ADMINISTRATION VON VERWALTETEN APPLE-IDS MITTELS APPLE SCHOOL MANAGER

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 Bereitstellung und das Verwalten von Apple-IDs im Schulkontext mit Hilfe des Apple School Managers (ASM). Die verwalteten Apple-IDs werden angelegt und Nutzerinnen und Nutzern zentral über den ASM zugeordnet. Unter den Nutzerinnen und Nutzern werden im schulischen Kontext die Schülerinnen und Schüler, die Lehrkräfte sowie beteiligte Mitarbeitende der Schulen verstanden.

Über den ASM stehen folgende Verwaltungsbereiche zur Verfügung:

- Verwaltung von Standorten
- Verwaltung von Nutzerinnen und Nutzern
- Verwaltung von Klassen und Zuordnung
- Verwaltung der Zugriffsberechtigungen
- Verwaltung von Geräten
- Verwaltung von Apps und Büchern

Über die Benutzerverwaltung können den Nutzerinnen und Nutzern Klassen, Funktionen und ein oder mehrere Standorte zugeordnet werden. Die Klassen entsprechen den Klassen bzw. Kursen aus der jeweiligen Schule. Der Standort bezieht sich auf eine Schule oder auf einen Standort der Schule. Die Funktionen entsprechend den Rollen, welche die Nutzerinnen und Nutzer im Schulkontext einnehmen und dienen der Zugriffsverwaltung im und für das ASM.

Folgende Funktionen stehen im ASM zur Auswahl: „Administratorin/Administrator“, „Standortmanagerin/Standortmanager“, „Personenmanagerin/Personenmanager“, „Geräteregistrierungsmanagerin/Geräteregistrierungsmanager“, „Managerin/Manager“, „Inhaltsmanagerin/Inhaltsmanager“, „Lehrkraft“, „Mitarbeiterinnen/Mitarbeiter“, „Schülerin/Schüler“.

Die Berechtigungen der Funktionsrollen sind in einer beiliegenden Beschreibung dokumentiert.

Die Funktion „Administratorin“ bzw. „Administrator“ besitzt über die Benutzerverwaltung hinaus für jede verwaltete Apple-ID die Möglichkeit, eine sogenannte Kontrolle zu aktivieren und damit über einen temporären Zugang auf das iCloud-Konto der verwalteten Apple-ID zuzugreifen.

1.3 Zweck der Datenverarbeitung

Zentrale Verwaltung von verwalteten Apple-IDs im schulischen Kontext. Dies ist notwendig, damit iPad-Geräte in einem kontrollierten und verwalteten Rahmen zur digitalen Unterrichtsgestaltung eingesetzt 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.[1]

1.5 Kategorien betroffener Personen

- Nutzerinnen und Nutzer: Schülerinnen und Schüler, Lehrkräfte, Mitarbeitende der Schule
- Personen, die an der Administration der Geräte beteiligt sind

1.6 Kategorien personenbezogener Daten

- Personendaten (Vor- und Nachname)
- Schulische Identifikationsdaten (verwaltete, frei wählbare Apple-ID, Zuordnung zu einer Klasse, Funktion/Rolle, Kursanmeldungen, Einrichtung/Standort der zugeordneten Schule, optional: E-Mail-Adresse der Lehrkräfte, ggf. auch weiterer Funktionen oder Rollen)
- Erstellungs- und Änderungsdatum bzgl. des Benutzeraccounts
- Ggf. „Schülerfortschritt“ bzgl. der App Schoolwork, sofern die Schule dies aktiviert (mehr dazu siehe Verarbeitungstätigkeit Nutzung Apple Schoolwork)
- Logfiles sowie Diagnose- und Technikdaten über die Nutzung des Dienstes durch Nutzerinnen und Nutzer (z. B. IP-Adresse sowie Informationen über die Geräte, Browser, System- und Anwendungssoftware und Peripheriegeräte der Nutzerinnen und Nutzer)
- Telefonnummer für Zwei-Faktor-Authentifizierung (nur bei Lehrkräften und Mitarbeitenden der Schule; Einsicht der Telefonnummer über den ASM ist nicht möglich; die Speicherung erfolgt im iCloud-Konto der jeweiligen Benutzerin bzw. des jeweiligen Benutzers)

1.7 Kategorien möglicher Empfänger

- Apple (persönliche Daten der Nutzerinnen und Nutzer zum Bereitstellen und Verbessern des Dienstes für Ausbildungszwecke und zur Einhaltung der anwendbaren Gesetze). Darüber hinaus siehe ASM-Vertrag, S. 24f.[2]
- IT des Schulträgers
- Digitales Kompetenzzentrum/regionale Kompetenzzentren

