Datenbanken enden mit dem Suffix .NSF „Notes storage facility". Datenbankvorlagen (Schablonen) enden mit dem Suffix .NTF „Notes template file".

17 Eine Datenbank hat folgende Identifikationsmerkmale:

- der Datenbanktitel: für den Anwender sichtbar
- der Dateiname: je nach darunterliegendem Dateisystem
- die Replik-ID: eine 16 Hex-Zeichen lange Zahl, die beim Erstellen der Datenbank zufällig generiert wird

18 Dokumente können eine hierarchische Beziehung zueinander haben (Main – Response – ResponseToResponse). Relationen werden in Notes-Datenbanken programmatisch hergestellt, wobei eine übliche Methode die Verwendung der @DocumentUniqueID ist, die auch für die hierarchische Verbindung Verwendung findet. Felder können Mehrfachwerte enthalten, was einer Master-Detail-Tabelle in einem RDBMS entspricht.

19 Notes speichert auch alle Design-Elemente in Notes-Dokumenten. Während das bei RDBMS für das Datenschema und die Ansichten ebenso üblich ist, speichert Notes auch Masken (*forms*) und Ressourcen (css, jpg, java etc.). Alle Design-Elemente sind signiert

5 Lotus Notes ist ein dokumentenorientiertes, verteiltes Datenbanksystem mit sehr enger E-Mail-Anbindung und ist wie andere Datenbankmanagementsysteme (DBMS) eine Plattform für die Entwicklung von Anwendungen. Lotus-Notes-Anwendungen sind Client-Server-Anwendungen. Dabei werden – vereinfacht dargestellt – die Daten auf dem Lotus Notes Domino-Server gespeichert und die Benutzer-Interaktionen auf dem Lotus Notes-Client durchgeführt. Immer häufiger kommt auch der Internet-Browser als Client zum Einsatz.

und erlauben so eine feingliedrige Ausführungskontrolle.

20 Notes-Dokumente sind nicht an Datenbanktabellen gebunden. Somit können Notes-Dokumente beliebige Felder enthalten. Eine Änderung am Masken- oder Ansichtenlayout hat keine Auswirkung auf gespeicherte Daten.

21 Notes-Ansichten (*views*) haben einen physikalischen Index (Views in RDBMS sind normalerweise „nur" Abfragedefinitionen ohne Index). Dies hat den Vorteil des schnellen Zugriffs und den Nachteil des Ressourcen- (*Index task*) und Platz-Verbrauches.

22 Zwischen zwei Rechnern werden ausschließlich Datenbanken repliziert, die dieselbe Replik-ID haben (die anderen Identifikationsmerkmale Datenbanktitel und Dateiname spielen hier keine Rolle).

