# Technisches und rechtliches Rezertifizierungs-Gutachten

Einhaltung datenschutzrechtlicher Anforderungen durch das Produkt „Elefant Profi Version 16.01“ der

**HASOMED GmbH**
**Magdeburg**

erstellt von:


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

Papenbergallee 34
25548 Kellinghusen
tel 04822 – 36 63 000
fax 04822 – 36 63 333
mob 0179 – 321 97 88
email bethke@datenschutz-guetesiegel.sh

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

Neustadt 56
24939 Flensburg
tel 0461 – 90 91 356
fax 0461 – 90 91 357
mob 0171 – 20 44 98 1
email sh@hansen-oest.com


Stand:
Januar 2016

# Inhaltsverzeichnis

## Änderungs- und Versionsverwaltung des Gutachtens

| | | |
|---|---|---|
| 01.08.2015 | Erstellung | Andreas Bethke, Stephan Hansen-Oest |
| 04.08.2015 | Ergänzung | Andreas Bethke |
| 02.09.2015 | Ergänzung | Stephan Hansen-Oest |
| 09.11.2015 | Ergänzungen nach Rückmeldung vom ULD | Andreas Bethke |
| 24.11.2015 | Ergänzungen nach Prüfung der neuen Version | Andreas Bethke |
| 04.12.2015 | Ergänzungen | Andreas Bethke |
| 18.12.2015 | Ergänzungen nach Rückmeldung vom ULD | Andreas Bethke |
| 29.12.2015 | Ergänzungen | Andreas Bethke |
| 19.01.2016 | Ergänzungen nach Rücmeldung vom ULD | Andreas Bethke |
| 22.01.2016 | Letzte Korrekturen | Andreas Bethke |
| | | |

## A. Einleitung

1 Mit dem vorliegenden Gutachten beabsichtigt die HASOMED GmbH (nachfolgend HASOMED genannt) ihr Produkt „*Elefant Profi*“ mit der Option „Security-Mode“ für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) rezertifizieren zu lassen.

Die Vorlage des Gutachtens beim ULD erfolgt durch den Auftraggeber.

Dem Gutachten wird der Anforderungskatalog in der Version 2.0 zu Grunde gelegt.

2 HASOMED möchte mit diesem Gutachten den Nachweis führen, dass das Produkt mit den Änderungen und Neuerungen, die seit der Erteilung des Gütesiegels vom 12.12.2007 und den Rezertifizierungen vom 18.05.2010 und vom 07.06.2013 gemacht worden sind, nach wie vor die datenschutzrechtlichen Anforderungen erfüllt.

## B. Zeitpunkt der Prüfung

3 Die Prüfung des Produktes fand vom 03.06.2015 - 29.12.2015 statt.

## C. Änderungen und Neuerungen des Produktes

4 Das Produkt „Elefant Profi“ mit der Option „Security-Mode“ wurde um folgende Funktionen erweitert:

- Erweiterung der „AMBO“-Schnittstelle
- Neue Felder für IBAN und BIC
- Neue Schnittstelle zur AGFEO-Telefonanlage
- Erstellung einer „1-Klick-Abrechnung“ für die KV
- Neues Feld „Supervisor“ in den Stammdaten
- Umsetzung der Forderung des Patientenschutzgesetzes 2013
- Erstellung eines Medikationsplans
- Integration des „Hogrefe Testverfahrens“
- Überarbeitung des „Beizettels“
- Überarbeitung der „AMBO“-Abrechnung
- Zwischenspeichern von XML-Daten beim Einlesen von Karten (eGK) in einer Zwischentabelle
- Anpassung der Datenstruktur an die elektronische Gesundheitskarte

Darüber hinaus gibt es noch eine weitere neue Funktion

- Einführung von „Freien Feldern“

Diese gehört jedoch nicht zum Begutachtungsgegenstand und ist somit vom Gütesiegel **ausgenommen**.

