Übersicht relevanter Datenschutzmechanismen* - bezogen auf die webbasierte Notenverwaltungssoftware FuxNoten®

	Gewährleistungsziele						
Schutzbedarf	**Datensparsamkeit**	**Verfügbarkeit**	**Integrität**	**Vertraulichkeit**	**Nichtverkettbarkeit**	**Tranzparenz**	**Intervenierbarkeit**
Normal	Rechte und Rollenkonzept	Rechte und Rollenkonzept	Rechte und Rollenkonzept	Rechte und Rollenkonzept	Rechte und Rollenkonzept	Rechte und Rollenkonzept	Rechte und Rollenkonzept
	rollen und aufgaben-abhängige Gestaltung der Eingabemasken	Backup von Daten und Konfiguration nach einem Backup-konzept	Festlegungen der jeweils erforderlichen Erfassungsfrequenz der Datenbestände	logische Trennung von Schulverwaltungsnetz und Netz für die Lehre	Mandantentrennung durch separate Verwaltung und Verabeitung der Daten mehrerer Schulen auf getrennten Portalen	Möglichkeit der Kenntnisnahme von gespeicherten Daten durch den Betroffenen	Möglichkeit der Einsicht von Erziehungsberechtigten ggfs. von Schülern in über sie gespeicherte Daten
	automatisierte Sperr- und Löschroutinen	Redundanz der zentralen Systeme	Prüfsummen, Hashverfahren	zentrale Administration des IT-Systems durch von der verantwortlichen Stelle Beauftragte	frühestmögliche Anonymisierung	Verfahrensdokumentation (u. a. Freigabe, Vorab-kontrolle, Verfahrens-beschreibung, Sicherheitskonzept, Verträge, Rechtevergabe, relevante Dienstan-weisungen und Dienst-vereinbarungen)	Möglichkeit des Aus-drucks der über den Betroffenen gespeicherten Daten auf Anforderung (z. B. Notenliste)
	Möglichkeit der An-bringung von Sperr-kennzeichen	geeignete dezentrale Backupmaßnahmen (z. B. Papierunterlagen oder Backupanleitung)	Integritätsbedingungen für Datenbanken (z. B. Vorgaben für Formate und Wertebereiche)	Zugriff nur mit Verfahren nach dem Stand der Technik (Kryptokonzept, sichere Passwortgestaltung, Verschlüsselung, Clientzertifikate)	zweckbezogene Pseudonymisierung		Einrichtung von Prozessen zur Be-richtigung, Sperrung oder Löschung von Daten
	Möglichkeit der Pseudonymisierung nach Bedarf	baulicher Datenschutz (z. B. Brand- und Zugangs-schutz)	Integritätsschutz für Software		Beschränkung der Datenschnittstellen auf das erforderliche Maß	Dokumentation von Einwilligungen und Widersprüchen (soweit relevant)	Rücknahmemöglich-keit von Einwilligungen
	Möglichkeit der Anonymisierung nach Bedarf	Schutz vor Schadsoftware	Protokollierungsver-fahren hinsichtlich der Eingabe und Änderung von Daten	baulicher Datenschutz (z. B. Zugangsschutz)	Beschränkung der Funktionalität der Software auf das erforderliche Maß	Dokumentation der Softwareversionsver-waltung und anderer Administrationshand-lungen	Möglichkeiten zur Einsicht in Protokoll-dateien bspw. zu Übermittlungsvorgängen
	vorkonfigurierbare Exportmöglichkeiten für verschiedene Zwecke	Firewall		Verpflichtung auf das Datengeheimnis	bei regelmäßiger Übermittlung von Daten an Dritte Bereitstellung eines separaten Abrufdaten-bestandes durch die verantwortliche Stelle	Protokollierungsver-fahren hinsichtlich der Eingabe und Änderung von Daten	Verfahren zur Beaus-kunftung von Daten-übermittlungen (ggf. unter Einbeziehung der Empfänger)
	abgestimmtes Software-änderungsmanagement	regelmäßige Wartung von Hard- und Software		klare vertragliche Regelungen (z. B. Auftragsdatenverarbeitung, Wartungsverträge)		Auswertungskonzept für Protokolle	
		Vertretungsregelungen für Personal					
		Festlegungen von Datenformaten					

	Gewährleistungsziele						
Schutzbedarf	**Datensparsamkeit**	**Verfügbarkeit**	**Integrität**	**Vertraulichkeit**	**Nichtverkettbarkeit**	**Tranzparenz**	**Intervenierbarkeit**
Normal		Festlegungen der Aufbewahrungsstrategie geeignete Mechanismen für Langzeitaufbewahrung		Mandantentrennung bei gemeinsamer Verabeitung von Daten mehrerer Schulen Bereitstellung von Verfahren zur Sperrung von Daten Einrichtung eines geregelten Verfahrens zur (ggf. auch elektronischen) Übergabe von Daten an das Archiv Protokollierung von Anmeldungen (erfolgreich und nicht erfolgreich)		Protokollierung von Übermittlungsvorgängen Verfahren zur Beauskunftung von Datenübermitttlungen (ggf. unter Einbeziehung der Empfänger)	Einrichtung von Prozessen zur Information des Betroffenen bei Änderung von Grunddaten
Hoch			besondere Integritätsmaßnahmen zum Schutz der hoch schutzbedürftigen Daten (vorzugsweise qualifizierte elektronische Signatur)	Anmeldung an der Anwendung mittels Zwei-Faktor-Authentifizierung Verschlüsselung der gespeicherten Daten			sofern im Rahmen der Selbstauskunft hoch schutzbedürftige Daten elektronisch eingesehen werden sollen, müssen zusätzliche Maßnahmen (z. B. Zwei-Faktor-Authentifizierung) getroffen werden
Sehr Hoch			Protokollierung lesender Zugriffe	weitere Einschränkungen der Zugriffsrechte auf das minimal erforderliche Maß			

* in Anlehung an den Datenschutz-Maßnahmenkatalog erarbeitet im Projekt „Datenschutz an den Schulen in Mecklenburg-Vorpommern“ im Mai 2017

von Software bzw. FuxMedia sichergestellt

Verantwortungsbereich der Bildungseinrichtung bzw. des Trägers