23 Die Replizierung bei der FinanzIT erfolgt über periodische Agenten, die einmal täglich die Daten replizieren.

24 Ein Notes-System kennt mehrere Sicherheitssysteme:

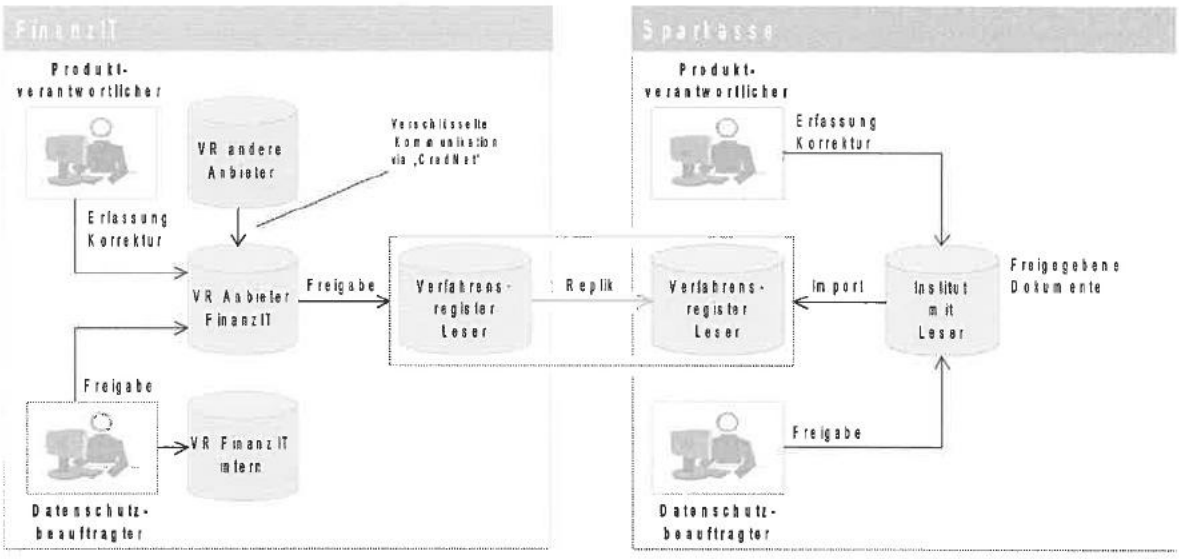
1. Zugriffssicherheit von Clients auf Server: Hier gibt es nicht nur eine Benutzername-/Passwort-Sicherheit, sondern es muss auch ein gültiges Zertifikat vorliegen und zwar bilateral: Der Server muss beim Verbindungsaufbau dem Client ein gültiges Zertifikat vorlegen und der Client dem Server.
2. Vertrauliche Daten können in einer Notes-Datenbank verschlüsselt abgelegt werden und zwar auf vier Arten:
    a) auf Feldebene mit den Öffentlichen Schlüsseln der Personen, die zum Lesen vorgesehen sind
    b) auf Feldebene mit einem eigenen (i.d.R. selbst erstellten) symmetrischen Schlüssel
    c) auf Datenbankebene mit dem Öffentlichen Schlüssel des Benutzers (bei lokal gespeicherten Datenbanken)
    d) auf Datenbankebene mit dem Öffentlichen Schlüssel des Servers (bei auf dem Server gespeicherten Datenbanken)

25 Diese Sicherheitssysteme sind im Lotus-Notes-System integriert und deswegen einfacher zu nutzen und zu administrieren als bei konventionellen Systemen, bei denen diese als separate Softwaresysteme installiert, konfiguriert und administriert werden müssen[6].

2. Systemübersicht und Datenfluss

26 Wie oben beschrieben wird das Verfahrensregister für die Verfahren der FinanzIT (und anderen Kooperationspartnern) zur Verfügung gestellt. Somit ergibt sich eine Aufteilung der Aufgaben.

27 Die Vorbefüllung der Verfahren im Verfahrensregister geschieht durch die FinanzIT. Die Verfahren werden durch den Datenschutzbeauftragten (der FinanzIT) geprüft und freigegeben. Anwendungen, die besondere Risiken für betroffene Personen darstellen, werden nach § 4d Abs. 5 BDSG einer Vorabkontrolle unterzogen. Anschließend wird die (Lotus-Notes-) Datenbank den Sparkassen zur Verfügung gestellt und von den Servern automatisch repliziert, so dass das Verfahren der einzelnen Sparkasse zur Verfügung steht. Nach einer internen Ergänzung oder Änderung der Angaben durch einen (Fach-)Verantwortlichen für das Produkt, erfolgt die Freigabe durch den bDSB der Sparkasse. Die Kommunikation erfolgt jeweils per Lotus-Notes-Mail.



6 Zum Beispiel das Verteilen von Schlüsseln auf viele Clients oder das Aktualisieren von abgelaufenen Zertifikaten bei vielen Benutzern.

3. Ansichten

28 Die Ansichten (views) sind nach folgenden Bereichen unterteilt:

- Inhalt
- Aktuelles
- Arbeitssichten
- Archiv

29 Die Ansichten im Bereich „Inhalt" bieten eine Übersicht über alle freigegebenen Verfahren. Diese Ansichten sind für alle Benutzer des Verfahrensregisters verfügbar. Sie sind nach verschiedenen Kriterien sortiert:

- Verfahren
- Datenkategorieren
- Personengruppen
- Empfänger
- Details

30 Die Ansicht „Aktuelles" bietet Ersteller und bDSB eine Übersicht über alle Verfahrensdokumente, die inhaltlich oder in ihrem Status in den letzten 30 Tagen verändert wurden.
In den „Arbeitssichten" erhält der Benutzer eine schnelle Übersicht aller Verfahren, die sich in einem bestimmten Status (wie beispielsweise „in Bearbeitung" oder „zur Freigabe") befinden.

