

Kurzgutachten für die Produktzertifizierung des Moduls „Firmendaten – FiDa“, der Stammdatenverwaltung für die „Erweiterte Verwaltungsanwendung – EVA“

1 Zeitpunkt der Prüfung

Die Prüfung und Begutachtung des IT-Produkts „Firmendaten-FiDa“ der „Erweiterten Verwaltungsanwendung – EVA“ nachfolgend („FiDa“) erstreckte sich auf den Zeitraum von August 2004 - August 2005.

2 Adresse der Antragstellerin

Antragstellerin ist die IHK Gesellschaft für Informationsverarbeitung mbH (nachfolgend: „IHK-GfI“), Emil-Figge-Str. 86, 44227 Dortmund.

3 Adressen des/der Sachverständigen

Die rechtliche Begutachtung ist durch die Luther Menold Rechtsanwaltsgesellschaft mbH, Rothenbaumchaussee 78. 1, 20148 Hamburg unter der Leitung von Herrn RA Dr. Fritjof Börner erfolgt. An der rechtlichen Begutachtung hat Herr RA Dr. Flemming Moos als Mitarbeiter der Prüfstelle mitgewirkt. Die technische Begutachtung hat Herr Birger Andre Fritzowski, Kattenbek 33, 24248 Mönkeberg vorgenommen.

4 Kurzbezeichnung des IT-Produktes

Bei dem begutachteten IT-Produkt handelt es sich um das Modul IHK FiDa - Firmendaten, welche die Stammdaten für die so genannte „Erweiterte Verwaltungsanwendung – EVA“ in der Version 2.05 bereitstellt.

5 Detaillierte Bezeichnung des IT-Produktes

Bei EVA handelt es sich um eine Branchenlösung für Industrie- und Handelskammern (IHKs), die vier fachbezogene Anwendungen in separaten Modulen umfasst. Die Entwicklung der vier Module FiDa, Beruf, Beitrag und ReWe erfolgt dabei stufenweise auf Basis bestehender Verwaltungssysteme. Bei den Modulen FiDa, Beruf und Beitrag handelt es sich um Eigenentwicklungen der IHK-GfI.

Die gesamte Anwendung wird zentral bei der IHK-GfI gehostet und den Bediensteten in den einzelnen IHKs über ein geschlossenes Wide Area Network – WAN zur Nutzung zur Verfügung gestellt, welches von der ecofis GmbH betrieben wird.

Gegenstand der Begutachtung ist somit nicht nur die Software-Anwendung an sich, sondern auch das Betriebsumfeld in Gegenstand des von der IHK-GfI betriebenen Rechenzentrums, in dem die Anwendung einschließlich der Daten zentral gespeichert sind, sowie das von der ecofis GmbH betriebene

WAN, über welches die Anwendung und die Daten den Nutzern in den IHKs zur Verfügung gestellt werden.

6 Tools, die zur Herstellung des IT-Produktes verwendet wurden

Siehe Kurzgutachten Technik

7 Zweck und Einsatzbereich

Das IT-Produkt EVA ist eine Branchenlösung, die IHKs zur IT-gestützten Erfüllung zahlreicher ihnen per Gesetz zugewiesener Aufgaben einsetzen können.

Bei dem Modul FiDa handelt es sich um ein Informationssystem über die IHK-Mitgliedsunternehmen, in dem Stammdaten der IHK-Mitgliedsunternehmen, wie insbesondere Firmierungen, Gesellschaftsformen, Anschriften, Branchen, Unternehmensgrößen etc. gespeichert und verarbeitet werden können. Darüber hinaus werden in dem Modul „FiDa“ Stammdaten zu den in den weiteren EVA-Modulen „Beruf“, „Betrag“ und „ReWe“ gespeicherten „Kernobjekten“ (also z.B. Auszubildende, Ausbildungsstätten, Kreditoren, Debitoren) vorgehalten.

8 Modellierung des Datenflusses

Siehe Kurzgutachten Technik

9 Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog Version 1.1, Stand: 6. März 2002

10 Zusammenfassung der Prüfungsergebnisse

Insgesamt entspricht das Modul FiDa den Rechtsvorschriften über den Datenschutz und die Datensicherheit in adäquater Weise.

Beim Einsatz des Moduls FiDa werden sowohl Primär- als auch Sekundärdaten erhoben und verarbeitet.

Bei den mittels FiDa verarbeiteten Primärdaten kann es sich sowohl um Informationen über Einrichtungen, wie z.B. Firmen und Institutionen, als auch über die mit diesen Einrichtungen in Verbindung stehenden Personen und die sich daraus ergebenden Beziehungen handeln. Innerhalb des Moduls FiDa sind einzelne Gruppen von Primärdaten zu so genannten „Objekten“ zusammengefasst. Ein Objekt entspricht dabei in aller Regel einer Bildschirm-Maske.

Zentraler Bezugspunkt jeder in FiDa gespeicherten Information ist immer ein so genanntes „Kernobjekt“. Ein Kernobjekt steht immer für eine bestimmte Firma, eine bestimmte Person oder ein bestimmtes Gremium. Jedem Kernobjekt wird eine individuelle Identifizierungsnummer (Identnummer)

zugewiesen. Um den verschiedenen Firmen-, Personen- und Gremientypen bei der Erfassung in FiDa Rechnung zu tragen, werden insgesamt neun verschiedene Kernobjekttypen unterschieden: „Hauptsitz (HS)“, „Zweigniederlassung (ZN)“, „Betriebsstätte (BST)“, „Kleingewerbetreibender (KGT)“, „Gesellschaft bürgerlichen Rechts (GBR)“, „Person (PERS)“, „Gremium (GREM)“, „Institution (INST)“, „Nebenstelle (NST)“.

Daneben existieren eine Reihe weiterer Objekte, in denen jeweils Gruppen von Einzelinformationen thematisch zusammengefasst sind, und die diesen Kernobjekten zugeordnet sind. Dabei wird differenziert zwischen so genannten „Zwangs-Objekten“, „Muss-Objekten“ und „Kann-Objekten“. Ein Kernobjekt kann technisch nicht angelegt werden, ohne dass die dazugehörigen Zwangs-Objekte ebenfalls angelegt werden. Solche Zwangs-Objekte sind die Objekte „Anschrift (ANS)“ und „Verwaltungsdaten (VERW)“. Im Unterschied dazu verhindern fehlende oder unvollständige Muss-Objekte zwar nicht die Anlage eines Kernobjekts, sie bewirken aber den Status „unvollständig“. Solche Muss-Objekte sind z.B. die Objekte „Firmenbasisdaten (BAS)“, „Branchen (BRAN)“ und „Handelsregister (REG)“. Bei allen übrigen Objekten handelt es sich um Kann-Objekte. Diese können, müssen aber nicht angelegt werden. Sie haben keinen Einfluss auf den Status des Kernobjekts.

