FÜHRUNGSAKADEMIE
BADEN-WÜRTTEMBERG

BILDUNG21

Datenschutz und Datensicherheit

Integriertes Bildungsmanagementsystem

Version 2.3
Dr. Siegfried Mauch
Juni 2010

Führungsakademie Baden-Württemberg
Hans-Thoma-Str. 1
76133 Karlsruhe
Telefon: (07 11) 126 - 1014
Telefax: (07 11) 126 - 1019
E-Mail: siegfried.mauch@um.bwl.de

Inhaltsverzeichnis

1 Vorbemerkung

Das vorliegende Konzept ist das Datenschutzkonzept des integrierten Bildungsmanagements von BILDUNG21. Im ersten Schritt werden neben der Zielsetzung und dem Geltungsbereich Funktionsumfang, Datenstruktur und Funktionen beschrieben. Danach folgt mit Unterstützung des Informatikzentrums Baden-Württemberg (IZLBW) eine Beschreibung des technischen Konzepts. Anschließend werden die rechtlichen Positionen der beteiligten Stellen definiert, die Datenverarbeitung unter rechtlichen Gesichtspunkten und die Rechte der betroffenen Lerner gewürdigt sowie die Gewährleistung der Datensicherheit beschrieben. Die Konzeption schließt ab mit einer Würdigung und Bedienung des Schutzbedarfs personenbezogener Daten und einer Risikoanalyse.

2 Zielsetzung

Die vorliegende Konzeption ist Bestandteil der Datenschutz- und Datensicherheitskonzeption von BILDUNG21. In ihr werden die innerhalb des Teilsystems „integriertes Bildungsmanagementsystem“ zu verarbeitenden personenbezogenen Daten hinsichtlich ihres Personenbezugs und ihres Schutzbedarfs analysiert und beschrieben. Die Konzeption berücksichtigt auch spezifische Gefährdungslagen der Anwendungsdaten. Wie die Zugriffe der Anwender auf personenbezogene Daten geregelt ist, ist im Rollen-Rechte-Konzept dargestellt.

3 Geltungsbereich

Die vorliegende Konzeption gilt für die Basisanwendungen des integrierten Bildungsmanagementsystems. Sie umfasst nicht ressortspezifische Anpassungen. Die Konzeption gilt für interne und externe Lernende, für Bildungsverantwortlichen, Administratoren sowie für Tutoren, Dozenten und Unterkunftssteller. Die Rollen sind in Nr. 8 der Strukturkonzeption beschrieben. Weichen die Ressorts von den in dieser Konzeption beschriebenen Anforderungen ab, ist den datenschutzrechtlichen Anforderungen in gesonderten Datenschutzkonzeptionen zu entsprechen. Es unterscheidet zwei unterschiedliche Mandantentypen: den Ressortmandant und den Bildungsträgermandant.

4 Beschreibung des integrierten Bildungsmanagementsystems

4.1 Funktionsumfang

4.1.1 Ressortmandant

Im integrierten Bildungsmanagementsystem werden fachliche und fachübergreifende Bildungsmaßnahmen einschließlich der Lern- und Ausstattungsressourcen sowie der Dozenten, Trainer und Unterkünfte angelegt und über dieses System elektronisch gebucht. Vor der ersten Buchung geben die Nutzer in eine Registrierungsmaske personenbezogene Daten ein. Die Registrierungsmaske enthält Basisanforderungen. Die Ressorts können weitere Anforderungen aufnehmen oder in der Basisanwendung vorgesehene Anforderungen ausblenden. Die registrierten Nutzer werden von einem zuständigen Bildungsverantwortlichen (BV) zugelassen (vgl. Nutzerregistrierung). Mit der einmaligen Zulassung erhalten die Nutzer Zugang in das integrierte Bildungsmanagement und können dort Bildungsmaßnahmen buchen, hinterlegte Inhalte lesen oder in virtuellen Lerngruppen zusammenarbeiten. Mit der Zulassung wechseln die Nutzer ihren Status und werden künftig als Lernende bezeichnet. Wird die Zulassung verweigert, werden die eingegebenen Daten gelöscht (vgl. Personenstammdaten). Der Bildungsverantwortliche kann diese Entscheidung begründen. Sie geht dem Nutzer elektronisch zu.

Wie der Registrierungsprozess folgt auch die Buchung einer Bildungsmaßnahme dem Self-Service-Ansatz. Die Lernenden wählen dazu die aus einem auf die Bedarfe des Ressorts zugeschnittenen Katalog eine bestimmte Bildungsmaßnahme aus. Wird keine geeignete Bildungsmaßnahme angeboten, können sie einen entsprechenden Bedarf anmelden (vgl. Bedarfsmeldung). Sie führen die Zustimmung ihrer unmittelbaren Vorgesetzten herbei und senden den Antrag ab (vgl. Buchungs- und Genehmigungsprozess). Die Lernenden können sich freiwillig zu Fahrgemeinschaften zusammenfinden und sich bereits im Vorfeld als künftige Teilnehmer anderen Teilnehmern vorstellen und dazu in eine Teilnehmerliste eintragen lassen (vgl. Fahrgemeinschaft). Dieser Anmeldeprozess läuft elektronisch ab. Ebenso ist auch der anschließende Genehmigungsprozess elektronisch im System abgebildet. Bei Bedarf und im Einzelfall kann er auch abgeschaltet werden. Die Lernenden haben dann die Möglichkeit unmittelbar nach der Buchung die Bildungsmaßnahme aufrufen zu können.

Der zuständige Bildungsverantwortliche lässt den Lernenden zu Bildungsmaßnahmen zu (vorläufig oder endgültig, je nachdem ob ein einstufiger oder zweistufiger Workflow im Mandanten gewählt worden ist), stellt ihn zurück oder lehnt ihn ab. Der Bildungsverantwortliche kann die Entscheidung begründen. Die Entscheidung einschließlich der Begründung wird dem Lernenden per Mail zugesandt. Der Prozess der Entscheidungsfindung wird auch in der Buchungshistorie des Lernenden abgebildet und kann von ihm dort verfolgt werden (vgl. Buchungshistorie).

Der Bildungsverantwortliche bestätigt vor der Entscheidung, dass „die erforderliche Mitwirkung der Personalvertretung und der Gleichstellungsbeauftragten vorliegt“. Um diese Mitwirkung herbeizuführen, hat er die Möglichkeit eine Liste mit den Anmeldungsdaten der Lerner zu generieren, um diese eingebunden an eine E-Mail den zuständigen Personalvertretern und Gleichstellungsbeauftragten zuzusenden (vgl. Datenexport).

Mit der Zustimmung des Bildungsverantwortlichen zu einer Bildungsmaßnahme ist der Lerner zu dieser Bildungsmaßnahme gebucht (vgl. Genehmigungsprozess). Dieser Genehmigungsprozess und die dabei abgegebenen Begründungen können in der Buchungshistorie eines Lerners eingesehen werden. Sowohl der Lernende als auch der zuständige Bildungsverantwortliche können diese Daten abrufen (vgl. Buchungshistorie). Mit der Buchung werden die Daten, die der Bildungsträger zur Durchführung und Abwicklung der Bildungsmaßnahme braucht, an diesen übergeben.

Über eine persönliche Seite erhalten die Lernenden Zugang zu ihren Bildungsmaßnahmen und zu lernunterstützenden Informationen oder elektronischen Lernmedien (vgl. persönliche Seite des Lernenden). Ist die Bildungsmaßnahme abgeschlossen und wurde die Teilnahme nicht innerhalb von vier Wochen widerrufen, wird sie in der Historie der jeweils lernenden Person gespeichert (vgl. Bildungshistorie). Sowohl die lernende Person als auch die/der zuständige Bildungsverantwortliche können diese Daten abrufen (vgl. persönliche Seite des Bildungsverantwortlichen).

Da sich eine Bildungshistorie auch Bildungsmaßnahmen umfassen kann, die außerhalb des Systems gebucht sind, bietet das System die Möglichkeit, diese Bildungsmaßnahmen nacherfassen zu können. Der Prozess verläuft analog der Anmeldung und Genehmigung einer Bildungsmaßnahme. Der Lernende entscheidet selbst, welche Maßnahme er nacherfasst haben möchte. Er gibt diese über Maske ein und fügt dieser die externe Teilnahmebestätigung bei (upload). Der Bildungsverantwortliche entscheidet über die Aufnahme in die Bildungshistorie oder lehnt dies ab.

Alle im System hinterlegten Daten können statistisch ausgewertet werden. Dabei ist im System eine Sperre hinterlegt, dass die Bildungsverantwortlichen nur die Daten einsehen können, die ihrer Behörde zugeordnet sind.

Dem Bildungsträger stehen nach Abschluss der Bildungsmaßnahmen die Daten noch so lange zur Verfügung, wie er sie zur Erfüllung gesetzlicher Pflichten braucht (Belegdaten nach § 257 HGB und § 147 AO). Unter diesem Vorbehalt steht dann auch das Widerrufsrecht des Lerners gegenüber dem Bildungsträger.

4.1.2 Bildungsträgermandant

Lernende können Bildungsmaßnahmen nicht nur über ihr Ressort buchen (vgl. Ressortlerner), sondern auch bei den Bildungsträgern unmittelbar (vgl. Bildungsträgerlerner). Dazu bedürfen sie einer eigenen Registrierung mit einer neuen Nutzerkennung bei dem jeweiligen Bildungsträger. Diese Registrierung ist unabhängig von der Registrierung im Ressort. Werden Bildungsmaßnah-

men unmittelbar beim Bildungsträger gebucht, wird der elektronische Genehmigungsprozess nicht ausgelöst. Die durchgeführte Bildungsmaßnahme erscheint auch nicht in der Bildungshistorie der lernenden Person. Der Kosten der Bildungsmaßnahme werden mit der lernenden Person unmittelbar abgerechnet.

4.2 Datenstruktur

4.2.1 Stammdaten

Das integrierte Bildungsmanagementsystem unterscheidet personenbezogene Daten und systemtechnische Daten.

4.2.1.1 Personenbezogene Daten

Stammdaten sind die bei der Nutzerregistrierung erfassten personenbezogenen Daten. Die personenbezogenen Daten sind als Pflichtfelder und optionale Felder ausgestaltet (Vgl. dazu die Ausführungen unter Nr. 4.5.1). Der Nutzer gibt diese Daten selbst nach Weisung seines Ressorts ein. Über die Zulassung des Nutzers entscheidet der zuständige Bildungsverantwortliche. Der Nutzer wird von der Zulassung elektronisch unterrichtet. Nach der Zulassung pflegt er seine Daten selbst.

4.2.1.2 Systemtechnische Daten

Für die technische Verwaltung ist die Hinterlegung von Systemdaten erforderlich. Diese sind eine automatisch generierte persönliche ID-Nummer sowie die bei jeder Buchung automatisch generierte Buchungsnummer und die bei der Anlage einer Organisationseinheit entstehende Nummer (Kostenstellennummer). Des Weiteren werden alle Aktivitäten bei der Anmeldung und Buchung, beim Widerruf von Anmeldungen und der Stornierung von Seminarteilnehmern protokolliert. Dabei werden folgende Daten aufgezeichnet: Datum, Art der Aktivität, Person. Die Daten werden im Backoffice des jeweiligen Mandanten gespeichert. Sie dienen ausschließlich der systemtechnischen Verwaltung.

4.2.2 Teilnahmedaten

Teilnahmedaten bestehen aus einer Verbindung der personenbezogenen Daten mit Veranstaltungsdaten. Die erforderlichen Veranstaltungsdaten pflegt der Mandantenadministrator oder der Ressortbildungsverantwortliche im Backoffice (Antrago) ein. Er ordnet dem Seminar auch die erforderlichen Verbundinformationen zu (Tutor/ Dozenten, Unterkunft u.a). Der Mandantenadminist-

rator oder der Ressortbildungsverantwortliche gibt das Seminar für den Seminarkatalog seines oder eines anderen Mandanten frei. Er ändert in Antrago den Seminarstatus auf Freigabe zur Bearbeitung und speichert die Statusänderung ab. Das System repliziert die Seminardaten in Corporate Learning (CL), der BILDUNG21 zur Verfügung gestellten Lernplattform der Telekom und ins Webfrontend. Die Bildungsmaßnahme ist dann in den Seminarkatalogen eines Ressorts sichtbar, für die sie freigegeben und sofern sie übernommen wurde.

4.3 Systemaufbau

Das integrierte Bildungsmanagementsystem ist als Gesamtlösung entwickelt. Es verbindet das Webfrontend (CMS) über ein Lernmanagementsystem (Corporate Learning) mit einem Bildungsmanagement (Backoffice-System / Antrago).

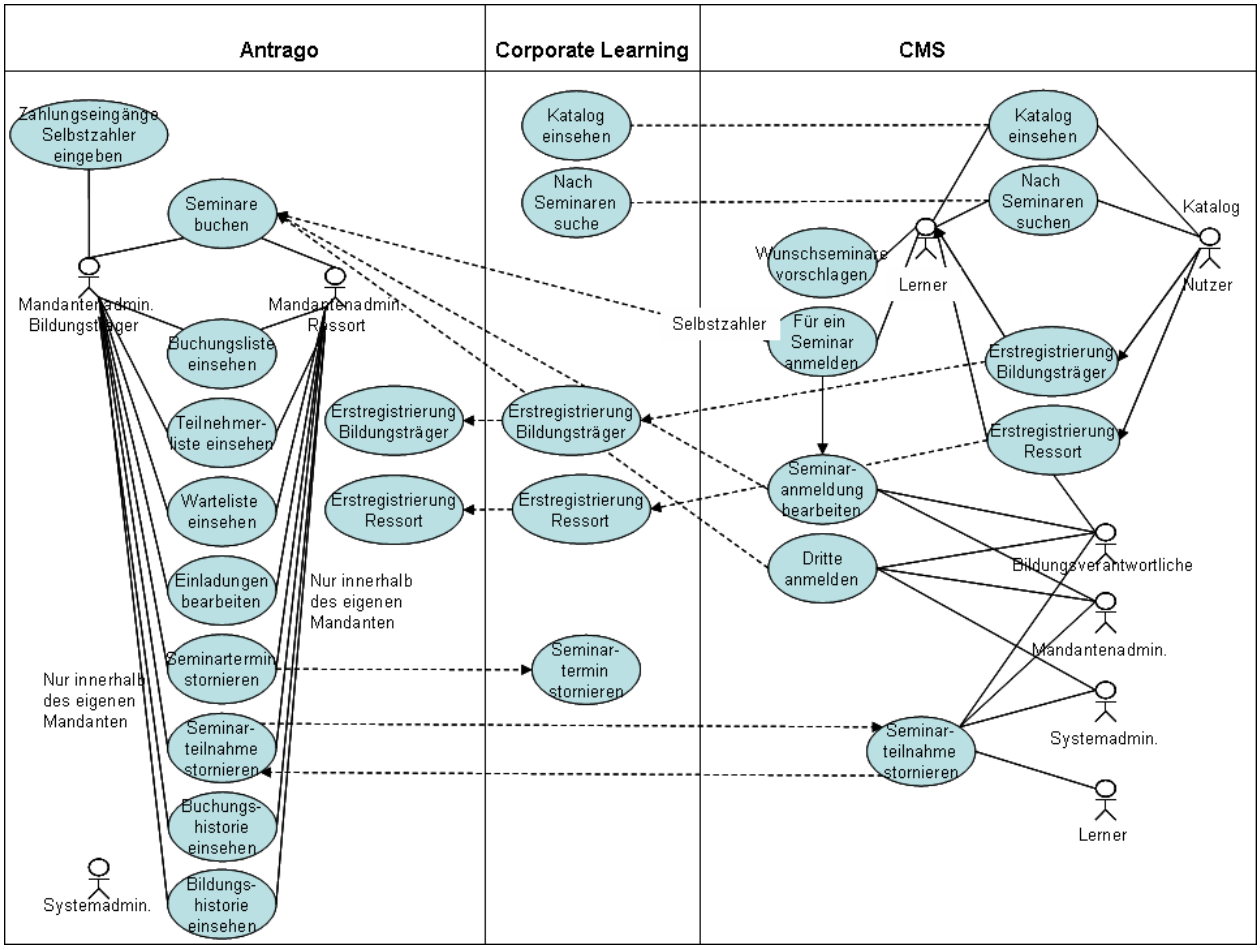

Abbildung 1 Diagramm einer Seminaran und -abmeldung

Im Webfrontend (CMS) registrieren sich die Lernenden und buchen ihre Bildungsmaßnahme. Hier werden die Bildungsmaßnahmen und die personalisierten Seiten der Lernenden und Bildungsver-

antwortlichen abgebildet und die Buchungs- und Genehmigungsprozesse ausgelöst und Statusabfragen durchgeführt. Hier können auch Inhalte eingegeben und Foren für vom übrigen System gesondert gespeicherte Nutzer angelegt werden.

Das Lernmanagementsystem (Corporate Learning = CL) ist das führende System. In ihm werden im Wesentlichen die Grundeinstellungen zur Systemnutzung (Anpassung der Registrierungsmaske an die Ressortbedürfnisse) vorgenommen, die Registrierungen der Lerner erfasst und die Ressourcen für elektronische Lernprogramme oder Lernhilfen zugeordnet.