### 1. Erweiterung der „AMBO“-Schnittstelle

5 Vorab noch einmal eine kurze Wiederholung zum gesetzlichen Hintergrund der Schnittstelle: Die Abrechnung der psychiatrischen Institutsambulanzen nach §118 SGB V muss

seit dem 01.07.2010 über den Datenträgeraustausch nach §301 SGB V vorgenommen werden. Hierzu wurde zwischen der Deutschen Krankenhausgesellschaft (DKG) und dem GKV-Spitzenverband eine Vereinbarung nach § 120 Abs. 3 SGB V über Form und Inhalt der Abrechnungsunterlagen für die Einrichtungen nach §§ 117 bis 119 SGB V geschlossen. Danach ist, zusätzlich zu den bisherigen papiergebundenen Rechnungen, eine elektronische Datenübermittlung notwendig.

In der aktuellen Version wurde diese Schnittstelle nun um Gutschrift, Zahlungserinnerung, Mahnung 1 und Mahnung 2 erweitert, die die gleichen Daten wie eine Rechnung enthalten. Lediglich ein Feldeintrag (quasi der Status) ist anders. Es werden aber keine Daten verändert. Sie bleiben in der der Rechnung erhalten.

### 2. Erweiterung um IBAN und BIC

6 Im Zuge der SEPA-Einführung wurde der Elefant um die nötigen Felder erweitert. Die Erweiterung wurde im Reiter „Bank/Steuern“ vorgenommen und werden nur für die Rechnungstellung benutzt.

### 3. Neue Schnittstelle zur AGFEO-Telefonanlage

7 Es handelt sich bei der Schnittstelle um eine Unterstützung beim Wählen von Telefonnummern. D.h. über die Software der Anlage kann ein externes Programm gestartet werden. Diesem Programm wird die gewählte Telefonnummer übergeben. Die Telefonnummer wird dort nicht gespeichert.

Bei eingehenden Anrufen speichert die Software der Telefonanlage die Telefonnummern in einer Datei „ElefantAgfeo.dat“ ab. Beim Öffnen der Patientenliste wird nach Patienten mit Telefonnummern aus dieser Datei gesucht. Wird ein Patient mit passender Telefonnummer gefunden, wird er in der Liste angezeigt. Beim Schließen der Patientenliste wird die Datei „ElefantAgfeo.dat“ gelöscht. Eine Telefonhistorie wird nicht gespeichert.

### 4. Erstellung einer „1-Klick-Abrechnung“ für die KV

8 Über die 1-Click-Abrechnung der KV – Telematik können die niedergelassenen Ärzte und Psychotherapeuten ihre Quartalsabrechnung elektronisch direkt aus dem ELEFANT heraus versenden. Hierbei wird eine E-Mail erstellt, die eine mittels KBV-Verschlüsselungsmodul verschlüsselte Abrechnungsdatei noch einmal über ein Zertifikat verschlüsselt. Der gesamte Verschlüsselungsvorgang geschieht über das KV-Connect. Der Hersteller hat hierauf keinen Einfluss.

### 5. Neues Feld „Supervisor“ in den Stammdaten

9 Sofern sich ein Psychotherapeut noch in der Therapie-Ausbildung befindet, steht ihm ein

sog. „Supervisor“ zur Seite, mit dem er seine Fälle bespricht. Um den Namen des Supervisors zu speichern wurde ein neues Feld in den Stammdaten angelegt. Es handelt sich nicht um eine Zugriffsberechtigung, sondern nur um eine Information für die Ausbilder. Eine gesonderte Patienteneinwilligung zur Supervision erfolgt außerhalb des Elefant über die einsetzende Stelle.

### 6. Umsetzung der Forderung des Patientenschutzgesetzes 2013

10 Gemäß der Änderung des Patientenrechtegesetz aus dem Jahr 2013 muss jede Änderung an den Patientendaten dokumentiert werden (vgl. § 630f BGB). Dies passierte bisher nur im „Security-Mode“. Um die Forderung zu erfüllen, wurde die Protokollierung für alle Nutzer frei geschaltet. Ausnahme ist die Protokollierung des Ein- und Ausloggen der Benutzer, die nur im aktivierten Security-Mode geschieht.