31 Im Bereich „Archiv" werden alle archivierten Verfahrensdokumente angezeigt. Diese Ansicht ist nur für Ersteller, Datenschutzbeauftragte oder Datenbank-Manager verfügbar.

4. Zugriffsrechte

32 Der Zugriff auf eine Datenbank wird grundsätzlich über die sog. Zugriffskontrollliste (ACL) kontrolliert. Mittels dieser Liste werden den Servern und Personen die erforderlichen Rechte eingeräumt.

33 Nachfolgende Tabelle gibt eine entsprechende Übersicht:

Gruppe/Name	Zugriffsrecht	Cr Doc	Dl Doc	Per AG	Per Fid	Shr Fid	Lsc AG	Rd Pub	Wr Pub	Zugriffsrolle
Default	Kein Zugriff	0	0	0	0	0	0	0	0	
Anonymous	Kein Zugriff	0	0	0	0	0	0	0	0	
Notes-Administrator	Manager	1	1	1	1	1	1	1	0	[DomainAdmin] [DBManager]
LocalDominoServer	Manager	1	1	1	1	1	1	1	0	[DomainServer]
DB-Manager, Anwendugnsadministrator	Editor	1	1	0	0	0	0	1	0	[DBManager]
Dokumentenersteller	Autor	1	0	0	0	0	0	1	0	[Ersteller]
DSB	Editor	1	0	0	0	0	0	1	0	[DSB]

34 Bei den Einzelrechten verbergen sich folgende Rechte hinter den Abkürzungen:

- CrDoc = Dokumente erstellen
- DIDoc = Dokumente löschen
- PerAG = persönliche Agenten erstellen
- PerFid = persönliche Ordner/Ansichten erstellen
- ShrFid = gemeinsame Ordner/Ansichten erstellen
- LscAG = LotusScript/Java Agenten erstellen
- RdPub = öffentliche Dokumente lesen
- WrPub = öffentliche Dokumente schreiben

35 Diese Rechte werden durch so genannte Zugriffsrollen eingeschränkt. Die Zugriffsrollen werden vom Datenbankadministrator vorgenommen. Einer Zugriffsrolle können beliebige Nutzer oder Gruppen zugewiesen oder entzogen werden, nachdem diese in die ACL aufgenommen werden. Allerdings dürfen nur die Rollen zugewiesen werden, die in der Verantwortung des jeweiligen Datenbank-Benutzers auch tatsächlich ausgeführt werden dürfen.
Benutzer mit der „Ersteller"-Rolle dürfen Verfahrensdokumente erstellen und bearbeiten.
In der Rolle „DSB" dürfen Dokumente freigegeben und zurückgezogen werden.
Der „DBManger" darf die Datenbank administrieren und konfigurieren.
Die Rolle „DomainAdmin" ist für den Domino-Administrator gedacht und die Rolle „DomainServer" dient der Replizierung innerhalb einer Domäne.

5. Webbasierte Anwendung des Produktes

35a Neben dem Standardzugriff auf das Produkt Verfahrensregister über den Lotus-Notes-Client besteht die Möglichkeit eines webbasierten Zugriffes via Browser. Zur Einschränkung ist zu erwähnen, dass der Zugriff auf die webbasierte Version des Produktes nur innerhalb eines geschlossenen Netzwerkes (internes Finanz-IT-Netzwerk bzw. Institutsnetzwerk) erlaubt ist. Das heißt, auch webbasierte Zugriffe aus einem Institut auf institutsfremde Datenbanken sind nicht möglich. Sinn und Zweck der webbasierten Anwendung ist u.a., dass in einigen Instituten bzw. auf einigen Clients die Ausführung nicht möglich ist. In diesen Fällen soll den betreffenden Instituten bzw. Mitarbeitern der Zugriff auf das Verfahrensregister über einen Browser möglich sein. Der Zugriff und die Ausgabe von Inhalten aus der institutseigenen Datenbank ist dabei über das Content-Management-System TYPO3 realisiert worden.