Im Bildungsmanagement (Antrago) werden die personenbezogenen Daten der Lernenden eines Mandanten gespeichert und die Bildungsmaßnahmen einschließlich ihrer Ressourcen angelegt. Ressourcen in diesem Sinne sind auch Dozenten und Trainer mit ihren personenbezogenen Daten. Wie das Lernmanagementsystem ist auch das Bildungsmanagement mandantenfähig. Daher verfügt jeder Mandant über sein eigenes Backoffice. Nur in dessen Grenzen können die einem „Ressortmandanten“ zugeordneten personenbezogenen Daten verarbeitet werden. Die Speicherorte der Daten sind wie folgt verteilt:

Daten	**Ort der Speicherung**
Seminardaten (Metadaten)	Antrago/CL (iBMS- Kataloge werden mittels Zugriff auf die CL-DB erstellt)
Seminardaten (Lerninhalte)	CL
Personendaten	Antrago/CL (Alle Daten)
	CMS (Alle Daten ohne Tutoren, da Tutoren direkt auf CL zu greifen sollen)
Bildungs- und Buchungshistorien	Antrago/CL/CMS
Alle Daten für den Genehmigungsworkflow	Antrago/CMS
Wartelisten	Antrago/CMS
Buchungslisten	Antrago/CMS
Anmeldelisten	Antrago/CMS
Unterkunftsdaten	Antrago/CL
Veranstaltungsdaten	Antrago/CL
Ressourcendaten	Antrago/CL
Daten der Organisationseinheit (Kostenstellendaten)	Antrago/CMS
systemfremde Bildungsmaßnahmen	CMS

4.4 Zweck der Datenverarbeitung

Zweck der elektronischen Datenverarbeitung ist es, den Prozess der Bildung effizient und effektiv zu gestalten, in dem der Erfassungsaufwand auf den einzelnen Lernenden delegiert und der administrative Aufwand für personalbewirtschaftende und personalentwicklerische Maßnahmen mit Hilfe elektronischer Prozessgestaltungen auf wenige zentrale Aktionen reduziert, statistische Auswertungen ermöglicht und ein jederzeit aktuelles Bildungsprogramm angeboten werden können. Des Weiteren ist es nur über elektronische Systeme möglich elektronische Lernprogramme und lernunterstützende Inhalte anzubieten, kollaboratives Lernen zu ermöglichen und Lernkooperationen zu fördern.

Mit Hilfe des integrierten Bildungsmanagements wird die Errichtung eines virtuellen Bildungsmarktplatzes für den öffentlichen Sektor im Land angestrebt. Dieser Marktplatz besteht aus einer Inputkomponente, über die der jeweilige Anbieter einer Bildungsmaßnahme bestimmen kann (Ressortmandant oder Bildungsträger gleichermaßen), welchem Adressatenkreis (Ressort) er seine Bildungsmaßnahmen anbieten möchte und einer Outputkomponente, über die der Adressat entscheiden kann, ob er die ihm angebotenen Bildungsmaßnahmen in seinen individuellen Katalog übernehmen möchte. Um als Anbieter oder als Adressat von Bildungsmaßnamen aktiv werden zu können, müssen diese Mandanten des Systems sein. Damit der Marktplatz über ein breites Angebot verfügt wird angestrebt, wichtige Bildungsträger im Land und die Ressorts als Anbieter insbesondere fachlicher Bildungsangebote zu gewinnen.

Der Vorteil des Systems zeigt sich für die Ressorts vor allem dann, wenn sämtliche Bildungsmaßnahmen über das System gebucht werden oder im System erfasst sind. Dann können die Ressorts mit wenigen Aktionen Bildungsmaßnahmen buchen und haben einen Überblick über die Bildungshistorien ihrer Mitarbeiterinnen und Mitarbeiter. Bildungsmaßnahmen können gezielt angesetzt sowie Erkenntnisse und Erfahrungen aus besuchten Bildungsmaßnahmen besser genutzt werden. Deswegen wird auch angestrebt, bereits abgeschlossene Bildungsmaßnahmen, die von einem nicht das System nutzenden Bildungsträger bezogen oder die in der Vergangenheit durchgeführt worden sind, über eine vom Lernenden auszufüllende und vom Bildungsverantwortlichen zu genehmigenden Eingabemaske nacherfassen zu lassen .

4.5 Beschreibung der einzelnen Funktionen

4.5.1 Nutzerregistrierung

Das System unterscheidet Ressortlerner und Bildungsträgerlerner. Beide Lernertypen entsprechen getrennten Mandantentypen. Deshalb finden auch jeweils getrennte Nutzerregistrierungen und Datenspeicherungen statt.

4.5.1.1 Ressortlerner

4.5.1.1.1 Pflichtfelder für den Lernenden

Der Zugang in einen Ressortmandanten des integrierten Bildungsmanagements erfolgt über ein gesondertes Nutzerregistrierungsverfahren. Da das System sowohl über Internet als auch über Intranet zugänglich ist und vertrauliche Inhalte enthalten (bedarfsbezogene Bildungsmaßnahmen weisen immer auch auf Qualifizierungslücken hin) sowie kostenwirksame Leistungen auslösen kann, muss sichergestellt werden, dass nur berechtigte Personen Zugang haben.

Der berechtigte Personenkreis muss klar identifiziert werden können. Eine eindeutige Zuordnung zu entsprechenden im System hinterlegten Organisationseinheiten und Bildungsverantwortlichen muss möglich sein. Eine Zulassung in das System erfolgt daher nur dann, wenn sich der Nutzer nach den Anforderungen des jeweiligen Ressorts richtig registriert und der zuständige Bildungsverantwortliche einen Nutzer auch als potenziell Lernenden seines Verantwortungsbereichs zugelassen hat.

Sofern seitens eines Ressorts nichts anderes bestimmt wird, muss der jeweilige Nutzer zur erstmaligen Registrierung folgende personenbezogenen Daten in der Registrierungsmaske ein- bzw. angeben (Pflichtfelder):

- Anrede
- Vorname
- Nachname
- Dienstelle mit Postanschrift oder Postfach
- E-Mail-Adresse
- Telefonnummer / Fax
- Organisationseinheit[1]
- Amts- und Dienstbezeichnung
- Nutzerkennung
- Passwort
- Geheime Frage
- Antwort auf geheime Frage

Diese Angaben sind als Mindestangaben notwendig, um einen Nutzer ausreichend identifizieren und ein Mindestmaß an personalwirtschaftlicher und personalentwicklerischer Steuerung vornehmen zu können. Sie werden nach der Loginerstellung in Antrago und in CL des Ressortmandanten gespeichert. Des Weiteren sind die Datenschutzhinweise zur Kenntnis zu nehmen. Dazu ist eine Klickbox zu aktivieren.

[1] Mit dieser Bezeichnung wird nicht nur die Organisationseinheit erfasst, der der Lernende angehört, sondern zugleich auch die Kostenstelle.

Zur Begründung der fakultativ zu erhebenden Personalstammdaten im Einzelnen:

- Anrede, Name, Vorname sowie Amts- und Dienstbezeichnung sind notwendige Identifizierungsmerkmale einer Amtsperson. Die Anrede dient auch der geschlechtsspezifischen Erfassung der Lernenden nach § 5 Abs. 1 Nr. 2 LGIG. Die Amts- und Dienstbezeichnung ist in der hier zu beurteilenden Basisversion das Minimum, was an Pflichtdaten zur Durchführung einer effizienten Fortbildung erforderlich ist, um Zielgruppenzusammensetzungen zu steuern, verlässliche statistische Angaben für die Bedarfsplanung zu erhalten und Personen für die Durchführung der gesetzlich vorgesehenen Mitwirkungsrechte der Personalvertretungen und der Gleichstellungsbeauftragten unterscheidbar zu machen. Der Bezug auf die Amts- und Dienstbezeichnung entspricht auch der behördlichen Übung.
- Die Angabe der Beschäftigungsdienstelle und die Eingabe von Straße und Hausnummer sowie Ort bzw. Postfach, Postleitzahl und Ort dienen der Aussteuerung behördenspezifischer Informationsseiten und der Erreichbarkeit des Lernenden, insbesondere für die Zusendung von Teilnahmebestätigung und schriftlichen Lernunterlagen. Zu Bildungsmaßnahmen können auch solche Personen zugelassen werden, die infolge von Mutterschutz oder Erziehungszeiten gegenwärtig keiner Dienststelle zuzuordnen sind. Daher ist es notwendig ein offenes Eingabefeld vorzusehen.
- Die Eingabe einer E-Mail ist notwendig, um die automatisierten Informationen und Hinweise adressieren zu können. Dem Lernenden ist es freigestellt, ob er dazu eine dienstliche oder eine private E-Mail-Adresse eingibt.
- Die dienstliche Telefonnummer dient der kurzfristigen Erreichbarkeit des Lernenden.
- Die Angabe der Organisationseinheit ist notwendig, um eine Adressierung der Kosten und der genehmigenden Stelle vornehmen zu können. Die Ressorts haben die Möglichkeit über einen Organisationsakt zu bestimmten, welche Organisationseinheit bzw. genehmigende Stelle für welche Lernprogramme auszuwählen sind. Die Bildungsverantwortlichen haben die Möglichkeit die vom Lerner ausgewählte Organisationseinheit zu verändern.
- Nutzerkennung, Passwort sowie geheime Frage und die Antwort darauf dienen der Identifizierung der berechtigten Person und der Anmeldung in das System sowie der Gewährleistung einer wirksamen Anmeldung, falls das Passwort vergessen worden ist. Das Passwort muss mindestens 8 Zeichen und kann maximal 20 Zeichen enthalten. Die Übertragung und die Speicherung der personenbezogenen Daten einschließlich Nutzerkennung und Passwort im Internet werden nach SSL verschlüsselt (eine Verschlüsselung im Intranet erfolgt nicht, da das Landesverwaltungsnetz nach außen geschützt ist). Die Nut-

zerkennung kann numerisch und/oder alphabetisch erfolgen. Eine bestimmte Nutzerkennung kann im Gesamtsystem nur einmal vergeben werden. Ist die Nutzerkennung schon vergeben, generiert das System eine Fehlermeldung. Um dies zu vermeiden wird empfohlen als Nutzerkennung die Personalnummer zu verwenden, da nur diese Erkennung Einmaligkeit gewährleistet. Diese Angaben sind für Dritte nicht kenntlich. Um Doppelerfassungen bei der Eingabe zu vermeiden, wird durch das System geprüft, ob ein Datensatz mit diesen Daten bereits besteht. Wird eine Doppelerfassung festgestellt, erhält der Nutzer einen Hinweis.

Erst wenn die Pflichtfelder vollständig ausgefüllt und die Datenschutzhinweise zur Kenntnis genommen sind, wird der Nutzer darauf hingewiesen, dass seine Registrierung an den zuständigen Bildungsverantwortlichen weiter geleitet wird.

4.5.1.1.2 Optionale Felder für den Lernenden

Folgende Daten können von den Beschäftigten wahlweise zusätzlich angegeben werden, sofern die Ressorts nichts anderes bestimmen. Diese Datenfelder sind in der Basisversion besonders gekennzeichnet, so dass deutlich wird, dass diese Angaben freiwillig gemacht werden:

- Titel (akademische Anrede)
- Faxnummer
- Status
- Laufbahn
- Funktionsangaben
- Newsletter (Die Möglichkeit des Bezugs eines Newsletters von Bildungsträgern vorgesehen. Die Daten dieser Personen werden gesondert im Webfrontend gespeichert).

Sollten die Ressorts zusätzliche Erfassungsfelder als Pflichtfelder für erforderlich halten, könnten diese in einer Anlage zum Vertrag Auftragsdatenverarbeitung nach § 7 LDSchG mit angeführt werden. Die Erforderlichkeit der zusätzlichen Pflichtfelder wäre darin festzuhalten.

4.5.1.1.3 Einverständniserklärung des Lernenden

Die Registrierungsmaske enthält auch die Einverständniserklärungen für die Speicherung der Daten. Der Nutzer wird bei der Eingabe auf folgende Verwendungszwecke hingewiesen:

„Die in der Registrierungsmaske vorgesehenen personenbezogenen Daten werden durch Ihr Ressort erhoben und unter einem eigenen Mandanten auf einem gesonderten und gesicherten Rechner im Informatikzentrum des Landes (IZLBW) gespeichert. Um die von Ihnen gewünschte Bildungsmaßnahme durchführen und abrechnen zu können, werden mit der Ge-

nehmigung Ihrer Anmeldung folgende Daten an den zuständigen Bildungsträger weiter gegeben, verarbeitet und gespeichert: Anrede, Vorname, Nachname, Dienstelle mit Postanschrift oder Postfach, die angegebene E-Mail-Adresse, ihrer Telefonnummer, die Organisationseinheit, die ihre Bildungsmaßnahme genehmigt und die mit dieser abgerechnet werden sowie ihre Amts- und Dienstbezeichnung.

Die Speicherung der von Ihrem Ressort an den Bildungsträger übergebenen Daten können Sie per E-Mail, Fax, Telefon oder Brief widerrufen. Wer Bildungsträger einer bestimmten Bildungsmaßnahme ist, können Sie Ihrer persönlichen Seiten unter „Meine aktuellen Bildungsmaßnahmen" entnehmen. Der Widerruf kann allerdings erst realisiert werden, wenn gebuchte Bildungsmaßnahmen storniert oder abgeschlossen abgerechnet sind und gesetzliche Aufbewahrungsfristen (§ 257 HGB und § 147 AO nicht entgegenstehen. Ist der Widerruf vollzogen, erhalten Sie eine E-Mail vom entsprechenden Bildungsträger.

Hinweisen möchten wir Sie auch darauf, dass durch das Aufrufen der Webseite auf den im Informatikzentrum des Landes (IZLWB) stehenden Servern der Name Ihres Internetserverproviders, Ihrer aktiven Webseite und Ihre IP-Adresse zu Sicherungszwecken gespeichert werden. Diese Daten werden nicht personenbezogen verwendet. Bei E-Learning-Maßnahmen verwenden wir sog. „Session-Cookies", die auch nur für die Dauer der Durchführung der jeweiligen Maßnahme gespeichert und anschließend wieder gelöscht werden. Lerner werden den anderen teilnehmenden Personen derselben Lerngruppe angezeigt.

Ergänzend weisen wir Sie auf die allgemeinen Datenschutz- und Datensicherheitshinweise hin, die Sie am unteren rechten Ende der Webseite finden."

Die Lernenden bestätigen auf der Registrierungsmaske, dass sie die für die Teilnahme an Bildungsmaßnahmen erforderliche Kenntnisnahme der Datenschutzhinweise vollzogen haben.

4.5.1.2 Bildungsträgerlerner

4.5.1.2.1 Pflichtfelder für den Lernenden

Der Zugang in einen Bildungsträgermandanten erfolgt über ein gesondertes Nutzerregistrierungsverfahren. Da bei dieser Registrierung das Dienstleistungsverhältnis unmittelbar mit dem Lernenden zustande kommt und die Kosten auch mit diesem abgerechnet werden, ist auch dafür eine ausreichende Identifizierung erforderlich. Diese ist gewährleistet, wenn folgende Angaben gemacht werden:

- Anrede
- Vorname
- Nachname
- Postanschrift oder Postfachanschrift
- E-Mail-Adresse
- Telefonnummer
- Nutzerkennung
- Passwort
- Geheime Frage
- Antwort auf geheime Frage

Registriert sich ein Nutzer nicht bei seinem Ressort, sondern bei einem Bildungsträger, werden von den Personenstammdaten weder die Dienststelle noch die die Amts- und Dienstbe-

zeichnung erhoben, da davon auszugehen ist, dass diese Person als Privatpersonen an einer Bildungsmaßnahme teilnimmt. Die Nutzerkennung ist notwendig, da über diese der Lerner auf seine Bildungsinhalte zugreift.

4.5.1.2.2 Optionale Felder für den Lernenden

Die Lernenden haben auch hier des Weiteren die Möglichkeit optional noch ihren Titel und ihre Faxnummer anzugeben.

4.5.1.2.3 Einverständniserklärung des Lernenden

Die Registrierungsmaske enthält auch für diese Nutzer die Einverständniserklärungen für die Verarbeitung ihrer Daten. Im Bildungsträgermandanten werden sie bei der Eingabe ihrer personenbezogenen Daten auf folgende Verwendungszwecke hingewiesen:

„Für uns als Bildungsträger ist der Schutz Ihrer persönlichen Daten ein ernsthaftes Anliegen. Wir möchten Sie deshalb über die Verarbeitung Ihrer personenbezogenen Daten sowie über Ihre Möglichkeiten, diese zu widerrufen, informieren.

Sie willigen ein, dass mit der Registrierung und Anmeldung Ihr Namen, Ihre Adresse und Ihre E-Mail sowie Ihre Telefonnummer von dem Bildungsträger, bei dem Sie eine Bildungsmaßnahme gebucht haben, zur Durchführung, Abrechnung und zu Ihrer Information über weitere Bildungsangebote verarbeitet und auf einem gesonderten und gesicherten Rechner im Informatikzentrum des Landes (IZLBW) gespeichert werden dürfen.

Gegenüber jedem Bildungsträger können Sie die Speicherung Ihrer Daten per E-Mail, Fax, Telefon oder Brief widerrufen. Die Angaben des Bildungsträgers können Sie Ihrer persönlichen Seite unter "Meine aktuellen Bildungsmaßnahmen" entnehmen. Der Widerruf kann allerdings erst realisiert werden, wenn eine laufende Bildungsmaßnahme storniert, gebucht Bildungsmaßnahmen abgeschlossen und abgerechnet sind oder gesetzliche Aufbewahrungsfristen (§ 257 HGB und § 147 AO) nicht entgegenstehen. Ist der Widerruf vollzogen, erhalten Sie eine E-Mail vom Bildungsträger. Davon unabhängig können Sie jederzeit der Verwendung Ihrer personenbezogenen Daten zu Informationszwecken widerrufen. Folge eines Widerrufs ist, dass Sie bei dem entsprechenden Bildungsträger sich zunächst neu einloggen müssen, bevor Sie dort erneut eine Bildungsmaßnahme buchen können..

Hinweisen möchten wir Sie auch darauf, dass durch das Aufrufen unserer Webseite auf unserem Server der Name Ihres Internetserverproviders, Ihre aktive Webseite und Ihre IP-Adresse zu Sicherungszwecken gespeichert werden. Diese Daten werden nicht personenbezogen verwertet. Bei E-Learning-Maßnahmen verwenden wir ausschließlich sog. "Session-Cookies", die auch nur für die Dauer der jeweiligen Sitzung gespeichert und anschließend gelöscht werden.“ Lerner werden den anderen teilnehmenden Personen derselben Lerngruppe angezeigt.

Die Lernenden bestätigen auf der Registrierungsmaske, dass sie die für die Teilnahme an Bildungsmaßnahmen erforderliche Kenntnisnahme der Datenschutzhinweise vollzogen haben.