---

[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

[2] *„Apple nutzt die Daten nicht dazu, Werbung zu erstellen, zu entwickeln, zu betreiben, anzubieten oder zu verbessern. Personalisierte Werbung ist standardmäßig für alle Geräte deaktiviert, die den verwalteten Apple-IDs zugeordnet sind, welche durch den Dienst erstellt wurden. Apple kann nicht persönlich identifizierbare Diagnose-, Technik-, Nutzungsdaten und zugehörige Informationen verwenden, einschließlich, aber nicht beschränkt auf Kennungen, Informationen über Autorisierte Geräte, System- und Anwendungssoftware und Peripheriegeräte sowie Cookies, um den Dienst bereitzustellen und zu verbessern, die Bereitstellung von Softwareupdates, Produktsupport und anderen Features im Zusammenhang mit dem Dienst zu unterstützen, zu Sicherheits- und Accountverwaltungszwecken und um die Einhaltung der Bestimmungen dieses Vertrags zu überprüfen. Apple kann zum Beispiel nicht persönlich identifizierbare Daten über die Nutzung von Schoolwork (die nicht mit einer Verwalteten Apple-ID verbunden ist) durch Ihre Schüler verwenden, um die App bereitzustellen und zu verbessern.“*

1.8 Löschkonzept

Beim Verlassen der Nutzerinnen bzw. Nutzer des schulischen Kontextes oder des Kontextes des zuständigen Schulträgers werden die verwalteten Apple-IDs gelöscht. Entsprechende Informationen werden zwischen den Schulen und den Schulträgern ausgetauscht. Die Löschung der Daten bei Apple erfolgt nach spätestens 30 Tagen automatisch.[3]

Sofern von der Schule oder dem Schulträger der ASM nicht mehr verwendet wird, werden die Schülerdaten spätestens nach 180 Tagen von Apple gelöscht.[4]

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-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:

- Verwendung von generischen Apple-IDs, innerhalb derer keine Klarnamen enthalten sind.
- Keine Verwaltung der Telefonnummern für die Zwei-Faktor-Authentifizierung über den ASM, da die Zwei-Faktor-Authentifizierung über das iCloud-Konto des jeweiligen Benutzenden gesteuert wird.
- Einsatz eines Berechtigungskonzepts für die Zugriffsverwaltung im ASM mit einer Beschreibung der Funktionen und einer Konfigurationsvorgabe für jede Funktion.

---

[3] https://support.apple.com/de-de/HT208525, Abschnitt „Speicherung und Aufbewahrung von Schülerdaten“ 2. Abs. (Abruf: Juli 2023).

[4] https://support.apple.com/de-de/HT208525, Abschnitt „Speicherung und Aufbewahrung von Schülerdaten“ 4. Abs. (Abruf: Juli 2023).

- Die Nutzung der Funktionen ist organisatorisch beschränkt auf:
  - Administratorin/Administrator,
  - Lehrkraft,
  - Schülerinnen und Schüler sowie
  - Mitarbeiterinnen und Mitarbeiter.
- Die Beantragung und die Nutzung der Kontrollfunktion durch die Rolle „Administratorin“ bzw. „Administrator“ wird im ASM protokolliert und ist über die Verwaltung der Standorte auf dem betreffenden Standort nachvollziehbar. Die Nutzung der Kontrollfunktion ist über die Berechtigungen der Funktionen eingeschränkt; für Lehrkräfte ist die Kontrollfunktion deaktiviert. Die Prüfer können nur Accounts überwachen, die in der Hierarchie der Organisation unter ihnen stehen.[5]
- Die Nutzung der Kontrollfunktion ist organisatorisch eingeschränkt:
  A) auf den Einsatz in Disziplinar-Verfahren gegenüber der betroffenen Person und