6. Protokollierung

35b Um eine revisionssichere Anwendung des Produktes zu gewährleisten, verfügt das Produkt über eine Protokollierung. Protokolliert wird, welcher Benutzer wann ein Verfahren bearbeitet (erstmalig erstellt bzw. geändert) hat. Ferner wird protokolliert, welcher Benutzer wann ein Verfahren freigegeben hat. Die Protokolldaten werden in der Datenbank zum jeweiligen Verfahren gespeichert. Wenn ein Verfahren gelöscht wird, weil es z.B. nicht mehr aktiv bei der veantwortlichen Stelle genutzt wird, dann werden damit auch die Protokolldaten gelöscht. Solange ein Verfahren aktiv, also im Einsatz befindlich ist, sind alle Protokolldaten historisch gespeichert, so dass im Nachhinein auch ältere Versionen eines Verfahrensverzeichnisses über die Änderungshistorie wieder hergestellt werden können.

D. Zweck und Einsatzbereich

36 Das Produkt dient als Verfahrensregister i.S.d. §§ 4d, 4g Abs. 2 Satz 1 BDSG bzw. § 7 LDSG-SH und kann entsprechend bei verantwortlichen Stellen für die Erfassung einer Übersicht über die Verfahren, mit denen automatisiert personenbezogene Daten verarbeitet werden, eingesetzt werden. Das Produkt ist derzeit für den Einsatz bei Finanzinstituten und insbesondere bei Sparkassen konfiguriert. Da Sparkassen i.d.R. als Körperschaften öffentlichen Rechts organisiert sind, ist das Verfahren grundsätzlich auch für den Einsatz bei bzw. durch öffentliche Stellen des Landes Schleswig-Holstein geeignet.

E. Besondere Eigenschaften des IT-Produktes

I. Datenarten-Anforderungsprofil für Primärdaten

37 Die Darstellung eines Datenarten-Anforderungsprofils im herkömmlichen Sinne gestaltet sich vorliegend schwierig, da keine Primärdaten i.S.v. personenbezogenen Daten mit dem Produkt verarbeitet werden. Mit dem Produkt wird die das Produkt einsetzende verantwortliche Stelle bei der Erstellung und Führung der gesetzlich erforderlichen Verfahrensübersicht unterstützt.

38 Für die Beurteilung des Produktes im Hinblick auf die Einhaltung der einschlägigen datenschutzrechtlichen Vorschriften sind daher die gesetzlichen Anforderungen an die Erstellung der Verfahrensübersicht für den betrieblichen bzw. behördlichen Datenschutzbeauftragten und die Möglichkeit der Prüfung der Verfahrensübersicht durch den Datenschutzbeauftragten zur Prüfung heranzuziehen. Die gesetzlichen Anforderungen sind weitest gehend schon unter C. I. dargestellt worden. Hierauf wird ausdrücklich Bezug genommen.

39 Im Wesentlichen muss das Produkt geeignet sein, die gesetzlichen Anforderungen an die Verfahrensübersicht bzw. einem Verfahrensverzeichnis i.S.d. § 7 LDSG-SH, die dem betrieblichen Datenschutzbeauftragten nach § 4g Abs. 2 Satz 1 BDSG zur Verfügung zu stellen ist, zu erfüllen. Danach muss das Produkt die verantwortliche Stelle in die Lage versetzen, die Angaben nach § 4e BDSG in geeigneter Form zusammen zu fassen und dem behördlichen bzw. betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen.

40 Im Rahmen der Prüfung des Produktes für die Erteilung eines Gütesiegels für IT-Produkte durch das ULD ist hinsichtlich der Bewertung des Produktes ferner zu berücksichtigen, ob das Produkt den Anwender bei der Einhaltung der datenschutzrechtlichen Anforderungen unterstützt bzw. den Datenschutz allgemein fördert.

41 Auch wenn mit dem vorliegenden Produkt grundsätzlich keine personenbezogenen Daten i.S.v. Primärdaten verarbeitet werden, so ist vom Produkthersteller dennoch dafür Sorge zu tragen, dass die erforderlichen technischen und organisatorischen Maßnahmen i.S.d. §§ 5, 6 LDSG-SH bzw. § 9 BDSG und der Anlage zu § 9 BDSG eingehalten werden. Dies resul-