4.5.1.3 Zugangssteuerung

4.5.1.3.1 Ressortlerner

Nach der erst- und einmaligen Registrierung des Nutzers in seinem Ressort wird dieser von seinem Bildungsverantwortlichen zugelassen. Dieser erhält dazu einen elektronischen Hinweis.

Zur Zulassung einer Person ruft der Bildungsverantwortliche unter „seinen persönlichen Funktionen“ die Unterseite „Neue Nutzerregistrierung“ auf und erfährt dort „Namen“, „Dienststelle“ und „Registrierungsdatum“ der zuzulassenden Person. Unter „Namen“ können alle die Angaben aufgerufen werden, die bei der Registrierung angegeben wurden. Der Bildungsverantwortliche entscheidet über die Annahme der Registrierung und damit über die Freischaltung oder über die Ablehnung und damit über die Löschung der Daten. Bildungsverantwortliche können in jeder Behörde angesiedelt sein. Damit kann gewährleistet werden, dass der freigebenden Stelle die zuzulassenden Personen persönlich bekannt sind. Weitere die Identifizierung unterstützende Verfahren wie die Versendung eines im System generierten Zulassungslinks sind daher nicht erforderlich.

Der Login eines zugelassenen Lerners kann vom Bildungsverantwortlichen deaktiviert und wieder aktiviert werden. Die personenbezogenen Daten bleiben während dieser Zeit gespeichert.

Den Bildungsverantwortlichen bestimmt der Nutzer bei der Registrierung selbst. Ihm steht dazu ein mit dem Ressort abgestimmtes Auswahlfeld zur Verfügung. Dieses Feld ist mit „Organisationseinheit“ gekennzeichnet. Abbildung 2 zeigt den Datenfluss bei der Erstregistrierung. Nach der Freischaltung des Lernerlogins durch den Bildungsverantwortlichen sind die Daten im Ressortmandanten des entsprechenden Ressorts verfügbar.

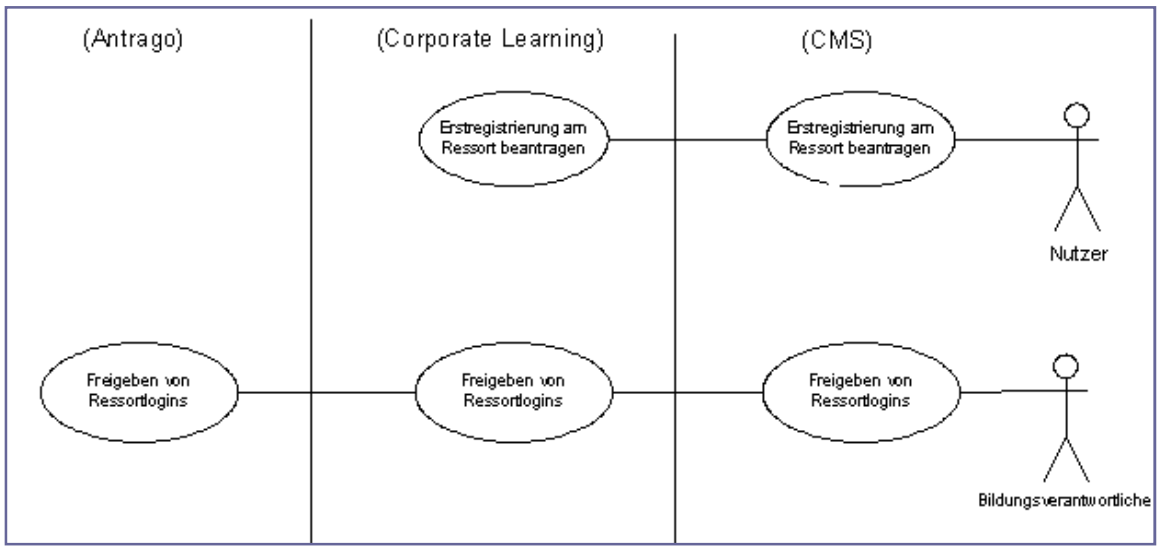

Abbildung 2 Nutzerregistrierung

4.5.1.3.2 Bildungsträgerlerner

Die erstmalige Registrierung beim Bildungsträger verläuft analog zu der beim Ressortmandanten. Die eingegebenen Daten werden nur im jeweiligen Mandanten des Bildungsträgers gespeichert.

4.5.1.4 Änderung und Administrierung der personenbezogenen Daten

4.5.1.4.1 Ressortlerner

Die Lernenden haben die Möglichkeit, nach dem Login im Webfrontend über „Meine persönlichen Funktionen im Bildungsbereich“ und „Meine persönlichen Daten“ alle ihrer persönlichen Daten einzusehen und erforderlichenfalls zu korrigieren.

Der Ressortmandantenadministrator und der Bildungsverantwortliche können im Backoffice (Antrago) alle persönlichen Daten und den Status eines Lernenden seines Ressorts bearbeiten. Beide Rollen sind insoweit weitgehend gleichberechtigt. Welche Aufgaben in welcher Rolle wahrgenommen werden, ist durch Organisationsakt des Ressorts zu bestimmen. Änderungen in den Stammdaten werden an die Bildungsträgermandanten oder zu fremden Ressortmandanten, zu denen die Daten zum Zweck der Seminarabwicklung weitergegeben wurden, übertragen. Abbildung 3 zeigt dazu den Datenfluss. Auf die Löschung der Daten wird unter Nr. 8.3 gesondert eingegangen.

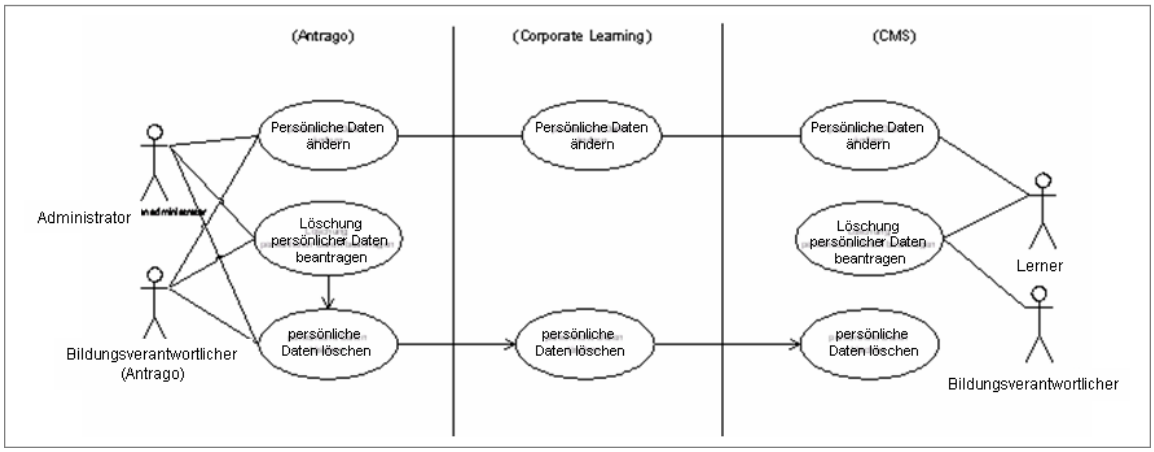

Abbildung 3 Datenänderung und Datenbearbeitung

4.5.1.4.2 Bildungsträgerlerner

Die unter Nr. 4.5.1.4.1 für Ressortlerner gemachten Ausführungen treffen auf den Bildungsträgerlerner mit der Einschränkung zu, dass die Lernenden zu dem entsprechenden Bildungsträgermandanten einen eigenen Login besitzen.

4.5.1.5 Passwortänderungsverfahren

4.5.1.5.1 Ressortlerner

Aufgrund der hohen Nutzerzahl ist eine manuelle Reaktion bei Vergessen des Passwortes durch die Betriebsstelle nicht handhabbar. Daher ist eine Funktion „Passwort vergessen“ vorgesehen. Ruft der User diese Funktion auf, wird ihm die von ihm im Zuge der Erstanmeldung angegebene, persönliche Frage gestellt. Vergisst ein Benutzer sein Passwort, kann er nach Vorlage der Frage und deren korrekter Beantwortung in einem Änderungsdialog ein neues Passwort verdeckt eingeben. Dazu kann er über eine gesonderte Funktion ein Formular „Passwort ändern“ aufrufen.

4.5.1.5.2 Bildungsträgerlerner

Das Verfahren bei Bildungsträgerlernern verläuft analog.

4.5.1.6 Verfahren bei falschem Login

4.5.1.6.1 Ressortlerner

Nach fünfmaliger falscher Eingabe von Nutzerkennung und Passwort erfolgt eine Sperrung des Zuganges. Die Betriebsstelle erhält eine Nachricht über diese Sperre, in der

- Vor- und Zunamen,
- Nutzerkennung
- Datum
- Uhrzeit
- IP-Adresse der Arbeitsstation, von der aus der Zugriff erfolgte und
- Art des Fehlers

mitgeteilt werden. Diese Nachrichten werden auf dem Server in einem Logfile gespeichert. Die Betriebsstelle entscheidet über die weiteren Maßnahmen und schaltet nach einer Prüfung der Ursache den Nutzer mit Nutzerkennung und Passwort frei.

4.5.1.6.2 Bildungsträgerlerner

Das Verfahren bei Bildungsträgerlernern verläuft analog.

4.5.2 Bedarfsmeldung

4.5.2.1.1 Ressortlerner

Die Lernenden haben die Möglichkeit über eine besondere Eingabemaske ihren nicht im allgemeinen Programm erfassten Bildungsbedarf einzugeben und damit ein entsprechendes Bildungsinteresse zu bekunden. Bei Ressortlernern erhält der Bildungsverantwortliche des Ressorts eine durch das System generierte Nachricht, dass eine neue Bedarfsmeldung eingegangen ist. Als Adressat werden die Kennung des Lernenden, Anrede, Vornamen und Nachnamen, Telefonnummer sowie E-Mail-Adresse angegeben. Die Daten werden dazu aus den Loginangaben generiert. Der Nutzer erhält sofort automatisiert eine Bestätigung seines Eingangs. Zu einer Bedarfsmeldung können folgende Daten zusammengefasst werden:

- Titel einer Bildungsmaßnahme (Pflichtfeld)
- Inhalte (Pflichtfeld)
- Lernziele (Pflichtfeld)
- Funktion
- Laufbahn
- Status
- Dienststelle
- Tätigkeitsfeld
- Wunschtermin
- Bemerkungen

Die Angaben zu Titel, Inhalte und Lernziele sind notwendig, um bedarfsbezogen eine Bildungsmaßnahme entwickeln zu können. Die Angaben zu Funktionen, Laufbahn, Status, Dienststelle und Tätigkeitsfeld sind optional.

4.5.2.1.2 Bildungsträgerlerner

Das Verfahren bei Bildungsträgerlernern verläuft analog.

4.5.3 Buchungs- und Genehmigungsprozess

4.5.3.1.1 Ressortlerner

Die Anmeldung eines Landesbediensteten zu einer Bildungsmaßnahme erfolgt durch die Mitarbeiterin bzw. den Mitarbeiter selbst. Sie wird wirksam, wenn die erforderliche Zustimmung des Vorgesetzten (Genehmigung aus fachlicher und dienstlicher Sicht; Holschuld des Lerners, deren Erfüllung zu bestätigen ist) und die Genehmigung durch die Bildungsverantwortlichen (Genehmigung aus personalentwicklerischer Sicht und aus Kostensicht) vorliegen sowie die

erforderliche Mitwirkung der Personalvertretung und die Beteiligung der Frauenvertreterinnen durchgeführt worden sind. Die Anmeldungen werden im System des Ressortmandanten erfasst. Mit der Buchung einer Bildungsmaßnahme durch einen Ressortlerner wird geprüft, ob die Daten des Lerners schon bei dem Bildungsträger vorhanden sind. Sollte das nicht der Fall oder die Daten in einem fremden Mandanten mit einem Löschflag versehen sein, werden – sofern das Ressort nichts anderes bestimmt - folgende Stammdaten eines Lerners vom Ressortmandanten an den Bildungsträgermandanten oder an den fremden Ressortmandanten (der eigene zumeist fachliche Bildungsmaßnahmen anderen Ressorts angeboten hat und die in den dortigen Katalog übernommen werden sind) weiter gegeben:

- Anrede
- Titel, sofern angegeben
- Vornamen
- Nachnamen
- Dienststelle mit Bezeichnung, Straße, Hausnummer, PLZ und Ort
- E-Mail-Adresse
- Telefon
- Fax (sofern erhoben)
- Organisationseinheit des Lernenden
- Amts- und Dienstbezeichnung (sofern bei der Registrierung erfasst)

Die Buchung wird an die anderen Systeme (Antrago/CL) weiter gegeben. Seminaranmeldungen von Ressortlernern können folgenden Anmelde- und Buchungsstatus annehmen (beim zweistufigen Workflow wird zwischen einer vorläufigen Buchung und einer (endgültigen) Buchung unterschieden):

- Angemeldet
- Zugestimmt
- Anmeldung abgelehnt
- Zurückgestellt
- Anmeldung widerrufen
- Vorläufig gebucht
- Gebucht
- Gebucht in Warteliste
- Buchung storniert

4.5.3.1.2 Bildungsträgerlerner

Bildungsträgerlerner melden sich nach ihrer Registrierung mit ihren persönlichen Daten unmittelbar bei dem Bildungsträger an, bei dem sie eine Bildungsmaßnahme buchen. Ein Genehmigungsworkflow findet hier nicht statt.

4.5.4 Anmeldung durch Dritte

Der Bildungsverantwortliche und der Ressortmandantenadministrator können ihre Ressortlerner für alle Seminare anmelden, die in den Ressortkatalog aufgenommen wurden, sich im Status „Publiziert“ befinden und der Anmeldeschluss noch nicht abgelaufen ist. Bei der Seminaranmeldung durch Dritte (durch den Bildungsverantwortlichen selbst) entfällt der Genehmigungsworklfow über den Bildungsverantwortlichen.

4.5.5 Fahrgemeinschaft

Der Lerner hat auf einer gesonderten Seite die Option PLZ, Ort und Telefonnummer einzugeben, um sein Interesse an der Bildung einer Fahrgemeinschaft zu bekunden oder seine Daten für die Teilnehmerliste freizugeben. Nach der Freigabe werden diese Daten an den die Bildungsmaßnahme durchführenden Bildungsträger übertragen. Die Daten können dort als Attribut einer gebuchten Bildungsmaßnahme aufgerufen werden.

4.5.6 Datenexport zur Abstimmung mit der Personalvertretung

Der Datenexport der Seminaranmeldungen dient der Abstimmung mit der Personalvertretung und den Gleichstellungsbeauftragten außerhalb der Systems. Dazu können der Bildungsverantwortliche und der Ressortmandantenadministrator den Export von Anmeldelisten über das Internet-/Intranet-Webfrontend durchführen. Bei dem Export werden Daten der Anmeldeliste in ein CSV-Format umgewandelt und in einer TXT-Datei auf dem Rechner des Nutzers in einem lokalen Verzeichnis abgespeichert. Der Nutzer kann diese dann drucken oder mittels einer anderen Software (Excel) weiter bearbeiten. Es werden folgende Daten übertragen:

Inhalt	**Name des Attributs im CSV-Format**
Anmeldestatus	Anmeldestatus
Vorname des Lerners	Vorname
Nachname des Lerners	Nachname
Telefonnummer	Telefon
Dienststelle	Dienststelle
Titel der Maßnahme	Titel
Preis der Maßnahme	Preis
Organisationsname	Kst.
Tag der Anmeldung	Anmeldung
Beginn der Maßnahme	Termin
Ende der Maßnahme	Schluss

Die über diese Schnittstelle übermittelten Daten an die Personalvertretungen und an die Gleichstellungsbeauftragten dienen der Wahrnehmung gesetzlicher Rechte durch die jeweils betroffene Behörde (§ 80 Abs. 1 Nr. 9 LPVG und § 10 Abs. 3 LGStG).

4.5.7 Stornierung von Bildungsmaßnahmen

4.5.7.1.1 Ressortlerner

Lerner und Bildungsverantwortlicher können via systemgenerierter E-Mail zur Service-Hotline des Anbieters einer Bildungsmaßnahme ihre eigenen Seminarbuchungen stornieren oder Seminaranmeldungen ihres Verantwortungsbereichs widerrufen. Ressortmandantenadministratoren können Seminarbuchungen auch direkt in ihrem Antrago-Client durchführen.

Die Stornierungsaufforderungen werden vom Internet-/Intranet- Webfrontend via E-Mail an die „Service Hotline"- E-Mailadresse des Mandanten, der Anbieter des zu stornierenden Seminars ist, versendet. Der Mandantenadministrator des seminaranbietenden Mandanten muss dann von Hand die Stornierung aus der „Service Hotline"- E-Mail in den Antrago-Client übertragen.

Der Anmelde- und Buchungsstatus (CL/CMS) der Seminarbuchung verbleibt bis zur Ausführung der Stornierung (durch eine Service-Person mit Mandantenadministrationsrechten in Antrago) im aktuellen Status. Nach der Statusänderung in Antrago, kann der Lerner beim nächsten Aufruf die Durchführung der Stornierung in seiner persönlichen Seite einsehen. Bei Lernenden in der Warteliste führt der Widerruf der Anmeldungen unmittelbar zur Löschung der Buchungsdaten.

4.5.7.1.2 Bildungsträgerlerner

Das Verfahren bei Bildungsträgerlernern verläuft analog.

4.5.8 Persönliche Seite des Lernenden

4.5.8.1.1 Ressortlerner

Jeder Lernende hat eine Seite mit seinen persönlichen Funktionen im Bildungsbereich. Mit Hilfe dieser Seite kann er mit Nutzerkennung und Passwort folgende Informationen aufrufen:

- Meine persönlichen Daten mit allen bei der Registrierung erfassten Daten und der Möglichkeit diese zu verändern
- Meine aktuellen Bildungsmaßnahmen mit einer Übersicht der gebuchten Bildungsmaßnahmen
- Meine Bildungshistorie mit einer Übersicht der durchgeführten Bildungsmaßnahmen

- Meine Stornierungen mit einer Übersicht der stornierten Bildungsmaßnahmen
- Neue Bildungsmaßnahmen vorschlagen mit einer Maske, um neue Bildungsmaßnahmen vorschlagen zu können.