### 7. Erstellung eines Medikationsplans

11 Die Nutzergruppen der Software unterteilen sich in therapeutische Psychologen und psychotherapeutische Ärzte. Um die zweite Benutzergruppe zu unterstützen kann man in der aktuellen Version des *Elefant* in der „Patientenakte“ unter der Karte „Arzt“ einen Medikationsplan Version 1.3 der Arbeitsgruppe Arzneimitteltherapiesicherheit der Bundesärztekammer erstellen. Um diese Funktion zu benutzen, muss sie in den Systemparametern vom Benutzer gesetzt sein und so eingestellt sein, dass der Benutzer in der Praxis als Arzt tätig ist. Der Medikationsplan ist ein Dokument, welches ausschließlich dem betroffenen Patienten übergeben wird. Um dem Benutzer die Arbeit bei der Erstellung zu erleichtern, können die Daten über einen auf dem Medikationsblatt ausgedruckten Barcode eingelesen werden.

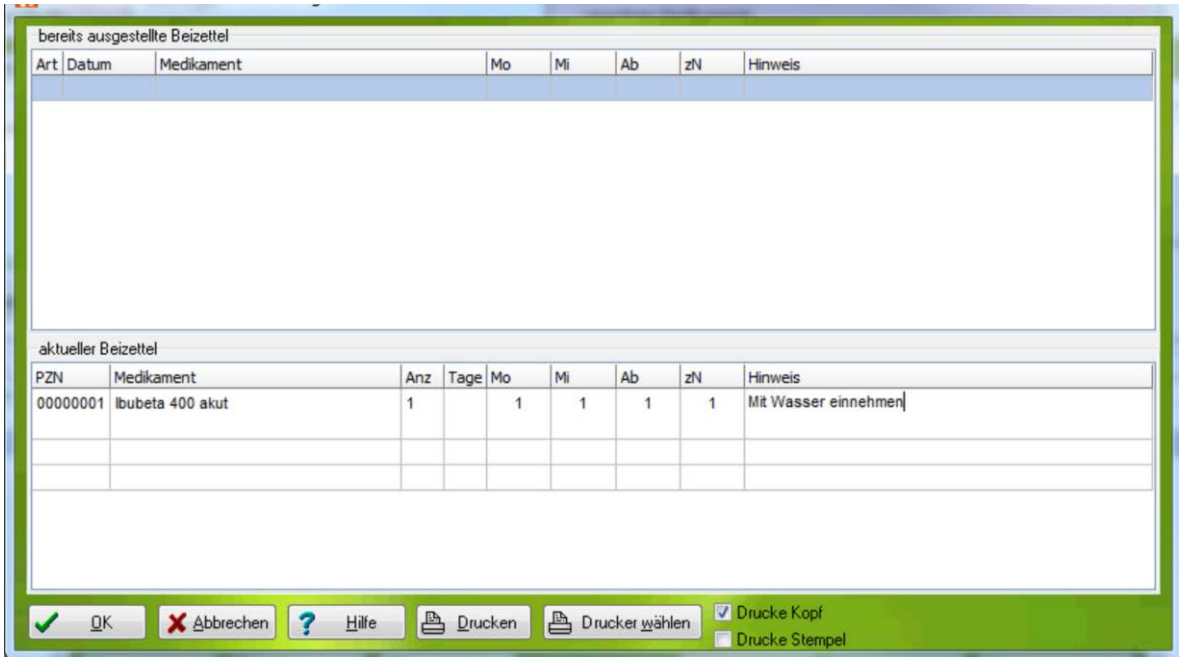
### 8. Integration des „Hogrefe Testverfahrens“