tiert zumindest daraus, dass die FinanzIT für die Sparkassen bzw. Institute als Auftragsdatenverarbeiter tätig wird und nach den § 11 BDSG bzw. § 17 LDSG-SH entsprechende Mindestvoraussetzungen an diesen zu stellen sind. Auch hier ist jedoch zu berücksichtigen, dass das datenschutzrechtliche Institut der Auftragsdatenverarbeitung im engeren Sinne gar nicht anwendbar ist, da keine Erhebung, Verarbeitung und Nutzung personenbezogener Primärdaten stattfindet. Bei einer Prüfung eines Produktes im Rahmen einer Zertifizierung für das Gütesiegel für IT-Produkt sind jedoch im Hinblick auf allgemeine Anforderungen an technische und organisatorische Maßnahmen zu Datenschutz und auch Datensicherung Anforderungen zu stellen, die aus den §§ 5, 6 LDSG-SH bzw. § 9 BDSG hergeleitet werden können. So ist neben allgemeinen Anforderungen an einen Rechenzentrumbetrieb insbesondere Sorge dafür zu tragen, dass ein Zugriff auf das Verfahrensregister nur berechtigten Personen möglich ist. Dies erfordert eine wirksame Authentifizierung des Nutzers über einen Benutzernamen und ein Passwort erforderlich. Dies gilt in gleichem Maße für die webbasierte Anwendung.

II. Datenarten-Anforderungsprofil für Sekundärdaten

42 Als Sekundärdaten kommen vorliegend nur die Protokolldaten in Betracht. Diese enthalten im Gegensatz zu den Primärdaten auch personenbezogene Daten, da durch die Protokollierung von Benutzernamen ein Personenbezug für verantwortliche Stelle besteht bzw. bestehen kann. Für die rechtliche Bewertung des Produktes besteht jedoch eine Besonderheit. Hierbei ist zunächst zu berücksichtigen, dass im Rahmen der Zertifizierung der Einsatz des Produktes bei einer öffentlichen Stelle des Landes Schleswig-Holstein und damit die Anwendung der Vorschriften des LDSG-SH maßgeblich sind. Der Kreis der Adressaten, die Anwender des Produktes sein können, ist hier jedoch beschränkt, da es sich hierbei regelmäßig um Sparkassen bzw. Landesbausparkassen handelt. Bei diesen Stellen handelt es sich um öffentlich-rechtliche, der Aufsicht des Landes unterstehende Unternehmen mit eigener Rechtspersönlichkeit, die am Wettbewerb teilnehmen[7]. Nach § 3 Abs. 2 LDSG-SH gilt für diese Stellen nur § 23 LDSG-SH. Im Übrigen sind die Vorschriften des BDSG anzuwenden. § 23 LDSG-SH regelt den Schutz von Daten von Arbeitnehmern bzw. Beschäftigten. Während § 23 Abs. 1 LDSG-SH vorliegend in Ermangelung der Erhebung, Verarbeitung oder Nutzung von Personalaktendaten nicht anzuwenden ist, sind jedoch die Vorgaben des § 23 Abs. 2 LDSG-SH zu beachten. Danach dürfen Daten von Beschäftigten,

7 Vgl. ULD, Hinweise zur Anwendung des Schleswig-Holsteinischen Gesetzes zum Schutze personenbezogener Informationen, Anm. zu § 3 Ziff. 5

die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 5 und 6 LDSG-SH gespeichert werden, nicht zu Zwecken der Verhaltens- und oder Leistungskontrolle ausgewertet werden. Da die Durchführung technischer und organisatorischer Maßnahmen (wie z.B. die Protokollierung von Datenverarbeitungsvorgängen) sich jedoch stets – bezogen auf den Zertifizierungsgegenstand - auf die Protokollierung von Verarbeitungsvorgängen bzgl. personenbezogener Primärdaten richtet, ist § 23 Abs. 2 1. Alt. LDSG-SH dem Wortlaut nach nicht anwendbar. Nach § 23 Abs. 2 2. Alt. LDSG-SH unterliegen aber auch Daten von Beschäftigten, die in einem automatisierten Verfahren gewonnen werden, der besonderen Zweckbindung des § 23 Abs. 2 LDSG-SH. Da die Protokollierungsfunktion des Produktes ein automatisiertes Verfahren darstellt, muss daher gewährleistet sein, dass beim Einsatz des Produktes die Auswertung der Daten von Beschäftigten zu Zwecken der Leistungs- und Verhaltenskontrolle verhindert werden kann.

