SYNCHRONISATION DER APPLE APP-DATEIEN ODER APP-METADATEN IN DIE ICLOUD

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 die automatische Synchronisation der auf dem iPad im Schulkontext über Apple Apps erzeugten Dateien oder App-Metadaten in die iCloud.

In den Einstellungen der verwalteten iPads muss für jede App individuell aktiviert sein, dass eine Synchronisation in die iCloud als Speichermedium erfolgen soll. Für folgende Apps wird die Synchronisation der Daten in die iCloud berücksichtigt:

- Pages
- Keynote
- Numbers
- Notizen
- Freeform
- GarageBand

Die Speicherung der Daten erfolgt in dem iCloud-Konto der Benutzerin oder des Benutzers, der mit der verwalteten Apple-ID an dem verwalteten iPad angemeldet ist, von welchem die Synchronisation ausgeht. Die Speicherung der Daten erfolgt in der Cloud auf Serversystemen von Apple.

Die Synchronisation zwischen mehreren Geräten außerhalb der verwalteten iPads ist nicht vorgesehen.

1.3 Zweck der Datenverarbeitung

Synchronisation von Dateien und App-Metadaten in die iCloud. Dies ist aus zwei Gründen notwendig:

- Datensicherung der im Schulkontext angefertigten Unterrichtsinhalte
- Voraussetzung, um mit anderen Schülerinnen und Schülern oder Lehrerinnen und Lehrern Unterrichtsinhalte zu teilen und gemeinsam bzw. kollaborativ an Unterrichtsinhalten zu arbeiten (Betrachtung in separaten Verarbeitungstätigkeiten)

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.[1]

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 (mittels iCloud)
- 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 mittels ASM und
- Administration von verwalteten iPads mittels Jamf School.

1.9 Auftragsverarbeiter und AVV

Apple Irland als Hosting-Dienstleister der iCloud (hierzu muss der ASM -Vertrag abgeschlossen werden).

Die Auftragsverarbeitung des ASM-Vertrags stellt dementsprechend den Rahmen für die Verarbeitung von personenbezogenen Daten durch mit dem Apple School Manager verbundene Dienste dar. Wenn die Schule den Apple School Manager verwendet, um den Zugriff der Schülerinnen und Schüler auf Dienste zu aktivieren, fungiert Apple als Auftragsverarbeiter im Auftrag der Schule. Die Verantwortung und die Kontrolle über die Schülerdaten verbleiben bei der Schule.

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 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-

[1] 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

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:

- Anmeldung am iCloud-Konto mit einer verwalteten Apple-ID, einem Kennwort sowie einem zweiten Faktor. Bei Lehrerinnen und Lehrern und Mitarbeitenden wird der zweite Faktor per SMS über eine von diesen Personen angegebene Telefonnummer übermittelt, bei Schülerinnen und Schülern ist der zweite Faktor ein fester zusätzlicher Code.
- Vorgaben durch das Bildungsministerium für die Einschränkung der Nutzung und des Funktionsumfangs der iPad-Geräte und der iCloud über Profile.

  Auszug:
  - *Sichern in iCloud wird erlaubt.*
  - *iCloud-Dokumente und Daten werden erlaubt.*
  - *iCloud-Schlüsselbund wird nicht erlaubt.*
  - *iCloud-Fotomediathek wird nicht erlaubt.*
  - *Synchronisation verwalteter Apps mit iCloud wird erlaubt.*
  - *Fotostream wird nicht erlaubt.*
  - *Gemeinsamer Fotostream wird nicht erlaubt.*
  - *iCloud Privat Relay wird erlaubt.*
- Zugelassene Apps werden über das MDM festgelegt und verwaltet.
- Die Synchronisation der Daten eines iCloud-Kontos einer verwalteten Apple-ID mit einem nicht verwalteten Gerät ist nicht möglich.
- Aufnahme der zugelassenen Apps in eine Whitelist unter „Positiv und Negativliste“ in Jamf School.
- Sicherheitsmaßnahmen der Apple-Plattform mit Bezug auf „iCloud-Sicherheit“[2]:
  - Verschlüsselte Übertragung der Daten in die iCloud[3]

Weitere Informationen zu den von Apple getroffenen technischen und organisatorischen Maßnahmen finden sich in den unten aufgeführten Verweisen.[4]

---

[2] https://support.apple.com/de-de/guide/security/secacde2d0da/web (Abruf Juli 2023).

[3] https://support.apple.com/de-de/guide/security/secacde2d0da/web (Abruf Juli 2023).

[4] 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

2.3 Gefährdungslage

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

- Unbefugter Zugang zu iCloud-Konten verwalteter Apple-IDs.
- Vergessen der Zugangsdaten zum iCloud-Konto und damit Verlust der Ende-zu-Ende verschlüsselten Daten in der iCloud.
- Synchronisation von Daten in die iCloud, die nicht gemäß der Verarbeitungsbeschreibung vorgesehen sind.

3 BEWERTUNG DER RECHTMÄßSIGKEIT

Der Einsatz des Verfahrens lässt sich zumindest vertretbar 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.
- 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.
- Ein AVV mit Apple ist abzuschließen.
- Eine Nutzungsordnung und Datenschutzhinweise werden erstellt.
- Vor Einführung der Verfahren wird empfohlen, die Vertretung der Schülerinnen und Schüler und der Eltern anzuhören.

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 Synchronisation der Apple App-Dateien oder App-Metadaten in die iCloud muss eine „umfangreiche Verarbeitung von Daten über Kinder“ in die Betrachtung einbezogen werden,[5] 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

---

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).

[5] https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_OE.pdf.

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.