12 Das Hogrefe Testsystem (HTS) ist ein externes System zur computerunterstützten Psychodiagnostik. Zielsetzung des HTS ist es, Durchführung, Auswertung und Interpretation der wichtigsten professionellen psychologischen Testverfahren, die sich für eine computergestützte Umsetzung eignen, in eine einheitliche Umgebung zu integrieren und damit die psychodiagnostische Tätigkeit zu vereinfachen. Die Tests dienen der besseren Einschätzung des Patienten. In der aktuellen Version ist ein solches Testsystem in den Elefant integriert. Dabei erhält jeder Test durch das Hogrefe-Testsystem eine eigene (hochgezählte) ID, die im Elefant zum Patienten gespeichert wird, um Auswertungen zum Test zu erzeugen. Als weitere Parameter werden die Patientennummer, Name, Vorname und das Alter zur Ergebniserzeugung an das System übergeben. Die Patientendaten werden hierbei nicht außerhalb der Elefant-Datenbank gespeichert. Lediglich das Alter und Geschlecht des Patienten werden in der Hogrefe-Datenbank gespeichert. Die Datenbank ist

mit einem AES-128-Bit-Verfahren verschlüsselt. Zugriff auf diese Datenbank hat nur derjenige, der auch über den Elefant authentifiziert ist. Die Hogrefe-Datenbank ist jeweils nur auf dem lokalen Rechner installiert. Ein punktuelles Löschen von Daten in der Hogrefe-Datenbank ist nicht vorgesehen. Es kann nur die gesamte Hogrefe-Datenbank gelöscht werden.

### 9. Überarbeitung des „Beizettels“

13 Der sog. „Beizettel“ (Medikamentenzettel) wurde gem. folgender Maske neu überarbeitet.




### 10. Überarbeitung der „AMBO“-Abrechnung

14 Ein kurzer Rückblick auf die „AMBO-Schnittstelle“: Die Abrechnung der psychiatrischen Institutsambulanzen nach §118 SGB V muss seit dem 01.07.2010 über den Datenträgeraustausch nach §301 SGB V vorgenommen werden. Hierzu wurde zwischen der Deutschen Krankenhausgesellschaft (DKG) und dem GKV-Spitzenverband eine Vereinbarung nach § 120 Abs. 3 SGB V über Form und Inhalt der Abrechnungsunterlagen für die Einrichtungen nach §§ 117 bis 119 SGB V geschlossen. Danach ist, zusätzlich zu den bisherigen papiergebundenen Rechnungen, eine elektronische Datenübermittlung notwendig.

15 Die Schnittstelle ist seit mehreren Jahren im Einsatz. In der aktuellen Version wurden nun Verbesserungen beim Handling der Fehlernachrichten und der Anzeige-Filterung der Protokolle durchgeführt. So ist es jetzt möglich, Fehlernachrichten zu lesen, die mit einem alten Zertifikat verschlüsselt worden sind. Die Fehlernachrichten von der KV sind dabei in verschlüsselten Dateien der Kassen hinterlegte Fehlercodes (gem. AMBO-

Schnittstellenbeschreibung), die vor Anzeige entschlüsselt und für den Benutzer in eine verständliche Form gewandelt werden müssen, damit dieser die notwendigen Korrekturen an den Daten vornehmen kann. Die entschlüsselten Dateien mit den Fehlercodes werden nach der Anzeige sofort wieder gelöscht.

### 11. Zwischenspeichern von XML-Daten beim Einlesen von Karten (eGK) in einer Zwischentabelle

16 Das Einlesen von Patientendaten geschieht in der Regel mittels elektronischer Gesundheitskarte. Dabei werden die Daten auf der Karte in ein XML-Format eingelesen und temporär in einer Zwischentabelle der Elefant-Datenbank gehalten. Die Daten bleiben dort solange erhalten, bis der Patient über die Zwischenablage des Elefanten geöffnet wird. Dabei werden die Patientendaten im Elefant gemäß der KBV-Anforderungen aktualisiert. Danach werden diese Daten in der Tabelle gelöscht.