Innerhalb von FiDa können folgende Kann-Objekte angelegt werden: „Außenwirtschaftsbasisdaten“, „Bankdaten“, „Betriebsaufgabe“, „Beteiligungen“, „Carnetbasis“, „Chronologie“, „Einladungen“, „Firmenabhängige Personen“, „Steuernummern“, „Gremien zu einer Firma/Person“, „Industriedaten“, „Klassifikationen“, „Konjunktur“, „Kontakte“, „Länderbeziehungen“, „Mitgliedschaften in Gremien“, „Nebenstelle zur Institution“, „Personen aus Firmen“, „Personenbasisdaten“, „Produkte“, „Postzeitungsdienst“, „Register und Basis“, „Telekommunikation“, „Termine“, „Texte“, „Vertreter“ und „Wahlen“.

10.1 Zulässigkeit der Datenverarbeitung

Eine Vielzahl der in den Objekten des Moduls FiDa speicherbaren Daten beziehen sich ausschließlich auf juristische Personen und unterliegen deshalb für sich genommen nicht den datenschutzrechtlichen Vorschriften. Dies gilt insbesondere für die in den Objekten „Firmenanschrift“, „Firmenbasisdaten“, „Branchen“, „Handelsregister“, „Außenwirtschaftsbasisdaten“, „Bankdaten“, „Betriebsaufgaben“, „Beteiligungen“, „Carnetbasis“, „Chronologiedaten“, „Steuernummern“, „Industriedaten“, „Klassifikationen“, „Konjunktur“, „Länderbeziehungen“, „Produkte“, „Postzeitungsdienst“, „Texte und Wahlen“ enthaltenen Informationen, soweit sie sich nicht auf Einzelkaufleute, Personenvereinigungen oder so genannte „Ein-Mann-GmbHs“ beziehen. Der Anwendung der datenschutzrechtlichen Vorschriften steht es allerdings nicht entgegen, dass es sich bei einem Teil der Daten um nicht personenbezogene Daten handelt. Insoweit reicht es für die Anwendbarkeit der datenschutzrechtlichen Vorschriften auf Datenverarbeitungsvorgänge im Hinblick auf einen Gesamtdatenbestand aus, dass ein Teil der Daten Personenbezug aufweist. Personenbezogene Daten können insbesondere in den Objekten „Anschrift-

ten (Personenanschrift)", „Verwaltungsdaten“, „Beteiligungen“, „Firmenabhängige Personen“, „Kontakte“, „Mitgliedschaften in Gremien“, „Personenbasisdaten“, „Telekommunikation“, „Texte“ und „Benutzer“ gespeichert werden.

Die Zulässigkeit der mit dem Modul FiDa erfolgenden Datenverarbeitungsschritte ergibt sich aus der spezialgesetzlichen Ermächtigungsvorschrift des § 9 Abs. 1 IHKG und zahlreichen weiteren, fachgesetzlichen Erlaubnisvorschriften sowie der Generalklausel in § 11 LDSG SH.. Die kammerspezifische Datenschutzregelung in § 9 IHKG steht zu den datenschutzrechtlichen Regelungen des LDSG SH dabei im Verhältnis der Spezialität: soweit § 9 IHKG eine Regelung trifft, gilt diese vorrangig vor dem LDSG SH; soweit weder in § 9 IHKG noch in anderen speziellen Vorschriften eine Regelung enthalten ist, gilt subsidiär das LDSG SH. Im Einzelnen ergibt sich die Rechtmäßigkeit der einzelnen Datenverarbeitungen aus folgenden Erwägungen:

10.1.1 Daten der Gewerbeüberwachungsbehörden

Nach § 9 Abs. 1 IHKG dürfen die IHKs zur Erfüllung der ihnen nach dem IHKG übertragenen Aufgaben die Daten nach § 14 Abs. 5 Satz 1 Nr. 1 der Gewerbeordnung (GewO) bei den Kammerzugehörigen erheben, soweit diese Daten ihnen nicht von der zuständigen Behörde übermittelt worden sind. Darüber hinaus dürfen sie Daten über angebotene Waren und Dienstleistungen sowie über die Betriebsgrößenklasse bei den Kammerzugehörigen erheben. Außerdem dürfen die IHKs gemäß § 9 Abs. 2 IHKG die zur Festsetzung der Beiträge der Kammerzugehörigen die in § 3 Abs. 3 IHKG genannten Bemessungsgrundlagen bei den Finanzbehörden erheben.

Somit sind die IHKs insbesondere berechtigt, die Daten zu erheben, welche die Gewerbeüberwachungsbehörden auch von sich aus nach § 14 Abs. 5 Satz 1 Nr. 1 GewO den Kammern regelmäßig übermitteln dürfen. Die in Betracht kommenden Daten ergeben sich aus § 14 Abs. 4 GewO, insbesondere aus den der Gewerbeordnung als Anlagen beigefügten Formularmustern für die Gewerbeanmeldung, Gewerbeummeldung und Gewerbeabmeldung.

Die in § 9 Abs. 1 und 2 IHKG genannten Daten dürfen die IHKs gemäß § 9 Abs. 3 S. 1 IHKG speichern und nutzen, soweit dies zur Erfüllung der ihnen nach dem IHKG übertragenen Aufgaben erforderlich ist. Die Zulässigkeit (Erforderlichkeit) einer konkreten Datenspeicherung und –verarbeitung ist somit von der verantwortlichen Stelle einzelfallabhängig zu prüfen und sicher zu stellen. Dabei ist es zwanglos denkbar, dass in bestimmten Fällen, sämtliche der in § 9 Abs.1 und 2 IHKG aufgeführten Daten gespeichert und verarbeitet werden müssen. Die zu begutachtende Software-Anwendung erfüllt deshalb schon dann die an sie zu stellenden Anforderungen, wenn die Eingabefelder über diesen Maximalbestand an erforderlichen Daten nicht hinausgehen. Eine Einschränkung dieses Maximalbestandes – etwa aufgrund des Erforderlichkeitsprinzips – kann lediglich dadurch erfolgen, dass bestimmte Felder nicht befüllt werden. Dies haben die IHKs als verantwortliche Stellen in der Hand. Die

zu begutachtende Software gibt den IHKs den nötigen Freiraum auf den Verzicht der Speicherung nicht erforderlicher Daten dadurch, dass es kaum „Zwangsfelder“ gibt, die zwingend zu befüllen sind.

