ADMINISTRATION VON VERWALTETEN IPADS MITTELS JAMF SCHOOL

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 Verwaltung von iPad-Geräten im Schulkontext mit Hilfe des MDM Jamf School. Die verwalteten iPads werden zentral vom zuständigen Supporter über Jamf-Benutzer mit verwalteten Apple-IDs zugeordnet.

Über Jamf School stehen folgende Konfigurationsbereiche zur Verfügung:

- Dashboard
- Geräte
- Benutzer
- Klassen
- Vorfälle
- Profile
- Apps
- Dokumente
- Skripte
- Hintergrundbilder
- Organisation

Jamf School ermöglicht als MDM eine zentrale Geräteverwaltung, App-Verwaltung, Benutzerverwaltung und Verwaltung von Konfigurationsprofilen zur Einschränkung der verwalteten iPad Geräte.

Über Jamf School werden die verwalteten iPads Benutzern zugeordnet. Die Zuordnung von Benutzern zu Klassenverbänden ist ebenfalls in Jamf School möglich, soll jedoch bevorzugt über den ASM erfolgen. Zur einfacheren Verwaltung der Geräte werden die iPads in Gerätegruppen zusammengefasst. Es werden die folgenden Gerätegruppen unterschieden:

- Geräte Lehrkräfte
- Geräte Schülerinnen und Schüler

Über die Gerätegruppen werden den zugeordneten verwalteten iPads Apps, Dokumente und Konfigurationsprofile zugewiesen.

Jamf School kommuniziert im Hintergrund mit dem Apple School Manager (ASM) der Schule oder des Schulträgers und synchronisiert den Bestand der im ASM angelegten Benutzer und der verwalteten iPad-Geräte.

1.3 Zweck der Datenverarbeitung

Zentrale Geräte-, App-, Benutzer- und Profilverwaltung von iPad-Geräten im schulischen Kontext mittels MDM. Dies ist notwendig, damit iPad-Geräte zur digitalen Unterrichtsgestaltung zentral kontrolliert und verwaltet 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

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

1.6 Kategorien personenbezogener Daten

- Personendaten (Vor- und Nachname)
- Schulische Identifikationsdaten (E-Mail-Adresse, Gruppenzugehörigkeit)
- Logfiles

1.7 Kategorien möglicher Empfänger

- Jamf (möglicherweise Nutzungs- und Diagnosedaten, die im Hintergrund an Jamf versendet werden.)
- IT des Schulträgers
- Digitales Kompetenzzentrum/regionale Kompetenzzentren

1.8 Löschkonzept

Beim Verlassen der Nutzerinnen und Nutzer des schulischen Kontextes oder des Kontextes des zuständigen Schulträgers, werden die verwalteten Apple-IDs im Apple School Manager gelöscht. Entsprechende Informationen werden zwischen den Schulen und den Schulträgern ausgetauscht. Durch die Synchronisation zwischen Jamf School und ASM werden die Löschungen der Benutzerdaten an das MDM übertragen und dort übernommen. Die Benutzerdaten und die Zuordnungen der Benutzerinnen und Benutzer zu den verwalteten iPad-Geräten werden damit gelöscht.

Sofern eine Löschung des Geräts (bspw. bei Rückzug eines Geräts) notwendig ist, eine Löschung der verwalteten Apple-ID jedoch nicht erfolgt, kann über Jamf School der Schnellaktionsbefehl „Gerät löschen“ durchgeführt werden.[2]

Bei einem Diebstahl oder dem Verlust eines iPads werden die Geräte per Fernzugriff über das MDM vollständig gelöscht.[3]

Eine direkte Löschung der Benutzerdaten über Jamf School ist nicht vorgesehen.

---

[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] https://docs.jamf.com/de/jamf-School/documentation/Wipe_Device.html (Abruf Juli 2023).

[3] https://support.apple.com/de-de/guide/deployment/dep0a819891e/web (Abruf Juli 2023).

1.9 Auftragsverarbeiter und AVV

JAMF Software, LLC als Hosting-Dienstleister der JAMF-Cloud (AVV muss abgeschlossen sein).

Der AVV ist bei privacy@jamf.com anzufragen.

Nach Prüfung sieht JAMF Folgendes vor: JAMF ist eine E-Mail-Adresse zu nennen, an die der AVV seitens JAMF mittels DocuSign geschickt wird.

Jamf behält sich vor, statistische, Nutzungs-, Konfigurations- und Leistungsdaten der Dienste zu erfassen, um die Leistung, Integrität und Stabilität der Dienste zu überwachen.[4]

1.10 Übermittlung außerhalb EU

Eine Übermittlung außerhalb der EU kann nicht ausgeschlossen werden[5], da es sich um einen US-amerikanischen Anbieter handelt. Jamf hält sich nach eigenen Angaben[6] an die Standard Contractual Clauses (SCC) als Mittel zur Datenübertragung.

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 mittels Benutzername und Kennwort.
- Zentrale Verwaltung von Jamf School über den Schulträger.
- Verwaltung der Geräte nicht personenbezogen, sondern über Gerätegruppen.
- Konfigurationsvorgabe für die administrative Konfiguration von Jamf School durch das Bildungsministerium.
- Verschlüsselung der Kommunikation zwischen Jamf School und verwalteten Geräten mittels TLS 1.2.[7]
- Verschlüsselung der Jamf School Datenbank im Ruhezustand mittels AES-256 Bit, einschließlich Protokolle, Backups und Snapshots.[8]
- Durchführung von automatisierten Penetrationstests und Schwachstellenprüfung für Jamf School vor jeder Veröffentlichung sowie jährliche Penetrationstest und Schwachstellenbewertungen durch externe Sicherheitsberaterinnen oder -berater.[9]

---

[4] https://www.jamf.com/de/privacy-policy/ (Abruf: Juli 2023).

[5] https://www.jamf.com/jamf-subprocessors/ (Abruf: Juli 2023).

[6] https://www.jamf.com/de/trust-center/privacy/ (Abruf: Juli 2023).

[7] https://docs.jamf.com/de/security/jamf-School-security-overview/Communication_Encryption_Jamf_Pro.html und https://www.jamf.com/de/trust-center/information-security/ (Abruf: Juli 2023).

[8] https://docs.jamf.com/de/security/jamf-School-security-overview/Database_Encryption_in_Jamf_School.html und https://www.jamf.com/de/trust-center/information-security/ (Abruf: Januar 2023).

[9] https://docs.jamf.com/de/security/jamf-School-security-overview/Vulnerability_Assessments_Jamf_Pro.html (Abruf: Juli 2023).

- Verwaltung der installierten Apps durch die Person mit der Rolle „App-Manager“ im MDM; Schülerinnen und Schüler und Lehrkräfte können keinen eigenen Apps herunterladen, auch keine kostenlosen.
- Vorgaben durch das Bildungsministerium für die Einschränkung der Nutzung und des Funktionsumfangs der iPad-Geräte über Profile.

2.3 Gefährdungslage

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

- Fehlerhafte Zuordnung von Geräten zu Benutzerinnen oder Benutzern
- Fehlerhafte Konfiguration von Einschränkungsprofilen

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.
- Der Jamf-Vertrag, 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

Es handelt sich zwar um „Daten zu schutzbedürftigen Betroffenen“ (z. B. Schülerinnen und Schüler) sowie Lehrerinnen und Lehrer, jedoch liegt bzgl. der Verwaltung der iPads vertretbar keine „umfangreiche Verarbeitung von Daten über Kinder“ vor,[10] aus der hohe Risiken für die Rechte und Freiheiten der Betroffenen gemäß Artikel 35 DS-GVO resultieren.

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