4.5.8.1.2 Bildungsträgerlerner

Das Verfahren bei Bildungsträgerlernern verläuft analog.

4.5.9 Buchungshistorie

Bei der Genehmigung einer vorläufigen oder endgültigen Buchung einer Bildungsmaßnahme werden neben den Personendaten der Lernenden (vgl. Registrierung), dem Termin der gebuchten Bildungsmaßnahme, dem Titel, dem Anbieter und dem Status auch – sofern beigefügt – eine den Status verändernde Begründung der entscheidenden Stellen erfasst. Dazu wird der Text, der nach der Abspeicherung des Seminaranmeldungen und dem Wechsel des Buchungsstatus in einer E-Mail an den Lerner ergeht, in die Ansicht der Bildungshistorie übernommen.

Diese Inhalte können sowohl der jeweilige Lernende als auch der zuständige Bildungsverantwortliche einsehen. Die Buchungshistorie wird in Antrago gespeichert. Sie kann solange eingesehen werden, solange die dazugehörende Bildungsmaßnahme in Antrago gespeichert ist. Die Buchungshistorie steht nur Ressortlernern zur Verfügung.

4.5.10 Bildungshistorie

In der Bildungshistorie eines Lerners werden die Bildungsmaßnahmen erfasst, an denen er tatsächlich teilgenommen oder gebucht war und nicht teilgenommen hat. Dazu versetzen die Bildungsträger die Personen, die nachweislich nicht an Bildungsmaßnahmen teilgenommen haben, in den Status „nicht teilgenommen“. Ist das nicht der Fall wir der Lernende automatisch nach vier Wochen als teilgenommen erfasst. Der vierwöchige Zeitraum ist angemessen, um seitens des Bildungsträgers die gebuchten mit den teilgenommenen Lernern abgleichen zu können. Der Automatismus ist wegen großer Nutzergruppen, wie sie insbesondere bei reinen E-Learning Maßnahmen auftreten können, erforderlich. In der Bildungshistorie werden neben den Personenstammdaten auch folgende Teilnahmedaten erfasst: Termin, Titel, Produktnummer, Inhalte, Lernziele, Anbieter, Status der Bildungsmaßnahme. Die Bildungshistorie können nur der jeweilige Lerner und der zuständige Bildungsverantwortliche einsehen.

Die Bildungshistorie wird in Antrago gespeichert. Bei der Löschung einer Bildungsmaßnahme werden folgende Seminarinformationen in einer separaten Tabelle gesichert: Titel, Produktnum-

mer, Inhalte, Lernziele und Termine. Die Bildungshistorie steht nur beim Ressortlerner nicht beim Bildungsträgerlerner zur Verfügung.

4.5.11 Persönliche Seite des Bildungsverantwortlichen

4.5.11.1.1 Funktionsüberblick

Jeder Bildungsverantwortliche hat eine Seite mit seinen persönlichen Funktionen im Bildungsbereich. Mit Hilfe dieser Seite können mit der Nutzerkennung und dem Passwort folgende Funktionen und Informationen aufgerufen werden:

- Funktion: Neue Nutzerregistrierung mit folgenden Daten: Name der angemeldeten Person, Dienststelle, Datum der Registrierung.
- Funktion: Mitarbeiter des Ressorts mit folgenden Daten: Name des Lerners, Amts- und Dienstbezeichnung, Dienststelle, Organisationseinheit und über ein Bearbeitungsfeld („wählen“) Termin und Titel der Bildungsmaßnahme, Anbieter und Status der Genehmigung, die Registrierungsdaten des Lernenden, die Bildungshistorie des Lernenden, evtl. Stornierungen und Ablehnungen sowie über den „Status“ die Buchungshistorie des Lernenden.
- Funktion: Anmeldung zu Bildungsmaßnahmen mit folgenden Daten: Name des Lernenden, Datum, Titel der Bildungsmaßnahme, Buchungsschluss.
- Funktion: Teilnehmer Buchen mit folgenden Daten: Name, Amts- und Dienstbezeichnung, Dienststelle und Organisationseinheit.
- Funktion: Teilnehmer stornieren mit folgenden Daten: Name, Amts- und Dienstbezeichnung, Dienststelle und Organisationseinheit.
- Funktion: Dienststellen und Gruppenverwaltung (hier können die im System hinterlegten einzelnen Dienststellen nur vom System- oder Mandantenadministrator zu Gruppen wie beispielsweise Abteilung oder Behörden zusammengeführt werden; personenbezogene Daten werden damit nicht erfasst oder bearbeitet).
- Funktion. Katalogkonstante (hier können vom System- oder Mandantenadministrator Texte hinterlegt werden, die dann im Bildungskatalog erscheinen, wenn einem Navigationspunkt keine Bildungsmaßnahmen mehr zugeordnet erscheinen, weil die Seminare begonnen haben; personenbezogene Daten werden hier nicht erfasst oder bearbeitet).
- Funktion: Katalogverwaltung (hier können vom Mandantenadministrator eine mandantenspezifische und anbieterunabhängige Navigation aufgebaut und Bildungsmaßnahmen auch mehrfach zugeordnet werden; personenbezogene Daten werden hier nicht erfasst oder bearbeitet).

- Funktion: CL-Verwaltung (hier erhalten die von den zuständigen Mandanten-/Ressortbildungsverantwortlichen und Administratoren bestimmte Tutoren einen direkten Zugang auf die Lernplattform).
- Funktion: Web-Statistik mit folgenden Daten, die im Mandanten gespeichert sind: Seminardaten, Verantwortliche am Buchungsprozess, Buchungsdaten und Lernerdaten.
- Funktion: E-Mail-Vorlagen (hier können die Mandantenadministratoren systemseitig ausgelöste Mails inhaltlich anpassen und allgemein adressieren; personenbezogene Daten werden hier nicht erfasst oder bearbeitet).

Für den Fall, dass mehrere Bildungsverantwortliche einem Ressortmandanten zugeordnet sind, gibt es keine Wertigkeit unter diesen. Alle Bildungsverantwortliche haben bezogen auf ihre Organisationseinheit die gleichen Rechte. Differenzierungen sind durch Organisationsakte des Ressorts zu regeln.

4.5.11.1.2 Allgemeine Funktionen

Die Funktionen Nutzerregistrierung, Mitarbeiter des Ressorts, Anmeldung zu Bildungsmaßnahmen, Buchung und Stornierung von Teilnehmern sind allgemeine Anforderungen zur Ermöglichung einer ordnungsmäßigen Genehmigung und Buchung von Bildungsmaßnahmen.

4.5.11.1.3 Statistische Auswertungen

Die Statistik im Funktionskreise der Bildungsverantwortlichen dient der Auswertung sämtlicher Daten, die im Mandanten gespeichert sind. Dabei können sowohl personenbezogene als auch seminarbezogene Auswertungen durchgeführt werden. Diese Auswertungen sind grundsätzlich nur dienststellenbezogen möglich. Ein Bildungsverantwortlicher oder Ressortbildungsverantwortlicher kann daher nur die Daten des Lernenden aufrufen, für die er zuständig ist. Einzige Ausnahmen bilden der Mandantenadministrator und der Systemadministrator. Diesen sind Kraft ihrer Funktionen alle Daten zugänglich.

Diese Daten können in ein CSV-Format umgewandelt und in einer TXT-Datei auf dem Rechner des Nutzers in einem lokalen Verzeichnis abgespeichert werden und der Nutzer kann diese dann drucken oder mittels einer anderen Software (Excel) weiter bearbeiten. Zu Herbeiführung personalentwicklerischen und personalwirtschaftlichen Entscheidungen sind neben Seminardaten auch folgende personenbezogene Daten erforderlich und in das CSV-Format übertragbar:

Seminarbezeichnung, Organisation, Verantwortlicher Rolle, Annmeldedatum, Buchungsstatus, Anrede, Titel, Vorname, Nachname, Email, Strasse, PLZ Strasse, Postfach, PLZ Postfach, Ort, Ergänzende Angaben, Telefonnummer und Faxnummer.

4.5.12 Datenverarbeitung besonderer Personengruppen

4.5.12.1 Bildungsverantwortliche

Bildungsverantwortliche der Ressorts sind die für die Personalentwicklung zuständigen Stellen, sowie die Sachbearbeiter für Aus- und Fortbildung mit einer eigenen Zugangsberechtigung. Im Rahmen des Registrierungsverfahrens und des Genehmigungsverfahrens haben Bildungsverantwortliche Rechte, um Lerner zulassen und bei ihren Buchungen Statusveränderungen vornehmen zu können. Sie können Bildungsmaßnahmen anlegen und entsprechende Ressourcen zuordnen. Unterschieden werden Bildungsverantwortliche, die ausschließlich im Web arbeiten (BV-Web) und solche, die auch im Backoffice-System arbeiten können (BV-Antrago). Die jeweiligen Berechtigungen sind in der Rollen-Rechte-Konzeption dargestellt. Die Unterscheidung beruht auf lizenzrechtlichen und bedienungspraktischen Gesichtspunkten. Die Bildungsverantwortlichen werden vom Systemadministrator über den Antrago-Client angelegt und administriert und einer Organisation (Kostenstelle) zugeordnet. Ihre Personendaten sowie Login und Passwort werden an CL/CMS übertragen (vgl. Abbildung 4).

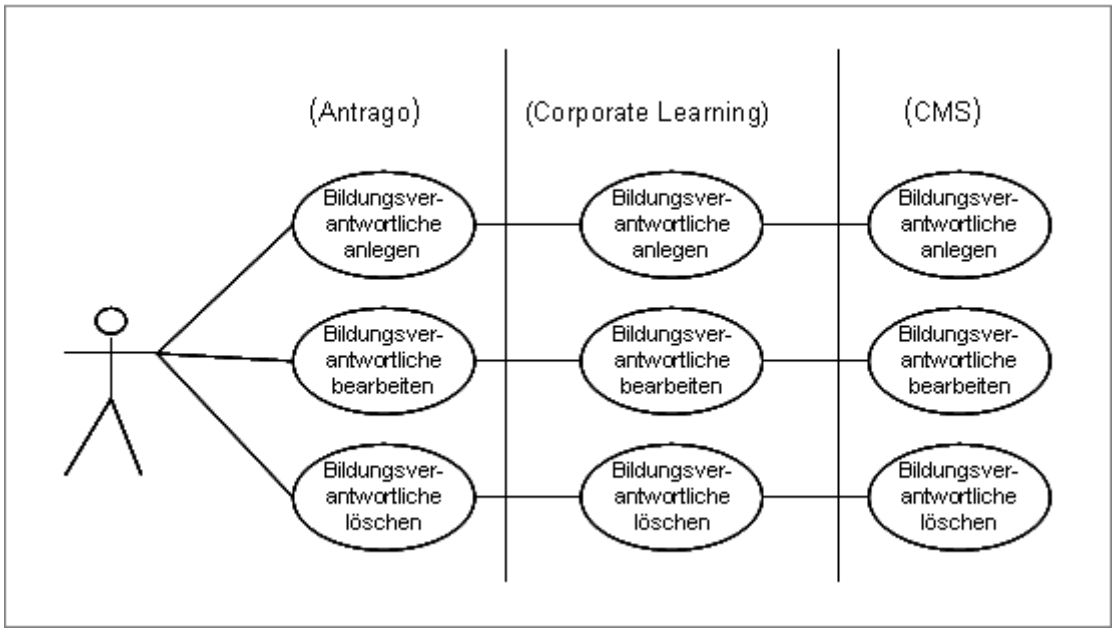

Abbildung 4 Administrierung von Bildungsverantwortlichen

Der Systemadministrator legt einen Bildungsverantwortlichen mit folgenden Daten an:

- Anrede
- Titel
- Vorname
- Name
- E-Mail-Adresse
- Telefon
- Dienststellenadresse
- Login
- Passwort
- zugeordnete Organisation (Kostenstelle)

Die Logindaten werden dem Bildungsverantwortlichen per Telefon oder Brief zugestellt. Der Systemadministrator löscht einen Bildungsverantwortlichen. Danach sind die Daten in allen Systemen nicht mehr verfügbar.

4.5.12.2 Dozenten und Tutoren

Dozenten und Tutoren können von dem Bildungsträgermandantenadministrator, dem Ressortmandantenadministrator und dem Bildungsverantwortlichen in Antrago administriert werden. Die Dozenten- und Tutorendaten sind nur innerhalb des Mandanten zu sehen, in dem die Daten eingepflegt wurden. Die Daten werden von Antrago in den eigenen CL-Mandaten repliziert (Abbildung 5).

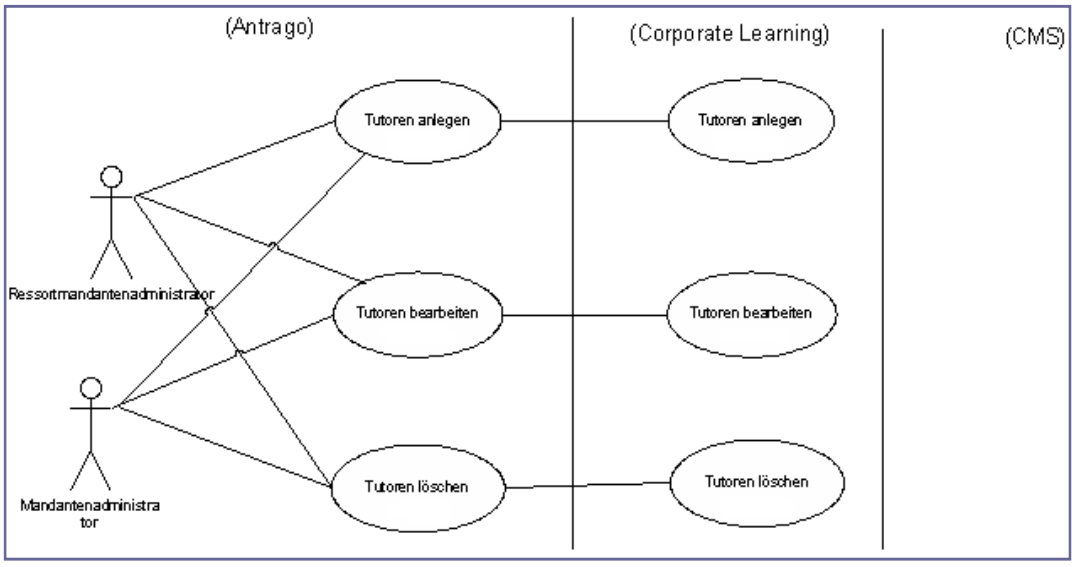

Abbildung 5 Administration von Dozenten und Tutoren

Von Dozenten und Tutoren werden folgende Daten erhoben, sofern sie vorliegen:

- Anrede, Titel
- Vor- und Nachname
- Firma
- Adresse
- Anschrift
- Telefon und Fax
- Mail- und Webadresse
- Lichtbild
- Berufserfahrungen, Referenzen, Veröffentlichungen
- Honorar
- Bankverbindung

Nach dem Löschen der Dozenten- und Tutordaten in Antrago werden die Daten auch aus CL gelöscht, sofern der Dozent oder Tutor für kein aktuelles oder zukünftiges Seminar gebucht ist und die Kosten abgerechnet sind. Nach der Löschung in Antrago sind die Daten innerhalb des gleichen Mandanten auch in CL nicht mehr verfügbar.

4.5.12.3 Inhaber von Unterkünften und Veranstaltungsorten

Unterkünfte und Veranstaltungsorte können sowohl im Ressort- als auch im Bildungsträgermandanten angelegt und Bildungsprodukten als Ressource zugeordnet werden. Folgende Daten werden erhoben:

- Anrede
- Vor- und Nachname
- Firma
- Adresse
- Anschrift
- Preis
- Telefon und Fax
- Mail- und Webadresse
- Namen und Funktion des Ansprechpartners.

Die Daten werden in Antrago gespeichert und in den eigenen CL- Mandaten repliziert. Die Datenlöschung erfolgt analog der von Dozenten und Tutoren.

4.6 Administration

Die Administrationsaufgaben teilen sich in folgende Funktionen auf:

- Administration der Betriebsplattform und Server
- Administration der Leitungswege (Landesverwaltungsnetz)
- Administration der Anwendung allgemein
- Ressortspezifische Administration der Anwendung.

Die Administration der Betriebsplattform und der Server wird durch Beschäftigte des IZLBW wahrgenommen. Diese werden von der Fa. T-Systems unterstützt. Die näheren Einzelheiten werden in entsprechenden Vereinbarungen nach § 7 LDSG BW sowie Wartungsverträgen geregelt. Die Administration der Leitungswege obliegt dem IZLBW. Hierzu wird auf die für den Betrieb des Landesverwaltungsnetzes erstellten Konzeptionen und Anweisungen verwiesen.

Die Administration der Anwendung „BILDUNG21" obliegt der Betriebsstelle der Führungsakademie in Zusammenarbeit mit T-Systems. Die weitere Ausgestaltung ist in der „Konzeption der Betriebsstelle BILDUNG21" näher dargestellt. Näheres hierzu wird in einer Vereinbarung über die Datenverarbeitung im Auftrag nach § 7 LDSG geregelt.

Die vorgesehenen Administrationsrechte ermöglichen z.B. Lesen, Speichern und Verändern bzw. Löschen von Inhalten, die Bearbeitung von Anwender-Stammdaten und –Konten sowie die Vergabe von Rechten. Da das integrierte Bildungsmanagement allen Ressorts zur Verfügung steht, sind erforderlichenfalls auch ressortinterne Administrationsaufgaben durchzuführen. Hierfür wird ein „Ressortadministrator" vorgesehen, der über die Administrationsrechte für alle Beschäftigten seines Geschäftsbereiches verfügt.

5 Technisches Konzept

5.1 Netzstruktur

Für das integrierte Bildungsmanagement wird die vorhandene DV-Infrastruktur der Landesverwaltung Baden-Württemberg genutzt, die als Client-Server-Architektur auf LAN-Basis aufgebaut ist. Die Arbeitsplatzrechner, von denen auf das integrierte Bildungsmanagement zugegriffen wird, sind Bestandteil des Landesverwaltungsnetzes (LVN).