Im Ergebnis dient § 9 Abs. 1 IHKG i.V.m. § 9 Abs. 3 S. 1 IHKG deshalb als Erlaubnisvorschrift für die Erhebung und Speicherung der in folgenden Objekten des Moduls FiDa enthaltenen Daten: Anschriften – ANS; Firmenbasisdaten – BAS; Branchen – BRAN; Handelsregister – REG; Betriebsaufgaben – BAUF; Firmenabhängige Personen – FAP; Klassifikationen – KLAS; Personenbasisdaten – PBAS und Telekommunikation – TEL.

Aus datenschutzrechtlicher Sicht besonders relevant sind in diesem Zusammenhang die Informationen über das Sterbedatum und den Geburtsnamen, welche in dem Modul „PBAS“ eingegeben werden können. Die Erforderlichkeit zur Speicherung des Sterbedatums kann sich insbesondere im Zusammenhang mit einer Betriebsaufgabe ergeben, etwa um das Datum und den Grund einer Betriebsaufgabe anzugeben, wie es gemäß Ziffer 17 bzw. 23-25 des Gewerbeabmeldungsformulars vorgesehen ist. Eine Speicherung des Geburtsnamens kann insbesondere zur eindeutigen Personenzuordnung notwendig sein: neben dem Geburtsdatum wird auch der Geburtsname zur eindeutigen Identifizierung von ansonsten gleichnamigen Personen herangezogen.

10.1.2 Daten über Waren, Dienstleistungen und Betriebsgrößenklassen

Über die sich aus § 14 Abs. 4 GewO ergebenden Daten hinaus können die IHKs nach § 9 Abs. 1 Satz 2 IHKG auch Daten über die von ihren Kammerzugehörigen angebotenen Waren- und Dienstleistungen sowie über die Betriebsgrößenklassen bei ihren Kammerzugehörigen erheben. Auch für diese Daten gilt zwar die Einschränkung des Satzes 1, wonach die IHKs diese Daten nur zur Erfüllung der ihnen übertragenen Aufgaben erheben dürfen. Diese Voraussetzung ist aber regelmäßig gegeben, weil die IHKs diese Daten zur Förderung der gewerblichen Wirtschaft, insbesondere zur Förderung von Geschäftsabschlüssen und die Daten über die Betriebsgrößenklassen zusätzlich auch zur Beurteilung und Gewichtung von Meinungsäußerungen der Kammerzugehörigen bei der Abgabe von Stellungnahmen und für statistische Zwecke benötigen, wie es in der Aufgabenzuweisung gemäß § 1 Abs. 1 IHKG vorgesehen ist. § 9 Abs. 1 S. 2 IHKG bildet deshalb insbesondere für die in die Objekte Konjunktur – KOJU und Produkte – PROD einzutragenden Informationen die datenschutzrechtliche Grundlage, wobei einige der in dem Modul Konjunktur – KOJU speicherbaren Daten im Zusammenhang mit Konjunkturumfragen der IHKs erhoben und insoweit nur aufgrund einer Einwilligung der Betroffenen erhoben werden dürfen.

10.1.3 Daten bzgl. dem Wirtschaftsverkehr dienenden Bescheinigungen

Des Weiteren ist den IHKs in § 1 Abs. 3 IHKG die Aufgabe zugewiesen, Ursprungszeugnisse und andere dem Wirtschaftsverkehr dienende Bescheinigungen auszustellen. Ursprungszeugnisse sind nach

internationalen Handelsabkommen vielfach im Warenverkehr zur Feststellung des Herkunftslandes vorgeschrieben. Rechtsgrundlage für die Ausstellung von Ursprungszeugnissen durch die IHKs sind neben § 1 Abs. 3 IHKG das internationale Abkommen zur Vereinfachung der Zollformalitäten vom 3. November 1923, in Kraft für Deutschland seit dem 30. Oktober 1925 (RGBL. II, 812), sowie der Zollkodex der EG (VO/EWG Nr. 291/92 vom 12. Oktober 1992, ABL.EG Nr. 1303), wo die Artikel 22 bis 26 den Ursprung und die Ursprungszeugnisse behandeln.

Die dafür benötigten Informationen dürfen die IHKs auf Grundlage § 1 Abs. 3 IHKG i.V.m. § 11 Abs. 1 Satz 3 LDSGSH bzw. einer etwa einschlägigen bereichsspezifischen Erlaubnisvorschrift erheben. Diese Vorschriften können folglich insbesondere für die in dem Objekt „Länderbeziehungen- LAND“ zu speichernden Daten herangezogen werden.

Zu den anderen dem Wirtschaftsverkehr dienenden Bescheinigungen im Sinne von § 1 Abs. 3 IHKG gehören auch die internationalen Zollpapierhefte, die so genannten „Carnets“. Carnets erleichtern die vorübergehende Verbringung von Berufsausrüstung, Messegut und Warenmuster ins Ausland, indem sie die Zahlung oder Hinterlegung von Zöllen und sonstigen Abgaben in den Einfuhr- bzw. Durchfuhrländern entbehrlich machen. Für die Ausstellung und Bearbeitung eines solchen Carnets können die IHKs insbesondere auf die Objekte Bankdaten – BANK und Carnetbasis – CBAS zurückgreifen. Die Erlaubnis zur Erhebung der in diesen Objekten enthaltenen Informationen kann sich folglich aus § 1 Abs. 3 IHKG i.V.m. § 11 Abs. 1 Nr. 3 LDSGSH ergeben.

10.1.4 Daten aus öffentlichen Quellen, insbesondere Handelsregisterdaten

§ 11 Abs. 2 LDSGSH gestattet die Verarbeitung personenbezogener Daten, die allgemein zugänglichen Quellen entnommen werden können, soweit schutzwürdige Belange der Betroffenen nicht beeinträchtigt sind. Solche öffentlich zugänglichen Quellen sind u.a. Zeitungen, das Handelsregister sowie der Bundesanzeiger. Zur Speicherung der so veröffentlichten Daten dienen bei FiDa insbesondere die Objekte Firmenbasisdaten – BAS; Handelsregister – REG; Chronologiedaten – CHRO; Beteiligungen – BET und Texte – TXT. Die Beurteilung der Frage, ob dabei jeweils ein schutzwürdiges Interesse des Betroffenen einer Speicherung der Daten überwiegt, obliegt der jeweiligen IHK. Im Ergebnis kann also § 11 Abs. 3 LDSGSH als Rechtsgrundlage für die Speicherung der Daten in den genannten Objekten herangezogen werden.

Im Hinblick auf die Chronologiedaten war unter dem Aspekt der Erforderlichkeit näher zu prüfen, aus welchem Grund solche historischen Informationen während der gesamten Dauer der Kammerzugehörigkeit gespeichert werden dürfen. Insoweit lässt sich insbesondere die Datenkonsistenz als Rechtfertigungsgrund anführen: insbesondere können die Chronologiedaten zur eindeutigen Identifizierung von Mitgliedsunternehmen (z.B. nach Firmenänderungen) herangezogen werden. Im Ergebnis kann

es also durchaus erforderlich sein, die Chronologiedaten während der gesamten Dauer der Kammerzugehörigkeit eines Unternehmens zu speichern.