  B) auf expliziten Kontrollwunsch durch eine aufsichtsberechtigte Person der betroffenen Person oder die betroffene Person selbst.
- Warten von 15 Minuten bei wiederholter Anforderung der Nutzung der Kontrollfunktion.
- Der Grund des Einsatzes wird dokumentiert und kann über die Protokollierung im ASM nachvollzogen werden. Die Protokolle zeigen den Namen der Prüferin oder des Prüfers, die verwaltete Apple-ID, auf die dies Prüferin oder der Prüfer Zugriff angefordert hat, die Uhrzeit der Anfrage und die Angabe, ob die Überprüfung stattgefunden hat oder nicht. Diese Protokolldaten werden von der oder dem Datenschutzbeauftragten der Schule in regelmäßigen Abständen auf Zulässigkeit des Zugriffs geprüft.
- Anmeldung durch alle Rollen (bis auf Schülerinnen und Schüler sowie Mitarbeiterinnen und Mitarbeiter) am ASM mittels Benutzernamen und Kennwort.
- Deaktivierung von „FaceTime“, „iMessage“ „Apple Pay“, „iCloud-Schlüsselbund“, „HomeKit“ und „Wo ist?“ für die verwalteten Apple-IDs in ASM.
- Bei verwalteten Apple-IDs können Schülerinnen und Schüler nicht beliebige Inhalte im App Store, iBooks Store oder iTunes Store erwerben. Apple Pay, Meine Freunde suchen, Mein iPhone suchen, iCloud Mail, HomeKit und iCloud Schlüsselbund sind ebenfalls deaktiviert.[6]
- Deaktivierung der Benutzeraccount-Suche in ASM.
- Beschränkung von „Teilen“ auf innerhalb der Organisation.
- Die Schülerinnen und Schüler erhalten von der Schule die Apple-ID und die Zwei-Faktor-Authentifizierung.
- Für Accounts, die erstmalig importiert oder erstellt werden, erstellt der Apple School Manager temporäre Passwörter. Mit diesen temporären Passwörtern melden sich die Benutzerinnen und Benutzer der Accounts zum ersten Mal mit ihrer verwalteten Apple-ID an. Dabei müssen die Nutzerinnen und Nutzer ihr Passwort ändern. Der Apple School Manager zeigt das von den Schülerinnen und Schülern gewählte Passwort niemals an, sobald das temporäre Passwort ersetzt wurde.

[5] https://support.apple.com/de-de/guide/security/sec049674014/web (Abruf Juli 2023).

[6] https://www.apple.com/de/education/docs/Data_and_Privacy_Overview_for_Schools.pdf.

- Die Apple-IDs setzen Passwörter voraus, die:
  - sechsstellig sein müssen und Zahlen enthalten,
- Apple sendet E-Mails, Push-Benachrichtigungen oder beides an Benutzerinnen und Benutzer, wenn wichtige Änderungen am Account durchgeführt werden, z. B. wenn das Passwort geändert oder die Apple-ID auf einem neuen Gerät für die Anmeldung verwendet wurde. Wenn Benutzerinnen oder Benutzern etwas verdächtig erscheint, sollten sie sofort das Passwort für ihre Apple-ID ändern.
- Beschränkung der Eingabeversuche beim Anmelden oder Zurücksetzen des Passworts sowie eine aktive Betrugsüberwachung.
- Definition der Passwortrichtlinie für die verwaltete Apple-ID durch einen Administrator in ASM.
- iCloud schützt die Benutzerdaten, indem sie verschlüsselt über das Internet gesendet und in verschlüsseltem Format auf dem Server abgelegt werden (mindestens eine 128-Bit AES-Verschlüsselung) und gibt den Verschlüsselungsschlüssel niemals an Dritte heraus. Apple speichert die Verschlüsselungsschlüssel in eigenen Rechenzentren. iCloud speichert Passwörter und Anmeldedaten von Schülerinnen und Schülern so, dass Apple sie weder lesen, noch auf sie zugreifen kann.

Weitere Informationen zu den von Apple getroffenen technischen und organisatorischen Maßnahmen finden sich in den unten aufgeführten Verweisen.[7]

2.3 Gefährdungslage

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

- Fehlerhafte Zuordnung von Funktionen (Rollen) zu Benutzerinnen oder Benutzern und Missbrauch von Zugriffsberechtigungen.
- Missbrauch der Kontrollfunktion durch Administratoren.

[7] 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://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).

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, auch, sofern der „Schülerfortschritt“ aktiviert werden soll.
- Verwendung pseudonymisierter Apple-IDs und ausschließlich Verwendung schulseitig bereitgestellter und datensparsam konfigurierter Endgeräte.
- Es wird eine Kontrolle der Speicherdauer empfohlen, z. B. einmal jährlich, um deaktivierte Accounts und deren Daten zu löschen, die bis dahin ggf. noch nicht gelöscht wurden.
- Der ASM-Vertrag[8], der auch einen AVV enthält, 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,[9] 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.

[8] https://www.apple.com/legal/education/apple-school-manager/ASM-DE-DE.pdf

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