Auf der Grundlage eines Application Managementvertrages wird das integrierte Bildungsmanagementsystem von T-Systems gewartet. Dazu unterhält T-Systems eine gesicherte Verbindung über das Internet mit definiertem Anschluss an das BMS-Subnetz des IZLBW einen für Zwecke der Anwendungsentwicklung erforderlichen Administrationszugang zum Anwendungsserver. Der Zugang zu den BMS-Servern erfolgt über den RAS-Zugang (Remote Access System) des IZLBW (Zugriff über das zentrale Firewall-System des IZLBW, Verschlüsselung mit DES3-Algorithmus, Authentifizierung der Benutzer über Sicherheits-Token-Karten und einen Authentifizierungs-Server, Produkt: ActivCard One der Fa. ActivCard und einen Authentifizierungs-Server nach RSA - Rivest-Shamir-Adleman-, Produkt:ActivPack der Fa. ActivCard).

Die Einwahl erfolgt über das Internet ins IZLBW. Das Internet-Firewall-System des IZLBW fragt nach Benutzerkennung und Passwort. Nachdem der Remote-Benutzer sich auf dem Einwahl-Router bzw. sich auf dem Firewall-System authentifiziert hat, wird die Benutzerkennung an den Authentifizierungs-Server des IZLBW weitergeleitet. Der Authentifizierungs-Server veranlasst den Remote-Benutzer zu einer weiteren Authentifizierung. Diese erfolgt über die Sicherheits-Token-Karte. Das ermittelte Passwort muss dann der Anwender für den RAS-Zugriff am Remote-PC eingeben.

Nach der Authentifizierung kann der Remote-PC die Verbindung über die Firewall-Systeme des IZLBW zu der BK-Umgebung der Dienststelle aufbauen. Die Firewall-Systeme lassen über Filterregeln nur die beantragten und erlaubten Verbindungen und Protokolle zu. Der Datenverkehr zwischen dem Remote-PC und den Firewall-Systemen des IZLBW wird verschlüsselt (3DES-Verfahren).

Das IZLBW hat für die RAS-Zugänge ein Sicherheitskonzept erstellt (Sicherheitsmaßnahmen für RAS-Verbindungen über die Firewall-Systeme des IZLBW, Stand 01.02.2006). Das IZLBW stellt sicher, dass die darin enthaltenen Maßnahmen für den Verbindungsaufbau zwischen der Firma T-Systems und dem IZLBW tatsächlich auch angewandt werden. Dazu tragen im Wesentlichen folgende Maßnahmen bei:

- Das IZLBW lässt die zu den Firewall-Systemen gehörenden Komponenten (dazu gehören auch die RAS-Anschlüsse) regelmäßig von unabhängigen Spezialfirmen auf Sicherheitsbelange überprüfen und behebt die dabei gefundenen Mängel unverzüglich.
- Der Verbindungsaufbau ist nur mit einer Authentifizierungskarte (alternativ mit Tokenkarte) und einer speziellen Remote-Verschlüsselungs-Software möglich, die vom IZLBW zur Verfügung gestellt werden. Die Software muss auf dem Remote-PC der Fa. T-Systems installiert werden.
- Ein Konzept über die Sicherheitsmaßnahmen für RAS-Verbindungen über die Firewall-Systeme des IZLBW.

Das Konzept des IZLBW kennt nur die eine oben beschriebene Option (Authentifizierungskarte, Remote-Verschlüsselungs-Software). Das IZLBW wird vertraglich verpflichtet, die zugesagten Sicherheitsstandards einzuhalten und die Führungsakademie von den entsprechenden Prüfergebnissen zu unterrichten. Die Führungsakademie verpflichtet die Firma T-Systems zu folgenden Maßnahmen:

- Der Remote-PCs darf nicht an andere Netze angeschlossen werden.
- Vom Remote-PC darf während einer Verbindung ins LVN nicht gleichzeitig eine weitere Verbindung ins Internet aufgebaut werden.
- Remote-PCs sind in abschließbaren, für Unbefugte unzugänglichen Räumen zu benutzen.
- Die Firma T-Systems hat Virenschutzprogramme zu installieren und die Virensignaturen regelmäßig zu aktualisieren.

Die Server sind im LAN des IZLBW installiert und an das zentrale Firewall-System angeschlossen (vgl. Abbildung 6).

Zur Fernüberwachung und –administration durch T-Systems wird eine Internet-Verbindung benutzt. Die Verbindung verläuft wie folgt:

- PC von T-Systems – VPN-Tunnel durch Internet – Firewall-System des IZLBW – BMS-Server
- Die Verbindung wird verschlüsselt (IPSEC). Die Verschlüsselung erfolgt von dem zentralen Firewall-System des IZLBW bis zum Überwachungs- und Administrations-PC der Fa. T-Systems. Auf dem PC der Fa. T-Systems wird zu diesem Zweck die erforderliche Verschlüsselungs-Software installiert. Diese wird vom IZLBW zur Verfügung gestellt.
- Der Überwachungs- und Administrations-PC hat keine weiteren Netz-Verbindungen (Stand-Alone-PC) außer der zu den BMS-Servern im IZLBW. Das bedeutet insbesondere, dass der PC nicht mit dem internen Netz der Fa. T-Systems und mit dem Internet verbunden ist.

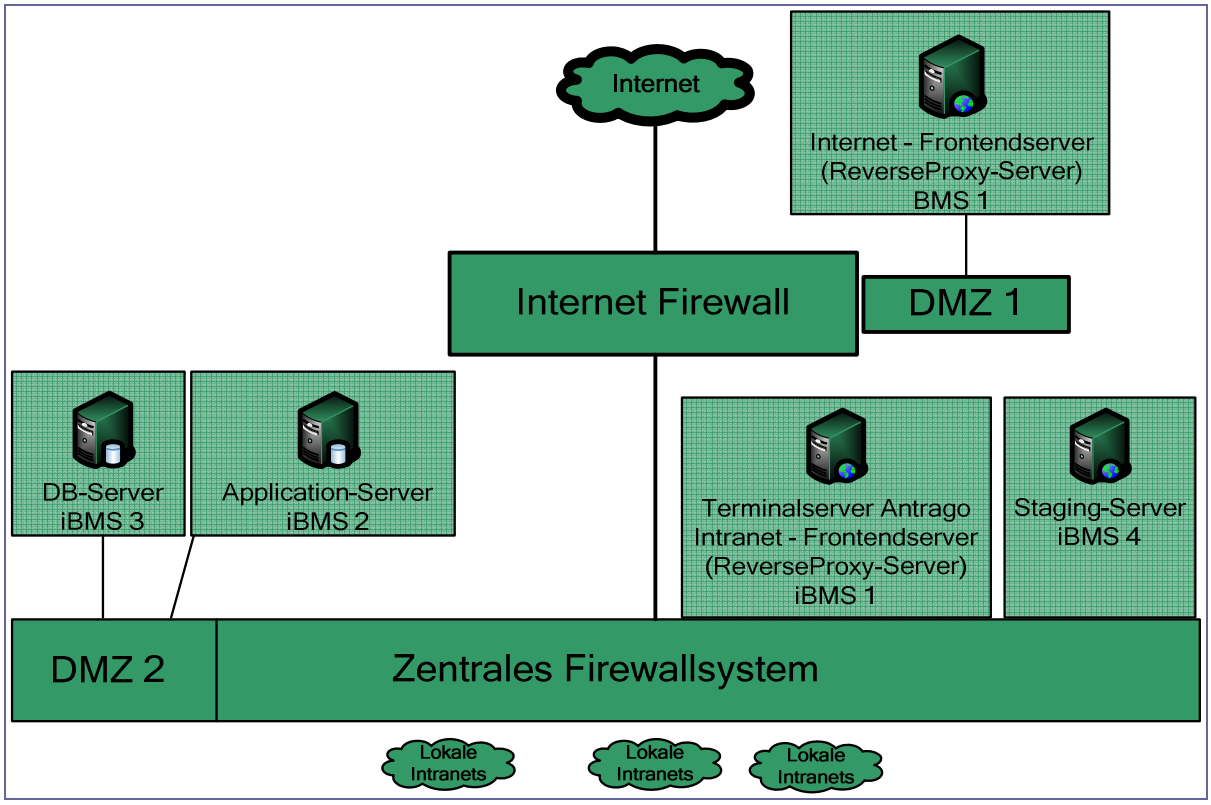

Abbildung 6 Systemübersicht

5.2 Hardware

5.2.1 Arbeitsplatz

Die Bediensteten nutzen die Arbeitsplatzrechner gemäß dem vorhandenen Ausstattungssoll.

5.2.2 IZLBW

Die Server für BILDUNG21 sind im IZLBW installiert. Sie stehen für Zugriffe aus allen Intranets der Landesverwaltung und aus dem Internet zur Verfügung. Die dazu notwendigen Verbindungen sind gemäß dem Networkung-Konzept der Landesverwaltung gesichert.

Die Networking-Konzeption schreibt vor, Intranet-Verbindungen über sogenannte standardisierte Firewalls zu realisieren. Erlaubt sind dabei nur die Dienste SMTP. LDAP, DNS und HTTPS. Sollen intranetübergreifend weitere Dienste genutzt werden können, ist dafür eine Risikoanalyse durchzuführen und ein Sicherheitskonzept zu erstellen. Da für Zugriffe auf den BMS-Server HTTP verwendet wird, sind die unter Nr. 9.1.5 dargestellten Sicherheitsmaßnahmen erforderlich.

5.2.3 Integriertes Bildungsmanagementsystem

In der nachfolgenden Übersicht sind die Hardware- und Softwarekomponenten des integrierten Bildungsmanagementsystems zum Stand Juni 2007 aufgelistet.

1. BMS1 – Internet-Frontendserver (ReverseProxy-Server) PY RX100S4a/PD 925 (3,0 GHz) 4GB DDR2-533 PC2-4200 ub ECC CD-RW \ DVD ATAPI slimline Option hot-plug Festplatten RX100S4 2 x HD SATA 3Gb/s 160GB 7.2k hot plug 3.5" PCIe+PCI-X riser für RX100 S4 TP 4J VO Svc,NBD Rz,5x9 MS-Windows Server 2003 Apache HTTP Server (Reverseproxy-Server-SW für Internet)
2. iBMS1- Intranet-Frontendserver (ReverseProxy-Server) HP DL380 R05 Xeon E5440 Quad Core 2.83GHz/1333MHz -2x6MB 10 2GB RAM (2x 1GB + 2x 4GB) Smart Array P400/256MB Controller 2x 146GB 3Gb/s SAS 10k rpm SFF Single Port Hot Plug ENT HDD (2,5") 8x/24x Slimline DVD-ROM Drive Option Kit Hot Plug Redundant Power Supply MS-Windows Server 2003 MS-Terminalserver mit 40 Lizenzen Antrago (R&R-Soft; Backoffice-SW) MS-Office 2003 Professional Apache HTTP Server (ReverseProxy-Server-SW für Intranet)
3. iBMS2 - Application-Server HP DL380 R05 X5260 Dual Core 3.33GHz/1333MHz -6MB 10 2GB RAM (2x 1GB + 2x 4GB) Smart Array P400/256MB Controller 2x 146GB 3Gb/s SAS 10k rpm SFF Single Port Hot Plug ENT HDD (2,5") 8x/24x Slimline DVD-ROM Drive Option Kit Hot Plug Redundant Power Supply MS-Windows Server 2003 iBMS (Lösung der MMS ins ASP und ASP.NET) ContentXXL (Portamundi; CMS) ProductivityNet (Communardo; Wissensmanagementsystem) MS SQL Server 2000 (nur als Backup zur Productiv-DB auf iBMS 3)
4. iBMS3 – Datenbank-Server HP DL380 R05 Xeon E5440 Quad Core 2.83GHz/1333MHz -2x6MB

10 2GB RAM (2x 1GB + 2x 4GB) Smart Array P400/256MB Controller 2x 146GB 3Gb/s SAS 10k rpm SFF Single Port Hot Plug ENT HDD (2,5") 8x/24x Slimline DVD-ROM Drive Option Kit Hot Plug Redundant Power Supply MS-Windows Server 2003 MS SQL Server 2000 (Datenbanken aus iBMS, ContentXXL, ProductivityNet und Antrago) Applikationen iBMS, ContentXXL und ProductivityNet nur als Backup zu iBMS 2
5. iBMS4 – Staging Server HP DL380 R05 Xeon E5440 Quad Core 2.83GHz/1333MHz -2x6MB 10 2GB RAM (2x 1GB + 2x 4GB) Smart Array P400/256MB Controller 2x 146GB 3Gb/s SAS 10k rpm SFF Single Port Hot Plug ENT HDD (2,5") 8x/24x Slimline DVD-ROM Drive Option Kit Hot Plug Redundant Power Supply MS-Windows Server 2003 MS-Virtual Server Standard 2005 R2 (Abbildung des LIVE-Systems als virtuelle Server)

5.2.4 Betriebsstelle BILDUNG21

Die Hardwareausstattung des Betriebsstelle „BILDUNG21“ erfolgt nach dem Betriebsstellenkonzept (Anlage 4).

5.3 Software

5.3.1 Arbeitsplatz

Die Arbeitsplatzrechner werden unter der vom jeweiligen Ressort festgelegten PC-Konfiguration betrieben. Für den Zugriff auf „BILDUNG21“ steht ein Webbrowser (Microsoft Internet Explorer 5.x, Netscape Navigator 4.7x) zur Verfügung. In den Browser-Einstellungen sind „Java“ (nur für Admins), „Java-Script“ und „Cookies“ (Session-Cookies) aktiviert.

Diese Session-Cookies werden zu Authentifizierung und damit zur Autorisierung der Nutzer und zur Steuerung von Zugriffsrechten verwendet. So wird dadurch z.B. sichergestellt, dass administrative Seiten nicht ohne vorherigen Login, der diese Cookies setzt, angezeigt werden können.

Die Lernplattform CL verwendet Session Cookies. Dies ist eine technische Gegebenheit dieser Plattform. Die verwendeten Cookies sind ausschließlich temporäre Cookies, die nach Schließen des Browsers gelöscht werden, d.h. es werden keine weiteren Daten auf den Clients gehalten.

Zur ggf. lokalen Verarbeitung von Daten wird die verfügbare dienstliche Software genutzt (z.B. MS-Office-Paket). Zur Anzeige bestimmter Inhalte von „BILDUNG21“ ist die temporäre oder dauerhafte Installation von Plug-Ins (z.B. Acrobat Reader, Macromedia Flash, Macromedia Shockwave, WinZip o.ä.) vorgesehen.

5.3.2 Server

Die BMS-Server werden unter dem Betriebssystem Windows Server 2003 betrieben. Führendes System im integrierten Bildungsmanagement von „BILDUNG21” ist die Lernplattform „Corporate Learning (CL)“ in der jeweils aktuellen Version.

- Betriebssystem MS Windows Server 2003 Server SP 1
- Datenbank MS SQL 2000
- Webserver MS IIS 5.0
- Corporate Learning 3.0

5.3.3 Betriebsstelle BILDUNG21

Die Betriebsstelle setzt HTML-basierte Administrationstools in der jeweils aktuellen Version ein. Damit lassen sich alle administrativen Vorgänge gemäß Nr. 4.6 durchführen. Für den Datenaustausch mit den BMS-Servern werden http und ftp Protokolle verwendet und eine Remotedesktopverbindung genutzt.

5.4 Datensicherung

Die Datensicherung ist vereinbarungsgemäß Aufgabe des IZLBW. Sie wird entsprechend den technischen Möglichkeiten automatisiert gesteuert und überwacht. Das IZLBW übernimmt die Montage und sichert die Lagerung der Datenträger in einem feuerfesten Tresor zu.

Der gesamte Datenbestand des BMS-Servers wird zur Sicherung einmal täglich inkrementell (i.d.R. zwischen 01:00 Uhr und 05:00 Uhr) sowie einmal wöchentlich als Vollsicherung auf Magnetbandkassetten gesichert und 5 Wochen aufbewahrt. Die ArchivLog-Dateien werden einmal täglich gesichert.

5.5 Integration mit anderen DV-Systemen

Es findet keine Integration und kein Datenabgleich mit anderen Systemen statt.

6 Begriffsbestimmungen

6.1 Verantwortliche Stelle nach § 3 Abs. 3 LDSchG

Verantwortliche Stelle nach § 3 Abs. 3 LDSchG ist jede Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt. Verantwortliche Stelle für Ressortlerner ist jedes Ressort, das über das Bildungsmanagementsystem von BILDUNG21 Bildungsmaßnahmen bucht. Beauftragt ein Ressort einen Bildungsträger mit der Durchführung von Bildungsmaßnahmen, ist auch das auftraggebende Ressort als verantwortliche Stelle gemäß § 3 Abs. 3 LDSchG anzusehen.

Des Weiteren ist auch jeder Bildungsträger verantwortliche Stelle für die Bildungsträgerlerner, die Bildungsmaßnahmen nicht über ein Ressort, sondern unmittelbar bei ihm buchen. Werden von einem das Bildungsmanagementsystem nutzenden Ressort Daten eines Ressortlerners an einen Bildungsträger zur Durchführung einer Bildungsmaßnahme weitergeleitet, ist auch dieser Empfänger verantwortliche Stelle, da Daten durch ihn verarbeitet werden (vgl. § 3 Abs. 2 Nr. 2 LDSchG) bzw. mit Zustimmung des Betroffenen in Form der Einsichtnahme in die Teilnehmerliste auch an Dritte wie andere Seminarteilnehmer übermittelt werden (vgl. § 3 Abs. 2 Nr. 4 LDSchG). Bietet die Führungsakademie oder ein anderer Bildungsträger als Mandant in eigener Regie Bildungsmaßnahmen an, so ist sie hierfür als Bildungsträger selbst verantwortliche Stelle gem. § 3 LDSchG.

