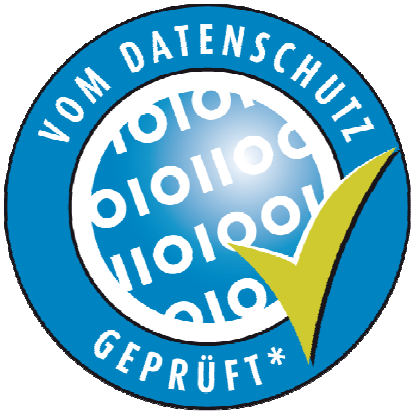

Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR)

Datenschutz- und IT-Sicherheitsmanagement der ZIAF-Informationssysteme

Erstellungszeitraum: Juni 2008 bis Juli 2009

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Autor:	LD7.3
Tel.:	0431/988-1217
Fax:	0431/988-1223
E-Mail:	ULD73@datenschutzzentrum.de
Datum:	06.07.2009
Version:	1.0

Inhaltsverzeichnis

1	**Zusammenfassung**	**4**
2	**Gegenstand des Audits**	**5**
2.1	Vereinbarung	5
2.2	Vorgehen bei der Auditierung	5
2.3	Datenschutz- und Datensicherheitsziele	6
3	**Ergebnisse des Audits**	**7**
3.1	IT-Sicherheitsmanagement	7
3.2	Dokumentation	7
3.3	Betreibervertrag	8
3.4	Grundschutzkonformität	8
3.5	Ergebnisse des Grundschutzaudits	9
4	**Datenschutzrechtliche Bewertung**	**11**
4.1	Rechtsvorschriften	11
4.2	Datenschutz- und Grundschutzkonformität	12
4.3	Dokumentation	12
4.4	Auftragsdatenverarbeitung	12
4.5	Zusammenfassende Bewertung	13

1 Zusammenfassung

Wirksamer Datenschutz und wirksame IT-Sicherheit erfordern die dauerhafte Aufrechterhaltung eines effektiven Datenschutz- und IT-Sicherheitsmanagement-Systems, das die vielfältigen und laufenden Veränderungen der betriebenen Verfahren in technischer, organisatorischer und rechtlicher Sicht begleitet, bewertet und dafür Sorge trägt, dass auch nach Veränderungen von Verfahren Datenschutz und IT-Sicherheit gewährleistet sind.

Das Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR) hat das Unabhängige Landeszentrum für Datenschutz (ULD) beauftragt, die IT-Sicherheit der in der Zahlstelle für den Europäischen Garantiefonds für die Landwirtschaft (EGFL) und den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) eingesetzten Informationssysteme sowie die Einhaltung der gesetzlichen Datenschutzvorschriften zu überprüfen.

Das MLUR setzt den IT-Sicherheitsstandard „ISO 27001 auf Basis von IT-Grundschutz" des Bundesamtes Sicherheit in der Informationstechnik (BSI) um und erfüllt somit die Anforderungen an die Zulassung ihrer Zahlstelle nach den Vorgaben der Verordnung (EG) Nr. 885/2006 der Kommission der Europäischen Gemeinschaft. Die Wirksamkeit des IT-Sicherheitsmanagement-Systems wurde vom BSI durch die Erteilung eines Zertifikates (BSI-IGZ-0040-2009) bestätigt. Die Begutachtung wurde von einem Gutachter des ULD durchgeführt, der vom BSI als Auditor für ISO 27001-Audits auf Basis von IT-Grundschutz anerkannt ist.

Darüber hinaus wurden durch das ULD im Rahmen des Datenschutzaudits zusätzlich die datenschutzrechtlichen Anforderungen für einen ordnungsgemäßen Betrieb der ZIAF-Verfahren[1] überprüft. Das Ergebnis der Begutachtung zeigt, dass das MLUR sowie der von ihm beauftragte Dienstleister Dataport die datenschutzrechtlichen Betriebsanforderungen vollständig erfüllen.

Die inhaltliche Überprüfung der ZIAF-Fachverfahren wie z.B. die Berechnung von Auszahlungen, die ordnungsgemäße Verbuchung von Zahlungen, die datenschutzgerechte Durchführung oder die Veröffentlichung von Subventionsempfängern waren nicht Gegenstand des Audits.