42a Die FinanzIT wird für die Sparkassen bzw. Institute als Auftragsdatenverarbeiter tätig. Da zumindest die Protokollierungsdaten einen Personenbezug aufweisen können, richtet sich die Zulässigkeit der Verarbeitung und Nutzung etwaiger personenbezogener Daten im Wege der Auftragsdatenverarbeitung nach § 11 BDSG. Danach bleibt die öffentliche datenverarbeitende Stelle weiterhin für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Sie muss dafür Sorge tragen, dass personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Der Auftrag bzw. die Aufträge, ergänzende Weisungen und die etwaige Zulässigkeit von Unterauftragsverhältnissen sind schriftlich festzulegen. Sie hat ferner bei der Auswahl des Auftragnehmenden besondere Sorgfalt walten zu lassen.

43 Außerdem muss die verantwortliche Stelle ggf. durch entsprechende Verpflichtungen dafür sorgen, dass Kontrollen der Datenverarbeitung möglich sind. Um den Anforderungen an eine Auftragsdatenverarbeitung gerecht werden zu können, ist schließlich eine Protokollierung der Datenverarbeitung erforderlich, damit der Zeitpunkt und der Umfang der Datenverarbeitung festgestellt werden kann (vgl. § 5 Abs. 1 Nr. 3 LDSG-SH), und es ist erforderlich, dass die Erstellung und Änderung von Datenbeständen durch Nutzer protokolliert wird.

III. Zulässigkeit der Datenverarbeitung

44 Die Datenverarbeitung mit dem Produkt „Verfahrensregister 2.1" erfolgt in zulässiger Art und Weise. Das Produkt bildet die Anforderungen durch das BDSG an die Erstellung und das Führen einer Verfahrensübersicht in optimaler Weise ab. Die Software orientiert sich dabei direkt am Wortlaut des Gesetzes. So sind alle Inhalte der Meldepflicht i.S.d. § 4e BDSG umgesetzt. Bezüglich der § 7 Abs. 1 Nr. 7 LDSG-SH (aber nicht in § 4e BDSG) vorgesehenen Aufnahme der datenschutzrechtlichen Beurteilung des behördlichen Datenschutzbeauftragten zum Verfahrensverzeichnis, soweit diese vorliegt, ist festzustellen, dass die Nichtumsetzung dieser Angabe auf den bundesländerübergreifenden Einsatz des Produktes zurück zu führen ist und die Angaben ggf. manuell zum Verfahrensverzeichnis genommen werden können. Die datenschutzrechtliche Bewertung eines Verfahrens durch den behördlichen Datenschutzbeauftragten wird, sofern diese überhaupt – neben einem reinen Freigabevermerk – vorliegt, i.d.R. gesondert erfolgen, so dass die Nichtimplementierung dieser Funktion für die Prüfung der Zulässigkeit der Datenverarbeitung unschädlich ist. Rechtlich ist dies auch nicht negativ zu bewerten, da § 7 LDSG-SH wegen § 3 Abs. 2 LDSG-SH gar nicht anzuwenden ist, sondern § 4g Abs. 2 BDSG i.V.m. § 4e BDSG einschlägige Rechtsgrundlagen für die Bewertung sind.

45 Das Produkt kann nur durch berechtigte Personen nach Eingabe eines Benutzernamens und einem Passwort erfolgen. Eine wirksame Authentifizierung von Benutzern erfolgt schon durch den Einsatz des Lotus-Notes-Systems, das Voraussetzung für den Zugang und die Benutzung des Produktes ist. Dies geschieht über eine eigene sog. ID-Datei, die in Verbindung mit einem Passwort, dessen Länge vom Systemadministrator festgelegt werden kann, den Zugang zum System ermöglicht. Mit einer dedizierte Rechtevergabe auf Datenbankebene wie unter I.4 beschrieben wird die Einhaltung der technischen und organisatorischen Maßnahmen gewährleistet. Die Anforderungen der zu treffenden allgemeinen Maßnahmen zur Datensicherheit sind damit erfüllt.

