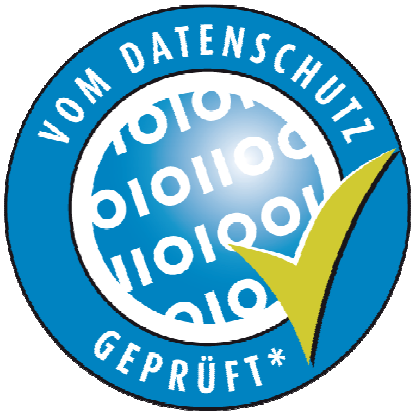

Kurzgutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Ministerium für Landwirtschaft, Umwelt und ländliche Räume

Sicherheit der ZIAF-Informationssysteme der Zahlstelle

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datum : 10.10.2007
Aktenz. : 16.01/05.012
Telefon : 0431 988 1200
Fax : 0431 988 1223
E-Mail : mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Audits

Das **Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR)** hat mit Vertrag vom 22. Juni 2005 das Unabhängige Landeszentrum für Datenschutz (ULD) mit der Begutachtung der **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 beauftragt, um die Einhaltung der von der **Europäischen Gemeinschaft (EG)** vorgegebenen **IT-Sicherheitsanforderungen** zu überprüfen.

Für die Umsetzung der IT-Sicherheit der in Zahlstelle eingesetzten Informationssysteme haben sich die deutschen Zahlstellen und somit auch das MLUR auf den **IT-Sicherheitsstandard des Bundesamtes 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. Sie wurde inhaltlich im Rahmen dieses Datenschutz-Audits auf ihre **Norm- und Rechtskonformität** sowie ihre **Umsetzbarkeit** überprüft. Die Konzeptinhalte sind neben der Berücksichtigung **datenschutzrechtlicher Vorschriften** vor allem auf die Erfüllung der Anforderungen des **BSI-Sicherheitsstandards**[1] 100-1 bis 100-3 durch die in der Zahlstelle eingesetzten ZIAF-Fachverfahren[2] ausgerichtet.

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-**

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

[2] **Z**ahlstellen und **I**nVeKoS-**A**grar-**F**örderprogramm (InVeKoS = Integriertes Verwaltungs- und Kontrollsystem)

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 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 BSI-Standards.

Die Zahlstelle des MLUR ist verpflichtet, für das Haushaltsjahr 2008 (16. Oktober 2007 bis 15. Oktober 2008), die Anforderungen des IT-Grundschutzes des BSI zu erfüllen und nachzuweisen. Im Rahmen dieses Datenschutz-Audits wird geprüft und bestätigt, dass die Zahlstelle des MLUR bereits vor Beginn des Haushaltsjahres 2008 die **sicherheitstechnische Konzeption der Zahlstelle** 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 gewährleistende „Stand der Technik“ der technisch-organisatorischen Sicherheitsmaßnahmen wieder.

Auf dieser Basis beabsichtigt das MLUR in einem laufenden Verfahren für das Haushaltsjahr 2008, die vollständige Umsetzung der Sicherheitskonzeption zur Erreichung der **BSI-Grundschutzkonformität** durch eine IT-Grundschutz-Zertifizierung nach ISO 27001 als Nachweis der Einhaltung der von der EG vorgegebenen IT-Sicherheitsanforderungen zu gewährleisten.

[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.

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

2 ZIAF-Organisation

2.1 EU-Fördermaßnahmen

Die gemeinsame **Agrarpolitik** der Europäischen Union (EU) umfasst Maßnahmen, die zur Entwicklung des ländlichen Raums beitragen sollen. Ihre Finanzierung erfolgt aus einem hierfür eingerichteten Europäischen Garantiefonds für die Landwirtschaft (EGFL) und den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER). Die Verantwortung für die Bearbeitung der Maßnahmen liegt bei der im Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR) eingerichteten **Zahlstelle**.

Fördermaßnahmen	
ELER-Maßnahmen	
Schwerpunkt 1: „Verbesserung der Wettbewerbsfähigkeit der Land- und Forstwirtschaft“	
1	Zielgruppenspezifische Fort- und Weiterbildungsveranstaltungen
2	Agrarinvestitionsförderung (AFP)
3	Förderung der Verbesserung der Verarbeitung und Vermarktung landwirtschaftlicher Erzeugnisse
4	Ländliche Neuordnung einschl. freiwilliger Landtausch (Flurbereinigung nach GAK)
5	Ländlicher Wegebau
6	Maßnahmen zur Verhütung von Hochwasserschäden
7	Küstenschutz im ländlichen Raum
Schwerpunkt 2: „Verbesserung der Umwelt und der Landschaft“	
8	Förderung landwirtschaftlicher Betriebe in benachteiligten Gebieten (Ausgleichszulage)
9	Natura 2000-Prämie (Grünlangerhaltungsprämie)
10	Dauergrünland-Programm
11	Förderung extensiver Grünlandnutzung (mit 2 Untermaßnahmen)

12	Halligprogramm
13	Reduzierung der Stoffeinträge in Gewässern
14	Modulation (Altverpflichtungen) mit 5 Untermaßnahmen
15	Ökologische Anbauverfahren (MSL)
16	Vertragsnaturschutz
17	Erstaufforstung landwirtschaftlicher Flächen
18	Waldentwicklung in Natura 2000-Gebieten
19	Waldumbau
Schwerpunkt 3: „Lebensqualität im ländlichen Raum und Diversifizierung der ländlichen Wirtschaft“	
20	Investitionen zur Diversifizierung (AFP/B)
21	Umnutzung land- und forstwirtschaftlicher Bausubstanz
22	Förderung von Unternehmensgründung und -entwicklung
23	Besucherlenkung und Besucherinformation im Naturschutz, Natura 2000
24	Förderung des Fremdenverkehrs
25	Initiative Biomasse und Energie
26	Anpassung von Kläranlagen an die allgemein anerkannten Regeln der Technik (Nachrüstung)
27	Dienstleistungseinrichtungen und Freizeit- und Kulturangebote zur Grundversorgung
28	Dorferneuerung und Dorfentwicklung
29	Erhaltung und Verbesserung des ländlichen Kulturerbes
30	Naturschutz und Landschaftspflege
31	Wasserrahmenrichtlinie (investive Maßnahmen) - Naturnahe Gestaltung von Fließgewässern, Wiedervernässung von Niedermooren
32	Berufsbildungs- und Informationsmaßnahmen für Wirtschaftsakteure
33	Maßnahmen zur Kompetenzentwicklung Förderungsveranstaltungen und Durchführung
Schwerpunkt 4: „LEADER“	
34	AktivRegion (nach LEADER-Methode)
35	Gebietsübergreifende und transnationale Zusammenarbeit
36	Betreiben der lokalen Aktionsgruppe (AktivRegion) sowie Kompetenzentwicklung und Sensibilisierung in dem betreffenden Gebiet

EGFL-Maßnahmen	
37	Entkoppelte Direktbeihilfen
38	Sonderbeihilfen für die Bienenzucht
39	Schulmilchverbilligung
40	Obst/Gemüse - Betriebsfonds der Erzeugerorganisation
41	Interventionen bei Fischereierzeugnissen

Die ordnungsgemäße Durchführung der Bearbeitung von Maßnahmen wird durch die Wahrnehmung der **Fachaufsicht** und durch **Verfahrensabläufe** sichergestellt, die im Einvernehmen mit dem Referat "Leitung der EGFL/ELER-Zahlstelle" erlassen werden. Dabei werden insbesondere die **Trennung** der **Funktionen der Antragsbearbeitung** und das **Vier-Augen-Prinzip** beachtet.

Das MLUR hat zusammen mit anderen Ländern für die automatisierte Bearbeitung der Maßnahmen das Mehrländerprogramm **ZIAF** entwickelt. Das Fachverfahren wird vom Dienstleister Dataport gehostet. Die vollständige Antragsbearbeitung wird nur für die Maßnahmen mit den Nrn. 8, 9, 11, 14, 15 und 37 automatisiert durchgeführt. Alle Maßnahmen werden mit dem ZIAF-Buchhaltungsprogramm (ravel c/s) verwaltet.

2.2 Organisationsstruktur der Zahlstelle

Leiter der Zahlstelle ist der **Staatsekretär** des MLUR. Bei der praktischen Durchführung der Maßnahmen wird die Bewilligungs- und Kontrollfunktion auch von dezentralen Ämtern wahrgenommen bzw. sie wurde an andere beauftragte Einrichtungen delegiert. Die aus dem EGFL und ELER finanzierten Fördermaßnahmen werden von organisatorischen Untereinheiten der Zahlstelle (Fachreferate) im MLUR bzw. dem Ministerium für Wissenschaft, Wirtschaft und Verkehr (MWV) des Landes Schleswig-Holstein verantwortlich gesteuert und administriert.