[1] Zahlstellen und InVeKoS-Agrar-Förderprogramm (InVeKoS = Integriertes Verwaltungs- und Kontrollsystem)

2 Gegenstand des Audits

2.1 Vereinbarung

Das Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR) hat mit Vertrag vom 02.01.2008 das Unabhängige Landeszentrum für Datenschutz (ULD) in einem abgestuften Verfahren mit der Begutachtung der in der Zahlstelle für den Europäischen Garantiefonds für die Landwirtschaft (EGFL) und den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) eingesetzten Informationssysteme beauftragt, um die Einhaltung der zu beachtenden IT-Sicherheits- und Datenschutzanforderungen zu überprüfen.

Für die Umsetzung der IT-Sicherheit der in Zahlstelle eingesetzten Informationssysteme haben sich die deutschen Zahlstellen und somit auch das MLUR in einem länderübergreifenden Ausschuss auf den IT-Sicherheitsstandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verständigt, um die Anforderungen an die Zulassung einer Zahlstelle nach den Vorgaben der Verordnung (EG) Nr. 885/2006 der Kommission der Europäischen Gemeinschaft zu erfüllen.

Als Basis für die Umsetzung der IT-Sicherheitsanforderungen der EG wurde zunächst eine Generaldokumentation als Konzeption der Zahlstelle des MLUR erstellt. Die Konzeptinhalte sind neben der Berücksichtigung datenschutzrechtlicher Vorschriften vor allem auf die Erfüllung der Anforderungen der BSI-Sicherheitsstandards[2] 100-1 bis 100-3 durch die in der Zahlstelle eingesetzten ZIAF-Fachverfahren ausgerichtet. Diese wurden inhaltlich im Rahmen des im Jahr 2007 durchgeführten Datenschutzaudits auf ihre Standard- und Rechtskonformität bereits begutachtet. Ferner wurde die Grundschutzkonformität durch einen Auditor des ULD für ISO 27001-Audits auf Basis von IT-Grundschutz festgestellt und vom BSI durch die Erteilung eines Zertifikates (BSI-IGZ-0040-2009) bestätigt.

2.2 Vorgehen bei der Auditierung

Das Datenschutzaudit beinhaltet die Begutachtung der Einhaltung der Datenschutzvorschriften in Bezug auf den ordnungsgemäßen Betrieb des ZIAF-Verfahrens und erfolgte zusammen mit der Auditierung nach dem Grundschutzstandard. Beide Audits umfassten unter Berücksichtigung der einzuhaltenden gesetzlichen Regelungen die Sichtung der Generaldokumentation des MLUR für das Verfahren ZIAF sowie die entsprechenden Dokumente des Dienstleisters Dataport für diejenigen IT-Systeme, mit denen Dataport im Auftrag des MLUR das ZIAF-Verfahren betreibt.

Es wurden die Plausibilität des Konzeptes von IT-Sicherheitsmaßnahmen vollständig sowie die Umsetzung des Konzeptes vor Ort stichprobenartig überprüft. Bestandteil dieser Stichprobe waren die aufbau- und ablauforganisatorische Einrichtung und Funktion des IT-Sicherheitsmanagements im MLUR und bei Dataport sowie die Umsetzung von IT-Sicherheitsmaßnahmen für das ZIAF-Verfahren. Die Überprüfungen umfassten auch den Einsatz von Verschlüsselung (Dataport), das

[2] Siehe http://www.bsi.bund.de/literat/bsi_standard/

Notfallkonzept (Dataport) sowie das Hard- und Softwaremanagement (MLUR).

Die Details dieser Prüfungen, interviewte Personen, geprüfte IT-Systeme und Organisationseinheiten sowie die Ergebnis wurden bereits in einem nicht öffentlichen Grundschutzauditbericht „ZIAF-Informationssysteme V 2.0" beschrieben.

Im Rahmen des Datenschutzaudits wurde zusätzlich ein Schwerpunkt auf die Erfüllung der datenschutzrechtlichen Anforderungen gelegt, die nicht durch das IT-Grundschutzaudit abgedeckt wurden. Die festgestellten Sachverhalte sind Bestandteil dieses Gutachtens. Das Gutachten über die IT-Grundschutzzertifizierung und das vorliegende Gutachten beschreiben zusammen den Auditierungsgegenstand dieses Datenschutzaudits.

