Anlage 2:
Technische und organisatorische Maßnahmen zum Datenschutz Baden-Württemberg

Vorbemerkung

Anlage 2 zum Vertrag zur Datenverarbeitung im Auftrag definiert die organisatorisch technischen Maßnahmen, die zum Schutz der im Vertrag gelisteten Anwendungen getroffen werden. Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers GmbH, im Folgenden BSV genannt, betreibt hierbei Datenverarbeitung im Auftrag der Schulen, die die Anwendungen einsetzen.

Verträge zur Auftragsdatenverarbeitung nach den Vorgaben der jeweiligen Landesdatenschutzgesetze sind erstellt. Hierin sind die Kontrollrechte des Auftragsgebers definiert.

Die technische Betreuung der Anwendungen erfolgt über die Westermann Digital GmbH im Folgenden EDV genannt.

Zum Schutz der personenbezogenen Daten in der Anwendung werden die folgenden organisatorisch-technischen Maßnahmen getroffen, um

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren (Zutrittskontrolle),

Zutritt zu den Räumlichkeiten im Rechenzentrum der Anwendung ist nur für autorisierte Personen möglich. Die Server sind in einem Sicherheitsbereich untergebracht, der überwacht ist und zu dem nur befugte Personen Zugriff haben. Dabei wird die Anwesenheit aufgezeichnet.

Der EDV-Bereich ist in einem gesonderten Sicherheitsbereich des Verlagsgebäudes untergebracht. Zugang haben nur die dort beschäftigten Mitarbeiter. Die Zugangskontrolle erfolgt über eine gesondert freigeschaltete Codekarte. Besucher dürfen sich nur in Begleitung eines EDV Mitarbeiters im Sicherheitsbereich aufhalten.

Datensicherungen auf Datenträgern werden in einem vom Serverbetrieb getrennten gesicherten Bereich des Rechenzentrums vorgehalten. Zugang zu den Datenträger zur Sicherung hat nur hierfür befugtes Personal des Rechenzentrums.

2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),

Datenträger sind im Rechenzentrum gegen unbefugtes Entfernen geschützt und regelmäßige Bestandskontrollen finden statt. Die Vernichtung von Datenträgern findet kontrolliert mit Protokollierung statt.

3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),

Die Passwörter für die Authentifizierung erfüllen die Voraussetzungen des BSI-Grundschutzes. Sie müssen regelmäßig geändert werden, der Änderungszeitraum ist softwaremäßig vorgegegeben.

Die Administratoren authentifizieren sich lokal oder über einen zentralen Authentifizierungsserver. Ein Login auf den Servern selbst ist nur per SSH möglich.

4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),

Der Zugriff auf Systemebene ist nur aus dem BSV-Intranet und dem Netz des Rechenzentrums möglich, sowie über eine zertifikatsbasierte, personalisierte VPN-Verbindung. Die Zertifikate haben eine Gültigkeit von 1 Jahr.
Das Betriebssystem und die Softwarekomponenten der Anwendung werden regelmäßig und zeitnah unter besonderer Berücksichtigung von Sicherheitsaspekten aktualisiert.
Der Netzwerkzugang zu den Anwendungen im Backend ist durch eine zweistufige Firewall Technologie geschützt. Zum einen über einen dedizierten Firewall Rechner für das über Internet erreichbare Westermann Teilnetz und darüber hinaus über IP-Filter direkt auf dem jeweiligen Applikationsserver.
Ein dediziertes System zur Intrusion Detection wird eingesetzt.
Administrative Zugänge auf den Anwendungsserver, den Datenbankserver und weitere administrative Systeme (z.B. Lizenzverwaltung) haben nur die unmittelbar mit der Systempflege beschäftigten Mitarbeiter des Rechenzentrums sowie die Internet-Administratoren der EDV.

5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
Der Zugriff auf Daten und Dienste auf den Servern der Anwendung wird über eine differenzierte Zugriffsregelung, basierend auf Gruppen geregelt.
Die Anwendung stellt sicher, dass eine Lehrkraft nur auf die Daten ihrer Klasse zugreifen kann. Es gibt keine übergreifenden Accounts, über die Lehrkräfte Zugriff auf Daten anderer Klassen ihrer Schule haben oder einen schulischen „Master-User“, der Zugriff auf Daten aller Klassen der Schule hat.

6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
Aus der Anwendung heraus lassen sich durch die Schule keine Daten für die Übermittlung an Dritte exportieren oder anderweitig eine Übermittlung anstoßen.
BSV betreibt Datenverarbeitung im Auftrag und gibt keine Daten weiter.

7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
Die Schule kann bei Anlage der Nutzer nur die für die Nutzung der Anwendung notwendigen Daten eingeben. Es stehen keine freien Datenfelder zur Angabe von Zusatzinformationen zur Verfügung. Insbesondere ist es nicht möglich, email- oder postalische Adresse einzugeben.
Die Anwendung logt das Anlegen, Ändern und Löschen der personenbezogenen Schülerdaten mit.
Die Eingabe und Änderung von personenbezogenen Schülerdaten in der Anwendung wird über die Lehrkraft durch ein https abgesichertes Webinterface vorgenommen.

8. zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
Verträge zur Auftragsdatenverarbeitung nach den Vorgaben der jeweiligen Landesdatenschutzgesetze sind erstellt. Hierin sind die Kontrollrechte des Auftragsgebers definiert.
Die Systeme, auf denen Datenverarbeitung im Auftrag betrieben werden, sind von den Systemen getrennt, in denen BSV eigene Daten verarbeitet.
Schüler/innen werden bei der Datenanlage der jeweiligen Schule zugeordnet. Die Schule hat die datenschutzrechtliche Verantwortung für diese Daten.

BSV verarbeitet die Daten nur gemäß den Anweisungen der verantwortlichen Stelle. Anweisungen haben auf dem Schriftweg zu erfolgen.

9. zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

Datenträger werden nur im Rechenzentrum selbst zu Backup Zwecken genutzt und nicht zum Transport von Daten.

Personenbezogene Daten werden beim Transfer zwischen Server und Nutzerrechner verschlüsselt übertragen.

10. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

Um die Gefahr des Datenverlustes zu minimieren werden RAID Systeme auf den Servern eingesetzt.

Eine tägliche Datensicherung der System- und Anwendungsdaten auf physischen Datenträgern wird vorgenommen (Sicherheits-Backup). Die Sicherheits Backups dienen der Systemwiederherstellung im Fehlerfall.

Das Rechenzentrum verfügt über Schutzmaßnahmen im Brandfall.

Es werden unterbrechungsfreie Stromversorgung, Dieselgeneratoren und Klimaanlagen eingesetzt.

11. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Für das Testen von Software Erweiterungen stehen Testsysteme zur Verfügung, die vom Produktivsystem getrennt sind. Es werden keine personenbezogene Daten von Nutzern in Testsystemen eingesetzt.

Der Datenschutzbeauftragte ist benannt. Verantwortliche für Datensicherheit, Auftragskontrolle und aktuelle Dokumentation der Verfahrensschritte sind definiert.

Die mit der Anwendung befassten Mitarbeiter/innen haben klar definierte Aufgaben und sind auf das Datengeheimnis verpflichtet.

Datenschutz und Datensicherheit sind elementare Bestandteile von Softwareverträgen.

Jede Hardware und Software durchläuft im Rahmen der Investitionsplanung ein Genehmigungsverfahren.

Software und Änderungen sind dokumentiert. Für jede eingesetzte Software sind die Zugriffsrechte geregelt und dokumentiert.