Die Zahlstelle hat ausreichend zu gewährleisten, dass

- die **Zulässigkeit der Anträge** und deren Übereinstimmung mit den Gemeinschaftsvorschriften vor der Anordnung der Zahlungen überprüft werden,
- die geleisteten Zahlungen **richtig** und **vollständig** in den Büchern erfasst werden,
- die in den Gemeinschaftsvorschriften vorgesehenen **Kontrollen** durchgeführt werden,

- die notwendigen Unterlagen **fristgerecht** und in der in den Gemeinschaftsvorschriften geforderten Form vorgelegt werden,
- die Unterlagen zugänglich sind und so aufbewahrt werden, dass ihre **Integrität**, **Gültigkeit** und **Lesbarkeit** langfristig gewährleistet sind.

Abb.: Organisationsstruktur der Zahlstelle

Die Zahlstelle bleibt in allen Fällen der Aufgabendelegation auf nach geordnete Ämter bzw. dezentrale Dienste und andere beauftragte Einrichtungen für die wirksame Verwaltung des EGFL und ELER verantwortlich. Sie überprüft regelmäßig bei den übertragenen Funktionen, ob die durchführenden Stellen über **wirksame Systeme** verfügen, um ihre **Verantwortlichkeiten** in zufrieden stellender Weise wahrnehmen zu können. Hierdurch gewährleistet die Zahlstelle, dass die Arbeiten in Übereinstimmung mit den Gemeinschaftsvorschriften durchgeführt werden. Insbesondere wird auf eine Trennung der Funktionen der **Bewilligung**, **Zahlung** und **Verbuchung** geachtet.

2.3 Informationstechnik und ZIAF-Betriebssteuerung

Das Referat „Informationstechnik und ZIAF-Betriebssteuerung“ des MLUR (V17) führt im Zusammenhang mit den IT-Fachverfahren der Zahlstelle folgende Aufgaben durch:

- Festlegung und Fortschreibung der IT-Strategien, -Konzepte und -Standards des Landes (in der IT-Kommission) sowie der ressortspezifischen Besonderheiten,
- IT-Budgetverwaltung,
- IT-Auftrags- und Vertragsmanagement und IT-Controlling,
- Übergreifende Koordination und Abstimmung der Verfahrensentwicklungen,
- Fachverantwortung für übergreifende Bausteine wie z.B. Rechte- und Nutzerverwaltung, Posteingangsbuch, Automaten, Auswerte-Tool, Grunddatenpflege und
- technische Betreuung der ZIAF-Komponenten im MLUR.

Ausgehend von den Anforderungen der unterstützten Maßnahmen und Fachbereiche hat die **Betriebssteuerung** ZIAF (BSZ) die **termingerechte** Verfügbarkeit der benötigten IT-Komponenten (Programme, Systeme und Netze) zu sichern (vgl. Tz. 3.5).

2.4 Interner Revisionsdienst

Der interne Revisionsdienst gehört zur Organisationsstruktur der Zahlstelle. Er ist im Referat V 10 des MLUR angesiedelt, jedoch dem Leiter der Zahlstelle fachlich unmittelbar unterstellt. Der interne Revisionsdienst überprüft, ob die **Verfahrensabläufe** in der Zahlstelle gewährleisten, dass die **Einhaltung der Gemeinschaftsvorschriften** überprüft werden und dass die **Buchführung** richtig und vollständig ist und sich auf dem neuesten Stand befindet. Die Arbeiten des Prüfdiensts sind nach international anerkannten Standards durchzuführen und münden in Berichte und Empfehlungen an die Leitung der Zahlstelle.

2.5 IT-Sicherheitsmanagement

Das IT-Sicherheitsmanagement des MLUR hat die Aufgabe, für einen übergreifenden Sicherheitsmanagementprozess der innerhalb der Zahlstelle eingesetzten ZIAF-Fachverfahren des EGFL und ELER zu sorgen. Das IT-Sicherheitsmanagement umfasst einen **IT-Sicherheitsbeauftragten** und ein ihn unterstützendes **IT-Sicherheitsmanagement-Team**. Das **IT-Sicherheitsmanagement** der Zahlstelle stützt sich zur Erfüllung seiner Aufgaben auf das IT-Sicherheitsmanagement seines Dienstleisters Dataport, um die Funktion der Sicherheitsmanagementprozesse für die von Dataport betriebenen ZIAF-Fachverfahren vollständig zu gewährleisten.

2.6 Bescheinigende Stelle

Die Bescheinigende Stelle gehört organisatorisch dem Finanzministerium an und wird als **Kontroll-** bzw. **Prüfinstanz** gegenüber der Zahlstelle tätig. Mit Begin des Haushaltsjahres 2008 am 16. Oktober 2007 hat das MLUR der bescheinigenden Stelle darzustellen, in welchem Umfang der aus der EU-Richtlinie geforderte **Sicherheitsstandard** vom MLUR umgesetzt wird. Die Bescheinigende Stelle hat dann der EU-Kommission in einer Erklärung zu beschreiben, wie die Zahlstelle die Sicherheit der Informationssysteme gewährleistet.

2.7 Zuständige Behörde

Zuständige Behörde im Sinne des Artikels 6 der Verordnung (EG) Nr. 1290/2005 i. V. m. Artikel 1 der VO (EG) Nr. 885/2006 ist das Finanzministerium (FM). Sie ist für die **Zulassung** und den **Entzug der Zulassung** der Zahlstelle zuständig und übt insbesondere auf Grundlage der von der **Bescheinigenden Stelle** erstellten Berichte eine **ständige Aufsicht** über die Zahlstelle aus.

2.8 Verwaltungsbehörde

Die **Verwaltungsbehörde** im Sinne des Artikels 75 der Verordnung (EG) Nr. 1698/2005 ist das Referat V 11 des MLUR. Hier erfolgt u.a. die Koordination des Zukunftsprogramms ländlicher Raum Schleswig-Holstein zur Durchführung des Finanzmanagements sowie zur Begleitung und Bewertung sowie der Berichterstattung und der Veröffentlichung („Publizität“).

3 Betrieb der ZIAF-IT-Komponenten

3.1 Standorte und Netze

Dataport betreibt im Auftrag des Ministeriums für Landwirtschaft, Umwelt und ländliche Räume (MLUR) im **Rechenzentrum in Altenholz** die zentralen Applikations- und Datenbank-Server der ZIAF-Fachverfahren. Die behördlichen Anwender greifen von dezentralen Standorten über Client-PC auf die ZIAF-Fachverfahren der zentralen Server zu.

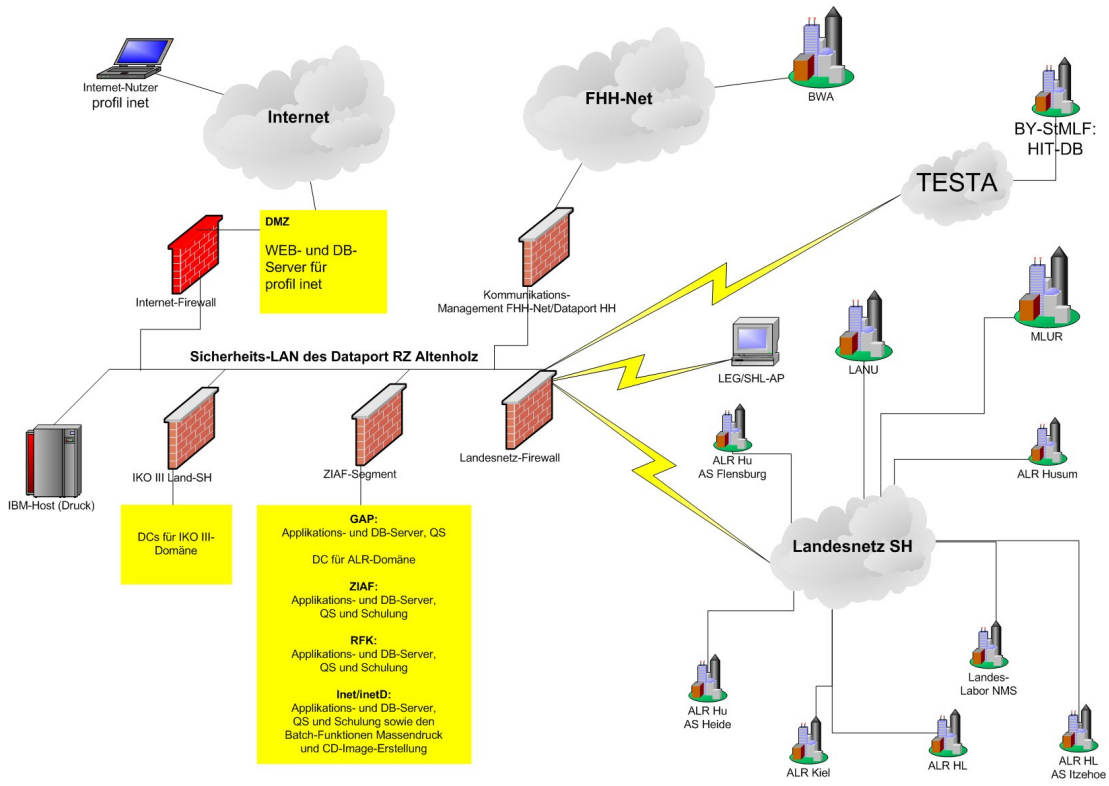

Abb.: Standorte und Netze

Die Kommunikation der ZIAF-Anwender mit den bei Dataport installierten Fachverfahren erfolgt über das **Landesnetz Schleswig-Holstein (SH)**, das vom Finanzministerium betrieben wird. Zusätzlich verfügt die Zahlstelle der Behörde für Wirtschaft und Arbeit in Hamburg über einen Zugriff auf die Daten der Zahlstelle des MLUR. Die Zusammenarbeit der Zahlstellen der Länder Schleswig-Holstein und Hamburg wurde im Gesetz zum Staatsvertrag zwischen dem Land Schleswig-Holstein und der Freien Hansestadt Hamburg auf dem Gebiet der Direktzahlungen

