

# INHALTSPRODUKTION MIT APPLE APP

## 1 ALLGEMEINE ANGABEN

### 1.1 Verantwortliche Stelle

Realschule plus und FOS im Einrich Katzenelnbogen

Im Gänsberg 7

56368 Katzenelnbogen

### 1.2 Beschreibung der Verarbeitungstätigkeit

Die Verarbeitungstätigkeit umfasst das allgemeine Erstellen, Arbeiten und Produzieren von Unterrichtsinhalten auf iPad-Geräten mit Anwendungen von Apple durch die Schülerinnen und Schüler sowie Lehrkräfte.

Dabei werden die Inhaltsproduktion, also das Erarbeiten von Unterrichtsinhalten, das Erledigen von Hausaufgaben sowie weiteren Tätigkeiten, mit Apple Apps im Unterrichtskontext oder in schulischen Arbeitsgemeinschaften (AGs) berücksichtigt. Als Apps werden hier die Anwendungen von Apple

- Pages
- Keynote
- Numbers
- Notizen
- iMovie
- Clips
- Freeform
- Safari
- GarageBand
- Kamera
- Photos
- Sprachmemos
- Swift Playgrounds

betrachtet. Die Speicherung der Daten erfolgt auf dem Gerät. Neben üblichen Unterrichtsinhalten oder Inhalten aus schulischen Arbeitsgemeinschaften werden keine Leistungsnachweise in den Anwendungsdaten oder Apps gespeichert.

### 1.3 Zweck der Datenverarbeitung

Inhaltsproduktion auf iPad-Geräten mit Apple Apps im schulischen Kontext. Dies ist notwendig, damit digitale Unterrichtsinhalte auf iPads vorbereitet und erarbeitet werden können.

### 1.4 Rechtsgrundlage

Bei Schulen als „Einrichtungen und sonstigen öffentlichen Stellen des Landes“ i. S. d. § 2 Abs. 1 Nr. 3 Landesdatenschutzgesetz Rheinland-Pfalz:

Art. 6 Abs. 1 S. 1 lit. e), Abs. 3 DS-GVO i. V. m. § 1 Abs. 6 i. V. m. § 67 Abs. 1 Schulgesetz Rheinland-Pfalz (SchulG RLP) und die dazugehörigen Schulordnungen.<sup>1</sup>

## 1.5 Kategorien betroffener Personen

- Nutzerinnen und Nutzer: Schülerinnen und Schüler, Lehrkräfte
- Personen, die von den Nutzerinnen und Nutzern angegeben werden

## 1.6 Kategorien personenbezogener Daten

- Personendaten (Vor- und Nachname)
- Schulische Identifikationsdaten (verwaltete Apple-ID, schulische E-Mail-Adresse, Gruppenzugehörigkeit)
- Schulische Arbeitsergebnisse (Office-Dokumente, Video- oder Tonaufnahmen, Textnachrichten, Fotos, Notizen, Kollagen)
- Logfiles

## 1.7 Kategorien möglicher Empfänger

- Apple (Nutzungs- und Diagnosedaten, die im Hintergrund an Apple versendet werden)<sup>2</sup>
- IT des Schulträgers (im Rahmen der Geräteverwaltung)
- Digitales Kompetenzzentrum/regionale Kompetenzzentren (im Rahmen des Supports zur Geräteverwaltung)

## 1.8 Löschkonzept

Beim Verlassen der Nutzerinnen und Nutzer eines verwalteten iPads des schulischen Kontextes oder des Kontextes des zuständigen Schulträgers erfolgt das Löschen personenbezogener Daten gemäß den Löschkonzepten der Verarbeitungstätigkeiten:

- Administration von verwalteten Apple-IDs und
- Administration von verwalteten iPads.

Bei dem Austausch oder Entzug des zugeteilten iPad-Geräts wird das Gerät über das MDM Jamf School mittels des Schnellaktionsbefehls „Gerät löschen“ gelöscht und dadurch die Daten der Nutzerinnen und Nutzer auf dem Gerät entfernt.<sup>3</sup>

Bei einem Diebstahl oder dem Verlust eines iPads werden die Geräte per Fernzugriff über das MDM vollständig gelöscht.<sup>4</sup>

## 1.9 Auftragsverarbeiter und AVV

Apple Irland als Hosting-Dienstleister der iCloud (AVV muss abgeschlossen sein).