### 12. Anpassung der Datenstruktur an die elektronische Gesundheitskarte

17 Im Zuge der Einführung der elektronischen Gesundheitskarte wurde die Datenstruktur an die der eGK angepasst.

### Ausnahme: Einführung von „Freien Feldern“

18 Wie bereits einleitend geschildert gehört diese Erweiterung nicht zur Begutachtung und ist somit vom Gütesiegel ausgeklammert. Die „freien Felder“ waren der Wunsch von Ausbildungsinstituten, um Eingabefelder mit patientenspezifischen Informationen für institutsinterne Zwecke selbst anzulegen und zu verwalten, die ein niedergelassener Psychotherapeut nicht benötigt. Dieser Ausschluss erfolgte aufgrund der Forderung nach den Kriterien des Datenschutzgütesiegels des ULD nach einer Zweckbindung solcher Felder, auf die der Hersteller keinen Einfluss hat. Eine Nutzung dieser Funktion ist zwar möglich, entspricht aber keiner datenschutzkonformen Anwendung, ähnlich wie die Desaktivierung des „Security-Mode“ um die Verschlüsselung auszuschalten. Unabhängig von den Festlegungen werden die Informationen in den „freien Feldern“ bei Nutzung des Security Modes verschlüsselt in der Datenbank gespeichert.

## D. Datenschutzrechtliche Bewertung

19 Seit der letzten Rezertifizierung wurde der Anforderungskatalog des ULD Gütesiegels angepasst. Darum soll an dieser Stelle die neue tabellarische Darstellung erfolgen.

| Anforderung nach Katalog oder sonstigen Rechtsnormen | Bewertung | Kommentare |
|---|---|---|
| **Komplex 1:** | | |
| 1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit | adäquat | |
| 1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung) | adäquat | Abstufung durch Freitextfelder |
| 1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung) | vorbildlich | |
| 1.4 Datenschutz-Schutzziel: Intervenierbarkeit | vorbildlich | |
| 1.5 Anpassung des IT-Produkts | vorbildlich | Anpassungen an gesetzliche Vorgaben werden quartalsweise umgesetzt |
| 1.6 Privacy by Default | vorbildlich | Im „Security-Mode“ sind alle Einstellungen auf „datenschutzfreundlich“ gesetzt. |
| 1.7 Sonstige Anforderungen | entfällt | |
| | | |
| **Komplex 2:** | | |
| 2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten | adäquat | |
| 2.1.2 Einwilligung des Betroffenen | adäquat | |
| 2.1.3.1 Vorschriften über die Datenerhebung | adäquat | |
| 2.1.3.2 Vorschriften über die Übermittlung | adäquat | |
| 2.1.3.3 Löschung nach Wegfall des Erfordernisses | adäquat | |
| 2.2.1 Zweckbindung und Zweckänderung | adäquat | |
| 2.2.2 Erleichterung der Umsetzung des Trennungsgebotes | adäquat | |
| 2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG) | adäquat | - |
| 2.3 Datenverarbeitung im Auftrag | adäquat | - |
| 2.4.1 gemeinsame Verfahren/Abrufverfahren | adäquat | - |
| 2.4.2 Trennung der Verantwortlichkeiten | adäquat | - |
| 2.4.3 Veröffentlichungen im Internet | adäquat | |
| 2.4.4 Weitere besondere technische Verfahren | adäquat | |
| 2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens | adäquat | |
| | | |
| **Komplex 3:** | | |
| 3.1.1. Physikalische Sicherung | vorbildlich | Sicherungen werden bei Programmende automatisch angeboten und protokolliert |
| 3.1.2 Authentisierung | adäquat | |
| 3.1.3 Autorisierung | adäquat | |
| 3.1.4 Protokollierung | vorbildlich | |
| 3.1.5 Verschlüsselung und Signatur | vorbildlich | Alle personenbezogenen Daten werden verschlüsselt |
| 3.1.6 Pseudonymisieren | entfällt | |
| 3.1.7 Anonymisieren | entfällt | |
| 3.2.1.1 Verfügbarkeit | adäquat | |
| 3.2.1.2 Integrität | adäquat | |
| 3.2.1.3 Vertraulichkeit | adäquat | |
| 3.2.1.4 Nicht-Verkettbarkeit | entfällt | |
| 3.2.1.5 Transparenz | adäquat | |
| 3.2.1.6 Intervenierbarkeit | adäquat | |
| 3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen | adäquat | |
| 3.2.1.8 Test und Freigabe | adäquat | Die Lizenz ist immer nur begrenzt gültig. Läuft sie ab, |