6.2 Auftragsverarbeitung nach § 7 Abs 1 und 3 LDSchG

Auftragsverarbeitende Stelle nach § 7 Abs. 1 LDSchG ist die Betriebsstelle der Führungsakademie Baden-Württemberg. Die Beauftragung wird in den mit jedem Ressort abzuschließenden Mandantenvertrag (auf der Grundlage des mit den Ressorts abgestimmten Geschäftsmodells) geregelt. Sie umfasst auch den jeweils nachgeordneten Bereich (§ 7 Abs. 2 Satz 5 LDSchG). Die Verarbeitung der personenbezogenen Daten ist nur im Rahmen dieses Auftrags und der Weisungen zulässig. Dies gilt auch für Bildungsträger, die selbständig ihre Dienste anbieten und für die Unternehmen (T-Systems einschließlich der Subunternehmen), die Wartungsarbeiten und vergleichbare Hilfstätigkeiten erbringen (§ 7 Abs. 5 LDSchG).

.

6.3 Empfänger nach § 3 Abs. 4 LDSchG

Empfänger ist jede Person oder Stelle, die Daten erhält, mit Ausnahme des Betroffenen. Empfänger in diesem Sinn sind die anderen an einer Bildungsmaßnahme teilnehmenden Personen sowie Dozenten oder Trainer von Bildungsmaßnahmen.

6.4 Mandant

Mandant im Sinne des integrierten Bildungsmanagements ist eine Organisationseinheit mit einer eigenen geschlossenen Nutzer- und Seminarverwaltung.

6.5 Kreis der Betroffenen

Betroffen vom integrierten Bildungsmanagement sind alle Beschäftigen der Ressorts, die dieses System nutzen. Betroffen sind auch natürliche und juristische Personen des Privatrechts, die selbst oder deren gesetzliche Vertreter und Bevollmächtigte im System als Bildungsanbieter (Institute, Dozenten, Trainer) oder als Unterkunftssteller (Hotels, Tagungsstätten) hinterlegt sind oder im System Bildungsmaßnahmen buchen bzw. Lerninhalte und andere Wissensbausteine abrufen.

6.6 Datenübermittlung an Dritte

Eine Übermittlung setzt voraus, dass Daten an Personen oder Stellen außerhalb der verantwortlichen Stellen (Dritte) geliefert werden. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, sofern keine Auftragsverarbeitung vorliegt (§ 3 Abs. 5 LDSchG). Dritte in diesem Sinn sind die für die Wartung zuständige Fa. T-Systems einschließlich deren Sublieferanten sowie die zuständigen Personalvertretungen und Gleichstellungsbeauftragten zur Abstimmung von Bildungsmaßnahmen nach dem Personalvertretungs- und Gleichstellungsgesetz.

7 Datenverarbeitung

7.1 Zulässigkeit der Datenverarbeitung

7.1.1.1 Ressortlerner

Nach § 36 Abs. 1 LDSchG dürfen personenbezogene Daten von Beschäftigten nur verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienst- Betriebsvereinbarung es vorsieht.

Dabei sind nach § 3 Abs. 1 LDSchG personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Soweit die Verarbeitung personenbezogener Daten von Beschäftigen der Landesverwaltung Baden-Württemberg im Rahmen der Nutzung des Bildungsmanagementsystems zur Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist oder eine Rechtsvorschrift dies vorsieht, liegt ein zulässiger Zweck vor (§ 36 Abs.1 LDSchG; vgl. auch den insoweit gleichlautenden § 113 Abs. 4 LBG).

Soweit Daten von der Führungsakademie als Bildungsträger oder von der Führungsakademie als Betriebsstelle verarbeitet werden, beruhen diese auf entsprechenden Auftragsverhältnissen mit dem die Daten erhebenden Ressorts im Sinne des § 7 LDSchG in dessen Auftrag eine bestimmte Person fortzubilden oder das integrierte Bildungsmanagementsystem zu betreiben.

Der Zweck des Arbeits- bzw. Dienstverhältnisses rechtfertigt auch die Speicherung von Protokolldaten, da die für die Bildung verantwortliche Stelle zu gewährleisten hat, dass personenbezogene Daten nur befugt verarbeitet werden (insbesondere Speicherkontrolle im Sinne von § 9 Abs. 3 Nr. 3 LDSchG, Übermittlungskontrolle im Sinne von § 9 Abs. 3 Nr. 6 LDSchG, Eingabekontrolle im Sinne von § 9 Abs. 3 Nr. 7 LDSchG; vgl. dazu die Ausführungen unter Nr. 10). Für diese Protokolldateien gilt die besondere Zweckbestimmung des § 12 Abs. 4 LDSchG. Diese Protokolldateien dürfen nur zu Kontroll- und Sicherungszwecken für die genannten Aufgaben verwendet werden; dies schließt nicht aus, diese Dateien bei aufgedeckten Verstößen gegen die Datenschutzgesetzgebung für sich daraus ergebende arbeits- oder dienstvertragliche Maßnahmen zu verwenden.

7.1.1.2 Bildungsträgerlerner

Soweit personenbezogene Daten von Bildungsträgern oder von Unterkunftsstellern unmittelbar erfasst werden, beruhen diese auf einer entsprechenden Einwilligung im Rahmen der Beauftragung (§ 4 Abs. 1 Nr. 2 LDSchG).

7.2 Erforderlichkeit der Datenverarbeitung nach § 13 Abs. 1 LDSchG

Nach § 13 Abs. 1 LDSchG ist für das Erheben personenbezogener Daten grundsätzlich Voraussetzung, dass die Kenntnis der Daten zur Erfüllung der Aufgaben der erhebenden (verantwortlichen) Stelle (vgl. § 3Abs. 3 LDSchG) erforderlich ist. Es dürfen nur die Daten erhoben werden, die zur Erfüllung einer konkreten, aktuellen Aufgabe benötigt werden.

Hierbei sind die Datenerhebung durch das Ressort und die Übermittlung der Daten an den zuständigen Bildungsträger sowie die Erhebung der Daten durch den Bildungsträger und die Systemadministration bei der Betriebsstelle zu unterscheiden.

7.2.1.1 Ressortlerner

Die Datenerhebung durch das Ressort erfolgt auf der Grundlage der mit dem Ressort abgestimmten Bedarfslage. Die erhobenen Daten dienen – wie insbesondere die Bildungshistorie zeigt – der Verbesserung der Einsatzsteuerung durch gezielte Qualifizierungsmaßnahmen. In § 54 Abs. 1 LVO ist eine Teilnahmepflicht an dienstlichen Fortbildungen postuliert, in Abs. 2 eine Pflicht der obersten Dienstbehörden die dienstliche Fortbildung zu regeln und in Abs. 3 eine entsprechende Förderungspflicht. Um diesen Pflichten nachkommen zu können, ist die Verarbeitung bestimmter Daten, die sowohl die Person selbst als auch deren Teilnahme an einer bestimmten Qualifizierungsmaßnahme erfassen, erforderlich. Die in der Basisanwendung erhobenen Daten decken dazu das erforderliche Mindestmaß. Je nachdem, welche personalentwicklerischen Schwerpunkte ein Ressort setzt, können bei der Konkretisierung dieser Pflicht zwischen den Ressorts Abweichungen auftreten. Gleiches gilt auch für die in § 5 des Tarifvertrags für den öffentlichen Dienst der Länder vom 12. Oktober 2006 genannte Qualifizierungsoption.

Die an den Bildungsträger zu übermittelnden Daten wurden mit dem Landesbeauftragen für den Datenschutz bereits in der Vorkonzeption 2003 abgestimmt. Die Nutzung und Speicherung der Daten erfolgt bis zum Ablauf der in § 256 HGB und § 147 AO genannten Aufbewahrungsfrist von 10 Jahren. Die an den Bildungsträger übermittelten Daten sind dort aufzubewahrende Belegdaten. Die Erforderlichkeit dieses Datentransfers ergibt sich auch daraus, dass die Teilnahme an Bildungsmaßnahmen grundsätzlich kostenpflichtig ist und mit der Anmeldung zu einer Qualifizierungsmaßnahme Kosten entstehen, die von dem Bildungsträger mit der entsprechen-

den Organisationseinheit (Kostenstelle) des Landes abgerechnet werden. Dazu sind die teilnehmenden Personen und der die Kosten auslösende Umstand für das Ressort wie auch für den Bildungsträger eindeutig zu identifizieren.

7.2.1.2 Bildungsträgerlerner

Bei Personen, die nicht über ein Ressort buchen, erfolgt die Datenerhebung und -verarbeitung mit Einwilligung des Betroffenen im beschriebenen Umfang. Die Erforderlichkeit auch dieser Daten wurde bereits 2003 festgestellt. Änderungen haben sich nicht ergeben. Auch die Datenerhebung bei den Dozenten, Trainern und Unterkunftsstätten sind erforderlich, um eine ordnungsgemäße Fortbildung gewährleisten zu können.

7.2.1.3 Betriebsstelle

Die Betriebsstelle verarbeitet personenbezogene Daten insoweit, als sie in Wahrnehmung ihres Verantwortungsbereichs diese Daten erhebt, speichert und übermittelt oder durch ihre Mitarbeiterinnen und Mitarbeiter verändert (Passwortzurücksetzung), sperrt (Logindeaktivierung) oder löscht (§ 7 Abs. 2 und 3 LDSchG). Diese Maßnahmen sind für einen ordnungsgemäßen Betrieb des integrierten Bildungsmanagementsystems erforderlich.

7.2.1.4 Bewertung

Durch die Übermittlung der im Ressort erhobenen Daten an den eine Bildungsmaßnahme durchführenden Bildungsträger sowie durch die Erhebung der Daten durch den Bildungsträger selbst sowie durch die Administration des Systems werden schutzwürdige Interessen der Betroffenen nicht übermäßig beeinträchtigt.

7.3 Technische und Organisatorische Maßnahmen nach § 9 LDSchG

Die Daten verarbeitenden Stellen sind nach § 9 LDSchG verpflichtet, die Anforderungen dieses Gesetzes durch technische und organisatorische Maßnahmen umzusetzen. Hieraus folgt die Verpflichtung zum Handeln, konkrete Anweisungen sind der Vorschrift nicht zu entnehmen (vgl. dazu die Ausführungen unter Nr. 9.)

7.4 Verfahrensverzeichnis nach § 11 LDSchG

Nach § 11 LDSchG führt jede öffentliche Stelle ein Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden (Verfahrensverzeichnis, vgl. Anlage 6). Der Inhalt der zu treffenden Festlegungen ist in § 11 Abs. 2 näher bestimmt. Auf der Grundlage der

Basisentwicklungen ist in der Anlage zu dieser Konzeption ein Mustereintrag enthalten. Ressortspezifische Anpassungen sind darin nicht erfasst.

8 Rechte der Betroffenen

8.1 Auskunft nach § 21 LDSchG

Die Lernenden erhalten auf Antrag jederzeit Auskunft über die zu ihrer Person gespeicherten Daten (§ 21 LDSG). Soweit der Lernende die Auskunft nicht online selbst abrufen kann, kann ein entsprechender formloser schriftlicher Antrag an die Betriebsstelle gerichtet werden. Die Auskunft ist zu dokumentieren.

8.2 Berichtigung nach § 22 LDSchG

Im integrierten Bildungsmanagementsystem hat der Lerner die Möglichkeit seine personenbezogenen Daten in eingeloggtem Zustand jeder Zeit selbst zu ändern. Sofern eine Berichtigung nicht online möglich ist, kann ein entsprechender formloser schriftlicher Antrag an die Betriebsstelle gereichtet werden. Die Berichtigung ist zu dokumentieren.

8.3 Löschung nach § 23 LDSchG

Nach § 23 LDSchG sind Daten zu löschen, wenn ihre Speicherung unzulässig ist, oder ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Die Erforderlichkeit bestimmt sich ausschließlich nach den von der verantwortlichen Stelle selbst festgelegten Regelungen. Zur Aufgabenerfüllung sind insbesondere solche Daten erforderlich, die im Rahmen gesetzlicher oder vertraglicher Aufbewahrungspflichten noch nicht gelöscht werden dürfen. Durch das Löschen werden die gespeicherten Daten unkenntlich gemacht (vgl. § 3 Abs. Satz 2 Nr. 7 LDSchG), so dass eine weitere Verarbeitung nicht möglich ist.

Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen der Betroffenen beeinträchtigt würden oder sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist (§ 23 Abs. 4 LDSchG).

Protokolldaten auf Systemebene werden im Falle von Systemstörungen nach durchgeführter Prüfung, sonst nach sechs Monaten gelöscht.

8.3.1.1 Ressortlerner

Die im Ressortmandanten gespeicherten Daten sind solche des Ressorts. Wann welche Daten gelöscht werden, obliegt daher der Regelung des jeweiligen Ressorts. Der Ressortlerner kann nicht die Zustimmung der Datenverarbeitung seiner personenbezogenen Daten bei seinem

Ressort widerrufen, da das Ressort die Datenhoheit besitzt. Daher kann die Löschung der persönlichen Daten von Ressortlernern nur vom Bildungsverantwortlichen beim Ressortmandantenadministrator beantragt werden. Unter Löschen wird im integrierten Bildungsmanagementsystem das sofortige und unwiederbringliche Vernichten des gesamten Datensatzes (z. B. einer Person) verstanden. Die Löschung ist nur zulässig bei Lernern, die nicht aktuell Teilnehmer in einer Bildungsmaßnahme sind, keine zukünftige Maßnahme gebuchten haben, für die keine Rechnung erstellt wird oder keine gesetzlichen Gründe gegen die Löschung sprechen. Die Datensätze von diesen Lernern werden nach dem Aufrufen der Löschfunktion entfernt werden. Die Löschung wird von Antrago an CL weiter gegeben.

Daten, bei denen die Löschung nicht zulässig ist, werden anonymisiert. Unter Anonymisieren wird das Überschreiben des Datensatzes (z. B. einer Person) mit Musterdaten (z.B. xxxxx) verstanden. Das Anonymisieren dient der Wahrung der mit einer Bildungsmaßnahme verbundenen Folgeprozesse. Die anonymisierten Daten werden nach Ablauf der organisatorischen Sperrfristen vom Mandantenadministrator gelöscht. Nach der Umsetzung der Datenanonymisierung ist eine Rückherleitung der anonymen Daten zu einer Person nicht mehr möglich. Bei der Anonymisierung erhält das Login zusätzlich den Status „deaktiviert“. Es wird das Löschflag gesetzt und die Zuordnung zu einer Organisationseinheit entfernt (vgl. dazu die Ausführungen zur Sperrung).

Wie die Löschung ist auch die Anonymisierung nur bei solchen Lernern zulässig, die nicht aktuell Teilnehmer in einem Seminar sind, keine Maßnahme gebuchten haben, alle Bildungsmaßnahmen abgeschlossen haben und für die die erforderlichen Rechnungen erstellt wurden. Die Datensätze von diesen Lernern werden nach dem Aufrufen der Anonymisierungsfunktion in Antrago mit Musterwerten überschrieben. Die Anonymisierung wird auch an CL weiter gegeben. Das System generiert nach der Durchführung der Löschung/Anonymisierung eine E-Mail an den Lerner.

Bei Lernern, für die eine Rechnung erstellt wurde, darf nach § 257 HGB und § 147 AO die endgültige Löschung der Datensätze mit den der Rechnungen zu Grunde liegen Belegdaten erst nach zehn Jahren erfolgen. Die Löschung nach Ablauf der Sperrfristen erfolgt mittels des Löschtools von Antrago. Mit diesem Tool können erst Seminare gelöscht werden, dann Rechnung und danach die Lerner (die zuvor eine Löschsperre infolge der erstellten Rechnung unterlagen). Die Lösch-Sperrfrist wird organisatorisch vom Mandantenadministrator überwacht.

8.3.1.2 Bildungsträgerlerner

Dem Bildungsträger stehen nach Abschluss der Bildungsmaßnahmen die Daten als Belegdaten noch zehn Jahre zur Verfügung, soweit sich diese Verpflichtung aus § 257 HGB und § 147 AO oder aus anderen Vorschriften ergibt. Unter diesem Vorbehalt steht der Anspruch die Daten zu

löschen bzw. zu anonymisieren oder deren Speicherung zu widerrufen. Die Ausführungen unter Nr. 8.3.1.1 treffen daher auf den Bildungsträgerlerner gleichermaßen zu. Der Bildungsträgerlerner wendet sich zur Löschung/Anonymisierung an den Bildungsträger, bei dem er sein Login hat.

8.4 Sperrung nach § 24 LDSchG

An die Stelle einer Löschung tritt nach § 24 Abs. 1 LDSchG eine Sperrung, wenn die Richtigkeit der Daten vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt (Nr. 1) oder in den Fällen des § 23 Abs. 4 LDSchG in denen eine Löschung unterbleibt, weil Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden oder sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Folge der Sperrung ist, dass eine weitere Verarbeitung der personenbezogenen Daten eingeschränkt wird (§3 Abs. 2 Nr. 5 LDSchG). Sie hat grundsätzlich daher in dem System zu erfolgen, in dem die Daten erfasst wurden, Folgesysteme sind zu korrigieren.

Personenbezogene Daten sind zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, dass die Daten zur Aufgabenerfüllung nicht mehr erforderlich sind (§ 24 Abs. 2 LDSchG). Bei automatisierten Verfahren kann die Sperrung auch durch zusätzliche technische Maßnahmen gewährleistet werden (§ 24 Abs. 3 LDSchG).

Sperrungen kommen insbesondere dann in Betracht, wenn Bedienstete aus einem Ressort ausscheiden und ihre Daten noch nicht gelöscht werden können. Wie unter Nr. 8.3 beschrieben, können Personendaten nur gelöscht werden, wenn keine Verknüpfungen mit anderen Daten mehr bestehen. Bestehen solche Verknüpfungen weiterhin, werden diese Daten anonymisiert und sind damit einer weiteren Verarbeitung nicht mehr zugänglich.

9 Datensicherheit

9.1 Zugangskontrolle

9.1.1 Rechner

Der Zugriff auf „BILDUNG21“ ist sowohl von jedem Arbeitsplatzrechner in der Landesverwaltung Baden-Württemberg als auch über das Internet von jedem anderen Rechner aus möglich. Daher verfügt jeder Mandant über zwei entsprechende Domainnamen.

