Bayerisches Staatsministerium für
Unterricht und Kultus

Berechtigungsmanagement

Stand: 28.01.2026

→ www.km.bayern.de / gestalten / digitalisierung / datensicherheit / berechtigungsmanagement

Inhaltsverzeichnis

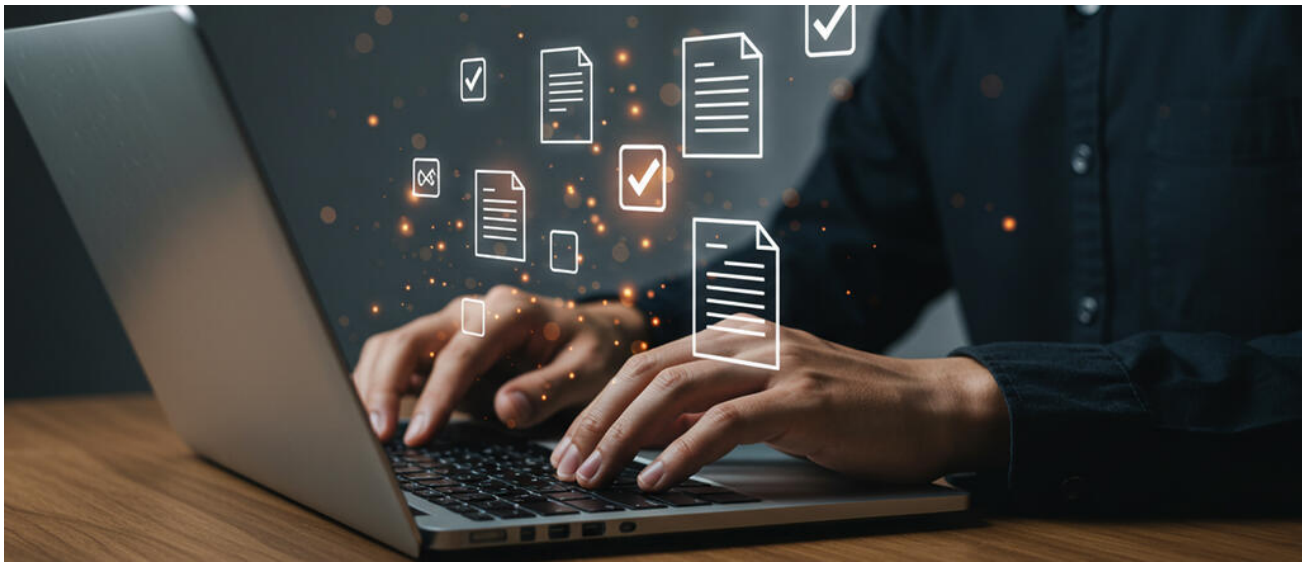
Berechtigungsmanagement 3

Netz- und Hardware-Ebene 4

Dienste- und Anwendungs-Ebene 4

Berechtigungsmanagement

Ein strukturiertes Berechtigungsmanagement stellt einen wesentlichen Bestandteil der Datensicherheit dar.



Need-to-know - Nur das sehen, was notwendig ist ©Block nomic Studio - stock.adobe.com

Das Berechtigungsmanagement stellt sicher, dass ausschließlich autorisierte Personen Zugang zu Daten und Systemen erhalten. In den Schulen existieren verschiedene Nutzergruppen – beispielsweise Lehrkräfte, Schüler, Verwaltungspersonal und Administratoren – die jeweils unterschiedliche Zugriffsrechte benötigen. Ein klares Berechtigungsmanagement gewährleistet sowohl die Einhaltung von Datenschutz- und Sicherheitsanforderungen als auch eine klare Aufgaben- und Verantwortungsverteilung.