des Europäischen Ausrichtungs- und Garantie-Fonds für die Landwirtschaft, Abteilung Garantie (EG-Direktzahlungen – Staatsvertrag) vom 26. April 2006[4] sowie in einer zwischen der Freien und Hansestadt Hamburg und dem Land Schleswig-Holstein abgeschlossenen Verwaltungsvereinbarung zur Durchführung des Staatsvertrages festgelegt. Die Kommunikation der Zahlstelle Hamburg erfolgt über das so genannte FHHNet der Hamburger Verwaltung.

Aufgrund der verschiedenen Netze (Lokale Netze der Anwender, Landesnetz SH, FHHNet) wird die Datenkommunikation zwischen den bei Dataport im Rechenzentrum aufgestellten ZIAF-Servern und allen Anwenderclients durch den Einsatz eines **Virtual-Private-Network** (VPN) verschlüsselt.

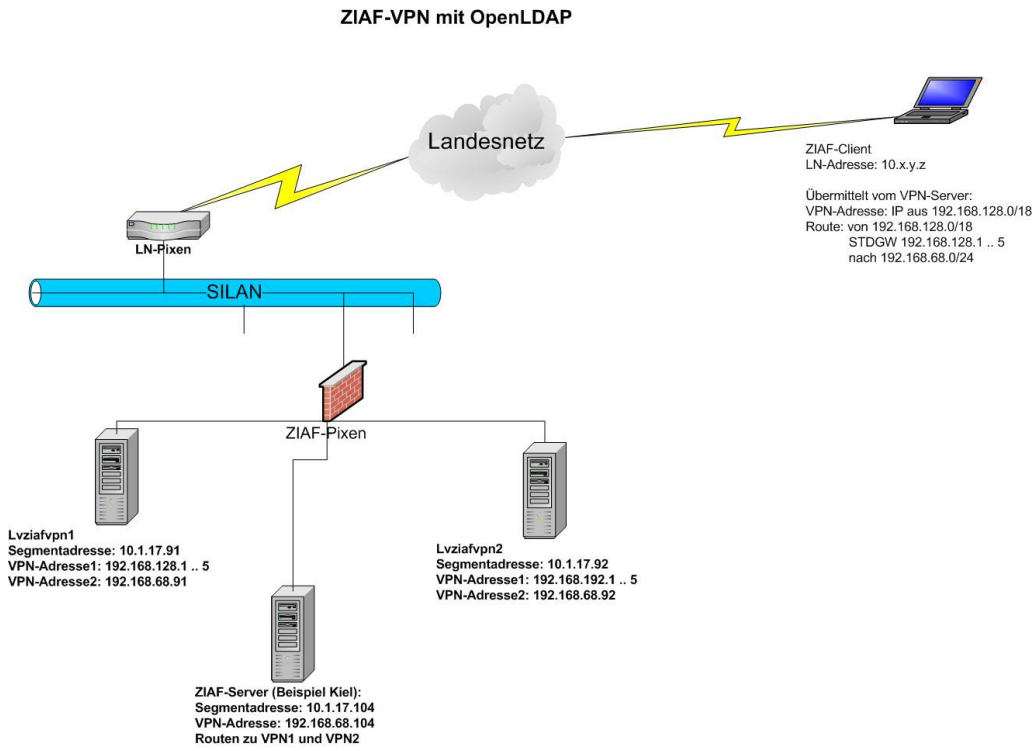

Abb.: ZIAF-VPN

Übergänge in das Landesnetz SH und das FHHNet sind durch Router mit Accesslisten realisiert. Die Zugänge der Fernwartungs- und Fernadministration sind über Firewalls abgesichert.

[4] GS Schl.-H. II, Gl.Nr. 7847-3

3.2 Fachverfahren

Die ZIAF-Fachverfahren setzen sich aus verschiedenen Teilapplikationen zusammen, die die Zahlstelle bei der Bearbeitung der Fördermaßnahmen unterstützen. Es besteht aus folgenden Hauptmodulen:

profident	Verwaltung der Antragsteller
profil c/s	Bearbeitung der Anträge
ravel c/s	Verbuchung
A-Tool	Allgemeines Auswertungswerkzeug
A-Copy	Routinen zum Umkopieren der Daten in die Auswertungsdatenbank
RFK	Referenzflächenkataster
profil inet	Online-Antrag
profil inetD	Erzeugung von Druckdateien

3.3 IT-Systeme

Die ZIAF-IT-Systeme sind in einer separaten **Sicherheitszone** in einem ZIAF-Segment des Rechenzentrums Dataport untergebracht. Das LAN des Dataport-Rechenzentrums ist in Sicherheitsbereiche, die so genannten SILAN-Segmente unterteilt. Dies stellt sicher, dass Serversysteme für unterschiedliche Kunden nur über definierte Kanäle kommunizieren können.

Im **ZIAF-Segment** werden mit Ausnahme der Geräte für profil inet nur ZIAF-IT-Systeme eingesetzt. Externe Serverkommunikationen bestehen zum IBM-Host für den Massendruck und zu den Domänencontrollern für die Nutzeranmeldung.

Die ZIAF-Systeme sind in eine **Produktions-, Qualitätssicherungs-, Test-** und **Schulungsumgebung** sowie für die **Datenverwaltung** wie folgt unterteilt:

- Produktionsumgebung

  Server für profident, profil c/s, ravel c/s, das Referenzflächenkataster (RFK) und die Erzeugung von Druckdateien (INETD)

- Qualitätssicherungsumgebung

Server für profident, profil c/s, ravel c/s, das RFK sowie für die Online Antragsstellung (INET)

- Schulungsumgebung

  Server für profident, profil c/s, ravel c/s, das RFK sowie für die Online Antragsstellung (INET)

- Storage-Area-Network

  Datenverwaltungssystem

Zur Absicherung des Betriebs gegen **Systemausfall** sind die einzelnen IT-Komponenten **redundant** ausgelegt.

3.4 Entwicklung

In der **Vereinbarung der ZIAF-Länder** zur Durchführung des Aktionsprogramms „Zahlstelle und InVeKoS-Agrar-Förderung 2000 innerhalb der Bundesrepublik Deutschland" (ZIAF2000) haben die Länder Schleswig-Holstein, Brandenburg, Sachsen-Anhalt, Mecklenburg-Vorpommern, Hamburg, Bremen und Berlin ihre Zusammenarbeit bei der Neu- und Weiterentwicklung der ZIAF-Fachverfahren und mit beauftragten Dritten geregelt.

Die einzelnen ZIAF-Applikationen werden von **Dataport** und der Firma **data experts GmbH (deg)** entwickelt. Dataport und die deg sind eine **Kooperation** zur Entwicklung der von den beteiligten Ländern gewünschten ZIAF-Applikationen eingegangen.

Die Vorgaben für neue Programmfunktionen werden in Zusammenarbeit mit den beteiligten Ländern in **Facharbeitsgruppen** erörtert und beschlossen, auf deren Basis **Detailkonzepte** erstellt werden.

Für das MLUR wird ein **Testsystem** mit **anonymisierten Datenbeständen** vorgehalten. Neue und geänderte Bausteine werden sowohl während der Entwicklung als auch im Rahmen von „Auslieferтests" in der Entwicklungstest-Umgebung getestet.

Auslieferтests erfolgen zur **Qualitätssicherung** vor Herausgabe der Programmpakete an das MLUR. Nach Abschluss der Entwicklungsarbeiten und ersten Vortests wird ein standardisiertes Programmpaket gepackt und auf das Referenzsystem installiert. In dieser Umgebung wird der abschließende Test vor der Auslieferung durchgeführt. Alle Aktivitäten und ausgelieferten Pakete werden dokumentiert.

