Empfehlungen für die Konfiguration und Verwaltung von dienstlich genutzten iPads - iOS/ iPad OS 14

Unter Berücksichtigung von Datenschutz und -sicherheit

Adressaten

Diese Empfehlungen richten sich an Personen, welche iPads als dienstliche Endgeräte für Lehrkräfte an Schulen in NRW einrichten und verwalten: Mitarbeiter aus der IT Abteilung des Schulträgers, Mitarbeiter eines vom Schulträger beauftragten Dienstleisters und in der Schule mit Administrationsaufgaben betraute Lehrkräfte.

Zielsetzung

Mit diesen Empfehlungen soll den Personen, welche iPads als dienstliche Endgeräte für die Verarbeitung von personenbezogenen Daten in der Schule einrichten und verwalten, eine Orientierung gegeben werden, wie sie die von ihnen betreuten Geräte mit Bezug auf die Sicherheit und den Schutz der auf den Geräten verarbeiten personenbezogenen Daten über das von ihnen genutzte Mobile Device Management (MDM)[1] konfigurieren können.

Die hier abgegebenen Empfehlungen sind, genau dieses - **Empfehlungen**. Wo sinnvoll, sind die einzelnen Einschränkungen bzw. Einstellungen mit Erläuterungen versehen. Diese sollen helfen, zu entscheiden, ob und wie Einschränkungen in bestimmten Bereichen gesetzt werden. Es muss letztlich jede Institution für sich entscheiden, wie eng man sich an diese Empfehlungen hält und wo man davon abweichen möchte. Dafür muss abgewogen werden zwischen den geplanten Nutzungszwecken und der damit einhergehenden Verarbeitung von personenbezogenen Daten sowie den sich daraus ergebenden Schutzbedarfen.

Rechtlicher Hintergrund

Im Rahmen der “Richtlinie über die Förderung von dienstlichen Endgeräten für Lehrkräfte an Schulen in Nordrhein-Westfalen” stellen viele Schulträger den Lehrkräften ihrer Schulen iPads als Dienstgeräte zur Verfügung. Diese sollen Lehrkräfte bei der rechtssicheren Verarbeitung von personenbezogenen Daten aus der Schule “*nach den Vorgaben der §§ 120 bis 122 des Schulgesetzes NRW und der Verordnung für die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I) und der Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer (VO-DV II) [...] unterstützen*”.[2] Die dienstlichen Geräte sollen dabei “*den Belangen des Datenschutzes und*

[1] Hinweis: nicht jedes MDM unterstützt alle von iOS zur Verfügung gestellten Einstellungen und Einschränkungen. Diese Empfehlungen orientieren sich an JamfSchool, welches die durch Apple bereitgestellten Möglichkeiten in großem Umfang verwendet.
[2] "BASS 2020/2021 - 11-02 Richtlinie über die Förderung von ...." https://bass.schul-welt.de/19244.htm. Abgerufen 10 Mai. 2021.

der Datensicherheit umfassend Rechnung tragen, insbesondere mit Blick auf die Verarbeitung personenbezogener Daten."[3]

Bei der Einrichtung und Verwaltung von dienstlich genutzten iPads stehen zwei Bereiche im Fokus, Datenschutz und Datensicherheit. Es geht einmal

- um die durch die Lehrkräfte verarbeiteten **personenbezogenen Daten aus der Schule** und dann auch
- um die der **Lehrkräfte als Nutzer** selbst.

Um die Vorgaben zur Verarbeitung von personenbezogenen Daten aus der Schule gemäß dem SchulG NRW, VO-DV I & II sowie allgemeinen datenschutzrechtlichen Grundsätzen einzuhalten, muss sichergestellt werden, dass

- die Verarbeitung sicher ist und
- die verarbeiteten Daten jederzeit verfügbar sind.

