**Datenschutzfolgeabschätzung bei der Einführung von JAMF School als MDM-System**

**Beschreibung der Verarbeitungsvorgänge und -zwecke**

Die erforderlichen Informationen sind im entsprechenden Dokument im VVT der Schule beschrieben.

**Bewertung der Erforderlichkeit und Verhältnismäßigkeit der Verarbeitung im Verhältnis zum Zweck der Verarbeitung**

Eine sachgerechte Erfüllung des Bildungsauftrages und der gegenüber den Schüler:innen bestehenden Fürsorgeaufgaben der Schule ist ohne Einsatz eines MDM-Systems nicht möglich. Nur durch die Möglichkeit der Beschränkung von Gerätefunktionalitäten kann die Einhaltung von z.B. Jugendschutzbelangen innerhalb des Schulgebäudes erreicht werden.

Bei der Durchführung von Prüfungen mit digitalen Endgeräten ist ein MDM zum Erreichen der Chancengleichheit unumgänglich. Der entsprechende Bezugserlass sieht dabei ausdrücklich die Möglichkeit des Einsatzes privat beschafften Endgeräte vor. Der Einsatz eines MDM, welches die Anforderungen des NLQ-Belastungstests erfüllt, ist dabei Voraussetzung für die Durchführung von Prüfungen mit zentraler Aufgabenstellung.

Die MDM-Lösung Jamf School ermöglicht dabei durch die Steuerung per App eine vergleichsweise datensparsame und organisatorisch unkomplizierte Realisierung durch die jeweilige Lehrkraft selbst.

**Risikobewertung**

Der Betrieb eines MDM-Systems ist mit Risiken für die Sicherheit der personenbezogenen Daten der Betroffenen verbunden. Betroffen sind in erster Linie die Schüler:innen und Lehrer:innen. Die betroffenen Datenkategorien sind dem Verzeichnis von Verarbeitungstätigkeiten zu entnehmen.

Konkret besteht das Risiko, dass unbefugte Dritte Zugriff auf die im MDM erfassten Daten nehmen. Insbesondere die Standort- und Logdaten sind hier kritisch zu sehen. Bei einer sachgerechten Bedienung der Software besteht hierfür nur ein geringes Risiko, zumal der Zugriff konzeptionell bedingt nur auf wenige autorisierte Personen beschränkt ist.

Unter Anwendung des Schutzstufenkonzepts der Landesbeauftragten für Datenschutz ist die Schutzstufe C betroffen. Die unsachgemäße Handhabung der personenbezogenen Daten könnte die Betroffenen in ihrer gesellschaftlichen Stellung beeinträchtigen. Deutlich wird dies am Beispiel der Standort- und Logdaten, die Rückschlüsse auf die Lebensumstände von Schüler:innen und Lehrkräften ermöglichen.

Es besteht jedoch nur eine geringe Eintrittswahrscheinlichkeit, da die Betreiberfirma von Jamf School in der geschlossenen Auftragsdatenverarbeitungsvertrag die volle Einhaltung der DS-GVO garantiert. Zudem sind die personenbezogenen Daten durch wirksame technische und organisatorische Maßnahmen vor dem unbefugten Zugriff durch Dritte geschützt.

Im Vergleich zu alternativen Umsetzungen – z.B. über den Apple School Manager und der Classroom-App sind die erforderlichen Daten in ihrem Umfang drastisch reduziert und es bedarf keines zusätzlichen Auftragsdatenverarbeitungsvertrages mit einem weiteren Anbieter.

Es bleibt das Risiko des Zugriff US-amerikanischer Ermittlungsbehörden auf die im MDM erfassten Daten. Diese Daten sind rein technisch jedoch auch auf anderen Wegen beschaffbar, etwa durch personalisiertes biometrisches Benutzertracking (Tipp- und Klickverhalten) auf Basis von JavaScript-Technologien.

Vor diesem Hintergrund ist grundsätzlich zu überlegen, mit pseudonymisierten Datensätzen zu arbeiten. Diese Pseudonyme würden dann in der Teacher Tool App anstelle der Klarnamen angezeigt werden. Lehrkräfte müssten in diesem Fall durch eine entsprechende Verkettungsliste die Pseudonyme auflösen können, um pädagogisch im Rahmen von z.B. binnendifferenziertem Unterricht agieren zu können. Im Rahmen von Prüfungen mit digitalen Endgeräten ist eine namentliche Zuordnung u.U. formal unumgänglich, um z.B. bei Täuschungsversuchen adäquat zu reagieren. Die Verwendung von Klarnamen umgeht diese Schwierigkeiten und ist aus pädagogischer Sicht bei Schüler:innen im Gegensatz zu einer pseudonymen ID eher dazu geeignet, einen bewussten sowie datensensiblen Umgang mit dem Gerät als Arbeitsgerät zu erreichen.

**Technische und organisatorische Maßnahmen zur Bewältigung der Risiken**

Der Einsatz eines MDM-Systems erfordert eine wirksame Beschränkung des zugriffsberechtigten Nutzer:innenkreises. Dies ist durch die prinzipbedingte Begrenzung auf wenige zugriffsberechtigte Personen gegeben, die darüber hinaus über spezifisches technisches Know-How verfügen müssen, um ihrer Aufgabe nachkommen zu können. Der Zugriff auf die Daten erfolgt über eine verschlüsselte Verbindung. Standardmäßig erfolgt eine präzise Erfassung Standortdaten nur, wenn die Geräte administrativ in den Lost-Modus versetzt werden. Die administrativen Zugänge lassen sich durch eine 2-Faktor-Authentifizierung schützen. Die Administrator:innen werden über ihre besondere Verantwortung informiert.

**Ergebnis**

Die Datenschutzfolgeabschätzung kommt zu dem Ergebnis, dass zwar ein Risiko der Schutzstufe C nach dem Schutzstufenkonzept der Landesbeauftragten für Datenschutz besteht, dieses jedoch durch die vorgesehenen technischen und organisatorischen Maßnahmen gut bewältigt werden kann. Da auch die Erforderlichkeit und Verhältnismäßigkeit der Verarbeitung im Verhältnis zum Zweck der Verarbeitung gegeben sind, bestehen nach Vornahme der Datenschutzfolgeabschätzung, keine Bedenken gegen die Einführung von Jamf School als MDM in Kombination mit dem IDM IServ.