

Heinrich-von-Kleist-Schule

Fiktives Fallbeispiel

Kooperative Gesamtschule des Wetteraukreises

Schulleitung: Dr. Elena Weber

Schulstraße 1

61169 Friedberg



Rechtlicher Hinweis:

Dieses Dokument wurde automatisiert mit dem Schulnetz-KI-Lotsen **DAVi** erstellt und dient zur Unterstützung der Dokumentationspflichten.

Weitere Informationen unter:

schulnetz-ki.cloud-atlas.org

Session-ID: DAVI-20261120-HVK-X89

(Fiktives Fallbeispiel)

Heinrich-von-Kleist-Schule · Schulstraße 1, 61169 Friedberg

Der Hessische Beauftragte für Datenschutz
und Informationsfreiheit (HBDI) Postfach

31 63

65021 Wiesbaden

Fiktives Fallbeispiel

Aktenzeichen Schule

HVK-WETTERAU-2026-N14

Zustellung

auf dem Postweg

Datum

Friedberg, den 20.11.2026

Meldung gem. Art. 33 DSGVO / Vorlage DSFA-Zusammenfassung

**IT-Notfallmigration und Dokumentation der Technisch-Organisatorischen
Maßnahmen (TOMs)**

Mandant: Heinrich-von-Kleist-Schule, Wetteraukreis

Sehr geehrte Damen und Herren,

hiermit legen wir die exekutive Zusammenfassung unserer Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO vor. Die Prüfung wurde infolge einer erforderlichen Notfallmigration unserer IT-Systeme durchgeführt.

1. Strukturdaten der Bildungseinrichtung

Zur sachgerechten Einordnung der Verarbeitungstätigkeiten fassen wir die strukturellen Kerndaten unserer Einrichtung wie folgt zusammen:

**Fiktives
Fallbeispiel**

Mail: direktion@hvk-wetterau.de

Tel.: 06031 / 555-0

Kategorie	Spezifikation
Schultyp	Kooperative Gesamtschule
Schulträger	Wetteraukreis
Anzahl der Schülerinnen und Schüler	1.240 (minderjährig, vulnerable Personengruppe)
Lehrkräfte und Verwaltungspersonal	95
Digitale Endgeräte	1.240 Apple iPads (10. Gen., Modell 2025), schuleigentumsfinanziert und zentral verwaltet (1:1-Ausstattung)

2. Auslösendes Ereignis: Notfallmigration (Art. 32 Abs. 1 lit. c DSGVO)

Am Wochenende des 14./15. November 2026 verursachte ein Leitungswasserschaden (ca. 8.000 Liter) im Kellergeschoss den irreparablen Totalausfall unserer lokalen *IServ*-Serverinfrastruktur. Die primären Backupsysteme im selben Raum wurden ebenfalls zerstört.

Um die gesetzliche Schulpflicht (§ 83 HSchG) aufrechtzuerhalten und die Verfügbarkeit der personenbezogenen Daten gemäß Art. 32 Abs. 1 lit. c DSGVO schnellstmöglich wiederherzustellen, wurde am 16. November 2026 eine unmittelbare Migration in die *IServ Hosted Cloud* vollzogen. Das Rechenzentrum des Betreibers befindet sich in Frankfurt am Main und ist nach ISO/IEC 27001 zertifiziert. Der Datenbestand konnte durch ein verschlüsseltes, externes Offline-Backup des IT-Administrators verlustfrei wiederhergestellt werden.

3. Technische Infrastruktur und Dienste-Trennung

Als Ergänzung zur Schulplattform wird *Google Workspace for Education* als Kollaborationsumgebung genutzt. Die Konfiguration orientiert sich strikt an den Vorgaben der Datenschutzkonferenz (DSK) sowie den aktuellen SIVON/SURF-Verifizierungsberichten (2024):

- **Beschränkung auf Kerndienste:** Es sind ausschließlich die vertraglich durch einen Auftragsverarbeitungsvertrag (AVV) abgedeckten Kerndienste aktiviert (Google Classroom, Drive, Docs, Gmail). Der Datenstandort ist fest auf die Europäische Union limitiert (*EU Data Region Policy*).
- **Deaktivierung von Zusatzdiensten:** Sämtliche Google-Zusatzdienste, die nicht der strengen AVV-Bindung unterliegen (z.B. YouTube, Google Maps), sind für die Konten der Schülerschaft auf Administrationsebene gesperrt.
- **Sperrung Generativer KI:** Der Zugang zum KI-System *Gemini* ist für alle minderjährigen Nutzer standardmäßig und unveränderlich deaktiviert. Ein Abfluss von Schülerdaten als Trainingsdaten für Sprachmodelle ist technisch und vertraglich ausgeschlossen.

4. Endgerätesicherheit via Mobile Device Management (MDM)

Die 1.240 digitalen Endgeräte (iPads) sind über das schuleigene Mobile Device Management (MDM) von *IServ* gekapselt. Die Konfiguration der eingesetzten Apps (insbesondere der Notizen-App *Goodnotes*) erfolgt zentral über vorgegebene Skripte (.plist-Dateien), um das Prinzip des *Privacy by Default* (Art. 25 DSGVO) zu gewährleisten:

- **Unterbindung von Drittanbieter-Clouds:** Datensynchronisationen mit Apple iCloud, Google Drive oder Microsoft OneDrive sind auf Geräteebeke blockiert (iCloudAllowed: false). Backups dürfen technisch ausschließlich auf die schuleigenen Server via WebDAV erfolgen.
- **Deaktivierung von Audioaufnahmen:** Die geräteinternen Diktier- und Aufnahmefunktionen innerhalb der Lern-Apps sind gesperrt (AudioRecording: false), um das nicht autorisierte Aufzeichnen des Unterrichts auszuschließen.
- **Lokale Datenverarbeitung:** Cloudbasierte Rechen- und Rechtschreibhilfen sind deaktiviert. Die Verarbeitung erfolgt ausschließlich lokal auf dem jeweiligen Endgerät (On-Device).

5. Zusammenfassung der Risikobewertung

Der Wechsel in eine professionell betriebene, zertifizierte Cloud-Infrastruktur hat die Ausfallsicherheit im Vergleich zum bisherigen On-Premise-Betrieb im Schulkeller signifikant erhöht. Durch die strikte Deaktivierung von Zusatzdiensten und generativer KI in der Google-Umgebung sowie die harten, Code-basierten Einschränkungen auf den Endgeräten durch das MDM wurden sämtliche identifizierten Risiken für die informationelle Selbstbestimmung der Betroffenen auf ein vertretbares Minimum reduziert.

Wir stehen Ihnen für Rückfragen sowie für die Einsichtnahme in die vollständigen Protokolle der Datenschutz-Folgenabschätzung jederzeit zur Verfügung.

Mit freundlichen Grüßen

Dr. Elena Weber
Schulleiterin

Anlage(n):

Anlage 1

MDM-Konfigurationsprofil (XML-Auszug Goodnotes)
Datei: MDM-Konfigurationsprofil-HVK.xml

Anlage 2

SIVON/SURF Verifizierungsbericht (2024)
Datei: SIVON_SURF_Verification_2024.pdf

**Fiktives
Fallbeispiel**