| Anforderung nach Katalog oder sonstigen Rechtsnormen | Bewertung | Kommentare |
|---|---|---|
| | | kann die Software weiter verwendet werden, aber neue Daten können nicht erfasst werden. |
| 3.2.2 Erleichterung der Vorabkontrolle | adäquat | |
| 3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses | adäquat | |
| 3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten | entfällt | |
| 3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten | | |
| 3.3.1 Verschlüsselung | adäquat | |
| 3.3.2 Anonymisierung oder Pseudonymisierung | entfällt | |
| 3.3.3.1 Mobile Datenverarbeitungssysteme | entfällt | |
| 3.3.3.1 Video-Überwachung und –Aufzeichnung | entfällt | |
| 3.3.3.1 Automatisierte Einzelentscheidungen | entfällt | |
| 3.3.3.1 Veröffentlichungen im Internet | entfällt | |
| 3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren | adäquat | |
| 3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung | entfällt | |
| 3.6 Sonstige Anforderungen | entfällt | |
| | | |
| **Komplex 4:** | | |
| 4.1 Aufklärung und Benachrichtigung | adäquat | |
| 4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten | entfällt | |
| 4.3 Auskunft | adäquat | |
| 4.4.1 Berichtigung | entfällt | |
| 4.4.2 Vollständige Löschung | adäquat | Backups werden ebenfalls gelöscht, sofern im Zugriff |
| 4.4.3 Sperrung | adäquat | |
| 4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung | entfällt | |
| 4.3.5 Gegendarstellung | entfällt | |
| 4.5 Sonstige Anforderungen | entfällt | |

**20** In datenschutzrechtlicher Hinsicht sind die zwischenzeitlich am IT-Produkt erfolgten Änderungen am Verfahren in technischer Hinsicht insgesamt positiv zu bewerten, da integrierten Schnittstellen auf Basis von technischen Neuerungen und auf gesetzlichen Grundlagen erfolgten.

**21** In rechtlicher Hinsicht hat es seit der letzten Rezertifizierung keine bewertungserheblichen Änderungen gegeben.

## E. Zusammenfassung

**22** Zusammenfassend kann dem Produkt Elefant-Profi in der Version 16.01. nach wie vor eine adäquate Umsetzung der Belange des Datenschutzes bescheinigt werden. Es bestehen

aus technischer und rechtlicher Sicht keinerlei Bedenken gegen eine Rezertifizierung des Verfahrens.

## F. Wie das Produkt den Datenschutz fördert

23 Das Produkt „Elefant Profi“ unterstützt den Benutzer zum einen durch eine sehr umfangreiche Dokumentation (Handbuch und Online-Hilfe), die viele Hilfestellungen, Anleitungen und Hinweise im Bezug auf Datenschutz und Datensicherheit enthält.

Zudem wird durch die „Security“-Option die Möglichkeit geboten die personenbezogenen Daten in der Datenbank zu verschlüsseln, so dass ein Zugriff nur mit der Lizenz möglich ist, mit der die Verschlüsselung angestoßen wurde.

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

Kellinghusen, den 19.01.2016

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

Flensburg, den 19.01.2016

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