Zentrale Prinzipien: Need-to-know und Least-Privilege

Das sogenannte Need-to-know-Prinzip bildet die Grundlage des Berechtigungsmanagements. Es besagt, dass Informationen und Zugriffsrechte ausschließlich denjenigen Personen zur Verfügung gestellt werden, die diese zur Erfüllung ihrer jeweiligen Aufgaben zwingend benötigen. Ergänzend dazu sollte auch das Least-Privilege-Prinzip berücksichtigt werden. Es stellt sicher, dass Nutzer nur die minimal erforderlichen Rechte erhalten – nicht nur in Bezug auf Informationen, sondern auch hinsichtlich Systemfunktionen und Ressourcen. Durch Anwendung dieser Prinzipien auf allen Ebenen und auf die verschiedenen IT-Systeme wird das Risiko unbefugter Zugriffe und Datenlecks wirksam minimiert.

Datenschutzrechtliche Vorgaben

Sofern personenbezogene Daten verarbeitet werden, fordert die DSGVO den Schutz vor „unbefugter und unrechtmäßiger Verarbeitung“ (Art. 5 Abs. 1 Buchst. f). Dies macht die Regelung von entsprechenden Zugriffsberechtigungen unmittelbar gesetzlich erforderlich.

Dabei spielt es keine Rolle in welcher Form (analog oder digital) die personenbezogenen Daten vorliegen.

Umsetzung und Dokumentation

Die Umsetzung des Berechtigungsmanagements erfolgt auf verschiedenen Ebenen, die nachfolgend näher beschrieben werden. Für die Planung, Vergabe, Dokumentation von Zugriffsrechten bieten sich sogenannte **Berechtigungsmatrizen** an. Diese stellen übersichtlich dar, welche Nutzergruppen auf welche Ressourcen mit welchen Zugriffsrechten zugreifen dürfen und ermöglichen eine regelmäßige Überprüfung und Anpassung der Rechtevergabe. Sie sind als technische bzw. organisatorische Maßnahme zu verakten.
Ein Beispiel für typische Nutzergruppen an den Schulen mit ihren Zugriffsrechten auf verschiedene Informationen ist in der nachfolgenden Tabelle abgebildet.

Netz- und Hardware-Ebene

Der Zugang zu einem Netzwerk und den Endsystemen sollte so weit wie möglich eingeschränkt werden. Das gilt sowohl für Netzwerkbereiche oder spezielle Server als auch für den **physischen Zugang**, wie bei einem Serverraum und den Endgeräten in den Räumen der Verwaltung oder im Lehrerzimmer.
Die Tabelle zeigt beispielhaft eine Berechtigungsmatrix für typische IT-Komponenten einer Schule und kann zur Weiterverarbeitung heruntergeladen werden.

Muster einer Berechtigungsmatrix
/download/4-25-06/250710_Berechtigungsmatrix_zur_Weiterverarbeitung.jpg

Dienste- und Anwendungs-Ebene

Für Anwendungen und (Cloud-)Dienste konkretisiert Anlage 2 zu § 46 BaySchO unter dem Punkt „Interne Empfänger/Zugriffsberechtigte“ die Vorgaben aus Art. 5 Abs. 1 Buchst. f DSGVO für die jeweilige Anwendung bzw. den (Cloud-)Dienst. Häufig werden dabei von den Anwendungen vorgegebene Rollenprofile angeboten, denen standardmäßig verschiedene Berechtigungen zugewiesen sind. Es ist zu prüfen, ob die Rolle den zugriffsberechtigten Personen entspricht; andernfalls müssen entsprechende Anpassungen vorgenommen werden.

Das folgende Dokument visualisiert die wesentlichen Zugriffsberechtigungen für die

einzelnen Abschnitte der Anlage 2 zu § 46 BaySchO als Berechtigungsmatrix.

Darstellungen der Zugriffsberechtigungen gemäß Anlage 2 zu BaySchO §46
/download/4-25-06/250710_BayScho_Berechtigungsmatrizen.jpg

Basiert die Verarbeitung von (personenbezogenen) Daten auf einer anderen Rechtsgrundlage als auf den in Anlage 2 zu § 46 BaySchO aufgeführten Abschnitten, ist entsprechend ein eigens angepasstes Rollen- und Berechtigungskonzept zu erstellen.