10.1.5 Daten aus Umfragen der IHKs

Die IHKs erheben weitere Informationen durch Umfragen bei ihren Mitgliedsunternehmen. Diese Umfragen beziehen sich u.a. auf Umsatzgrößen und Umsatzschwerpunkte in regionalen und nationalen Märkten, Mitarbeiterzahlen und –wachstum, Geschäftsfelder, Mitarbeiterstrukturen, Qualifikationen von Mitarbeitern, Standortfaktoren, Belegenheiten von Niederlassungen, Ausbildungsberufe, Länderverbindungen etc. Insbesondere führen die IHKs regelmäßig quartalsweise oder halbjährlich so genannte Konjunkturumfragen bei ihren Mitgliedern durch. Gegenstand der Konjunkturumfragen sind vor allem Fragen zur aktuellen und künftigen Geschäftslage, zu Entwicklungen des Exports, zur Höhe von Investitionen und zur Höhe und Entwicklung der Beschäftigtenzahlen. Weitere Fragen können die Auftragslage, Preiserwartungen und Investitionspläne betreffen. Diese Informationen werden u.a. in die Objekte Außenwirtschaftsbasisdaten – AUWI; Industriedaten – INDU; Konjunktur – KOJU; Länderbeziehungen – LAND und Texte – TXT aufgenommen.

Im Regelfall ist insoweit eine Einwilligung der Befragten erforderlich. Mit der Maßgabe der Einhaltung der datenschutzrechtlichen Anforderungen an eine wirksame Einwilligungserklärung, die in der Verantwortung der jeweiligen IHK liegen, können somit auch diese Informationen rechtmäßig erhoben und in FiDa gespeichert werden.

Das Produkt FiDa unterstützt dabei die Einholung wirksamer Einwilligungserklärungen durch die IHKs vor allem dadurch, dass im Benutzhandbuch ausdrückliche Hinweise auf die Notwendigkeit datenschutzrechtlicher Einwilligungserklärungen und Unterrichtungen sowie die gesetzlichen Anforderungen an die Wirksamkeit solcher Erklärungen enthalten sind und die Durchführung von Umfragen unter den Kammermitgliedern ausdrücklich als Beispiel angeführt ist. Im Ergebnis unterstützt das Produkt FiDa deshalb auch die Speicherung und Verarbeitung von Daten aus Umfragen der IHKs, für die eine Einwilligungserklärung erforderlich ist, in adäquater Weise.

10.1.6 Gremieninformationen

Bei den IHKs können gemäß § 8 IHKG Ausschüsse gebildet werden. Auf Basis dieser Vorschrift werden bei den IHKs in der Regel durch Satzung oder durch Beschluss der Vollversammlung zahlreiche Fach- und Regionalausschüsse gebildet. Oft handelt es sich bei den Mitgliedern der Fachausschüsse um leitende Angestellte kammerzugehöriger Unternehmen mit besonderen Kenntnissen auf einzelnen Fachgebieten, Angehörige der freien Berufe oder um Vertreter der Kommunalverwaltungen. Insbesondere die Fach- und Regionalausschüsse werden in dem Modul FiDa als so genanntes „Gremium“

verwaltet. In diesem Zusammenhang werden Informationen in die Module Mitgliedschaft in Gremien – MITG; Einladungen – EINL und Termine – TERM aufgenommen.

Die in diesen Objekten aufzunehmenden Informationen beziehen sich auf die Mitgliedschaft in einem solchen Gremium und dienen der Organisation der Gremientätigkeit durch entsprechende Termine für Gremiensitzungen und Einladungen zu diesen Sitzungen. Da die Bildung solcher Gremien gemäß § 8 IHKG zu den Aufgaben der IHKs zählt und auch in bereichsspezifischen Gesetzen die Einrichtung von Gremien und Ausschüssen durch die IHKs vorgesehen ist (etwa in § 39 Berufsbildungsgesetz – BBiG), ist die Erhebung und Speicherung personenbezogener Daten der Gremienmitglieder im Zusammenhang mit ihrer Mitgliedschaft und den Aufgaben der jeweiligen Gremien von § 11 Abs. 1 Nr. 3 LDSG SH gedeckt.

10.1.7 Informationen bezüglich Kammerwahlen

Gemäß § 5 Abs. 1 IHKG werden die Mitglieder der Vollversammlung von den Kammerzugehörigen gewählt. Gemäß § 4 Satz 2 Nr. 1 IHKG beschließt die Vollversammlung eine entsprechende Wahlordnung. In diesen Wahlordnungen der IHKs ist üblicherweise vorgesehen, dass die IHK-Zugehörigen zum Zwecke der Wahl und in bestimmte Wahlgruppen und Wahlbezirke eingeteilt werden. Die Wahlgruppen werden regelmäßig nach Wirtschaftsbereichen gebildet (z.B. Industrie und Bau, Einzelhandel, Großhandel, Dienstleistungen, Kreditinstitute etc.). Bei den Wahlbezirken handelt es sich um regionale Unterteilungen des Kammerbezirks. Diese Informationen können in dem Objekt „Wahlen – WAHL“ gespeichert werden. Insoweit bildet § 5 IHKG i.V.m. § 11 Abs. 1 Nr. 3 LDSGSH die datenschutzrechtliche Grundlage für die Erhebung und Speicherung dieser Daten.

10.1.8 Informationen zu Publikationen der IHKs

Zu den Aufgaben der IHKs gehört gemäß § 1 Abs. 1 IHKG u.a. auch die Förderung der gewerblichen Wirtschaft. Zu diesen Förderaufgaben zählt u.a. die Information der kammerzugehörigen Unternehmen. In Erfüllung dieses Informationsauftrages geben die IHKs deshalb regelmäßig Kammerzeitschriften und sonstige Informationsblätter heraus, welche die Kammerzugehörigen über neue wirtschaftspolitische oder wirtschaftsrechtliche Maßnahmen und Spezialfragen wirtschaftlicher Art unterrichten. Für die Speicherung von Informationen über den Bezug solcher Publikationen, die im Modul FiDa in dem Objekt „Postzeitungsdienst – PZD“ erfolgt, besteht somit in § 1 Abs. 1 IHKG i.V.m. § 11 Abs. 1 Nr. 3 LDSGSH eine hinreichende Grundlage.