## 1.10 Übermittlung außerhalb EU

Eine Übermittlung durch Apple Irland an Apple Inc. kann nicht ausgeschlossen werden. Apple stellt nach eigenen Angaben sicher, dass jede internationale Datenübertragung nur in ein Land erfolgt, das ein angemessenes Schutzniveau gewährleistet, angemessene

---

<sup>1</sup> So auch die DSK auf S. 4 in ihrer Orientierungshilfe für Online-Lernplattformen im Schulunterricht (Stand: 26.04.2018), [https://www.datenschutzkonferenz-online.de/media/oh/20180426\\_oh\\_online\\_lernplattformen.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf)

<sup>2</sup> <https://www.apple.com/de/privacy/labels/>.

<sup>3</sup> [https://docs.jamf.com/de/jamf-school/documentation/Wipe\\_Device.html](https://docs.jamf.com/de/jamf-school/documentation/Wipe_Device.html) (Abruf Juli 2023).

<sup>4</sup> <https://support.apple.com/de-de/guide/deployment/dep0a819891e/web> (Abruf Juli 2023).

Schutzvorkehrungen gemäß geltendem Recht, z. B. Artikel 46 und 47 der DS-GVO (Standard-Datenschutzklauseln), getroffen hat oder einer Ausnahmeregelung nach Artikel 49 der DS-GVO unterliegt. Solche Schutzvorkehrungen können die von Apple ausgefertigten Mustervertragsklauseln oder andere Datenübertragungsvereinbarungen umfassen.

## 2 ERWEITERTE ANGABEN

### 2.1 Bewertung des Schutzbedarfs

Unter Berücksichtigung der allgemeinen Angaben wird von einem normalen Schutzbedarf ausgegangen.

### 2.2 Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen werden zum Schutz der personenbezogenen Daten getroffen:

- Feste Zuordnung von iPads zu Nutzerinnen und Nutzern über die zentrale Administration von verwalteten iPad-Geräten
- Anmeldung an den iPads mittels Sperrcode (Empfehlung: mindestens 6 Zeichen)
- Vorgaben durch das Bildungsministerium für die Einschränkung der Nutzung und des Funktionsumfangs der iPad-Geräte über Profile.

Auszug:

- *Installation und Entfernen von Apps wird nicht erlaubt*
- *In-App-Käufe werden nicht erlaubt*
- *Siri wird nicht erlaubt*
- *Verwenden des iTunes Store wird nicht erlaubt*
- *Verwenden von Safari wird erlaubt (es greifen weitere Zusatzeinstellungen)*
- *Automatische App-Downloads werden nicht erlaubt*
- *iMessage wird nicht erlaubt*
- *Game Center, Book Store, Apple Music und Apple News werden nicht erlaubt.*
- *Entfernen von System-Apps wird nicht erlaubt.*
- *Senden von Diagnosedaten an Apple wird nicht erlaubt.*
- *Dokumente aus verwalteten Apps in nicht verwalteten Apps [verarbeiten] wird nicht erlaubt.*
- *Dokumente aus nicht verwalteten Apps in verwalteten Apps [verarbeiten] wird nicht erlaubt.*
- *Beschränktes Ad-Tracking wird erzwungen.*
- Änderungen an den vorgegebenen Geräte-Einschränkungen durch die Nutzerinnen und Nutzer sind nicht möglich.
- Aufnahme der zugelassenen Apps in eine Whitelist unter „Positiv und Negativliste“ in Jamf School.
- Sicherheitsmaßnahmen der Apple-Plattform mit Bezug auf „Sicherheit bei Apps“<sup>5</sup>:
  - Freiheit von Schadprogrammen
  - Schutz vor unbefugter Manipulation
  - Strenge Überwachung des Zugriffs auf Benutzerdaten
  - Ausführung der Apps in einer Sandbox

---

<sup>5</sup> <https://support.apple.com/de-de/guide/security/sec35dd877d0/1/web/1> (Abruf Juli 2023).

- Sicherheitsmaßnahmen der Apple-Plattform mit Bezug auf „Verschlüsselung und Datensicherheit“.<sup>6</sup>
  - „Datensicherheit“ auf iPads zur Dateiverschlüsselung mittels AES-256 im XTS-Modus<sup>7</sup>
  - „Data Vault“ auf iPads zur Einschränkung des App-Zugriffs auf Benutzerdaten<sup>8</sup>

Weitere Informationen zu den von Apple getroffenen technischen und organisatorischen Maßnahmen finden sich in den unten aufgeführten Verweisen.<sup>9</sup>

## 2.3 Gefährdungslage

Folgende Gefährdungen müssen grundsätzlich bei der hier beschriebenen Verarbeitung der personenbezogenen Daten berücksichtigt werden:

- Unbefugter Zugang von Benutzerinnen und Benutzern zu fremden iPads, die ihnen nicht zugeordnet sind.
- Verlust des iPad-Geräts und Zugriff durch unbefugte Dritte

## 3 BEWERTUNG DER RECHTMÄSSIGKEIT

Der Einsatz des Verfahrens lässt sich auf Art. 6 Abs. 1 S. 1 lit. e), Abs. 3 DS-GVO i. V. m. § 1 Abs. 6 i. V. m. § 67 Abs. 1 Schulgesetz Rheinland-Pfalz (SchulG RLP) und die dazugehörigen Schulordnungen stützen, solange Folgendes beachtet wird:

- Es werden ausschließlich pädagogische Aufgaben erfüllt.
- Bei Nutzung der iCloud: Es wird eine Kontrolle der Speicherdauer empfohlen, z. B. einmal jährlich, um inaktive Accounts und deren Daten zu löschen, die bis dahin ggf. noch nicht gelöscht wurden.
- Es ist ein AVV mit Apple abzuschließen.
- Eine Nutzungsordnung und Datenschutzhinweise werden erstellt.
- Vor Einführung der Verfahren wird empfohlen, die Vertretung der Schülerinnen und Schüler und der Eltern anzuhören.

---

<sup>6</sup> <https://support.apple.com/de-de/guide/security/sece3bee0835/1/web/1> (Abruf Juli 2023).

<sup>7</sup> <https://support.apple.com/de-de/guide/security/secf6276da8a/1/web/1> (Abruf Juli 2023).

<sup>8</sup> <https://support.apple.com/de-de/guide/security/secc01781f46/1/web/1> (Abruf Juli 2023).

<sup>9</sup> [https://www.apple.com/de/education/docs/Data\\_and\\_Privacy\\_Overview\\_for\\_Schools.pdf](https://www.apple.com/de/education/docs/Data_and_Privacy_Overview_for_Schools.pdf)

<https://support.apple.com/de-de/guide/security/welcome/web>

<https://support.apple.com/de-de/HT208525>

[https://www.apple.com/de/education/docs/Privacy\\_Overview\\_for\\_Parents.pdf](https://www.apple.com/de/education/docs/Privacy_Overview_for_Parents.pdf)

<https://studentprivacypledge.org/privacy-pledge-2-0/>

<https://www.apple.com/legal/education/apple-school-manager/>

<https://www.apple.com/de/privacy/>

<https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-de-ww.pdf>

<https://support.apple.com/de-de/HT202303> (Alle neuen Apple-IDs erfordern die Zwei-Faktor-Authentifizierung)

<https://support.apple.com/de-de/guide/apple-school-manager/welcome/web>

<https://support.apple.com/de-de/guide/deployment-education/welcome/web> (Stand: Juli 2023).

## 4 BEWERTUNG DER RISIKEN

Grundsätzlich handelt es sich bei Verarbeitungen im schulischen Umfeld um „Daten zu schutzbedürftigen Betroffenen“ (z. B. Schülerinnen und Schüler) sowie Lehrerinnen und Lehrer. Bzgl. der Inhaltsproduktion mit Apple Apps muss eine „umfangreiche Verarbeitung von Daten über Kinder“ in die Betrachtung einbezogen werden<sup>10</sup>, aus der Risiken für die Rechte und Freiheiten der Betroffenen gemäß Artikel 35 DS-GVO resultieren könnten. Auch hinsichtlich der Verarbeitung von Nutzungs- und Diagnosedaten durch Apple – vermutlich zur Verbesserung des Dienstes – können Risiken bestehen. Die von der verantwortlichen Stelle unter 2.2 dargestellten und zu ergreifenden technischen und organisatorischen Maßnahmen stellen in der Gesamtschau jedoch effektive Abhilfemaßnahmen für die identifizierten Risiken bei einem Einsatz der beschriebenen Apple Apps dar. Für sämtliche der genannten Risiken werden mehrere Abhilfemaßnahmen umgesetzt, die diese, wie zuvor zu den einzelnen Abhilfemaßnahmen beschrieben, teils erheblich reduzieren. Somit können sämtliche Risiken erheblich verringert und in Anbetracht des in Aussicht gestellten neuen Angemessenheitsbeschlusses der EU-Kommission für transatlantische Datentransfers in die USA auf ein datenschutzrechtlich vertretbares Maß reduziert werden.

---

<sup>10</sup> [https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA - Muss-Liste\\_RLP\\_OE.pdf](https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_OE.pdf).