

Anlage 6

Muster

Meldung zum Verzeichnissverzeichnis nach § 11 LDSchG für das integrierte Bildungsmanagementsystem

Ressort/Behörde

Ort,
Telefon:
Az.:
Bearbeiter:

**An den
behördlichen Datenschutzbeauftragten o.V.i.A**

Eingang der Meldung:

Meldung für das Verzeichnissverzeichnis

- Erstmeldung
 Änderung* (alter Stand:)
 Ergänzung* (alter Stand:)
 Löschung* (alter Stand:)

1. Verantwortliche Stelle (Org.Bezeichnung):

(Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.)

2. Bezeichnung des Verfahrens sowie zusätzlich Kurzbezeichnung:

(Eindeutiger Name, über den das Verfahren im DV-System der verantwortlichen Stelle oder eines beauftragten Auftragnehmers identifiziert werden kann.)

BILDUNG21, integriertes Bildungsmanagementsystem

3. a) Zweckbestimmung

b) Rechtsgrundlage der Verarbeitung:

(Angabe, ob die Verarbeitung aufgrund einer Einwilligung oder aufgrund einer Rechtsvorschrift erfolgt. Die Rechtsvorschrift ist zusammen mit den einschlägigen Paragraphen präzise anzugeben.)

a) Elektronische Anmeldung und Genehmigung der Teilnahme an Bildungsmaßnahmen, Ermöglichung des Lernens im Medienverbund, Transparenz der durchgeführten Bildungsmaßnahmen und Nutzung zu personalentwicklerischen Zwecken.

* Bitte Kopie der letzten Meldung beifügen.

b) § 36 LDSchG iVm § 54 Abs. 1 LVO

4. Art der gespeicherten Daten:

(Sachlich zusammengehörende Datenfelder sind zu sinnvollen Gruppen zusammenzufassen und diese Datenarten dann allgemein verständlich zu benennen)

Soweit die Ressorts nichts anderes bestimmen, werden folgende Pflichtdaten gespeichert:

- Anrede
- Vorname
- Nachname
- Dienststelle mit Postanschrift oder Postfach
- E-Mail-Adresse
- Telefonnummer
- Kostenstelle
- Amts- und Dienstbezeichnung
- Nutzerkennung
- Passwort
- Geheime
- Frage
- Antwort auf geheime Frage
- Anmeldung und Zulassung der Teilnahme sowie Teilnahme an Bildungsmaßnahmen
- Speicherung der Rolle als Lerner, Bildungsbeauftragter oder Ressortsadministrator

Optionale Daten sind:

- Titel
- Faxnummer
- Laufbahn
- Funktionsangaben

Erläuterungen dazu enthält die Datenschutz- und Datensicherheitskonzeption mit ihren Anlagen.

5. Kreis der Betroffenen:

- Alle Beschäftigten, die sich im nach Anweisung des Ressorts in Bildung21 registrieren, um über dieses System Bildungsmaßnahmen zu buchen und daran teilzunehmen.
- Alle Bildungsverantwortliche der Ressorts, die Bildungsmaßnahmen genehmigen oder entwickeln und einstellen.
- Alle Ressortadministratoren, die die Bediensteten ihres Mandanten selbst betreuen oder die von diesen beauftragten Stellen.

Anlage 6

6. 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**

(Empfänger ist nach § 3 Abs. 4 LDSG jede Person oder Stelle, die Daten erhält, mit Ausnahme des Betroffenen. Angaben sind sowohl bei einer Datenweitergabe an einen Dritten (Fall a) als auch bei einer Zweckänderung innerhalb der verantwortlichen Stelle (Fall b) oder bei der Einschaltung eines Auftragnehmers (Fall c) zu machen.)

- a) Personalvertretungen und Frauenvertretungen zur Durchführung der gesetzlichen Mitwirkung und Bildungsträger, die Bildungsmaßnahmen in BILDUNG21 anbeiten und bei denen Bildungsmaßnahmen gebucht werden.
- b) Die Ressorts selbst zur Nutzung der Daten zu personalentwicklerischen Zwecken.
- c) Die Betriebsstelle sowie deren Beauftragte zur Administration des Systems.

7. Fristen für

- a) die Prüfung der Sperrung und Löschung der Daten oder**
- b) für die Sperrung und Löschung:**

a) Daten werden wie folgt gelöscht:

- nach der Ablehnung des Login-Antrags
- nach Ablauf der zehnjährigen Aufbewahrungsfrist (§ 257 HGB, § 147 AO)
- nach Widerruf der Einwilligung der Speicherung der Stamm- und Teilnahmedaten
- nach Änderung der Rollen und Rechte
- nach vollzogenem Ressortwechsel ohne bestehende Verknüpfungen mit Teilnahmedaten
- nach Abschluss der auf Systemstörungen folgenden Prüfung

b) Daten werden wie folgt gesperrt:

- nach vollzogenem Ressortwechsel, bei bestehenden Verknüpfungen mit Teilnahmedaten.

8. Zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind:

(Die Zugriffsberechtigten sind funktionsbezogen aufzuführen. Die Angabe „Mitarbeiter des Personalreferats“ genügt nicht, da sie offen lässt, ob alle oder nur bestimmte Mitarbeiterinnen und Mitarbeiter des Referats zugriffsberechtigt sind. Stattdessen sollten Bezeichnungen wie z.B. „alle Mitarbeiter des Personalreferats, die Anträge auf... bearbeiten“, gewählt werden. Sofern sich die Zugriffsberechtigung auf unterschiedliche Datenarten bezieht, ist dies anzugeben.)

- Alle Bedienstete, die im Zusammenhang mit BILDUNG21 bildungsverantwortliche oder administrative Funktionen ausüben und dazu Bildungsmaßnahmen erstellen, einstellen, genehmigen, abrechnen oder auswerten.
- Alle Personalvertreter oder Frauenvertreterinnen, die an der Umsetzung des gesetzlichen Mitwirkungsrechts beteiligt sind.
- Alle Ressortsadministratoren oder die mit dieser Aufgabe beauftragten Stellen.
- Der Systemadministrator.

9. Allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software:

(Zu dokumentieren ist die von dem Standardarbeitsplatz IuK-UVM abweichende technische Infrastruktur, in der die verantwortliche Stelle ihre automatisierten Verfahren betreibt. Es sind Angaben zur Hardware [z. B. Anzahl der vorhandenen Großrechner, Server und Clients, Angaben zu aktiven Netzkomponenten], der Vernetzung [z. B. Typ und Topologie des lokalen Computernetzwerks wie Ethernet oder Token Ring, Anschluss an öffentliche Netze, Landes- oder kommunale Netze sowie Internet] und der eingesetzten Software [z. B. Betriebssysteme, Datenbanksysteme und Sicherheitssoftware] zu machen. Ferner ist zu dokumentieren, in welchem technischen Umfeld welches automatisierte Verfahren jeweils betrieben wird.)

Das integrierte Bildungsmanagementsystem besteht aus folgenden Komponenten (die technischen Beschreibungen der Komponenten sind in der Anlage zum Geschäftsmodell enthalten):

- Contentmanagementsystem: ContentXXL von Protamundi
- Lernmanagementsystem: Corporate Learning von der Deutschen Telekom AG
- Bildungsmanagement: Antrago von r+r Software

Serverbetrieb im IZLBW:

- Betriebssystem MS Windos Server 2003, Server SP 1
- Datenbank MS SQL 2000
- Webserver MS IIS 5.0

Hinweis: Nr. 9 ist nur dann auszufüllen, wenn das Verfahren – soweit möglich - nicht auf der Trägerplattform des Ressorts implementiert ist. Bei implementierten Verfahren ist auf die vom IuK-Referat erstellte „Allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software gemäß § 11 Abs. 2 Nr. 9 LDSG“ zu verweisen. Zusätzlich muss die Software angegeben werden, mit dem das Verfahren betrieben wird (z. B. MS-Access oder MS-Excel).

10. Technische und organisatorische Maßnahmen nach § 9 LDSG.

(Es ist konkret aufzuführen, welche Maßnahmen zusätzlich zu den in der Datenschutzkonzeption festgelegten Maßnahmen getroffen wurden.)

Die Betriebsstellenkonzeption sieht folgende organisatorischen Maßnahmen vor:

- Die Mitarbeiterinnen und Mitarbeiter der Betriebsstelle haben nur Zugriff auf die Daten und Programme, die sie zur Aufgabenerfüllung benötigen.
- Der Zugang zu dem System ist durch Identifizierung (Benutzererkennung) und Passwort geschützt.
- Es dürfen keine trivialen Passwörter verwendet werden. Das Passwort ist im Abstand von 3 Monaten zu verändern. Es darf nicht an Dritte – auch nicht innerhalb der Führungsakademie – weiter gegeben werden.

Anlage 6

-
- Bei der Bearbeitung von personenbezogenen Daten ist der Bildschirm so aufzustellen, dass Unbefugte die Daten nicht einsehen können.
 - Während der Betriebsbereitschaft hat der Bildschirm unter ununterbrochener Aufsicht des Benutzers zu sein. Ist das vorübergehend nicht der Fall, ist Vorsorge zu treffen, dass Unberechtigte keinen Einblick erhalten.
 - Der Raum der Betriebsstelle ist zu verschließen. Er muss auch während der regulären Arbeitszeiten gegen das Betreten Unbefugter geschützt sein.
 - Personenbezogene Daten dürfen nicht auf bewegliche Datenträger gespeichert werden.
 - Wartungsarbeiten sind zu protokollieren. Wartungstechnikern ist für die Zeit ihrer Tätigkeit ein Passwort zuzuweisen, das nach Beendigung der Tätigkeit wieder gelöscht wird. Muss ein PC zur Reparatur außer Haus gegeben werden, sind personenbezogene Daten auf der Festplatte zu löschen oder zu verschlüsseln.
 - Ein Testsystem für das Testen neuer Updates und Programme sowie ein Fehlermanagementsystem ist einzurichten.
 - Ist die Speicherung personenbezogener Daten nicht mehr für die Aufgabenerfüllung erforderlich, sind sie zu löschen.

Hinweis: Nr. 10 ist nur dann auszufüllen, wenn Maßnahmen zusätzlich zu den in der Datenschutzkonzeption festgelegten Maßnahmen getroffen wurden bzw. erforderlich sind.

(Unterschrift)