3.5 Betriebssteuerung ZIAF

Für das ZIAF-Verfahren (profil c/s, ravel c/s) werden von den Herstellern (Dataport und data experts) **Programmpakete** geliefert, die auf den unterschiedlichen Systemen (Produktion-, Qualitätssicherung-, und Schulungsumgebung) nach festen **Regeln** zu installieren und zu testen sind. Durch die Überwachung des Abnahmeverfahrens wird von der Betriebssteuerrung ZIAF (BSZ) gewährleistet, dass nur getestete und freigegebene Programme zur Anwendung gelangen.

Die **Betriebssteuerung** ZIAF (BSZ) hat hauptsächlich die fristgerechte Verfügbarkeit der Anwendung durch Bereitstellung der neuesten Software-Versionen nach den Anforderungen der Fachbereiche und die Einhaltung der IT-Sicherheitsleitlinie der EU-Kommission sowie des Haushalts- und Kassenrechts (HKR) und des Datenschutzes sicherzustellen.

4 Sicherheitstechnische Elemente der Generaldokumentation

4.1 Konzeption der Generaldokumentation

Ein wesentlicher Teil der **IT-Sicherheitsstrategie** der Zahlstelle ist die ordnungsgemäße Datenverarbeitung der automatisiert bearbeiteten Fördermaßnahmen. 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 sowie den Anforderungen des IT-Grundschutzes Rechnung trägt.

Die Generaldokumentation ist für das IT-Sicherheitsmanagement 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 und
- Revisionsfähigkeit des automatisierten Verfahrens.

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.

Im Anhang befindet sich eine **Übersicht** aller der Generaldokumentation zugeordneten Dokumente. Nachfolgend werden die im Rahmen der **Begutachtung** herangezogenen Dokumente dargestellt. Die Nummern der Dokumente verweisen auf die Generaldokumentation:

4.2 Betreibervertrag (Dokument Nr. 401)

Der zwischen dem MLUR und Dataport abgeschlossene **Betreibervertrag** enthält die Leistungen, die Dataport im Rahmen der Auftragsdatenverarbeitung für den Betrieb der ZIAF-Komponenten erbringt. Die bisherigen generisch gewachsenen vertraglichen Verpflichtungen werden 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
- Anlage 6: Entgeltvereinbarung

4.3 IT-Strukturanalyse (Dokument Nr. 100)

Die IT-Strukturanalyse in der Version 1.0 enthält eine grobe Darstellung über den Betrieb des ZIAF-Fachverfahrens. Es werden die Standorte, die Netzstrukturen sowie die ZIAF-Teilkomponenten kurz beschrieben. Das Dokument grenzt den für die Sicherheitsbetrachtung erforderlichen **IT-Verbund** ab und referenziert auf eine Liste

der Systemkomponenten, in der die einzelnen **technischen Zielobjekte** für den IT-Verbund dokumentiert sind.

4.4 Organisationsbereiche (Dokument Nr. 104)

Das in der Version 1.0 vorliegende Dokument „Organisationsbereiche“ beschreibt die **Aufbauorganisation** der Zahlstelle. Es werden alle Organisationsbereiche aufgeführt, in denen Aufgaben der Zahlstelle unter Einsatz von ZIAF-Informationssystemen durchgeführt werden (vgl. Tz. 2).

4.5 Organisationsablauf MLUR (Dokument Nr. 105)

Das Dokument „Organisationsablauf“ beschreibt in der Version 1.0 die in der Zahlstelle des MLUR **ablauforganisatorischen Zuständigkeiten** für die Bearbeitung der EGFL/ELER-Fördermaßnahmen (vgl. Tz. 2).

4.6 Organisationsstruktur Dataport (Dokument Nr. 108)

Das Dokument „Aufbauorganisation“ wurde vom Dienstleister Dataport in der Version 1.1 erstellt. Es beschreibt die Leistungen der Organisationseinheiten von Dataport, die mit der Entwicklung und dem Betrieb der ZIAF-Verfahren gemäß dem Betreibervertrag zwischen MLUR und Dataport befasst sind.

4.7 ZIAF-Betriebshandbuch (Dokument Nr. 112)

Für den Betrieb der ZIAF-Systeme liegen folgende Systemdokumentationen vor:

- Netzplan
- ZIAF-Kern
- Profil-Inet
- InetWebServer
- Sicherheitskonzept Networker
- ZIAF-Zugriffskonzept
- ZIAF-Dienste

- Dateisystem Sicherung und Rücksicherung
- Client-Aufruf-Konzept
- ZIAF-Installationsmenü
- Zentrale Datensicherung

Die einzelnen Dokumente beschreiben den Aufbau und die Betriebsabläufe für das Serverhosting der zentralen ZIAF-IT-Komponeten.

4.8 Sicherheitsleitlinie MLUR (Dokument Nr. 202)

Die Zahlstelle des MLUR hat eine **Sicherheitsleitlinie** für ihren Zuständigkeitsbereich erstellt und durch den **Leiter der Zahlstelle** in Kraft setzen lassen. Sie liegt in der Version 1.0 vom 29. November 2006 vor. Die zentralen Punkte sind:

- Die Zahlstelle wendet die Kriterien des **IT-Grundschutzes** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an.
- Der **Behördenleiter** trägt als Leiter der Zahlstelle die Gesamtverantwortung für die Einhaltung der für den Betrieb der Zahlstelle relevanten IT-Sicherheit.
- Die IT-Sicherheitsleitlinie gilt für die Zahlstelle und für die dezentralen Dienste im Geltungsbereich des MLUR. Für die anderen beauftragten Einrichtungen der Zahlstelle sind die Kernaussagen der IT-Sicherheitsleitlinie vertraglich zu vereinbaren.
- Die **Gewährleistung der Sicherheit** der Informationssysteme stellt unter Hinweis auf die EU-Verordnung (EG) Nr. 885/2006 ein wesentliches **Zulassungskriterium** der Zahlstelle dar.
- Die gesetzlichen Anforderungen für den **Datenschutz** und die **Datensicherheit** sind zu beachten.
- Die Vorgaben des **IT-Sicherheitsmanagements** sind integraler Bestandteil der Aufbau- und Ablauforganisation der Zahlstelle.
- Von der Zahlstelle ist für die automatisierte Datenverarbeitung ein **angemessenes Sicherheitsniveau** zu gewährleisten.
- Für die Entwicklung und den Betrieb der von der Zahlstelle und ihren Vertragspartnern eingesetzten Informationssysteme gelten folgende **Sicherheitsziele**:
  - Umsetzung einer nach **gesetzlichen** und **vertraglichen** Vorgaben ordnungs-

gemäßen Datenverarbeitung,

- Schutz **vertraulicher 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 sowie
- **transparente** und **nachvollziehbare** Gestaltung der Datenverarbeitungsprozesse.

- Alle mit Aufgaben der Zahlstelle befassten Mitarbeiterinnen und Mitarbeiter sind verpflichtet, die IT-Sicherheitsleitlinie strikt zu beachten. Die Behördenleitung wird auf ihre **Einhaltung** achten.
- Die IT-Sicherheitsleitlinie wird im **Intranet** des MLUR veröffentlicht. Sie wird allen mit Aufgaben der Zahlstelle befassten Mitarbeiterinnen und Mitarbeitern in geeigneter Weise bekannt gegeben.

4.9 Sicherheitsleitlinie Dataport (Dokument Nr. 201)

Die IT-Sicherheitsleitlinie in der Version 1.1 bildet die **Grundlage** für die Herstellung und den Erhalt des erforderlichen **Sicherheitsniveaus** für alle IT-Ressourcen im Verantwortungsbereich von Dataport. Sie schafft und erhält das Bewusstsein der Mitarbeiterinnen und Mitarbeiter für die IT-Sicherheit und legt die **IT-Sicherheitsstrategie** von Dataport fest. Ferner werden in ihr die **organisatorischen Strukturen** für das bei Dataport eingerichtete Informations-Sicherheits-Management-System (ISMS) beschrieben.

4.10 Sicherheitsmanagement-Leitlinie-MLUR (Dokument Nr. 205)

Die Zahlstelle des MLUR hat nach den Vorgaben der IT-Sicherheitsleitlinie ein **Sicherheitsmanagement** eingerichtet. Die entsprechenden Regelungen werden in dem Dokument „Sicherheitsmanagement-Leitlinie in der Version 1.1 festgelegt. Folgende Punkte sind von Bedeutung:

- Das IT-Sicherheitsmanagement umfasst einen **IT-Sicherheitsbeauftragten** und ein ihn unterstützendes **IT-Sicherheitsmanagement-Team**. Der IT-Sicherheitsbeauftragte baut eine eigene Fachkompetenz für IT-Sicherheit auf und ist für alle

IT-Sicherheitsfragen in der Organisation zuständig.