9.1.2 Betriebsstelle BILDUNG 21

Die Betriebsstelle „BILDUNG21“ ist bei der Führungsakademie des Landes Baden-Württemberg angesiedelt und in den Räumen in Stuttgart untergebracht. Die Rechner der Betriebsstelle werden gegen eine unbefugte Nutzung geschützt. Sie werden mit dem Betriebssystem MS-Windows Server 2003 betrieben. Der Zugang zu den Administrationsanwendungen ist passwortgeschützt.

Das Hosting der Server wird im IZLBW betrieben, das Application Management durch T-Systems. Näheres regeln der mit dem IZLBW abgeschlossene Hostingvertrag, das Betriebsstellenkonzept (Anlage 4) und der Application Managementvertrag (Anlage 8).

T-Systems unterstützt die Betriebsstelle bei der Wartung der Applikationen. Die Rechner von T-Systems, die einen Zugang zu „BILDUNG21“ haben, sind nicht in das Firmennetz integriert. Die Speicher dieser Rechner werden gegen unbefugten Zugriff durch Verschlüsselungssoftware besonders gesichert. Im Übrigen gilt das Sicherheitskonzept von T-Systems.

9.1.3 Server im IZLBW

Die Server sind in einem Raum mit Zugangskontrollsystem untergebracht (Maschinensaal). Zutritt haben nur explizit autorisierte Personen des IZLBW. Wenn der Zugang von Externen erforderlich ist, müssen sich diese über das Operating des IZLBW anmelden. Einlass erhalten nur vorher benannte und angemeldete Personen. Während des Aufenthalts werden die externen Personen von IZLBW-Mitarbeitern beaufsichtigt. Die Zugangsdaten werden protokolliert.

9.1.4 Fa. T-Systems

Die zur Administration vorgesehene Arbeitsstation befindet sich im Serverraum, der dem Sicherheitskonzept der Fa. T-Systems entsprechend gegen unbefugten Zugang besonders gesichert ist (zusätzliche mechanische Sicherungen gegen Einbruch/Diebstahl, Überwachung durch Wachun-

ternehmen, separate Alarmanlage). Eine Anbindung an das Firmennetz der Fa. T-Systems besteht nicht.

9.1.5 Zugriffe der Teilnehmer im LVN

Die BMS-Server sind im Server LAN des IZLBW installiert und an das zentrale Firewall-System angeschlossen. Somit greifen die Teilnehmer aus den Intranets des LVN über das zentrale Firewall-System des IZLBW auf die BMS-LVN-Zugangs-Server zu. Zugreifen kann das gesamte LVN.

Verbindungsdaten:

- Zugriffe aus dem LVN: IP-Adressbereich 10.0.0.0 bis 10.127.255.255
- Erlaubte Protokolle: http (Port 80), smtp (Port 25 von Seiten des Servers), ftp (Port 20 und 21), LDAP (Port 389),
- IP-Adressen des BMS-LVN-Zugangs-Servers: 10.127.255.115
- IP-Adressen des BMS-DB, und BMS-Web-Servers: 10.127.218.75 und 10.127.218.76

Sicherheitsmaßnahmen:

- Es werden über das zentrale Firewall-System des IZLBW nur die oben aufgeführten Verbindungen freigeschaltet.
- Für Zugriffe aus dem LVN auf den BMS-Server werden nur die o.a. erlaubten Protokolle zugelassen. Andere Protokolle werden abgewiesen.
- Es werden nur Verbindungen zum BMS-Server zugelassen. Verbindungen, die vom BMS-Server aufgebaut werden, werden abgewiesen (außer smtp).

9.1.6 Zugriffe der Teilnehmer aus dem Internet

Benutzer aus dem Internet können über den BMS-Internet-Zugangs-Server und über das Internet-Firewall-System auf die BMS-Server zugreifen. Der BMS-Internet-Zugangs-Server hat dabei die Funktion eines Reverse-Proxy-Servers. Der Reverse-Proxy stellt die Verbindung stellvertretend für die Benutzer zum BMS-Web-Server zur Verfügung, so dass keine direkte Verbindung der Benutzer zum BMS-Web-Server und damit ins LVN erfolgen kann.

Verbindungsdaten:

Zugriffe aus dem Internet auf den BMS-Internet-Zugangs-Server:

- Erlaubte Protokolle: http, https
- IP-Adresse des BMS-LVN-Zugangs-Servers: 193.197.148.90

Zugriffe vom BMS-Internet-Zugangs-Server auf den BMS-Web-Server:

- Erlaubte Protokolle: http, https
- IP-Adressen des BMS-DB-, und BMS-Web-Server: 10.127.218.75 und 10.127.218.76

Sicherheitsmaßnahmen:

- Es werden über das Internet-Firewall des IZLBW nur die oben aufgeführten Verbindungen freigeschaltet.

- Zugriffe der Internet-Benutzer sind nur auf den BMS-Internet-Zugangs-Server möglich. Der BMS-Internet-Zugangs-Server übernimmt stellvertretend den Verbindungsaufbau zum BMS-Web-Server.
- Direkte Zugriffe der Benutzer auf den eigentlichen BMS-Web-Server im Server-LAN des IZLBW sind nicht möglich. Unzulässige Verbindungen werden durch die Firewall-Systeme abgewiesen.
- Es werden nur Verbindungen zum BMS-Server zugelassen. Verbindungen, die vom BMS-Server aufgebaut werden, werden abgewiesen (außer smtp).

9.1.7 Zugriff der Fa. T-Systems

Zur Administration der Anwendung im Rahmen der Aufgabe der Unterstützung der Betriebsstelle wird eine RAS/VPN-Verbindung benutzt. Die Verbindung verläuft wie folgt:

- PC von T-Systems – VPN-Tunnel durch Internet – Firewall-System des IZLBW – BMS-Server

Verbindungsdaten:

- Zugriffe von Administrationsrechnern der Fa. T-Systems: IP-Adressen aus dem Bereich 10.127.232.0/24
- Erlaubte Protokolle: IPSec
- IP-Adressen des BMS-Servers: 10.127.255.115

Sicherheitsmaßnahmen:

- Die Verbindung wird verschlüsselt. Die Verschlüsselung erfolgt von dem zentralen Firewall-Server bis zum Überwachungs- und Administrations-PC der Fa. T-Systems.
- Auf dem PC der Fa. T-Systems wird zu diesem Zweck die erforderliche Verschlüsselungs-Software installiert. Diese wird vom IZLBW zur Verfügung gestellt.
- Der Überwachungs- und Administrations-PC darf keine weiteren Verbindungen (Stand-Alone-PC) haben, außer der zum BMS-Server im IZLBW. Das bedeutet u.a., dass der PC nicht an das Hausnetz der Fa. T-Systems und mit dem Internet verbunden ist.

9.2 Datenträgerkontrolle

9.2.1 Arbeitsplatzrechner

Die Datenträgerkontrolle am Arbeitsplatz erfolgt durch die mit der Systemadministration beauftragten örtlichen Endnutzerbetreuer (vgl. dazu die Ausführungen im Geschäftsmodell, Anlage 7).

Die lokale Speicherung von Daten auf Festplatten ist im Rahmen der Anwendung „BILDUNG21" möglich; die weitere Verwendung dieser Daten liegt in der Verantwortung des jeweiligen Lerners. Alle anderen Personen und Stellen (Bildungsverantwortliche sowie Personal- und Frauenvertre-

tungen), die zur Wahrnehmung ihrer Aufgaben für personenbezogene Daten eine Downloadmöglichkeit haben, haben diese Daten zu löschen, wenn sie zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind (§ 23 Abs. 1 LDSG). Die Ressorts werden gebeten, dies in ihren Datenschutzkonzeptionen zu berücksichtigen und die betroffenen Stellen zu unterrichten.

9.2.2 Betriebsstelle BILDUNG 21

Die Kontrolle der im Rahmen der Anwendungsadministration anfallenden Datenträger mit spezifischen Daten von „BILDUNG21" richtet sich nach der jeweils aktuellen DV-Dienstanweisung der Führungsakademie Baden-Württemberg für die Betriebsstelle (Vgl. dazu Anlage 4 mit dem Betriebsstellenkonzept).

9.2.3 Server im IZLBW

Die Systemkomponenten im Verantwortungsbereich des IZLBW unterliegen der dort vorhandenen technischen und organisatorischen Kontrolle. Das IZLBW hat für den Rechenzentrumsbetrieb Sicherheitsrichtlinien nach den Anforderungen des IT-Grundschutzhandbuchs des BSI und den E-Government-Richtlinien des Landes erstellt.

9.2.4 Fa. T-Systeme

Die Datenträgerkontrolle an der Arbeitsstation obliegt dem jeweiligen beauftragten Mitarbeiter. Dieser ist schriftlich über die Sicherheitsbestimmungen hinzuweisen.

9.3 Speicherkontrolle

9.3.1 Arbeitsplatzrechner

Mit der Anmeldung am Arbeitsplatzrechner erhalten die Landesbediensteten Zugang zu den jeweiligen DV-Anwendungen im Rahmen der ihnen erteilten Nutzungsrechte und damit auch zu „BILDUNG21".

Lernende können ihre eigenen Personalstamm- und Teilnahmedaten auf dem Anwendungsserver speichern. Sie sind zur ggf. lokalen Speicherung abgerufener Daten im Rahmen der jeweiligen Möglichkeiten des Betriebssystems bzw. der Anwendersoftware berechtigt.

9.3.2 Betriebsstelle

Die Beschäftigten der Betriebsstelle „BILDUNG21" erhalten in gleicher Weise mit der Arbeitsplatz-Anmeldung Zugang zu den DV-Anwendungen und damit auch zu „BILDUNG21". Sie sind nach Eingabe der Benutzerkennung (besondere Nutzerkennung + Passwort) im Rahmen der in der Benutzerverwaltung hinterlegten Rechte als Administratoren z.B. zum Lesen, Verändern und Löschen eingestellter Inhalte oder zur Bearbeitung von Nutzerkonten berechtigt.

9.3.3 Fa. T-Systems

Soweit es für Zwecke der Serveradministration, der Anwendungsentwicklung und der Aufrechterhaltung des Betriebs der Anwendung erforderlich ist, verfügt T-Systems im Rahmen seiner Administrationsaufgaben über entsprechende Speicherrechte.

9.4 Benutzerkontrolle

Der Zugang zum integrierten Bildungsmanagementsystem ist für Rechner innerhalb des LVN und aus dem Internet ermöglich. Damit können grundsätzlich alle Beschäftigten der Landesverwaltung, die sich als Lernende registriert haben und von ihrem Bildungsverantwortlichen zugelassen sind, zugriffsberechtigt sein. Ein ggf. erweiterter Zugriff auf eingeschränkte Inhalte und Anwendungen sowie die Ausübung von Administratorrechten richtet sich nach den in der Benutzerverwaltung hinterlegten Rechten des jeweiligen Anwenders.

Die Lernenden authentifizieren sich auf Anwendungsebene durch Eingabe von Nutzerkennung und Passwort.

Die Anlage, Veränderung und Löschung von Nutzerdaten und –konten werden in einer Log-Datei protokolliert und können nur von dafür berechtigten Administratoren der Betriebsstelle eingesehen werden.

9.5 Zugriffskontrolle

Der Zugang zum integrierten Bildungsmanagementsystem ist für Lernende mit Zugangsberechtigung grundsätzlich nach Eingabe der erforderlichen Identifizierungsmerkmale, bestehend aus Benutzerkennung und individuellem Passwort freigegeben. Der Zugriff auf einzelne Bereiche der Anwendung wird über die Rolle Lernender gesteuert.

9.6 Übermittlungskontrolle

Nur die unter Nr. 4.5.3 beschriebenen personenbezogenen Daten werden mit der Genehmigung einer Bildungsmaßnahme von einem Ressort an den die Bildungsmaßnahme durchführenden Bildungsträger übermittelt.

9.7 Eingabekontrolle

9.7.1 Protokollierungsverfahren

Innerhalb der Anwendung werden folgende Protokollierungen vorgenommen:

Zugriffe auf Webinhalte werden vom Programmteil „MS-Internet Information Server" in Log-Dateien gespeichert. Der entsprechende Benutzer kann nur anhand der IP-Adresse ermittelt werden.

Log-Dateien auf Anwendungsebene werden in nicht explizit freigegebenen Verzeichnissen gespeichert, ein Zugriff auf diese Daten ist nur für die Betriebsstelle mit Administratorrechten möglich.

Die Auswertung der Log-Dateien ist im Störungsfall zur Fehlereingrenzung und Behebung, sonst nur zur Datenschutzkontrolle zulässig. Diese Protokolle werden im Anschluss an eine anlassbezogene Auswertung, spätestens jedoch nach 6 Monaten gelöscht.

Durch das System werden folgende Daten protokolliert:

Logon – logoff:
User, Datum, Uhrzeit,

zu jedem Buchungsvorgang innerhalb des BMS:
User, Datum, Uhrzeit, Art des Buchungsvorganges

Das Logfile wird monatlich überschrieben.

9.7.2 Arbeitsplatzrechner/LAN

Eine Eingabekontrolle im Rahmen der landeseinheitlichen Konfiguration der Arbeitsplatz-PC ist nicht vorgesehen. Beim Einsatz des Browsers sind die jeweils festgelegten Einstellungen zu beachten. Gleiches gilt für die Arbeitsplatzrechner der Betriebsstelle.

9.7.3 IZLBW

Zugriffe auf den Server für die Administration (Konfiguration des Servers) werden passwortgeschützt eingerichtet. Die Passwörter werden in der Konfiguration verschlüsselt gespeichert.

9.8 Auftragskontrolle

Die Führungsakademie, das IZLBW und T-Systems werden mit der Verarbeitung personenbezogener Daten über die nach § 7 LDSG erforderliche Vereinbarung beauftragt. Darin werden Regelungen zum Datenschutz, die den Auftragnehmer betreffen wie z.B. die Verpflichtung der Mitarbeiter auf das Datengeheimnis oder die Voraussetzungen für den Zugriff auf die Nutzungsdaten, sowie zusätzliche technisch-organisatorische Maßnahmen zur Datensicherheit definiert. Weiter ist in der Beauftragung vorgesehen, dass dem Auftraggeber Möglichkeiten eingeräumt werden, sich von der Einhaltung der vertraglich vereinbarten Verfahrensweise zu überzeugen.

9.9 Transportkontrolle

Die Datenübertragung während der allgemeinen Nutzung von „BILDUNG21" innerhalb des LVN wird nicht verschlüsselt. Die Datensicherung erfolgt unverschlüsselt.

9.10 Organisationskontrolle

Die Landesbediensteten haben die Nutzungsbedingungen zu beachten und unterliegen während der Nutzung der allgemeinen Dienstaufsicht. Die Nutzungsbedingungen des IZLBW liegen als Anlage bei (Anlage 5).

10 Meldung an den Landesbeauftragten für den Datenschutz

Die Aktualisierung der Datenschutz- und Datensicherheitskonzeption des integrierten Bildungsmanagementsystems von BILDUNG21 wird gem. § 32 Abs. 1 LDSG dem Landesbeauftragten für den Datenschutz gemeldet.

11 Verzeichnis gem. § 10 LDSG

Das Verfahren wird dem Innenministerium Baden-Württemberg zur Aufnahme in das dortige Verzeichnis gem. § 11 LDSG gemeldet.

12 Schutzbedarfe

Die unter Nr. 4 beschriebenen Daten des integrierten Bildungsmanagementsystems werden nachfolgend folgenden vier Datenschutzzielen gegenüber gestellt, um deren individuellen Schutzbedarf zu bestimmen.

12.1 Schutzziele

Schutzziele definieren Anforderungen an IT-Systeme, die notwendig sind, um eine bestimmungs- und ordnungsgemäße Verarbeitung von Daten, Inhalten und Informationen zu gewährleisten. Diese Anforderungen sind durch technische und organisatorische Schutzmaßnahmen sicherzustellen. Ausgehend von den drei Grundbedrohungen werden folgende Schutzziele definiert[2]:

12.1.1 Vertraulichkeit

Vertraulichkeit ist der Schutz vor unberechtigtem Zugriff auf Daten/ Inhalte und Informationen der Systeme. Bei der Informationsverarbeitung ist darauf zu achten, dass systemabhängige Anforderungen an die Vertraulichkeit der gespeicherten, übertragenen oder verarbeitenden Daten sichergestellt werden. D. h. es ist durch technische oder organisatorische Maßnahmen zu verhindern, dass unberechtigte Dritte Kenntnis von Daten und Inhalten erhalten. Alle betroffenen Systeme und Übertragungsstrecken sind im Hinblick auf die Vertraulichkeit zu bewerten.

[2] Standards des E-Government-Konzepts Baden-Württemberg vom 1.1.2007, Nr. 9.3.

12.1.2 Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

12.1.3 Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

12.1.4 Verbindlichkeit

Unter Verbindlichkeit werden die IT-Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

12.2 Feststellung des Schutzbedarfs

Der Schutzbedarf eines Systems definiert, welcher Schutz für die betrachteten IT-Systeme, IT-Anwendungen und Informationen ausreichend und angemessen ist. Er gibt an, welche möglichen Schäden beim Einsatz des Systems entstehen können und wie wichtig es ist, den Eintritt solcher Schäden durch entsprechende Maßnahmen zu verhindern.

Die Schutzbedarfsfeststellung setzt sich grundsätzlich aus folgenden Schritten zusammen:

1. Definition der Schutzbedarfskategorien,
2. Feststellung des Schutzbedarfs der Anwendungen,

3. Ableitung des Schutzbedarfs der IT-Systeme (aus dem Schutzbedarf der Anwendungen) und
4. daraus abgeleitet Feststellung des Schutzbedarfs der Kommunikationsverbindungen und
5. der IT-genutzten Räume der Betriebsstelle[3].

Für die Nummern 3 und 4 gilt das Sicherheitskonzept des IZLBW. Daher wird hier auf diese in dieser Konzeption nicht zu verantwortenden Schutzbedarfe der IT-Systeme und die Kommunikationsverbindungen auch nicht eingegangen.