45a Die Einhaltung der rechtlichen Vorgaben zur besonderen Zweckbindung i.S.d. § 23 Abs. 2 LDSG-SH kann beim Einsatz des Produktes gewährleistet werden. Schon die FinanzIT als Auftragsdatenverarbeiter ist durch § 31 BDSG ebenfalls an die besondere Zweckbindung gebunden. Der Einsatz des Produktes bei den jeweiligen Instituten ist zudem Gegenstand individueller Vertragsverhandlungen. Die FinanzIT weist die Institute in diesem Zusammenhang grundsätzlich darauf hin, dass ggf. gesonderte organisatorische Maßnahmen in-

stitutsintern getroffen werden müssten, um sicher zu stellen, dass eine Verhaltens- und Leistungskontrolle unterbleibt. Da die Einführung technischer Verfahren, die eine Verhaltens- und Leistungskontrolle ermöglichen, grundsätzlich auch nach § 51 Gesetzes über die Mitbestimmung der Personalräte (Mitbestimmungsgesetz Schleswig-Holstein)[8] einen mitbestimmungspflichtigen Tatbestand darstellt, kann davon ausgegangen werden, dass auch institutsintern der besonderen Zweckbindung Rechnung getragen wird. Darüber hinaus kann der Produkthersteller die institutsinterne Einhaltung auch nicht gewährleisten. Die rechtlichen Voraussetzungen sind damit erfüllt.

45b Keine Bedenken bestehen bezüglich der Einhaltung der Voraussetzungen an eine ordnungsgemäße Auftragsdatenverarbeitung. Die FinanzIT hat umfangreiche Vorkehrungen für eine ordnungsgemäße Datenverarbeitung getroffen. Der Einsatz des Produktes bei den Sparkassen bzw. Instituten bedarf einer gesonderten vertraglichen Vereinbarung zwischen den Parteien. Hier können auch individuelle schriftliche Weisungen durch den Auftraggeber erfolgen. Die FinanzIT verwendet ansonsten regelmäßig einen sog. Rahmenvertrag, der auch Vereinbarungen zu Datenschutz und Sicherheit enthält. Der Vertrag ist dem rechtlichen Gutachter vorgelegt worden. Schon die dort enthaltenen Vereinbarungen sehen Verpflichtungen der FinanzIT vor, die eine ordnungsgemäße Verarbeitung der Daten im Auftrag gewährleistet, und als vorbildlich zu bewerten sind.

45c Auch die Speicherung der Protokolldaten erfolgt in zulässiger Weise. Die Speicherung der Protokolldaten ist für Zwecke des Nachweises einer ordnungsgemäßen Datenverarbeitung sowie für die Integrität der Daten erforderlich, solange ein Verfahren im Verfahrensregister im Einsatz ist. Da die Protokolldaten bei Deaktivierung eines Verfahrens in der betreffenden Datenbank gelöscht werden, bestehen auch keine Bedenken hinsichtlich der Dauer der Speicherung der Daten.

46 Das Produkt ist ein optimales Instrument für die verantwortliche Stelle und den jeweils zuständigen behördlichen (bzw. betrieblichen) Datenschutzbeauftragten. Der Datenschutzbeauftragte wird bei seiner täglichen Arbeit unterstützt, indem er bei Aufruf des Programms in der Rubrik „Aktuelles“ stets neue Verfahren bzw. Änderungen an Verfahren sehen kann, um diese zu prüfen und ggf. bewerten zu können. Ferner kann er auf diese Weise leicht

8 Gesetz über die Mitbestimmung der Personalräte (Mitbestimmungsgesetz Schleswig-Holstein - MBG Schl.-H.) vom 11. Dezember 1990, GVOBl. 1990, S. 577, zuletzt geändert durch Gesetz vom 28.3.2006, GVOBl. 2006, S. 28

feststellen, ob ggf. eine Vorabkontrolle zu initiieren und durchzuführen ist.

47 Der verantwortliche Stelle bzw. den jeweils verantwortlichen Mitarbeiter ist das Produkt eine gute Hilfe bei der Erstellung der jeweils erforderlichen Verfahrensverzeichnisse. Auf diese Weise wird sichergestellt, dass die nach § 7 Abs. 1 LDSG-SH bzw. § 4e BDSG erforderlichen Angaben vollständig erfolgen. Durch Ausfüllhinweise werden die Mitarbeiter zudem bei der Angabe der entsprechenden Informationen unterstützt.

47a Soweit in den Protkolldaten personenbezogene Daten enthalten sind, steht der Einsatz des Produktes einer Wahrung der Betroffenenrechte nach den §§ 33 ff. BDSG nicht entgegen.