- Funktion des IT-Sicherheitsmanagements ist die Gewährleistung eines übergreifenden **Sicherheitsmanagementprozesses** für die innerhalb der Zahlstelle eingesetzten automatisierten IT-Verfahren des EGFL und ELER.
- Das IT-Sicherheitsmanagement der Zahlstelle greift bei der Umsetzung seiner Aufgaben auf das IT-Sicherheitsmanagement seines **Dienstleisters Dataport** zu, um die Funktion der Sicherheitsmanagementprozesse für die von Dataport betriebenen und entwickelten IT-Verfahren vollständig zu gewährleisten.
- Der IT-Sicherheitsbeauftragte ist in der **Bewertung** der IT-Sicherheit fachlich **weisungsfrei** und hat direktes Vortragsrecht beim Leiter der Zahlstelle.
- Er muss zur Aufgabenerfüllung über die erforderliche Sachkunde verfügen und ist mit ausreichenden personellen und sachlichen **Ressourcen** auszustatten, um seine Aufgaben und Befugnisse erfüllen zu können.
- Er ist zuständig für die **Einhaltung** der innerhalb der Zahlstelle getroffenen Sicherheitsmaßnahmen.
- Er **kontrolliert** die Sicherheitsvorgaben der von der Zahlstelle beauftragten Dienstleister.
- Er ist **Ansprechpartner** für die IT-Verfahrensanwender.
- Der **Leiter der Zahlstelle** unterstützt den IT-Sicherheitsbeauftragten bei der Wahrnehmung seiner Aufgaben und gewährleistet die Bereitstellung ausreichender Haushaltsmittel für seine Aus- und Fortbildung.
- Der IT-Sicherheitsbeauftragte wird bei **sicherheitsrelevanten Entscheidungen**, bei der **Beschaffung von IT-Systemen** oder bei der **Gestaltung von IT-gestützten Prozessen** der Zahlstelle rechtzeitig beteiligt und angehört.
- Er **prüft** und **bewertet** regelmäßig die **Umsetzung**, **Wirksamkeit** und **Praktikabilität** der in dem Sicherheitskonzept getroffenen Sicherheitsmaßnahmen.
- Alle Mitglieder des IT-Sicherheitsmanagement-Teams müssen für ihre Aufgabenerfüllung über die erforderliche **Sachkunde** verfügen.
- Das IT-Sicherheitsmanagement-Team wird vom IT-Sicherheitsbeauftragten bei **sicherheitsrelevanten Entscheidungen** informiert.
- Es führt **Sitzungen** durch, in denen aktuelle Sicherheitsthemen behandelt werden.

4.11 Sicherheitsmanagement Dataport (Dokument Nr. 204)

Das Sicherheitsmanagement Dataport ist für die dauerhafte **Aufrechterhaltung** einer angemessenen Sicherheit zuständig. Entscheidend für den **Erfolg** des Sicherheitsmanagements ist die **Verankerung in den Unternehmensstrukturen**. Für das Sicherheitsmanagement wurde ein „IT-Sicherheits- und Datenschutz-Managementhandbuch“ in der Version 1.1 erstellt, das die **IT-Sicherheits-Prozesse** und deren **Zusammenwirken** beschreibt. Das IT-Sicherheits-Managementhandbuch gilt für den **gesamten** Tätigkeitsbereich von Dataport. Das Konzept wurde am 28. August 2007 mit Blick auf die Anforderungen des IT-Grundschutzes gemäß § 43 Abs. 2 LDSG auditiert[5].

4.12 Sicherheitsvorfälle und Notfallmanagement (Dokument Nr. 206)

Das Dokument „Sicherheitsvorfälle und Notfallmanagement“ in der Version 1.0 beschreibt die Behandlung von **Sicherheitsvorfällen** innerhalb der Zahlstelle des MLUR. In dem Dokument werden **Ansprechpartner** für die Bearbeitung von Sicherheitsvorfällen benannt und der **Bearbeitungsprozess** beschrieben.

4.13 Schutzbedarfsfeststellung (Dokument Nr. 207)

Die **Schutzbedarfsfeststellung** liegt in der Version 1.0 vor und wurde auf der Grundlage der **IT-Sicherheitsleitlinie** für die IT-Verfahren der Zahlstelle des EGFL- und ELER-Fonds durchgeführt. Das Ziel der Schutzbedarfsfeststellung ist die Bestimmung des **Schutzbedarfs** für alle im Bereich der Zahlstelle eingesetzten IT-Systeme, mit denen (personenbezogene) Daten über IT-Verfahren des EGFL- und ELER-Fonds (ZIAF-Verfahren) verarbeitet werden. Der für die Datenverarbeitung erforderliche Schutzbedarf ist vom **Leiter der Zahlstelle** des MLUR auf **„hoch“** eingestuft worden. **Nach der Umsetzung** der Grundschutz-Standardmaßnahmen wird deshalb eine **ergänzende Sicherheitsanalyse** notwendig. Basierend auf ihren Ergebnissen werden zusätzliche Maßnahmen festgelegt.

[5] www.datenschutzzentrum.de/audit/kurzgutachten/a0717/a0617.pdf

4.14 Sicherheitsmaßnahmenkatalog (Dokument Nr. 208)

Die ausgewählten Sicherheitsmaßnahmen und der Stand ihrer Umsetzung sind vom MLUR und dem Dienstleister Dataport in Form eines GSTool-Reports dokumentiert. Dieser Report enthält eine Übersicht über die Maßnahmenumsetzung und detaillierte Informationen zur Umsetzung jeder einzelnen Maßnahme.

4.15 Restrisikobetrachtung (Dokument Nr. 209 und 210)

Das Dokument „Restrisikobetrachtung“ beinhaltet die Dokumentation der ergänzenden **Sicherheitsanalyse** und der **Risikoanalyse** nach dem im BSI-Standard 100-3 vorgeschlagenen Verfahren.

In der Risikoanalyse werden im ersten Schritt die betroffenen Systeme, Komponenten und Kommunikationsverbindungen identifiziert (ergänzende Sicherheitsanalyse).

Im zweiten Schritt werden die Gefährdungslagen aus den bereits modellierten Bausteinen identifiziert, die sich in der Auswirkung oder der Eintrittswahrscheinlichkeit vom Schutzbedarf normal unterscheiden.

Anschließend werden bezogen auf Telearbeit, mobiles Arbeiten sowie die Anwendung ZIAF zusätzliche Gefährdungslagen identifiziert.

Im letzten Schritt werden die Handlungsoptionen für das Management der identifizierten, zusätzlichen Risiken analysiert und zusätzliche Maßnahmen für deren weitere Reduktion definiert. Die verbliebenen Restrisiken werden benannt.

Die „Zusätzlichen Maßnahmen“ betreffen im Wesentlichen:

- **Redundanz** von kritischen Systemen, Netzwerkkomponenten und Leitungswegen
- **Einsatz von Ende-zu-Ende-Verschlüsselung** für die Datenkommunikation zwischen ZIAF-Clients und Anwendungsservern, Verschlüsselung von Festplatten für mobile Clients und Verschlüsselung administrativer Zugänge beim Dienstleister Dataport
- **Ergänzende Infrastruktur für Notfälle** und
- **Modellierung** der ZIAF-Anwendung unter Rückgriff auf die Bausteine B1.10 (**Standardsoftware**) und B5.7 (**Datenbanken**) unter Anwendung ergänzender, spezifische Sicherheitsmaßnahmen.

4.16 Virenschutzkonzept (Dokument Nr. 214)

Das **Virenschutzkonzept** behandelt die Gefährdungslagen und Maßnahmen des Bausteins B1.6 (Computer-Virenschutz-Konzept). Es beschreibt die Risiken, gegen die Schutzmaßnahmen erforderlich sind, sowie die Maßnahmen zur Reduktion dieser Risiken. Das Virenschutzkonzept wird durch eine **betriebliche Dokumentation**, die zum IKOTECH III-Standard für Arbeitsplätze gehört, ergänzt. Sie enthält die Leistungsmerkmale und gewählte Konfiguration der eingesetzten Virenschutzlösung sowie das Virenschutzmanagement (Aktualisierung, betrieblicher Prozess des Umgangs mit Virenmeldungen etc.).

4.17 Notfallhandbuch (Dokument Nr. 215 und 216)

Das **Notfallhandbuch** besteht aus drei Bänden.

Band 1 behandelt die spezifischen Gegebenheiten der Standorte des Verfahrens sowie die zugehörigen Notfallverantwortlichen, Melde- und Alarmierungswege. In diesem Band ist auch der Fall eines eingeschränkten IT-Betriebes geregelt.