10.1.9 Steuernummern

Die IHKs sind sowohl für die Feststellung der Kammerzugehörigkeit, die von der Gewerbesteuerpflicht abhängt, vor allem aber für die Erhebung der Beiträge auf die Mitteilung der Gewerbeerträge, der Zer-

legungsanteile und gegebenenfalls auf die Mitteilung von Gewinnen durch die Finanzbehörden angewiesen. Die Finanzbehörden sind zu diesen Mitteilungen nach § 31 AO berechtigt. In § 9 Abs. 2 IHKG ist das spiegelbildliche Recht der IHKs, zur Erhebung der Beitragsbemessungsdaten bei den Finanzbehörden geregelt. Im Rahmen der Beitragsbemessung benötigen die IHKs die Gewerbesteuernummern für den Ertrags und die Einkommenssteuernummern für den Gewinn im Rahmen der Zuordnung der entsprechenden Erträge und Gewinne zu einzelnen Kammermitgliedern (die kammerintern nach Identnummern geführt werden). Für die Speicherung der in dem Objekt FISK speicherbaren Steuernummern bietet somit § 9 Abs. 2 IHKG eine hinreichende Rechtsgrundlage.

10.1.10 Informationen über Kontakte

Im Rahmen der Förderung der gewerblichen Wirtschaft gemäß § 1 Abs. 1 IHKG erteilen die IHKs auch Auskünfte, sprechen Empfehlungen und Warnungen aus und erbringen Beratungsleistungen. Zur Bearbeitung entsprechender Anfragen der Kammerzugehörigen kann es deshalb erforderlich sein, Informationen über den Anfragenden und die Art der Anfrage zu speichern, wie es das Objekt „Kontakte – KONT“ ermöglicht. Somit kann auch eine Erhebung und Speicherung der in diesem Objekt zu hinterlegenden Daten auf Grundlage von § 1 Abs. 1 IHKG i.V.m. § 11 Abs. 1 Nr. 3 LDSGSH in datenschutzrechtlich zulässiger Weise erfolgen.

10.1.11 Sonstige Informationen

Darüber hinaus bestehen eine Reihe weiterer Aufgabenzuweisungen an die IHKs (z. B. Unterrichtung für Geschäftsführer und Mitarbeiter von Bewachungsunternehmen gemäß § 34 a GewO, Sachkundeprüfung für bestimmte Tätigkeiten im Bewachungsgewerbe gemäß § 34 a GewO, Stellungnahmen zu Anträgen auf Ausnahmen vom Ladenschlussgesetz, Stellungnahmen zur persönlichen Zuverlässigkeit und Sachkunde vor Erteilung einer gewerberechtlichen Erlaubnis für Pfandleiher, Bewachungsgewerbe, Versteigerer, Makler gemäß §§ 34 a, 34 b, 34 c GewO, Stellungnahmen im Gewerbeuntersuchungsverfahren gemäß § 35 Abs. 4 GewO, Stellungnahmen zur Erteilung von Genehmigungen für den gewerblichen Güterkraft- und Straßenpersonenverkehr, für die Änderung von Taxitarifen sowie für die Verhängung von Fahrverboten gemäß §§ 14, 39, 83 Güterkraftverkehrsgesetz und §§ 14, 39, 51 Personenbeförderungsgesetz, Dringlichkeitsbescheinigungen für Ausnahmegenehmigungen vom Sonn- und Feiertagsfahrverbot für LKW gemäß § 46 StVO etc.)

Für die Erfüllung dieser gesetzlichen Aufgaben sind die IKHs vielfach darauf angewiesen, Daten – seien sie personenbezogen oder nicht – zu erheben und zu speichern. Zu diesem Zweck steht insbesondere das Objekt „Texte – TXT“ bereit.

Im Ergebnis lässt sich deshalb sagen, dass für sämtliche Informationen, die in dem Modul FiDa nach seiner Zweckbestimmung gespeichert werden sollen, eine datenschutzrechtliche Grundlage vorhan-

den ist. In der überwiegenden Zahl der Fälle greift § 9 IHKG als Ermächtigungsgrundlage ein. Daneben umfasst das Modul FiDa eine Reihe von Eingabefeldern, in die Daten aufgenommen werden können, die die IHKs – über die Ermächtigung gemäß § 9 IHKG hinaus – im Rahmen ihrer Aufgabenerfüllung gemäß § 1 Abs. 1 IHKG benötigen und nach Maßgabe von § 11 Abs. 1 Nr. 3 LDSGSH auch erheben und speichern dürfen. Schließlich existieren auch einige Eingabefelder, die nur auf Grundlage einer Einwilligung der betroffenen Personen gefüllt werden dürfen, was aber der Möglichkeit eines datenschutzkonformen Einsatzes der Software-Anwendung nicht entgegensteht, so dass insoweit eine adäquate Umsetzung der Vorgaben gegeben ist.

10.1.12 Übermittlung personenbezogener Daten

Die Anwendung FiDa ermöglicht eine Übermittlung von Daten an andere IHKs in Gestalt der so genannten „kammerübergreifenden Suche“. Im Rahmen der kammerübergreifenden Suche kann gemäß einer Verständigung aller angeschlossenen IHKs nur auf die Daten in den Objekten Anschriften – ANS; Basisdaten – BAS; Betriebsaufgaben – BAUF; Beteiligungen – BET; Branchen – BRAN; Chronologiedaten – CHRO; Firmenabhängige Personen – FAP; Steuerdaten – FISK; Firmen zur Person – PAF; Registerdaten – REG; Telekommunikationsdaten – TEL und Texte – TXT zugegriffen werden. Bei der Nutzung dieser Informationen durch andere IHKs im Rahmen der kammerübergreifenden Suche handelt es sich regelmäßig nicht um eine zweckändernde Nutzung, da der primäre Zweck der kammerübergreifenden Suche darin besteht, die Informationen zu Hauptsitzen von Kammermitgliedern zu erfassen, die außerhalb des eigenen Kammerbezirks liegen, wenn und soweit im eigenen Kammerbezirk ein Betriebsstätte errichtet wird.

Dabei unterstützt das Modul FiDa die Zweckbindung beim Zugriff auf Daten einer anderen Kammer, indem jeder Nutzer unmittelbar nach der Anmeldung im System zum Zugriff auf den Datenbestand einer anderen Kammer in einem eigenen Bildschirmfenster darauf hingewiesen wird, dass er nun Zugriff auf Daten einer anderen IHK hat und er die Daten nur für die Zwecke nutzen darf, für die ihm der Zugriff eingeräumt worden ist. Der Anwender muss auf den in diesem Hinweisfenster befindlichen „OK“-Button klicken, um das Fenster zu schließen.

Der Zugriff auf Daten anderer IHKs im Wege der kammerübergreifenden Suche ist im Ergebnis von der Erlaubnisvorschrift in §§ 11, 13 Abs. 2 – 6 LDSGSH gedeckt.