IV. Bewertung der besonderen Eigenschaften

48 **Datenart:** _Primärdaten_____

Da keine personenbezogenen Primärdaten mit dem Produkt erhoben, verarbeitet oder genutzt werden, ist eine Bewertung bzgl. der Datenart „Primärdaten" nicht möglich.

Datenart: _Sekundärdaten_____

49

B. Anforderungsprofil für Protokolldaten	Bewertung	Kommentare
Komplex 1:		
1.1. Datenvermeidung und Datensparsamkeit	adäquat	
1.2 Transparenz	adäquat	
1.3 Sonstige Anforderungen <benennen!>		
Komplex 2:		
2.1 Rechtsgrundlage für die Erhebung und Verarbeitung der Protokolldaten	vorbildlich	§ 9 BDSG analog
2.2 Unterstützung der Einhaltung der Zweckbindung	adäquat	
2.3 Löschung	adäquat	
2.4 Sonstige Anforderungen <benennen!>		
Komplex 3:		
3.1 Fragestellungen aus 3.1.1.3		
3.2 Zugriffsschutz für Protokolldaten	vorbildlich	
3.3 Informationsgehalt der Protokolldaten	adäquat	
3.4 Unterschiedliche Speicherfristen	adäquat	
3.5 Sonstige Anforderungen <benennen!>		

F. Zusammenfassung

50 Zusammenfassend kann das Produkt „Verfahrensregister“ als vorbildlich umgesetzt bewertet werden. Die Bewertung als vorbildlich mag sich zwar nicht unmittelbar aus dem Bewertungsschema ergeben; dieses Schema bildet jedoch auch nur die reine Verarbeitung der Protokolldaten ab. Sinn und Zweck der Vergabe eines Gütesiegels für IT-Produkte ist neben der Einhaltung datenschutzrechtlicher Anforderungen auch, Produkte, die den Datenschutz besonders fördern, entsprechend durch Verleihung eines Siegels zu würdigen. Das Produkt „Verfahrensregister 2.1“ hat nicht die Verarbeitung oder Nutzung von Primärdaten zum Gegenstand. Lediglich Protokolldaten fallen an, bei denen ein Personenbezug entsteht bzw. entstehen kann. Eine reine Bewertung der Verarbeitung dieser Daten würde zu einer adäquaten Bewertung des Produktes führen, die dem Gesamteindruck des Produktes – gerade im Hinblick auf die Förderung des Datenschutzes – nicht gerecht werden würde.

51 Nach Auffassung der Unterzeichner verdient die Software, die Gegenstand der Prüfung ist, eine insgesamt vorbildliche Bewertung. Das Produkt bildet die gesetzlichen Anforderungen vollständig und nach der ausdrücklichen Vorstellungen des Gesetzgebers im Hinblick auf die Verantwortlichkeiten optimal ab. Da sich das Produkt bei der Umsetzung ganz eng an den Gesetzeswortlaut angelehnt hat, kann diesbezüglich von einer vorbildlichen Umsetzung gesprochen werden. Auch die sog. webbasierte Variante des Produktes ist nicht anders zu bewerten, da der Zugriff nur nach einer ordnungsgemäßen Authentifizierung und nur innerhalb eines geschlossenes Netzwerkes möglich ist.

52 Besonders positiv hervorzuheben ist, dass den Produktanwendern beim Ausfüllen der entsprechenden Formularfelder gute Hinweise gegeben werden, die die Eingabe der erforderlichen Daten erleichtern, was den Datenschutz bzw. die Einhaltung der datenschutzrechtlichen Anforderungen erheblich fördert.

53 Das Produkt entspricht in seiner Ausrichtung und Ausgestaltung dem Ideal einer Software, die den Datenschutz und besonders die Tätigkeit des behördlichen bzw. betrieblichen Datenschutzbeauftragten fördert, und ist daher als insgesamt vorbildlich zu bewerten.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Flensburg, den 7.3.06

Mühlenbarbek, den 7.3.06

[redacted]

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum
für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für
IT-Produkte (rechtlich)

Andreas Bethke
Dipl. Informatiker (FH)
Beim Unabhängigen Landeszentrum
für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für
IT-Produkte (technisch)