Band 2 behandelt die verfahrensspezifische zentrale Infrastruktur (System- und Netzinfrastruktur). Hier sind basierend auf Standardszenarien (Schrank-, Raum- und Standortkatastrophe) Planungen für Sofortmaßnahmen und das Wiederanlaufen definiert. Dieser Band enthält auch die Beschreibung von notfallbedingten Restrisiken für das Verfahren.

Band 3 behandelt die zentrale Infrastruktur im Rechenzentrum einschließlich der Sofortmaßnahmen und Wiederanlaufpläne beim Eintreten spezifischer Ereignisse, die Notfälle auslösen können. Auch in diesem Band sind Notfallverantwortliche und Alarmierungswege im Rechenzentrum geregelt.

5 Umsetzung der Konzeption

5.1 Prüfungsverlauf

Nach Prüfung der vorgelegten Dokumentation wurden die zu prüfenden Organisationen, Termine und Bausteine aus den IT-Grundschutz-Katalogen für die Vor-Ort-Überprüfung ausgewählt. Diese waren:

- LANU (19.09.07): Bausteine B1.10 (Standardsoftware), B2.1 (Gebäude), B2.2 (Verkabelung), B2.3 (Büroraum), B2.4 (Serverraum), B2.201 (Allgemeiner Client) und B2.09 (Client unter Windows XP).
- Das MLUR (20.09.07): Bausteine B2.1 (Gebäude), B2.2 (Verkabelung), B2.3 (Büroraum), B2.4 (Serverraum), B2.201 (Allgemeiner Client) und B2.09 (Client unter Windows XP).
- ALR Lübeck, Außenstelle Itzehoe (21.09.07): Bausteine B1.10 (Standardsoftware), B2.1 (Gebäude), B2.2 (Verkabelung), B2.3 (Büroraum), B2.4 (Serverraum), B2.201 (Allgemeiner Client) und B2.09 (Client unter Windows XP).
- Dataport (20. – 21. und 24.09.07): Bausteine B1.1 (Organisation), B1.8 (Behandlung von IT-Sicherheitsvorfällen), B1.13 (IT-Sicherheitssensibilisierung und -Schulung), B2.1 (Gebäude), B2.3 (Büroraum), B2.9 (Rechenzentrum), B3.101 (Allgemeiner Server) und B3.201 (Allgemeiner Client).

5.2 Sicherheitsmanagement

Das **Sicherheitsmanagement** arbeitet auf der Basis einer spezifischen Leitlinie (vgl. Tz. 4.10). Es arbeitet im Wesentlichen mit den folgenden Prozessen:

- Prozess zur Aktualisierung und Umsetzung der Sicherheitskonzeption für ZIAF, gestützt auf das Sicherheitsmanagement-Team; zu den Aufgaben dieses Prozesses zählen auch die Durchführung interner und externer Audits sowie die Erstellung und Umsetzung eines Schulungskonzeptes.
- Sicherheitsvorfallmanagement und Notfallmanagement, gestützt auf das Sicherheitsvorfallmanagement-Team; das Sicherheitsvorfallmanagement behandelt auch Informationen über Sicherheitslücken, z.B. auf Basis von CERT-Meldungen. Diese Informationen werden vom Dienstleister Dataport zentral aufbereitet und von dem Sicherheitsbeauftragten im MLUR bewertet.

Die Management-Teams (Sicherheitsmanagement-Team und Sicherheitsvorfallmanagement-Team) setzten sich aus Koordinatoren und Ansprechpartnern der nach geordneten Behörden und des Dienstleisters Dataport unter Leitung des Sicherheitsbeauftragten für das Verfahren im MLUR zusammen.

Das Sicherheitsmanagement folgt im Aufbau den im Standard BSI 100-2 vorgegebenen Anforderungen und ist somit grundschutzkonform.

5.3 Sicherheitskonzeption

Die Sicherheitskonzeption erfolgt nach der IT-Grundschutzmethodik. Sie stützt sich auf die folgenden Dokumente:

- „Sicherheitsleitlinie für die Zahlstelle des EGFL- und ELER-Fonds“ V. 1.0 vom 23.11.06 sowie die „Leitlinie IT-Sicherheitsmanagement“ V. 1.1 vom 15.03.07.
- Dokumente zum IT-Sicherheitskonzept, insbesondere
  - IT-Strukturanalyse V. 1.0 vom 09.07.07
  - Schutzbedarfsfeststellung V. 1.0 vom 18.06.07
  - Restrisiko-Analyse nach BSI-Standard 100-3 V. 1.1 vom 23.07.07
  - Sicherheits- und Notfallmanagement V 1.0 vom 25.07.07
  - Notfallhandbuch (Bände 1 bis 3) vom 21.08.07
  - Datensicherungskonzept V. 1.0 vom 19.07.07
  - Virenschutzkonzept V 1.0 vom 17.07.07
  - Kryptokonzept V. 1.2 vom 26.07.07
  - Vermerk Archivierung vom 23.07.07
  - Konzept Berechtigungsverwaltung V. 1.0 vom 16.07.07.
- GSTool-Report über die Modellierung und den Umsetzungsstand der IT-Grundschutzmaßnahmen beim MLUR, den nach geordneten Behörden und dem Dienstleister Dataport.

Die Sicherheitskonzeption ist grundschutzkonform, d.h. sie folgt den BSI-Standards 100-2 und 100-3.

5.4 Betriebliche Abläufe

Für die IT-Sicherheit des Verfahrens sind insbesondere die folgenden betrieblichen Prozesse relevant:

- **Anforderungsmanagement** und Weiterentwicklung der ZIAF-Anwendung mit den zugehörigen Test- und Freigabeverfahren,
- **Störungs- bzw. Fehlermanagement** und
- Prozess zur **Nutzerverwaltung** und dem **Rechtemanagement** in der Betriebs-

steuerungszentrale (BSZ) im MLUR.

Die genannten Prozesse sind nachvollziehbar beschrieben. Das Anforderungsmanagement behandelt wesentliche Anforderungen für die Optimierung der ZIAF-Anwendung unter Sicherheitsgesichtspunkten. Das Störungs- und Fehlermanagement ist ein etablierter Prozess, der über Institutionsgrenzen auch in Zusammenarbeit mit dem Dienstleister für die Softwareentwicklung (deg) funktioniert. **Die Vergabe von Benutzerrechten ist einschließlich der entsprechenden Grundlagen dokumentiert**. Hierzu soll zukünftig auch ein Tool zur Unterstützung eingesetzt werden. Änderungen bei Mitarbeitern werden zuverlässig erfasst, die Rechte entsprechend angepasst. Eine Revision vergebener Benutzerrechte findet statt.

5.5 Prozessreifegradmodell

In der „Leitlinie für die Sicherheit der Informationssysteme in den Zahlstellen“[6] wird das **Capability-Maturity-Model (CMM)** als **Auditinstrument** vorgeschrieben. Das CMM erlaubt die Bewertung der Umsetzung von Prozessen, es ist aber nicht für die Bewertung von technischen Sicherheitsmaßnahmen geeignet. Zur Unterstützung der Bescheinigenden Stelle bei der **Bewertung des Sicherheitsmanagements** in der Zahlstelle (einschließlich der nach geordneten Behörden und des Dienstleisters Dataport) wird das Capability-Maturity-Model auf die Ergebnisse dieses Audits angewandt. In der genannten Leitlinie sind zu bewertende Aspekte des Sicherheitsmanagements benannt. Diese sind

- das Erkennen und Mitteilen des Problems (bzw. der Aufgabe),
- die Politik,
- assoziierte Prozesse und Schulungen zur Umsetzung der Politik und
- die Messung der Effizienz der Politik und der assoziierten Prozesse und darauf aufbauend Vornahme von Verbesserungen.

In der Leitlinie werden folgende Stufen dargestellt:

- Stufe 1: Ausgangszustand (Initial level / ad hoc level), Chaotisch, eher Projekte als Prozesse; Input und Ergebnis sind nicht definiert, Abläufe wiederholen sich nur

[6] Leitlinie AGRI-2004-60334-01-00-DE-TRA-00 vom 15.10.2004

selten.

- Stufe 2: Reproduzierbar aber intuitiv (Repeatable but intuitive), auf Ebene der kleinsten Organisationseinheiten ist der Prozess organisiert; Input und Ergebnis sind definiert.
- Stufe 3: Definiert (Defined process), Arbeitsschritte und Teilprozesse laufen wiederholbar ab, Prozess ist dokumentiert.
- Stufe 4: Lenkbar und messbar (Managed and measurable), es existieren für Arbeitsschritte und Teilprozesse Qualitätskriterien, so genannte Key Performance Indikatoren (KPI); diese werden auf Teilprozessebene für die Optimierung des Prozesses eingesetzt.
- Stufe 5: Optimiert (Optimised level), der gesamte Prozess wird unter Auswertung der KPI beständig optimiert (Deming- oder PDCA-Zyklus).