2.3 Datenschutz- und Datensicherheitsziele

Das MLUR hat mit der Erstellung ihrer Sicherheitskonzeption für die Zahlstelle folgende Datenschutzziele festgelegt:

- Beachtung von Rechtsvorschriften, Richtlinien und sonstigen Arbeitsanweisungen zur Datensicherheit und zur Ordnungsmäßigkeit der Datenverarbeitung,
- Umsetzung der IT-Sicherheit unter Berücksichtigung der IT-Grundschutz-Methodik,
- Anwendung des IT-Grundschutz-Standards nach dem BSI-Qualifizierungsverfahren über die „IT-Grundschutz-Einstiegs- und -Aufbaustufe" hin zur ISO-27001-Zertifizierung[3] auf der Basis von IT-Grundschutz,
- Erarbeitung eines übergreifenden IT-Sicherheitskonzepts nach den Vorgaben der BSI-Standards „Managementsysteme für Informationssicherheit" (100-1), „IT-Grundschutz-Vorgehensweise" (100-2) und „Risikoanalyse auf der Basis von IT-Grundschutz" (100-3),
- Schaffung geeigneter und einheitlicher Schnittstellen zum IT-Sicherheitsmanagement der beteiligten ZIAF-Organisationen und beim Dienstleister Dataport sowie
- Festlegung und Überprüfung der vom Dienstleister Dataport vertraglich vereinbarten Leistungen inklusive der zugesicherten Umsetzung der genannten BSI-Standards.

[3] Die internationale Norm ISO/IEC 27001:2005, „Information technology – Security techniques – Information security management systems – Requirements" spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.

3 Ergebnisse des Audits

3.1 IT-Sicherheitsmanagement

Die Zahlstelle des MLUR hat nach den Vorgaben der IT-Sicherheitsleitlinie ein IT-Sicherheitsmanagement eingerichtet. Die entsprechenden Regelungen werden in dem Dokument „Sicherheitsmanagement-Leitlinie“ festgelegt. Im Rahmen des Audits wurde festgestellt, dass folgende Sicherheitsziele erfüllt werden:

- Umsetzung einer nach gesetzlichen und vertraglichen Vorgaben ordnungsgemäßen Datenverarbeitung,
- Schutz der vertraulichen Daten aller Beteiligten,
- Gewährleistung der Integrität und Verfügbarkeit der Daten und der Informationssysteme,
- Gewährleistung der Vollständigkeit und Authentizität der Daten,
- Sicherstellung der Kontinuität der Arbeitsabläufe,
- transparente und nachvollziehbare Gestaltung der Datenverarbeitungsprozesse,
- Verpflichtung der für die Zahlstelle tätigen Vertragspartner auf die im IT-Sicherheitskonzept festgelegten Maßnahmen und auf ihre Einbindung in das IT-Sicherheitsmanagement,
- Festlegung von Regelungen für das Test- und Freigabeverfahren für die in der Zahlstelle und bei ihren Vertragspartnern eingesetzten Informationssysteme sowie
- Überprüfung der im Sicherheitskonzept festgelegten Maßnahmen durch die Durchführung interner und externer Audits.

3.2 Dokumentation

Um die Datenverarbeitungsprozesse anschaulich und nachvollziehbar zu gestalten, wurde vom MLUR in Zusammenarbeit mit dem Dienstleister Dataport eine umfassende Generaldokumentation des Verfahrens erstellt, die den datenschutzrechtlichen Dokumentationsverpflichtungen Rechnung trägt.

Die Generaldokumentation ist für das Datenschutzmanagement der Zahlstelle die Grundlage aller Aktivitäten. Es werden mit ihr folgende Ziele erreicht:

- Zusammenfassung aller relevanten Grundlagen für das automatisierte Verfahren und damit Informationsquelle der Zahlstelle für die Verfahrensbeteiligten,
- Transparenz des Verwaltungshandelns,
- Revisionsfähigkeit des automatisierten Verfahrens,
- Dokumentation der Steuerung und Verbesserung des Datenschutz- und IT-

Sicherheitsmanagements.