Die **Sicherheit der Verarbeitung** wird gewährleistet durch a) den **Zugriffsschutz** und b) die **Verschlüsselung der Daten** auf dem iPad. Während die Verschlüsselung sämtlicher Daten auf dem Gerät im Standard aktiviert ist, muss der Zugriffsschutz durch die Verwaltung vorgegeben oder vom Nutzer selbst aktiviert werden. Die **Verfügbarkeit** wird zum einen durch die Sicherheit der Verarbeitung gewährleistet und zum anderen durch eine **regelmäßige Sicherung** der verarbeiteten Daten außerhalb des Gerätes.

Vorüberlegungen

Grundsätzliches

Ein Gerät - zwei Nutzungszwecke

Die dienstlichen iPads sind gemäß der Richtlinie zur Unterstützung von Lehrkräften bei der rechtssicheren Verarbeitung von personenbezogenen Daten gedacht. Damit ist jedoch nicht nur die Verarbeitung von personenbezogenen Daten im Rahmen der pädagogischen Dokumentation und der schulinternen Verwaltung gemeint. An vielen Schulen sind iPads bereits für pädagogische Zwecke im Einsatz. iPads wurden dort als Dienstgeräte für die Lehrkräfte ausgewählt, um diese iPads auch im Unterricht für pädagogische Zwecke einzusetzen, etwa zur Kontrolle und Steuerung der Schüler iPads über Apple Classroom oder zum Verteilen von Materialien via AirDrop. Bei der Einrichtung und Verwaltung der Geräte sollte dieser Umstand der dualen Nutzung berücksichtigt werden.

Angemessenheit der Maßnahmen

Über Einschränkungen ist es möglich, viele Funktionen von iPads und über iOS[4] und die iCloud mit dem Gerät verbundene Dienste komplett zu unterbinden. Je stärker über das MDM in diese Funktionen eingegriffen wird, umso mehr schränkt dies die Nutzbarkeit des

[3] "Fragen und Antworten zu dienstlichen Endgeräten für Lehrkräfte ...." https://www.schulministerium.nrw/themen/schulpolitik/fragen-und-antworten-zu-dienstlichen-endgeraeten-fuer-lehrkraefte. Abgerufen 10 Mai. 2021.

[4] Wenn in den folgenden Empfehlungen von iOS die Rede ist, meint dieses auch immer iPad OS.

Gerätes ein. Aus diesem Grund ist bei der Einrichtung und Verwaltung der dienstlichen iPads eine Abwägung zu treffen zwischen den für eine Verarbeitung von personenbezogenen Daten erforderlichen Schutzmaßnahmen und den für eine unterrichtliche Nutzung sinnvollen Freiheiten. Dabei ist zu berücksichtigen, dass die Schutzbedarfe auch von den Arten von personenbezogenen Daten, welche eine Lehrkraft verarbeitet, abhängen und zu treffende Schutzmaßnahmen von daher bezüglich der geplanten Nutzung differenziert zu betrachten sind.

Sollen auf einem dienstlichen iPad lediglich Noten verarbeitet werden, Bemerkungen über Schüler, Absenzen, Auswertungen von Klassenarbeiten, von Schülern erstellte Artefakte zur Bewertung und Fotos von Schülern, wie dieses bei einer Fachlehrkraft der Fall ist, dann ist der Schutzbedarf deutlich geringer als bei einer Lehrkraft mit Klassenleitungsfunktion, die auf ihrem iPad die kompletten Zeugnisnoten ihrer Schüler verarbeitet, Bemerkungen zum Sozialverhalten sammelt, Protokolle von Klassenkonferenzen und Beratungsgesprächen anfertigt und Elternanschreiben bezüglich Ordnungsmaßnahmen darauf erstellt. Noch höher ist der Schutzbedarf, wenn eine Person in einer Schulleitungsfunktion ist und über das Gerät Zugriff auf in der Schulverwaltung gespeicherte personenbezogene Daten hat, darauf dienstliche Beurteilungen erstellt und Informationen über Lehrkräfte speichert oder bei einer Förderschullehrkraft, welche auf dem Gerät personenbezogene Daten im Zusammenhang mit AO-SF Verfahren verarbeitet.

