In das Verfahrensverzeichnis sind einzutragen:	
1. Name und Anschrift der verantwortlichen Stelle,	Die Adressliste der Schulen, die Moodle BelWü einsetzen, wird regelmäßig über das KM, mindestens jedoch halbjährlich, aktualisiert.
2. die Bezeichnung des Verfahrens,	Lernplattform "Moodle BelWü" Über den Provider BelWü (Baden-Württemberg extended Lan) Die betreffende Technik ist in die Netzinfrastruktur des Hochschulnetzes und damit in das Sicherheitskonzept des Landes Baden-Württemberg eingebunden.
3. die Zweckbestimmung und die Rechtsgrundlage der Verarbeitung,	– Zweckbestimmung: elektronisch unterstützte Bildungsmaßnahmen (E-Learning und Blended-Learning) der Beschäftigten im Kultusbereich – Rechtsgrundlage: a) Schüler: § 13 Abs. 1, § 15 Abs. 1 LDSG i.V.m. der VwV "Datenschutz an öffentlichen Schulen" vom 25.11.2009 b) Lehrkräfte: § 36 Abs. 1 und 2 i.V.m. § 13 Abs. 1, 15 Abs. 1 LDSG und §§ 113 bis 113 g LBG i.V.m. der VwV "Datenschutz an öffentlichen Schulen" vom 25.11.2009 Insbesondere wird auf die Rahmendienstvereinbarung • Rahmendienstvereinbarung zum Einsatz einer Lernplattform" KuU v. 5. Sept. 2008 (Az.: 21-6760/202) verwiesen.
4. die Art der gespeicherten Daten,	Folgende persönliche Daten werden auftrittsspezifisch auf der Lernplattform "Moodle BelWü" gespeichert. a) Zugangsdaten: Benutzerdaten: Name, Vorname, Anmeldename, E-Mail-Adresse, Stadt/Ort, Land; b) Daten, die im Rahmen der Arbeit mit der Plattform entstehen: Log-in/Logout-Zeitpunkt; Zugriff auf Angebote; Erledigung von Aufgaben; Beiträge in Foren;
5. der Kreis der Betroffenen,	Schulleitung, Lehrkräfte, Referendare, Schüler,
6. die Empfänger der Daten oder Gruppen von Empfängern sowie die jeweiligen Datenarten, wenn vorgesehen ist, a) die Daten zu übermitteln, b) sie innerhalb der öffentlichen Stelle für einen weiteren Zweck zu nutzen oder c) sie im Auftrag verarbeiten zu lassen.	a) nicht vorgesehen b) nicht vorgesehen c) nicht vorgesehen Hinweis. Falls vorgesehen dürfen nur anonymisierte Daten weitergegeben werden (z. B. Daten öffentlicher Kurse).
7. die Fristen für die Prüfung der Sperrung und Löschung der Daten oder für die Sperrung und Löschung,	Art und Umfang der gespeicherten Daten sind abhängig von der Lernplattform – Protokollierung der Benutzeraktivitäten (z.B. Login/Logout-Zeitpunkt, Zugriff auf kursspezifische Benutzeraktivitäten) – Automatisierte Löschung der Protokollierung des Benutzerverhaltens spätestens nach 35 Tagen. – Benutzeraccounts werden spätestens 1 Jahr nach dem Ausscheiden aus der Schule gelöscht.

8. die zugriffsberechtigten Personengruppen oder Personen, die allein zugriffsberechtigt sind,	– Die Beschäftigte bei öffentlichen Stellen unterliegen dem Datengeheimnis, § 6 LDSG. – Moodle Rollenkonzeption Die Dokumentation der Rollenkonzeption kann über den Lehrerfortbildungsserver unter http://lehrerfortbildung-bw.de/moodle-info/admin/ eingesehen werden. Sie beschreibt die speziellen Rechteanpassungen für folgende Moodlerollen: Moodleadmin(s), Trainer, Trainer ohne Editierrecht, Teilnehmer, Gast
9. eine allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software und	Allgemein Beschreibung: • Eingesetzt wird als Webserver Apache 2.2 mit php5 und fastcgi und suexec. Das Betriebssystem ist Solaris 10. • Die verwendete Hardware ist eine Sun M5000. • Die Moodledaten werden mittels nfs aus unserem SAN gemounted. • Als Datenbank werden 2 geclusterte Sun V880 mit MySql 5 eingesetzt. • Die Zugriffe erfolgen ausschließlich vom Webserver mittels tcp/ip. • Der Zugiff erfolgt über das Internet per HTTPS-Verbindung. Merkmale des Webservers: • Zugang für Kunden zum Hochladen von Files nur per SCP/SFTP/rsync over ssh (verschlüsselte Verbindung) oder über Moodle. • Jedes Moodle erhält eine eigene IP-Adresse. • Jedes Moodle kann mit http oder https angesprochen werden. • PHP Scripte können mit der Endung .php im htdoc Verzeichnis ausgeführt werden. • CGI-Scripte sind im cgi-bin Verzeichnis lauffähig, hier sind keine html Dateien erlaubt. • Jedes Moodle erhält Zugriff auf eine Mysqldatenbank. • Mittels einer .htaccess Datei lassen sich Verzeichnisse Passwort schützen und https Zugang erzwingen. Sicherheitsbedingte Einschränkungen: • PHP: Systemaufrufe über PHP mittels system und shell_exec sind aus Sicherheitsgründen deaktiviert. • HP: popen, procopen, passthru, show_source sind aus Sicherheitsgründen deaktiviert. • PHP: Upload limit von 128 MB • PHP: open_basedir Beschränkung auf das vhostdata Verzeichnis • PHP: url_fopen ist deaktiviert • PHP: register_globals ist ausgeschaltet • Directory Listings sind aus Sicherheitsgründen nicht möglich. • Shellzugang für Kunden ist nicht möglich. • Überschreiben der Konfiguration des Webservers mittels .htaccess ist nur für die Authentifizierung erlaubt. • Datensicherung muss jeder Nutzer selbst vornehmen.