10.1.13 Einwilligungserklärungen

Nur für wenige Daten sind Einwilligungserklärungen der Betroffenen erforderlich. Das Modul FiDa unterstützt dabei die Einholung wirksamer Einwilligungserklärungen durch ausdrückliche Hinweise auf die Notwendigkeit solcher Einwilligungen im Benutzerhandbuch.

10.1.14 Sonstige Rechtmäßigkeitsvoraussetzungen

Das Modul FiDa ermöglicht auch eine Speicherung von Informationen über die Herkunft von Daten in dem Objekt Texte – TXT. Zu diesem Zweck ist in dem Objekt Texte – TXT ein eigenes Thema „Datenherkunft“ eingerichtet.

10.2 Zweckbindung und Trennungsprinzip

Das Modul FiDa unterstützt die Beachtung der nach dem LDSG SH vorgeschriebenen Zweckbindung durch die Anwender durch ein ausdifferenziertes Berechtigungssystem und die Möglichkeit der Kennzeichnung bestimmter Daten durch ein so genanntes „Datenschutzkennzeichen“.

Die Berechtigungssteuerung in dem Modul FiDa erfolgt durch zwei sich ergänzende Berechtigungskonzepte: Zum einen erfolgt eine Rechtevergabe für bestimmte Objekte und die mit diesen Objekten verbundenen Funktionen, zum anderen kann die Zugriffsberechtigung auf bestimmte Daten beschränkt werden. Durch die Objektberechtigung wird festgelegt, welche Module und Bildschirmmasken ein Benutzer aufrufen darf, wobei jedes Objekt weiter feldweise eingeschränkt werden kann, indem einem Benutzer nur bestimmte Funktionen erlaubt werden. Dabei kann auch die Funktion „Geschützt“ gesetzt werden, welche bewirkt, dass das entsprechende Feld dem jeweiligen Benutzer gar nicht angezeigt wird. Berechtigungen zur Bearbeitung von Objekten müssen in jedem Fall explizit vergeben werden. Ist ein Objekt in den Berechtigungsdaten eines einzelnen Benutzers oder einer Benutzergruppe nicht aufgeführt, dann kann der Benutzer diese Daten nicht bearbeiten. Durch die Datenberechtigung wird darüber hinaus festgelegt, auf welche Identnummern, bereichsbezogenen Informationen etc. ein Anwender Zugriff erhält

Aufgrund des Berechtigungskonzepts erhalten die Anwender grundsätzlich nur Zugriff auf den Datenbestand ihrer eigenen IHK. Dies ist dadurch gewährleistet, dass im Rahmen der Anmeldeprozedur die Benutzerkennung anzugeben ist und diese mit der Benutzerdatei der IHK abgeglichen wird. Zugang wird nur gewährt, wenn eine Übereinstimmung gegeben ist. Dadurch ist es ausgeschlossen, dass beispielsweise ein Angehöriger der IHK Kiel bei der Anmeldeprozedur die Kammernummer der Handelskammer in Hamburg eingibt und so Zugriff auf deren Datenbestand erhält.

Darüber hinaus sieht das Modul FiDa in den Objekten AUWI, INDU und LAND die Angabe eines Datenschutzkennzeichens vor, wobei es sich bei diesen Datenschutzkennzeichen in den Objekten AUWI und INDU um ein so genanntes „Muss-Feld“ handelt. Wenn das Datenschutzkennzeichen gesetzt ist, erscheint in der Kopfzeile der jeweiligen Maske der Hinweis „Gesperrt“. Auf diese Weise werden die Anwender darauf hingewiesen, dass eine Übermittlung oder anderweitige Verarbeitung der gekennzeichneten Daten – etwa wegen eines Widerspruchs im Sinne von § 9 Abs. 4 IHKG – nicht oder nur eingeschränkt zulässig ist.

Den Anforderungen an das Trennungsprinzip wird das Modul FiDa insbesondere dadurch gerecht, dass sämtliche Informationen – und damit auch sämtliche personenbezogenen Daten – immer nur zu einem bestimmten Kernobjekt, also einem bestimmten Unternehmen oder einer bestimmten natürlichen Person, gespeichert werden, die durch eine eindeutige Identifikationsnummer (sogenannte „Identnummer“) individualisiert ist. Sollen also personenbezogene Informationen zu einer bestimmten Person übermittelt oder in anderer Weise verarbeitet werden, lassen sich diese Informationen von personenbezogenen Daten anderer Betroffener durch die Auswahl der entsprechenden Identnummer separieren. Eine weitere Unterstützung des Trennungsprinzips erfolgt durch die Realisierung des oben erläuterten Berechtigungskonzepts, wonach den Nutzern in den IHKs der Zugriff auf Objekte und Daten technisch unterbunden werden kann.

10.3 Auftragsdatenverarbeitung durch die IHK GfI

Von der Begutachtung mit umfasst ist auch das Betriebsumfeld des Moduls FiDa in Gegenstand des von der Antragstellerin als Auftragsdatenverarbeiterin betriebenen Rechenzentrums, in dem die Anwendung einschließlich der Daten zentral gespeichert sind. Die Auftragsdatenverarbeitung durch die Antragstellerin ist gesetzeskonform begründet und ausgestaltet. Auch die im Rechenzentrum ergriffenen technischen und organisatorischen Maßnahmen sind adäquat und entsprechen dem Stand der Technik.

Des Weiteren ist das von einem Dienstleister im Auftrag der Antragstellerin betriebene WAN, über welches die Anwendung und die Daten den Nutzern in den IHKs zur Verfügung gestellt werden, von der Begutachtung erfasst. Auch insoweit konnte das Vorhandensein der erforderlichen technischen und organisatorischen Maßnahmen festgestellt werden.

10.4 Datenvermeidung und Datensparsamkeit

Das Modul FiDa ermöglicht eine datensparsame Datenverarbeitung durch die Differenzierung so genannter „Zwangs-, Muss- und Kann-Objekte“, wobei lediglich die so genannten Zwangsobjekte aus technischer Sicht vorhanden sein müssen, damit ein Kernobjekt (also ein Unternehmen oder eine Person) angelegt werden kann. Diese Zwangsobjekte sind auf das zur eindeutigen Identifizierung der Kernobjekte absolut notwendige Maß beschränkt. Darüber hinaus ermöglicht es das Modul FiDa, auch innerhalb eines Objekts für die einzelnen Informationen festzulegen, ob es sich um Zwangs-, Muss- oder Kann-Felder handelt. Analog zu den Zwangs-, Muss- und Kann-Objekten ist der aus technischer Sicht erforderliche Datenbestand wiederum auf die Zwangs-Felder begrenzt. Dabei handelt es sich vor allem um so genannte „Schlüsselfelder“, die notwendig sind, um einen Datensatz eindeutig identifizieren zu können.