12.2.1 Definition der Schutzbedarfskategorien

Unterschieden werden drei Schutzbedarfskategorien mit jeweils sechs Schadenszenarien[4]. Nachfolgend werden die Anforderungen beschrieben. Unter 12.2.2 wird beschrieben, inwieweit diesen Anforderungen entsprochen wird.

Ausprägung	Tatbestände	Beschreibung
Schutzbedarf normal	Verstöße gegen Gesetze, Vorschriften und Verträge	Verstöße gegen Vorschriften Gesetze und Verträge mit geringen Konsequenzen.
	Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die dienst- oder arbeitsrechtlichen Verhältnisse des Betroffenen.
	Negative Innen- oder Außenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
	Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerierbar eingeschätzt werden. Die maximale tolerierbare Ausfallzeit größer als 24 Stunden.

[3] Zur Risikoanalyse vgl. Standards des E-Government-Konzepts Baden-Württemberg vom 1.1.2007 , Nr. 9.3 und die Ausführungen des Bundesamts für Sicherung der Informationszwecke: www.it-grundsschutz.de Stand: Juni 2007.
[4] BSI-Standards 100-2 des Bundesamts für Sicherheit in der Informationstechnik mit entsprechenden Anpassungen an die Gegebenheiten des integrierten Bildungsmanagements.

Ausprägung	Tatbestände	Beschreibung
	Finanzielle Auswirkungen	Der finanzielle Schaden kann regelmäßig innerhalb der Haushaltsansätze aufgefangen werden.
	Berücksichtigung der Grundsätze: Datenvermeidung, Datenspeicherung	Die Grundsätze sind im Großen und Ganzen berücksichtigt.
Schutzbedarf hoch	Verstöße gegen Gesetzte, Vorschriften und Verträge	Verstöße gegen Vorschriften, Gesetze und Verträge mit hohen Konsequenzen.
	Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich; Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die dienst- oder arbeitsrechtlichen Verhältnisse des Betroffenen.
	Negative Innen- oder Außenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
	Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
	Finanzielle Auswirkungen	Der Schaden bewirkt einen Haushaltsansatzübergreifenden Ausgleich.
	Berücksichtigung der Grundsätze: Datenvermeidung, Datensparsamkeit	Die gespeicherten Daten sind nicht tolerierbar.
Schutzbedarf sehr hoch	Verstöße gegen Vorschriften, Gesetze und Verträge	Fundamentaler Verstoß gegen Vorschriften, Gesetze und Verträge. Vertragsverletzungen, deren Haftungsrisiko ruinös ist.
	Beeinträchtigung des informationellen Selbstbestimmungsrechts	Eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen ist gegeben. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen die dienst- oder arbeitsrechtlichen Verhältnisse offen legen.

Ausprägung	Tatbestände	Beschreibung
	Negative Innen- oder Außenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung ist denkbar.
	Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als 1 Stunde.
	Finanzielle Auswirkungen	Der finanzielle Schaden erfordert einen Nachtragshaushalt.
	Berücksichtigung der Grundsätze: Datenvermeidung, Datensparsamkeit	Die Grundsätze sind erheblich verletzt.

12.2.2 Feststellung des Schutzbedarfs

Im integrierten Bildungsmanagementsystem werden personenbezogene Daten erhoben, verarbeitet und genutzt. Da diese Daten mit dem Dienstverhältnis eines Beamten in einem unmittelbaren inneren Zusammenhang stehen und damit Teil der Personalakte sind, sind die Daten vertraulich zu behandeln (§ 113 Abs. 1 LBG). Des Weiteren werden Prozesse der Landesverwaltung abgebildet bzw. unterstützt. Diese und die daraus generierten Informationen müssen verlässlich sein. Auf Grund der gesetzlichen Anforderungen, dem Sensibilisierungsgrad der gespeicherten Inhalte und den Nutzungszwecken (Durchführung von Bildungsmaßnahmen einerseits und Personalentwicklung andererseits), wird bezogen auf Verarbeitung personalbezogener Daten für die Schutzbedarfsfeststellung von folgenden Szenarien auszugehen:

iBMS		Schutzbedarfsfeststellung			
Nr	**Bezeichnung**		**Grundwert**	**Schutzbedarf**	**Begründung**
1	Nutzerregistrierung		Integrität normal	Personendaten sind vertraulich zu behandelnde Daten.	Die Daten werden vom Nutzer selbst eingegeben und gepflegt. Auf dieser Grundlage erfolgt die Freigabe regelmäßig von einem die örtlichen Verhältnisse kennenden Bildungsverantwortlichen mit Backoffice-Berechtigung (BV). Unberechtigte Nutzer können vom BV jederzeit deaktiviert werden. Die bei der Registrierung zu erfassenden

iBMS		Schutzbedarfsfeststellung			
Nr	**Bezeich-nung**		**Grundwert**	**Schutzbedarf**	**Begründung**
					personenbezogenen Daten werden - ausgehend von Basisanforderungen – mit dem jeweiligen Ressort abgestimmt.
			Verbindlich-keit normal	Informationen erreichen die Berechtigten.	Der Nutzer kann die Daten, wozu auch seine Mail-Adresse gehört, jederzeit einsehen und ändern. Der Nutzer wird mit seiner pers. ID erfasst. Die Prozesse sind so gestaltet, dass sie den jeweils zuständigen BV erreichen. Nicht zuständige BV können eine Bearbeitung mit entsprechendem Vermerk gegenüber dem Nutzer ablehnen.
			Vertraulich-keit hoch	Unberechtigte erhalten keine Kenntnis	Die Nutzerkennung und Passwort werden sowie der Transfer aller personenbezogen Daten im Internet wird verschlüsselt gespeichert. Die Nutzer werden im Backoffice-System eines Mandanten gespeichert. Dieses System ist mandantenscharf abgegrenzt. Personenbezogene Daten können grundsätzlich nur innerhalb dieses Mandanten von den dazu berechtigten Personen gelesen oder bearbeitet werden. Folge dieser mandantenscharfen Abgrenzung ist, dass personenbezogene Daten nicht zwischen Mandanten transferiert werden.
			Verfügbarkeit normal	Funktionsfähig-keit des Systems	Die Verfügbarkeit ist gekoppelt mit der Verfügbarkeit des Landesverwaltungsnetzes und der entsprechenden Ressortanbindung. Das System wird zeitweise für wenige Minuten abgeschaltet, wenn Updates oder Upgrades eingespielt werden. Dauert die Unterbrechung länger, werden die Bildungsverantwortlichen unterrichtet, die ihrerseits ihre Lernenden unterrichten können.
2	Buchung von Bildungsmaß nahmen		Integrität normal	Schutz vor Verfälschungen	Der Schutz ist gewährleistet, da im System nur eigene Daten verarbeitet werden.
			Verbindlich-keit normal	Authentizität der Daten	Vgl. Nr. 2 „Integrität“
			Vertraulich-keit normal	Schutz vor Veröffentlichung	Die Gefahr besteht nur dann, wenn sie der Lerner selbst realisiert (nachträgliche Verfälschung der Mail-Adresse oder Weitergabe der Nutzerkennung an unberechtigte Personen).

iBMS		Schutzbedarfsfeststellung			
Nr	**Bezeichnung**		**Grundwert**	**Schutzbedarf**	**Begründung**
			Verfügbarkeit normal	Nachteile durch Datenausfall	Im IZLBW erfolgt eine Sicherung der Daten. Die Verfügbarkeit der Buchungshistorie ist nicht so zeit- und aufgabenkritisch, dass es die Nutzung des Systems unzumutbar einschränkt.
3	Durchführung von Bildungsmaßnahmen		Integrität normal	Schutz vor unberechtigten Veränderungen	Mit der Buchung gehen bestimmte zur Durchführung von Bildungsmaßnahmen erforderliche personenbezogene Daten an den jeweiligen Bildungsträger über. Der Bildungsträger kann diese Daten nicht zu Lasten des entsendenden Ressorts verändern.
			Verbindlichkeit normal	Eindeutigkeit der Identität	Das System gewährleistet, dass Bildungsmaßnahmen nur über die dazu berechtigten Bildungsverantwortliche an die Bildungsträger weiter gegeben werden und die Dienstleistung in deren Auftrag erbracht wird.
			Vertraulichkeit normal	Keine unberechtigte Kenntnis durch Dritte	Der Bildungsträger erhält nur die Daten, die zur Durchführung einer Bildungsmaßnahme erforderlich sind. In eine weitergehende Verwendung muss der Lerner gesondert einwilligen (Teilnehmerliste, Fahrgemeinschaft).
			Verfügbarkeit normal	Zeitnaher Datentransfer	Buchungen oder Lerninhalte können allenfalls dann zeitkritisch werden, wenn Buchungsfristen drohen abzulaufen oder zur Vorbereitung auf eine Präsenzveranstaltung bestimmte Lerninhalte nicht aufgerufen werden können. Vgl. dazu auch Nr. 1 Funktionsfähigkeit des Systems.
4	Datenlöschung		Integrität normal	Keine unerlaubte Löschung personenbezogener Daten	Personendaten werden manuell gelöscht, wenn ihre Verarbeitung nicht mehr erforderlich ist und sie nicht mit Bildungsmaßnahmen oder Bildungsinhalten (Teilnahmedaten) verknüpft sind. In dem Fall werden sie anonymisiert.
			Verbindlichkeit normal	Endgültigkeit der Löschung	Gelöschte oder anonymisierte Daten können nicht mehr reaktiviert werden.
			Vertraulichkeit hoch	Keine Löschung schutzwürdiger Daten	Teilnahmedaten werden anonymisiert. Daten, für die gesetzliche Aufbewahrungsfristen gelten (Belegdaten), dürfen erst nach Ablauf der gesetzlichen Aufbewahrungsfrist von 10 Jahren gelöscht werden. Bei diesen Daten ist zu gewährleisten, dass sie nach Ablauf der gesetzlichen

iBMS		Schutzbedarfsfeststellung			
Nr	**Bezeichnung**		**Grundwert**	**Schutzbedarf**	**Begründung**
					Aufbewahrungsfrist auch physisch vernichtet werden. Dazu ist noch ein entsprechendes Löschkonzept zu entwickeln.
			Verfügbarkeit normal	Gewährleistung der Löschung	Die Anonymisierung bzw. Löschung steht den dazu berechtigten Personen zur Verfügung.
5	Buchungshistorie		Integrität normal	Schutz vor Veränderungen	In die Buchungshistorie werden nur Daten aufgenommen, die im System bereits vorhanden sind. Neue Datensätze können nicht aufgenommen und bestehende nicht abgeändert werden.
			Verbindlichkeit normal	Gewährleistung der Richtigkeit	Das System gewährleistet, dass die Daten nur von den Beteiligten stammend generiert werden.
			Vertraulichkeit normal	Schutz gegenüber Dritten	Die Daten erscheinen nur im System und können nur über die jeweilige Nutzerkennung abgerufen werden.
			Verfügbarkeit normal	Gewährleistung des Zugriffs	Die Daten sind während der Funktionsfähigkeit des Systems abrufbar. Der Abruf der Daten ist regelmäßig nicht zeitkritisch.
6	Bildungshistorie		Integrität normal	Schutz vor Veränderungen	In die Bildungshistorie werden nur Daten aufgenommen, die im System bereits vorhanden sind. Die Teilnahme an Bildungsmaßnahmen wird vier Wochen nach der Durchführung einer Bildungsmaßnahem erfasst, es sei denn der Bildungsträgers bestätigt zwischenzeitlich die Teilnahme nicht. Damit könne auch reine E-Learning Programme in der Buchungshistorie erfasst werden.
			Verbindlichkeit normal	Gewährleistung der Richtigkeit der Daten	Das System gewährleistet, dass die Daten nur von den Beteiligten stammend generiert werden.
			Vertraulichkeit normal	Schutz gegenüber Dritten	Die Daten erscheinen nur im System und können nur über die jeweilige Nutzerkennung abgerufen werden.
			Verfügbarkeit normal	Gewährleistung des Zugriffs	Die Buchungshistorie ist grundsätzlich erst vier Wochen nach der Durchführung einer Bildungsmaßnahme aktuell. Die Daten sind während der Funktionsfähigkeit des Systems abrufbar. Der Abruf der Daten ist regelmäßig nicht zeitkritisch.

13 Risikoanalyse

Die Richtlinien des Bundesamts für Sicherheit in der Informationstechnologie sieht eine individuelle Risikoanalyse nur bei Systemen ab einem hohen Schutzbedarf vor. Die in Kapitel 12 durchgeführte Schutzbedarfsanalyse hat für die Basisanwendung des integrierten Bildungsmanagementsystems einen hohen Schutzbedarf bei der Nutzerregistrierung und der Datenlöschung ergeben. Anhand einer individuellen Analyse wird die Sicherheitsrelevanz der Risikobereiche nach folgenden Kriterien näher untersucht:

1. Eintrittswahrscheinlichkeit einer Schutzzielverletzung
2. Auswirkungen auf die Schutzzielverletzungen
3. Risiko aus 1 + 2
4. Maßnahmen
5. Restrisiko

13.1 Eintrittswahrscheinlichkeit

Als Eintrittswahrscheinlichkeit wird die erwartete Wahrscheinlichkeit der Gefahrenrealisierung bezeichnet. Die beim Bildungsträger gespeicherten Belegdaten sind zehn Jahre zu speichern. Danach müssen sie gelöscht werden. Gelöscht werden können sie durch einen manuellen Eingriff. Werden sie nicht gelöscht oder werden bei der Löschung Daten übersehen, führt das zu einer Schutzverletzung. Ebenso müssen bei einem Ressortwechsel Daten des abgebenden Mandanten in den aufnehmenden Mandanten übernommen und die Daten bei abgebenden Mandanten gelöscht werden. Auf Grund der Fluktuation in der Landesverwaltung ist auch die Wahrscheinlichkeit des Eintritts dieses Umstandes recht groß.

13.2 Auswirkungen

Die Auswirkungsanalyse hat zum Ziel, das Gefahrenspektrum von dem eine denkbare Gefährdung ausgehen kann zu erfassen und vor dem Hintergrund der Schutzziele zu bewerten. Dabei sind die oben unter Nr. 12.2.1 definierten Schadenkategorien zu Grunde zu legen, diesmal jedoch aus einer Gesamtsicht betrachtet. Die Gefährdungslage ist als relativ gering anzusehen. Die der Fortbildung dienenden persönlichen Daten genießen zwar einen erhöhten Vertrauensschutz, dem jedoch kein konkretes Gefährdungsinteresse gegenübersteht. Eine über ein akzeptables Risiko hinausgehende Beeinträchtigung der Vertraulichkeit und der Verbindlichkeit können daher nicht angenommen werden, hingegen eine temporäre Beeinträchtigung der Verfügbarkeit und der Integrität der Daten, da diese entweder noch gespeichert werden (bei Ausscheiden oder nach Ablauf der Aufbewahrungsfrist) oder (bei Ressortwechsel) noch nicht in das neue Ressort transferiert wurden.

13.3 Risiko

Die Einschätzung des Risikos basiert auf einer Kombination der Eintrittswahrscheinlichkeit und der möglichen Auswirkungen einer Schutzzielverletzung (vgl. dazu die Ausführungen unter Nr. 13.2). Das Restrisiko stellt die Bedrohung dar, die nach der Implementierung der Schutzmaßnahme bleibt. Beide Einschätzungen sind in der die Maßnahmen beschreibenden Tabelle wieder gegeben.

13.4 Maßnahmen

Zur Gewährleistung des Schutzbedarfs werden folgende Maßnahmen vorgeschlagen, deren Umsetzung dazu beträgt, die Gefährdung der Schutzziele zu minimieren. Die Bewertung eines möglichen Restrisikos bildet den Abschluss der Analyse. Die Tabelle stellt dazu die die Entscheidung begründenden Umstände zusammen.

Nr	Gefahr	Auswirkung / Wahrscheinlichkeit	Risiko	Maßnahme	Aufwand	Restrisiko
1	Daten müssen bei Ressortwechsel und dem Ausscheiden aus dem Landesdienst gelöscht bzw. in das aufnehmende Ressort übernommen werden können.	hoch	hoch	Langfristig: Entwicklung und Umsetzung einer Datentransferkonzeption	hoch	keines
				Kurzfristig: Entwicklung einer Eingabemaske zur „Nacherfassung“ von Bildungsmaßnahmen.	gering	gering
2	Daten müssen manuell gelöscht werden. Ein Automatismus, dass diese nach Ablauf der Aufbewahrungsfrist auch physisch vernichtet werden, existiert bislang nicht.	mittel	mittel	Entwicklung und Umsetzung einer Datenlöschkonzeption	hoch	keines

13.5 Restrisiko

Die Tabelle zeigt, dass bereits mit kurzfristig realisierbaren Maßnahmen das Restrisiko bei einem durch Ressortwechsel veranlassten Datentransfer eingegrenzt werden kann. Da es sich hier um einen Wechsel einzelner Personen handelt, ist eine manuelle Datenlöschung im abgebenden

Mandanten noch vertretbar. Problematischer hingegen wird es bei Bildungsträgern. Hier laufen innerhalb eines Jahres eine Vielzahl von Buchungen auf, die nach Ablauf der Aufbewahrungsfrist für Belegdaten von 10 Jahren gelöscht werden müssen. Ob mit manuellen Löschprozeduren den datenschutzrechtlich verbindlichen Erfordernissen Rechnung getragen werden kann, ist problematisch. Daher ist innerhalb der nächsten zehn Jahre eine entsprechende Löschkonzeption zu entwickeln und umzusetzen.

14 Anlagen

- ***Anlage 1 Rollen-Rechte-Konzeption***
- ***Anlage 2 Datenspiegel***
- ***Anlage 3 Erläuterungen zum Datenschutz***
- ***Anlage 4 Betriebsstellenkonzept***
- ***Anlage 5 Nutzungsbedingungen des IZLBW***
- ***Anlage 6 Meldung zum Verfahrensverzeichnis nach §11 LDSchG (Muster)***
- ***Anlage 7 Geschäftsmodell***
- ***Anlage 8 Application Managementvertrag***