10. technische und organisatorische Maßnahme nach § 9 LDSG.	1.Zutrittskontrolle • Die Serverräume befinden sich am RUS und im NWZ. • Für den Zutritt zu den Serverräumen werden Chipkarten benötigt, die nur Administratoren und Netzwerktechniker von RUS und HLRS erhalten. • Die Server befinden sich in gesondert verschlossenen Racks. • Die Büros sind durch abschließbare Türen gesichert. 2.Datenträgerkontrolle • Die Serverschränke sind zusätzlich durch digitale Schlösser gesichert. Diesen 4-stelligen Zugriffscode erhalten nur Mitarbeiter des BelWü und nur diejenigen, die auch an die Serverschränke müssen. 3.Speicherkontrolle • Shell-Zugang für Admins ist nur über SSH-Schlüssel aus dem internen Netz möglich; die Webmaster/Moodleadmins haben keinen direkten Shellzugriff, sondern sind mittels scponly beschränkt. Die Datenbanken sind passwortgeschützt; durch die Firewall wird sichergestellt dass der Zugriff per Shell auf den Server via SSH nur aus dem internen Netzwerk des BelWü erfolgen kann. Das Intranet ist durch ACLs auf den Routern und IPF auf dem Server gesichert. Das Passwort für SCP Zugriffe und die Datenbanken der Benutzer wird von BelWü vergeben und enthält Sonderzeichen, Gross- und Kleinschreibung sowie Sonderzeichen. • Die virtuellen Hosts des Webservers werden mittels suexec mit unterschiedlichen Userids betrieben, so dass eine Einsicht in fremde Daten auf mit Filesystemrechten wirksam verhindert wird. • Zugriffe von Php auf das Filesystem werden mittels php.ini Einstellungen auf den jeweiligen Userbereich eingeschränkt. • Sessions und Uploads einzelner Vhosts werden in Verzeichnissen gespeichert welchen anderen Usern nicht zugänglich sind. 4.Benutzerkontrolle • Die Datenbank des Webservers ist über das Netz nur vom Webserver mittels User/Passwort ansprechbar, sowohl die Firewall als auch die Datenbank verwehren Zugriffe von anderen Stellen. • Der Bildschirm der internen Arbeitsplätze sperrt sich nach 15 Minuten automatisch und kann nur durch erneute Eingabe des Anmeldepasswortes wieder freigegeben werden. • Mitarbeiter haben keinen administrativen Zugang zum Webserver oder Datenbankserver. • Administrationszugriffe haben nur die BelWü-Sysadmins. Kunden können auf den Webserver nur per http/https oder aber mittels SCP/SFTP zugreifen. 5.Zugriffskontrolle • Der Web-Server und der Datenbankserver verwenden zfs und ufs als Dateisystem. • Die Verzeichnisrechte erlauben den Nutzern nur den jeweils erforderlichen Zugriff auf die jeweils erforderlichen Verzeichnisse. • Mitarbeiter haben keinen administrativen Zugang zu den Server- und Client-Systemen. • Administrationszugriffe haben nur die BelWü-Sysadmins. • Sie wird durch die Moodle-Rollenkonzeption sowie auftrittsbezogene Zugriffsrechte auf das Dateisystem realisiert.

	6.Übermittlungskontrolle • Entfällt, da keine Übermittlungen an andere Stellen vorgesehen sind. 7.Eingabekontrolle • Das System (Apache - WebServer) protokolliert alle Zugriffe mit Datum und IP-Adresse. Die Log-Dateien werden nach 14 Tagen im Rahmen der Log-Rotation überschrieben. • Die LOG-Dateien, die Moodle benutzerspezifischer erzeugt, können nur vom MoodleAdmin eingesehen werden und werden automatisiert nach spätestens 35 Tage gelöscht. In den Log-Dateien werden folgende Daten gespeichert: Kursbezeichnung, Zeit, Ip-Adresse, vollständiger Name, Aktion, Informationen 8.Auftragskontrolle • Entfällt, da keine Datenverarbeitung im Auftrag vorgesehen ist. 9.Transportkontrolle • Einsatz kryptograpischer Verfahren (SSL, SSH) 10.Verfügbarkeitskontrolle • Regelmäßige Updates, USV sowie Dieselgenerator • Der Webserver wird samt Kundendaten täglich gesichert. 11.Organisationskontrolle • Regelmäßige Mitarbeiterschulungen zum richtigen Umgang mit personenbezogenen Daten durch den fachlichen Ansprechpartner.