Darüber hinaus bietet das Modul FiDa den IHKs im Rahmen der so genannten „Datenparametrierung“ bzw. „Feldberechtigung“ die Möglichkeit, die Sichtbarkeit und Nutzung einzelner Datenfelder nutzerspezifisch weiter einzuschränken. Im Rahmen der Feldberechtigung kann festgelegt werden, ob ein Anwender einen Feldinhalt bearbeiten, nur ansehen bzw. weder bearbeiten noch ansehen darf. Auf diese Weise kann ein anwenderspezifischer Filter gesetzt werden, der dem Einzelnen nur Zugriff auf die Daten erlaubt, die er zur Erfüllung seiner Aufgaben benötigt. Dadurch ist eine sehr datensparsame Organisation der Datenverarbeitungsverfahren in den IHKs möglich, so dass die Vorgaben der Datensparsamkeit und Datenvermeidung insoweit vorbildlich umgesetzt sind.

Im Hinblick auf den Grundsatz der Datenvermeidung und der Datensparsamkeit kritisch zu würdigen waren die in dem Modul vorhandenen Freitext- und „Info“-Felder, die eine Freitexteingabe, teilweise zu einem von der Software selbst nicht vorgegebenen Zweck, ermöglichen. Insoweit war jedoch zu berücksichtigen, dass den IHKs von Gesetzes Wegen zahlreiche Aufgaben zugewiesen sind, für deren Wahrnehmung sie auch Informationen erheben und speichern müssen, die nicht in vordefinierten Feldern oder Auswahlmenüs abgebildet werden können. Die jeweilige gesetzliche Aufgabenzuweisung kann es deshalb erforderlich machen, dass eine IHK zu einem bestimmten Mitgliedsunternehmen oder einer bestimmten (firmenabhängigen) Person weitere Textinformationen speichert, für die in den übrigen Objekten oder Modulen keine Eingabefelder vorgesehen sind. Der Bedarf nach solchen Freitextfeldern ergibt sich zudem aus der Notwendigkeit, den einzelnen IHKs eine gewissen Flexibilität bei der Dateneingabe und –verwaltung zu geben, damit nicht jeder Bedarf nach individuellen Dateneingaben im Wege einer zentralen Datenbank- bzw. Softwareänderung für sämtliche IHKs erfolgen muss. Dieses Erfordernis ergibt sich daraus, dass die Aufgaben der IHKs – insbesondere nach Maßgabe der jeweiligen landesgesetzlichen Vorschriften – variieren mit der Folge, dass aufgrund dieser unterschiedlichen Aufgabenzuweisungen manche IHKs Daten erheben und speichern, die von anderen IHKs nicht benötigt werden. Da es sich bei dem IT-Produkt jedoch um eine zentral bei der IHK GfI gehostete Anwendung handelt, die sämtlichen IHKs zur Nutzung zur Verfügung gestellt wird, können kammerindividuelle Anpassungen nicht erfolgen.

Die Freitextfelder im Objekt „Texte – TXT“ sind von den Bearbeitern in den IHKs außerdem nur nutzbar, wenn zuvor der Administrator der jeweiligen IHK eine Themenummer einschließlich Bezeichnung des Themas vordefiniert hat. Texte können also weder ohne Themenummer noch ohne Themenbezeichnung eingegeben werden.

Schließlich war im Hinblick auf die Freitextfelder positiv zu beurteilen, dass die Antragstellerin im Laufe des Zertifizierungsverfahrens eine erhebliche Verringerung des Speicherplatzes für Freitexteingaben realisiert und außerdem explizite Datenschutzhinweise zu den Freitext- und Info-Feldern in die Anwendung aufgenommen hat. So ist neben den Freitext-Eingabefelder und den Info-Feldern dauerhaft der Hinweis „Datenschutz-Hinweis“ eingeblendet. Durch Eingabe eines „X“ in das Feld „Daten-

schutz-Hinweis“ wird eine weitere Bildschirmmaske aufgerufen, in der ausführliche Hinweise auf eine datensparsame Datenablage enthalten sind. Außerdem werden die Anwender in dem Benutzerhandbuch ausdrücklich angehalten, in den Textfeldern personenbezogene Daten nur einzugeben, soweit sie zur Aufgabenerfüllung der IHKs unbedingt notwendig sind.

Weiterhin war die Ausführlichkeit und Verständlichkeit des Benutzerhandbuchs positiv zu bewerten.

10.5 Technische und organisatorische Maßnahmen

§ 5 Abs. 1 LDSG SH statuiert die Verpflichtung – auch des Auftragnehmers im Sinne von § 17 LDSG SH – die Ausführung der Datenschutzvorschriften durch technische und organisatorische Maßnahmen sicherzustellen. Es werden drei nicht abschließende Sicherheitsziele genannt, bei deren Umsetzung von einer hinreichenden Datensicherheit ausgegangen werden kann. Es handelt sich um Maßnahmen des Zugangsschutzes, des Zugriffsschutzes und der Protokollierung.

Gemäß § 5 Abs. 1 Satz 2 Ziffer 1 LDSG SH ist Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren. Die Datenträger, auf denen personenbezogene Daten bei der IHK-GfI gespeichert werden, befinden sich in dem Rechenzentrum am Standort der IHK-GfI. In Bezug auf den Zugang zu den dort vorhandenen Datenträgern hat die IKH-GfI insbesondere Schutzmaßnahmen zur Datenträgerkontrolle und zur Zugangssicherung etabliert. Durch adäquate Maßnahmen der Speicherkontrolle, insbesondere die Verwendung von Benutzercodes, Passwörtern, Verschlüsselung beim Laptop-Einsatz etc., verhindert die IHK GfI zudem, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können.

Die berechtigten Mitarbeiter können nur unter Verwendung spezifischer Benutzercodes und Passwörter auf die Daten zugreifen. In einer Dienstanweisung „Behandlung von Passworten“ werden den Mitarbeitern Hinweise für eine sichere Gestaltung von Passwörtern gegeben. Außerdem existiert bei der IHK-GfI eine Dienstanweisung „Kennwortgeschützter Bildschirmschoner“. Durch die Installation eines solchen Bildschirmschoners mit Kennwortschutz wird eine Sperrung und Dunkelschaltung der Bildschirme in Arbeitspausen realisiert. Auf diese Weise wird nicht Berechtigten das Ablesen entsprechender Daten vom Bildschirm unmöglich gemacht. Soweit Mitarbeiter der IHK-GfI mittels tragbaren Computern auf die Datenbestände zugreifen, schreibt die Dienstanweisung „Notebook“ eine Verschlüsselung der Daten vor.