Die Umsetzung des Sicherheitsmanagements wird nach dem Prozessreifegradmodell (Capability-Maturity-Model - CMM) mit Stufe 4 bewertet.

6 Datenschutzrechtliche Bewertung

6.1 Landesdatenschutzgesetz (LDSG)

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 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. Die gesetzlichen Regelungen zur Datensicherheit beziehen sich auf den **allgemeinen anerkannten Standard der IT-Sicherheit** und die Anforderungen an ihre **Dokumentation**. Soweit die Umsetzung dieser Vorschriften unter Einbeziehung der Regelungen des IT-Grundschutzstandards des BSI erfolgt, ergeben sich folgende Schwerpunkte:

- Einrichtung eines **Sicherheitsmanagements**,
- Anforderungen an die **Administration** und ihre **Revisionsfähigkeit**,
- **Trennung von Entwicklung und Betrieb** sowie
- Anforderung an die **Dokumentation**.

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)**

§ 3 Verfahrensdokumentation

§ 4 Verfahrenszweck

§ 5 Verfahrensbeschreibung

§ 6 Sicherheitskonzept

§ 7 Test und Freigabe

§ 8 Verfahrensübergreifende Dokumentation und Protokolle

Die Begutachtung hat ergeben, dass die Zahlstelle des MLUR die konzeptionellen Anforderungen aus Datenschutz und IT-Sicherheit erfüllt. Mit der Einrichtung der IT-Sicherheitsprozesse wird die Einhaltung der datenschutzrechtli-

chen Anforderungen unterstützt.

6.2 Daten verarbeitende Stelle

Um die zu beachtenden Rechtsvorschriften den jeweiligem **Normadressaten** richtig zuzuordnen, ist zu klären, wer als **Daten verarbeitende Stelle** im Sinne des Landesdatenschutzgesetzes für den Einsatz der Fachverfahren für die Bearbeitung der EGFL- und ELER-Fördermaßnahmen in Frage kommt.

Festgestellt wurde, dass das eingesetzte ZIAF-Verfahren – Applikation und Datenbestände – vom MLUR zentral auf IT-Systemen des von ihm beauftragten **Dienstleisters Dataport** eingesetzt wird. Daran angeschlossen sind u.a. das MLUR sowie die Ämter für ländliche Räume, die die eingehenden Anträge mit dem Verfahren verwalten. Als Daten verarbeitende Stellen sind deshalb sowohl die Ämter für ländliche Räume als auch das MLUR anzusehen. Die **Verfahrensverantwortung** liegt beim MLUR, während die **Datenverantwortung** sowohl bei den Ämtern für ländliche Räume als auch beim MLUR anzusiedeln ist.

Aus datenschutzrechtlicher Sicht liegt aufgrund der gemeinsamen Nutzung der Applikation ZIAF ein Verfahren im Sinne des § 8 LDSG vor. Danach hat das MLUR **erhöhte** Sicherheitsanforderungen zu beachten.

Die Begutachtung hat ergeben, dass die Verfahrens- und Datenverantwortung vom MLUR und den dezentralen Organisationen den normativen Anforderungen entsprechend wahrgenommen wird. Die aufbau- und ablauforganisatorischen Zuständigkeiten für die ordnungsgemäße Durchführung der Aufgaben sind in der Generaldokumentation gut und transparent dargestellt. Der nach den Kriterien der IT-Grundschutzmethodik mit „hoch“ festgelegte Schutzbedarf entspricht den datenschutzrechtlichen Erfordernissen.

6.3 Vorabkontrolle

Bei dem ZIAF-Verfahren handelt es sich um ein **gemeinsames Verfahren** im Sinne des § 8 LDSG. Da mit dem Verfahren personenbezogene Daten verarbeitet werden, ist vom MLUR eine **Vorabkontrolle** gemäß § 9 LDSG durchzuführen. Bei Einrichtung oder wesentlichen Änderungen des Verfahrens ist innerhalb einer angemesse-

nen Frist dem **behördlichen Datenschutzbeauftragten** oder, wenn ein solcher nicht gemäß § 10 LDSG bestellt ist, dem Unabhängigen Landeszentrum für Datenschutz Gelegenheit zur **Prüfung** zu geben, ob die Datenverarbeitung zulässig und die vorgesehenen Sicherheitsmaßnahmen nach den §§ 5 und 6 LDSG ausreichend sind.

Mit der Begutachtung wurden die für die Vorabkontrolle erforderlichen Unterlagen geprüft. Mit der Auditierung der datenschutzrechtlichen und sicherheitstechnischen Konzeption des ZIAF-Verfahrens ist das Erfordernis der Vorabkontrolle erfüllt.

6.4 Auftragsdatenverarbeitung

Das MLUR bleibt trotz der Vergabe der ZIAF Datenverarbeitung an den Dienstleister Dataport für die **Einhaltung der EU- und Datenschutzvorschriften** verantwortlich. Im Rahmen der Auftragsdatenverarbeitung nach § 17 LDSG hat das MLUR dafür Sorge zu tragen, dass der **Betrieb** des ZIAF Verfahrens nur im Rahmen seiner **Weisungen** ausgeführt wird. Es hat die erforderlichen **technischen** und **organisatorischen Maßnahmen** zu treffen, um dies sicherzustellen.

Die Begutachtung hat ergeben, dass die Zahlstelle des MLUR mit ihrem Sicherheitsmanagement in der Lage ist, die von seinen Dienstleister einzuhaltenden Sicherheitsvorgaben zu überwachen.

6.5 IT-Grundschutz

In der von der Zahlstelle zu beachtenden Verordnung (EG) Nr. 885/2006 der Kommission vom 21. Juni 2006 sind **Sicherheitsanforderungen** für die in der Zahlstelle eingesetzten Informationssysteme festgelegt. Im **Anhang** der Verordnung werden für die Zahlstelle unter Textziffer 3 **Zulassungskriterien** beschrieben, die besonders die Einhaltung **eines internationalen IT-Sicherheitsstandards** fordern. Werden die Zulassungskriterien nicht oder nur mangelhaft erfüllt, kann dies gemäß Artikel 2 Abs. 3 der Verordnung zum Entzug der Zulassung der Zahlstelle führen.

Bundeseinheitlich haben die Bundesländer **IT-Grundschutz** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als Standard festgelegt.

Aus Sicht des Datenschutzes geben die Anforderungen des IT-Grundschutzes den

Stand der Technik der nach § 5 Abs. 2 LDSG erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen wieder.

Die Zahlstelle des MLUR wendet IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik an. Die einzelnen Schritte der Grundschutzmethodik werden eingehalten und durch das IT-Sicherheitsmanagement überwacht.

6.6 Zusammenfassende Bewertung

Im Auditverfahren „**Sicherheit der Informationssysteme der Zahlstelle**“ wurde festgestellt, dass die Zahlstelle des MLUR über eine rechts- und normenkonforme **Konzeption** (Generaldokumentation) verfügt, die die Festlegung und Umsetzung der Sicherheitsanforderungen der EU- und der Landesdatenschutzvorschriften beschreibt.

Die Praxistauglichkeit der Generaldokumentation wird durch seine Implementierung für das ZIAF-Fachverfahren bestätigt. Die Berücksichtigung der **BSI-Sicherheitsstandards**100-1 bis 100-3 gewährleistet die Bestimmung von wirkungsvollen IT-Sicherheitsprozessen sowie die dafür erforderlichen IT-Sicherheitsmaßnahmen.

Die Zahlstelle des MLUR hat die im Auditverfahren festgelegten Datenschutzziele erreicht. Es werden die Rechtsvorschriften, Richtlinien und sonstigen Arbeitsanweisungen zur **Datensicherheit** und zur **Ordnungsmäßigkeit** der Datenverarbeitung beachtet. Die Umsetzung der IT-Sicherheit erfolgt unter der Berücksichtigung der **IT-Grundschutz-Methodik.** Die **IT-Grundschutz-Standards** werden nach dem **BSI-Qualifizierungsverfahren** angewandt.

Die **Leitungsebene der Zahlstelle** ist sensibilisiert und übernimmt Aufgaben und Pflichten bezüglich der Informationssicherheit. Von ihr werden folgende **Managementfunktionen** wahrgenommen:

- Übernahme der Gesamtverantwortung für IT-Sicherheit,
- Festlegung der Sicherheitsziele und Sicherheitsstrategie,
- Integration der IT-Sicherheit mit Hilfe des IT-Sicherheitsmanagement.

Darüber hinaus wurden bei der Durchführung des Audits folgende „**datenschutzfreundliche**“ Aspekte als besonders erwähnenswert festgestellt:

1. Die Datenverarbeitung wird nach den Sicherheitszielen der **Verfügbarkeit, Vertraulichkeit, Integrität** sowie der **Ordnungsmäßigkeit** in einer geregelten Aufbau- und Ablauforganisation betrieben.