Die Generaldokumentation gliedert sich in

- Teil 0: Einleitung,
- Teil 1: IT-Konzept (BSI-Strukturanalyse),
- Teil 2: Sicherheitskonzept,
- Teil 3: Operative Dokumentation,
- Teil 4: Verträge und Vereinbarungen,
- Teil 5: Regelungen der EU, des Bundes und des Landes sowie
- Teil 6: Anhang.

3.3 Betreibervertrag

Der zwischen dem MLUR und Dataport abgeschlossene Betreibervertrag beschreibt die Leistungen, die Dataport im Rahmen der Auftragsdatenverarbeitung für den Betrieb der ZIAF-Komponenten erbringt. Die bisherigen generisch gewachsenen vertraglichen Verpflichtungen wurden aus Gründen der Transparenz zur Erfüllung der normativen Anforderung in einen neuen Betreibervertrag überführt. Der Vertrag enthält folgende Anlagen:

- Anlage 1: Leistungs- und Technische Systembeschreibung,
- Anlage 2: Datenschutz,
- Anlage 3: Service Level Agreements,
- Anlage 4: Sicherheitsmaßnahmen,
- Anlage 5: Obliegenheiten sowie
- Anlage 6: Entgeltvereinbarung.

Die Anlage 2 „Datenschutz“ enthält die von Dataport für die Zahlstelle des MLUR zu erfüllenden datenschutzrechtlichen Anforderungen der Auftragsdatenverarbeitung bzw. die Anforderungen des IT-Grundschutzes an die Vereinbarungen eines Outsourcing. Darüber hinaus enthält die Anlage 4 des Vertrages die von Dataport nach dem Stand der Technik nach § 5 Abs. 2 LDSG bzw. nach IT-Grundschutz zu erfüllenden wesentlichen IT-Sicherheitsmaßnahmen.

3.4 Grundschutzkonformität

Das MLUR hat die Grundschutzkonformität für das ZIAF-Verfahren im Rahmen eines Grundschutzaudits durch das ULD überprüfen lassen und erfolgreich eine Grundschutz-Zertifizierung nach ISO 27001 vom BSI erhalten. Der Grundschutzauditbericht „ZIAF-Informationssysteme V 2.0“ ist nicht öffentlich. Zum Verständnis werden im folgenden Abschnitt die wesentlichen Ergebnisse des Grundschutzaudits zusammengefasst dargestellt.

3.5 Ergebnisse des Grundschutzaudits

Das Grundschutzaudit erfolgte gemäß des Prüfschemas für ISO 27001-Audits des BSI in der Version 2.1[4]. Dieses Prüfschema sieht eine zweiteilige Prüfung vor, die zunächst die vorliegende Dokumentation auf Vollständigkeit, Aktualität und Plausibilität zu überprüfen. In diesem Zusammenhang wurden die Teile 1, 2 und 3 der Generaldokumentation gesichtet. Wesentliche Prüfpunkte an dieser Stelle waren:

- Einrichtung und Wirkungsweise des IT-Sicherheitsmanagements beim MLUR und beim Dienstleister Dataport,
- die Beschreibung des IT-Verbundes (Dokumentation von beteiligten Organisationen, IT-Anwendungen, Hard- und Software, Kommunikationsverbindungen und Räumen),
- die Analyse des Schutzbedarfes der IT-Anwendungen, Hard- und Software, Kommunikationsverbindungen und Räume hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität,
- die Plausibilität und Vollständigkeit der Modellierung des IT-Verbundes mit den Bausteinen der IT-Grundschutzkataloge des BSI,
- die Vollständigkeit und Plausibilität der Selbsterklärung zum Umsetzungsstand der Sicherheitsmaßnahmen, die gemäß der IT-Grundschutzkataloge auf die IT-Komponenten anzuwenden sind,
- die Plausibilität und Vollständigkeit der Risikoanalyse für diejenigen Komponenten des IT-Verbundes, für die ein hoher Schutzbedarf festgestellt wurde (Risikoanalyse, Festlegung zusätzlicher Schutzmaßnahmen, Analyse des Restrisikos).

Es waren kleinere Abweichungen zu verzeichnen, die größtenteils schon während der Begutachtungsphase abgestellt werden konnten. Verbleibende Nachbesserungen sind als Auditauflage zu beheben; die Überprüfung erfolgt turnusmäßig beim Überwachungsaudit im ersten Quartal 2010.