Ein unbefugter Zugriff auf die FiDa-Daten wird zusätzlich dadurch unterbunden, dass bei der IHK-GfI ein ständig aktiviertes automatisches Logging-Verfahren beim Zugriff auf das Datenbankmanagementsystem ADABAS, auf dem die FiDa-Daten gespeichert sind, eingesetzt wird. In diesem Zusammenhang protokollieren die Datenbanken sämtliche ändernden Zugriffe (Neuaufnahme, Löschungen und Änderungen) des gesamten FiDa-Datenbestandes. Es wird außerdem aufgezeichnet, von welchem Terminal aus (also von welchem Nutzer) und zu welchem Zeitpunkt der ändernde Zugriff erfolgt

ist. Die Protokollierung erfolgt dabei zur Eingabekontrolle im Rahmen der Gewährleistung der Datensicherheit. Die Log-Dateien werden bei der regelmäßigen abendlichen Datenbanksicherung auf Magnetbändern gesichert und – in Umsetzung von § 6 Abs. 4 S. 3 LDSG SH – ein Jahr lang aufbewahrt.

Zur Verhinderung unbefugter Verarbeitungen und Kenntnisaufnahmen kommen auch Firewalls zum Einsatz, die das Intranet, über das die IHKs auf die Datenbestände zugreifen, nach Außen gegen unbefugte Zugriffe schützen sollen. Auch die sonstigen, im Hinblick auf das von der Ecofis GmbH betriebene WAN ergriffenen Maßnahmen, sind ausreichend. Im Rahmen des Netzbetriebs hat die Ecofis GmbH keinen Zugriff auf die FiDa- oder sonstige EVA-Daten. Die Ecofis GmbH besitzt weder einen administrativen Zugang noch einen Benutzerzugang zu den FiDa- bzw. EVA-Datenbanken. Ebenso wenig besitzt sie einen SQL-Zugang zu den GfI-Systemen. Als Instrument zur Gewährleistung eines adäquaten Datenschutzniveaus und insbesondere zur Umsetzung geeigneter technischer und organisatorischer Schutzmaßnahmen hat die Ecofis GmbH ein Datenschutzhandbuch erstellt, welches von der Geschäftsleitung der Ecofis-Gruppe veranlasst und genehmigt ist und im Betrieb umgesetzt wird. Das Datenschutzhandbuch beinhaltet die Zusammenstellung bzw. die Dokumentation aller in der Ecofis-Gruppe für das Gebiet „Datenschutz“ erlassenen und gültigen organisatorischen Regeln. Speziell für die Netzwerksicherheit besteht bei der Ecofis GmbH darüber hinaus ein IT-Sicherheitshandbuch, das in seinem Anhang verbindliche Vorgaben für die Organisation der IHKs im Hinblick auf den WAN-Netzverbund beinhaltet. Nach einem Beschluss der Hauptgeschäftsführer der IHKs auf ihrer Konferenz am 29. Mai 2001 wird dieses Handbuch für die IHK-Organisation in allen sicherheitsrelevanten Fragen als verbindlich anerkannt. Insgesamt wird durch diese umfangreichen Sicherheitsmaßnahmen ein hohes Maß an Vertraulichkeit und Sicherheit der Datenbestände bei ihrer Übermittlung innerhalb des WAN sichergestellt.

11 Beschreibung, wie das IT-Produkt den Datenschutz fördert

Eine vorbildliche Wirkung für den Datenschutz geht insbesondere von den sowohl in der Anwendung selbst, als auch von den im Benutzerhandbuch zu dem Modul FiDa enthaltenen Hinweisen auf eine datenschutzkonforme und datensparsame Nutzung der Anwendung aus.

So ist etwa unmittelbar neben dem Freitext-Eingabefeld ein Textfeld „Datenschutz-Hinweis“ eingebettet. Durch Eingabe eines entsprechenden Befehls wird eine weitere Bildschirmmaske aufgerufen, in der weitergehende Hinweise auf eine datensparsame Datenablage enthalten sind. Außerdem werden die Anwender in dem Benutzerhandbuch ausdrücklich angehalten, in den Textfeldern personenbezogene Daten nur einzugeben, soweit sie zur Aufgabenerfüllung der IHKs unbedingt notwendig sind und den Grundsätzen der Datenvermeidung und der Datensparsamkeit genügen.

Bei dem Zugriff eines IHK-Mitarbeiters auf den Datenbestand einer anderen IHK wird er beim Start der Anwendung in einem eigenen Fenster darauf hingewiesen, dass er nun Zugriff auf Daten einer

anderen IHK hat und er die Daten nur für die Zwecke nutzen darf, für die ihm der Zugriff eingeräumt worden ist. Der Anwender muss auf den in diesem Hinweisfenster befindlichen „OK“-Button klicken, um das Fenster zu schließen.

Eine Förderung des Datenschutzes erfolgt außerdem durch das in der Anwendung vorgesehene „Datenschutzkennzeichen“, welches insbesondere eine Sperrung von Daten unterstützt. Mit Hilfe dieses Datenschutzkennzeichens wird gesteuert, ob in der Kopfzeile der Maske eine Anzeige „Gesperrt“ erscheint. Diese Anzeige wird dadurch bewirkt, dass der Anwender ein „J“ (für ja) in das Eingabefeld „Datenschutzkennzeichen“ eingibt. Bei künftigen Aufrufen des betroffenen Datenbestandes können die Anwender somit anhand des „Sperrhinweises“ erkennen, dass die in dem jeweiligen Objekt gespeicherten Daten nicht uneingeschränkt verarbeitet werden dürfen. Das Modul FiDa sieht darüber hinaus einen vordefinierten Text mit der Bezeichnung „Sperrhinweis“ vor, in dem die Anwender der Grund bzw. den Gegenstand der Datenschperung hinterlegen können.

Schließlich bietet das Modul FiDa den IHKs im Rahmen der Datenparametrierung und der Feldberechtigung die Möglichkeit, die Sichtbarkeit und Nutzung einzelner Datenfelder nutzerspezifisch festzulegen. Im Rahmen der Feldberechtigung kann etwa festgelegt werden, ob ein Anwender einen Feldinhalt bearbeiten, nur ansehen bzw. weder bearbeiten noch ansehen darf. Auf diese Weise kann ein anwenderspezifischer Filter gesetzt werden, der dem Einzelnen nur Zugriff auf die Daten erlaubt, die er zur Erfüllung seiner Aufgaben auch tatsächlich benötigt. Dadurch ist eine sehr datensparsame Organisation der Datenverarbeitungsverfahren in den IHKs möglich.

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

Hamburg, den 24. August 2005

Luther Menold

Rechtsanwaltsgesellschaft mbH