2. Die **Generaldokumentation** beschreibt umfassend den Einsatz und den Betrieb der in der Zahlstelle eingesetzten Informationssysteme. Sie enthält eine vorbildlich nachvollziehbare **Sicherheitskonzeption**.

3. Der Dienstleister Dataport verpflichtet sich über einen „**Betreibervertrag**“ zu Leistungen, die den Datenschutz und die Datensicherheit beinhalten. Darüber hinaus sichert der Dienstleister im Vertrag für den Betrieb des ZIAF-Fachverfahrens die Einhaltung des BSI-Grundschutzes zu.

4. Die Zahlstelle verfügt über ein **funktionierendes Sicherheitsmanagement**, dass aufbau- und ablauforganisatorisch in der Lage ist, die in der IT-Sicherheitsleitlinie festgelegten Ziele vollständig zu erreichen und dauerhaft aufrecht zu erhalten.

Die Prüfung hat ergeben, dass das in der Generaldokumentation beschriebene Konzept zur Sicherheit der ZIAF-Informationssysteme in Übereinstimmung mit dem BSI-Grundschutzstandard gestaltet ist und keinen Anlass zu datenschutzrechtlichen Beanstandungen gibt.

Kiel, 10. Oktober 2007

gez. Dr. Martin Meints, Heiko Behrendt

(Gutachter)

Anlage: Liste über vorgelegte Dokumente im Rahmen des Audits

Nr.	Dokument
	Teil 0: Einleitung
001	Struktogramme „allgemeiner Überblick über Verfahrensteile“ und „Organisation“
002	Modul IT-Strategie der Landesverwaltung S-H und des Mehrländer-Fachverfahrens ZIAF
	Teil 1: IT-Konzept (BSI-Strukturanalyse)
100	IT-Strukturanalyse
101	Modul Grundsätze über Organisation und Aufgaben der Zahlstelle
102	Modul EGFL/ELER-Förderprogramme
103	Modul Gesetzliche und mitgeltende Regelungen
104	Modul Organisationsbereiche
105	Modul Organisationsablauf im MLUR mit 5 Anlagen
106a	IKOTech III-Einsatzkonzept 2.0, Einführungskonzept ÄLR
106b	Richtlinien Landeslabor
107	Modul Antragsverfahren Internet
108	ZIAF-Organisationsstruktur bei Dataport
109	Berechtigungskonzept
110a	Modul Software-Entwicklung, Service und Pflege profil c/s
111	Modul Test und Installation bei Dataport
112	ZIAF-Betriebshandbuch
113a	Client-Richtlinie Dataport
113b	Client-Richtlinie ESARI
115	Modul Dezentrale Systeme in den ÄLR
116	Modul Anwendungsbetreuung durch Dataport
117	Modul Massendruckverfahren und CD-Erstellung
118	Modul Zentraler Betrieb
119	Modul IT-Planung
120	Modul Hard- und Softwaremanagement
	Teil 2: Sicherheitskonzept
201	Modul IT-Sicherheitsleitlinie Dataport
202	Modul IT-Sicherheitsleitlinie MLUR
204	Modul Sicherheitsmanagement Dataport
205	Modul Sicherheitsmanagement MLUR
206	Modul IT-SichVorfälle und Notfallmanagement MLUR
207	Modul Schutzbedarfsfeststellung
208	Modul Grundschutz-Sicherheitsmaßnahmen
209	Modul Restrisikobetrachtung Dataport
210	Modul Restrisikobetrachtung MLUR
211a	Modul Kryptokonzept MLUR

Nr.	Dokument
211b	Modul Kryptokonzept Dataport
212	Modul Datensicherungskonzept
213	Modul Archivierungskonzept
214a	Modul Virenschutzkonzept für IKOTECH III
214b	Modul Virenschutzkonzept Dataport
215a	Modul Notfallkonzept für allgemeine Dataport-Infrastruktur (Band 3 Notfall-Handbuch)
215b	Modul Notfallkonzept für Dataport-ZIAF-Infrastruktur (Band 2 Notfall-Handbuch)
216	Modul Notfallkonzept MLUR (Band 1 Notfall-Handbuch)
217	Modul Konzept Berechtigungs-Verwaltung MLUR
	Teil 3: Operative Dokumentation
301	Regelungen für externe Mitarbeiter
302	Dienst- und Arbeitsanweisungen für die Anwendung des IT-Verfahrens ZIAF
303	Aufgabenbeschreibung und organisatorische Regelungen zum Betrieb des IT-gestützten Verfahrens ZIAF
304	Arbeitsanweisung Nutzer- und Rechteverwaltung „Profil c/s“ des MLUR
305	Hinweise für die Einrichtung mobiler Arbeitsplätze
306	Checkliste der bescheinigenden Stelle für die Prüfung der IT-Sicherheit im EU-Haushaltsjahr 2004/2005 für EAGFL-G im Rahmen des Reifegradmodells (Capability Maturity Model –CMM–)
307	Anwenderhandbücher der deg und von Dataport
308	Allgemeine Arbeitsanweisungen Dataport
309	Dienstanweisung Berechtigungs-Verwaltung MLUR
310	ZIAF-Problem-Management
311	ZIAF-Installationsmanagement Dataport
312	ZIAF-Auslieferungs-Management MLUR
313	ZIAF-Fehlermanagement
	Teil 4: Verträge und Vereinbarungen
401	Vertrag zwischen MLUR und Dataport (Neufassung Betreibervertrag) nach EVB-IT
402	Vertrag zur Softwareauslieferung AGRIS und ZIAF
403	Vertrag zur Client-Administration
404	Vertrag zur Druckpauschale
405	Vertrag zwischen MLUR und Dataport über die Softwareüberlassung
406	Service-/Pflegevertrag profil c/s
407	Vereinbarung zur Hinterlegung der Programmquellen
408	Vertragliche Regelungen zur Anwendungsbetreuung ZIAF
409	Vereinbarung der Bundesländer zur Durchführung des Aktionsprogramms ZIAF 2000 + Anhang
410	Durchführungsverträge zur Erfüllung von Förderaufgaben zwischen MLUR und IB, Schleswig-Holsteinische Landgesellschaft
411	Nutzungsbedingungen über ZIAF zwischen MLUR und BWA HH (Staatsvertrag + Verwaltungsvereinbarung)

Nr.	Dokument
412	Vereinbarung HIT + ZID
413	Fernwartungsverträge
	Teil 5: EU-Verordnungen und EU-Leitlinien (Anlagen)
501	Verordnung (EG) Nr. 1290/2005 des Rates vom 21. Juni 2005 (ABl. EU L 209 vom 11.08.2005, S. 1) über die Finanzierung der Gemeinsamen Agrarpolitik
502	Verordnung (EG) Nr. 1782/2003 des Rates vom 29. September 2003 (ABl. EU L 270 vom 21.10.2003, S. 1) mit gemeinsamen Regelungen für Direktzahlungen im Rahmen der Gemeinsamen Agrarpolitik und mit bestimmten Stützungsregelungen für Inhaber landwirtschaftlicher Betriebe und zur Änderung der Verordnungen (EWG) Nr. 2019/93, (EG) Nr. 1452/2001, (EG) Nr. 1453/2001, (EG) Nr. 1454/2001, (EG) Nr. 1868/94, (EG) Nr. 1251/1999, (EG) Nr. 1673/2000, (EWG) Nr. 2358/71 und (EG) Nr. 2529/2001
503	Verordnung (EG) Nr. 1698/2005 des Rates vom 20. September 2005 (ABl. EU L 277 vom 21.10..2005, S. 1) über die Förderung der Entwicklung des ländlichen Raums durch den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER)
504	Verordnung (EG) 883/2006 der Kommission vom 21.06.2006 (ABl. EU L 171 vom 23.06.2006, S. 1) mit Durchführungsvorschriften zur Verordnung (EG) Nr. 1290/2005 des Rates hinsichtlich der Buchführung der Zahlstellen, der Ausgaben- und Einnahmenerklärungen und der Bedingungen für die Erstattung der Ausgaben im Rahmen des EGFL und des ELER
505	Verordnung (EG) 885/2006 der Kommission vom 21.06.2006 (ABl. EU L 171 vom 23.06.2006, S. 90) mit Durchführungsvorschriften zur Verordnung (EG) Nr. 1290/2005 des Rates hinsichtlich der Zulassung der Zahlstellen und anderen Einrichtungen sowie des Rechnungsabschlusses für den EGFL und den ELER
506	Leitlinien für die Sicherheit der Informationssysteme in den Zahlstellen vom 15.10.2004
	Teil 6: Anhang
601	Glossar
602	Abkürzungs-Verzeichnis