Im zweiten Prüfschritt wurde stichprobenartig die Umsetzung der Sicherheitsmaßnahmen überprüft. Dazu wurden gemäß Prüfschema den Bereichen MLUR und Dataport je zehn Bausteine teils zufällig, teils gezielt ausgewählt. Bei der Auswahl wurden besonders relevante Bausteine wie das Outsourcing von IT-Dienstleistungen oder der Einsatz kryptographischer Verfahren berücksichtigt sowie auf eine gleichmäßige Abdeckung der unterschiedlichen Standorte, IT-Systeme und Anwendungen geachtet, um eine repräsentative Prüfung zu gewährleisten. Bei jedem Baustein wurde überprüft, ob die zugehörigen Sicherheitsmaßnahmen gemäß IT-Grundschutzkatalog umgesetzt waren. Die Sicherheitsmaßnahmen der IT-Grundschutzkataloge sind nicht in allen Fällen einschlägig[5]; in diesen Fällen wurde überprüft, ob die Begründung der Nichtanwendbarkeit plausibel ist. Weiterhin wurde die Wirksamkeit zusätzlicher Sicherheitsmaßnahmen, die aufgrund eines erhöhten Risikos vom MLUR und von Dataport ausgewählt und implementiert wurden, überprüft.

[4] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz Prüfschema für ISO 27001-Audits, V 2.1, März 2008, http://www.bsi.de/gshb/zert/ISO27001/schema.htm

[5] Z. B. ist der Prüfpunkt „Sicherheit von PC-Mikrofonen" entbehrlich, wenn im vorliegenden Fall keine Mikrofone verbaut wurden.

Insgesamt wurden 240 Sicherheitsmaßnahmen im Bereich MLUR und 201 Sicherheitsmaßnahmen im Bereich Dataport überprüft. Dabei wurden kleinere Abweichungen festgestellt, die überwiegend während der Prüfungsaktivitäten vom MLUR und von Dataport abgestellt wurden. Lediglich eine bauliche Maßnahme konnte nicht während des Prüfungszeitraumes umgesetzt werden; sie ist im Rahmen einer Auditauflage zu beheben. Die Überprüfung erfolgt turnusmäßig beim Überwachungsaudit im ersten Quartal 2010.

Im Ergebnis wurden die Sicherheitsmaßnahmen vom Gutachter als umgesetzt bewertet. Das BSI folgte der Empfehlung des Gutachters, das IT-Grundschutzzertifikat zu verleihen.

4 Datenschutzrechtliche Bewertung

4.1 Rechtsvorschriften

Die in der Zahlstelle für die EGFL- und ELER-Fördermaßnahmen eingesetzten Informationssysteme verarbeiten personenbezogene Daten der Antragsteller. Antragsteller sind Landwirte, die mit den Anträgen Angaben über ihre persönlichen und wirtschaftlichen Verhältnisse machen. Diese unterliegen als personenbezogene Daten dem Schutz des Landesdatenschutzgesetzes (LDSG).

Das Landesdatenschutzgesetz sowie die Datenschutzverordnung (DSVO) finden infolgedessen neben den bereichsspezifischen Vorschriften (EU-Richtlinien) Anwendung. Mit beiden Regelungen hat der Gesetzgeber europäische Vorgaben, insbesondere der EG-Richtlinie zum Datenschutz 95/46/EG vom 24.02.1995 (ABl. EG L 281 vom 23.11.1995, S. 31) umgesetzt. Im Rahmen des Datenschutzaudit ergeben sich folgende Schwerpunkte:

- Einrichtung eines Datenschutz- und IT-Sicherheitsmanagements,
- Anforderungen an die Administration und ihre Revisionsfähigkeit,
- Test und Freigabeverfahren,
- Anforderung an die Dokumentation sowie
- Kontrolle der Auftragsdatenverarbeitung.

Für den Einsatz automatisierter Verfahren im Rahmen der EGFL- und ELER-Fördermaßnahmen sind folgende datenschutzrechtliche Vorschriften maßgeblich:

Landesdatenschutzgesetz (LDSG)

§ 4 Datenvermeidung und Datensparsamkeit

§ 5 Allgemeine Maßnahmen zur Datensicherheit

§ 6 Besondere Maßnahmen zur Datensicherheit beim Einsatz automatisierter Verfahren

§ 7 Verfahrensverzeichnis, Meldung

§ 8 Gemeinsame Verfahren und Abrufverfahren

§ 9 Vorabkontrolle

§ 11 Zulässigkeit der Datenverarbeitung

§ 13 Erhebung, Zweckbindung

§ 17 Verarbeitung personenbezogener Daten im Auftrag, Wartung

Datenschutzverordnung (DSVO)[6]

§ 3 Verfahrensdokumentation

§ 4 Verfahrenszweck

§ 5 Verfahrensbeschreibung

§ 6 Sicherheitskonzept

§ 7 Test und Freigabe

§ 8 Verfahrensübergreifende Dokumentation und Protokolle

4.2 Datenschutz- und Grundschutzkonformität

Die Zahlstelle des MLUR ist verpflichtet, die Anforderungen des IT-Grundschutzes des BSI zu erfüllen und nachzuweisen. Im Rahmen dieses Datenschutzaudits wurde festgestellt, dass die Zahlstelle des MLUR die datenschutzrechtlichen sowie insbesondere die sicherheitstechnischen Anforderungen des IT-Grundschutzes erfüllt. Aus datenschutzrechtlicher Sicht geben die Anforderungen des IT-Grundschutzes den von der verantwortlichen Stelle nach § 5 Abs. 2 LDSG zu gewährleistenden „Stand der Technik" der technisch-organisatorischen Sicherheitsmaßnahmen wieder.

4.3 Dokumentation

Die Anforderungen der Datenschutzverordnung 2001 werden erfüllt. Geräte- und Programmverzeichnisse, Schutzbedarfsanalyse, Maßnahmenkatalog, eine Restrisikoanalyse sowie Regelungen über das Test- und Freigabeverfahren liegen vor.

4.4 Auftragsdatenverarbeitung

Das MLUR ist als Auftraggeber mit der Vergabe der Datenverarbeitung an seinen Dienstleister für die Einhaltung der bereichsspezifischen Gesetze und der Datenschutzvorschriften verantwortlich. Es hat vertraglich sichergestellt, dass auch sein Dienstleister als Auftragnehmer diese Anforderungen erfüllt. Im Rahmen der Auftragsdatenverarbeitung hat das MLUR dafür Sorge getragen, dass der Betrieb des ZIAF-Verfahrens nur im Rahmen seiner Weisungen ausgeführt wird.

Das MLUR hat seinen Auftragnehmer (Dataport) verpflichtet, jederzeit von ihr veranlasste Kontrollen zur Einhaltung der gebotenen technischen und organisatorischen Maßnahmen zu ermöglichen.

Die Verpflichtung des Auftragnehmers Dataport, die gebotenen datenschutzrechtlichen Vorgaben für das Auftragsverhältnis umzusetzen und zu kontrollieren, hat das MLUR durch den mit Dataport

[6] Zum Zeitpunkt der Prüfung war für den geprüften IT-Verbund die Datenschutzverordnung in der Fassung vom 21.04.2001 gültig, auf die sich dieser Prüfbericht bezieht. Zum 01.01.2009 ist eine neue Datenschutzverordnung in Kraft getreten, die gemäß § 6 Abs. 2 DSVO bei wesentlichen Änderungen des Verfahrens im Rahmen der Vorabkontrolle, andernfalls gemäß § 6 Abs. 1 DSVO bis zum 01.01.2012 umzusetzen ist.

geschlossenen Vertrag sichergestellt.

Mit der Einrichtung eines Datenschutz- bzw. IT-Sicherheitsmanagements hat das MLUR Strukturen geschaffen, die eine sachkundige Kontrolle seiner Dienstleister ermöglichen. Das für das ZIAF-Verfahren festgelegte Sicherheitsniveau kann auf diese Weise dauerhaft aufrechterhalten werden.

4.5 Zusammenfassende Bewertung

Die Prüfung hat ergeben, dass die Wirksamkeit des Datenschutz-Managementsystems keinen Anlass zu datenschutzrechtlichen Beanstandungen gibt.

Kiel, 06.07.2009 gez. Dr. Probst (Gutachter)