Es wird sicher Schulen geben, an welchen dienstliche iPads für alle die oben beschrieben Zwecke eingesetzt werden sollen. Genauso werden andere Schulen aufgrund ihrer technischen Ausstattung in der Lage sein, iPads nur für einen Teil der beschriebenen Zwecke einzusetzen und für die anderen Zwecke auf alternative Geräte der Schule auszuweichen.

Differenzierte Profile

Konfiguration und Verwaltung der dienstlichen iPads sollten sich, wie auch in der FAQ des Ministeriums für Schule und Bildung vorgegeben, immer am geplanten Nutzungszweck der Geräte orientieren. Da Schulträger in der Regel nicht in der Lage sind, auf die Wünsche einer jeden Schule und Lehrkraft einzeln einzugehen, empfiehlt sich die Erstellung von drei Standard Profilen, von denen eines einem normalen Schutzbedarf Rechnung trägt, wie er für die von Fachlehrkräften verarbeiteten personenbezogenen Daten erforderlich ist, einem mit hohem Schutzbedarf, der die von Klassenleitungen verarbeiteten personenbezogenen Daten berücksichtigt, und einem sehr hohen Schutzbedarf, wie er für die von Klassenleitungen mit Schülern mit sonderpädadogischem Förderbedarf, Förderschulpädagogen und Schulleitungsmitgliedern verarbeiteten personenbezogenen Daten bestehen muss. Die Differenzierung in drei Profile ist ein Vorschlag. Vorstellbar wäre sicherlich auch eine Reduzierung auf zwei Profile, von denen eines einem normalen Schutzbedarf Rechnung trägt und das zweite einem mit hohem bis sehr hohem Schutzbedarf.

Technische und organisatorische Maßnahmen balancieren

Einen einhundertprozentigen technischen Schutz kann es nie geben bei der Verarbeitung von personenbezogenen Daten. Dieses sollte bei der Auswahl der Maßnahmen zum Schutz und zur Sicherheit der Verarbeitung von personenbezogenen Daten auf den dienstlichen

iPads berücksichtigt werden. Es ist deshalb sinnvoll, **technische Maßnahmen in Form der Einschränkung** von Funktionen über das MDM mit **organisatorischen Maßnahmen in Form von Verhaltensregeln** (als Nutzungsvereinbarung und/ oder Dienstanweisung) **und Schulungen der Nutzer** zu kombinieren, um größtmöglichen Schutz und Sicherheit bei der Verarbeitung zu erreichen, ohne dabei das Gerät durch technische Einschränkungen in seinen Funktionen zu stark zu beschränken. Dabei kann der Anteil der technischen und organisatorischen Maßnahmen von Schutzstufe zu Schutzstufe unterschiedlich ausfallen.

Adaptabilität von Maßnahmen

Nichts ist in Stein gemeißelt. Das gilt für diese Empfehlungen und es gilt für die technischen und organisatorischen Maßnahmen, auf die man sich letztendlich geeinigt hat und die man dann in die Praxis umsetzt. Schulträger und Schulen müssen bereit sein, diese Maßnahmen nachzujustieren, wenn sich zeigt, dass sie zu rigide sind, über das Ziel hinausschießen, in der Schule nicht alltagstauglich sind oder auch zu lax in einigen Bereichen. Auch wenn die Empfehlungen mit Blick auf Schule und den Alltag in Schule entwickelt wurden, so schauen sie wie vergleichbare Empfehlungen für die Nutzung von iOS Geräten in Wirtschaftsbetrieben und Behörden zuallererst auf die Sicherheit und den Schutz der verarbeiteten Daten. Sie gehen von Bedrohungsszenarien aus, die vielfach übertrieben scheinen, aber die Geräte absichern sollen für den Fall, dass doch etwas passiert, gemessen am Schutzbedarf der darauf verarbeiteten personenbezogenen Daten. Niemand käme auf die Idee, auf die Ausstattung von Autos mit Airbags und Sicherheitsgurten zu verzichten, weil Unfälle insgesamt doch recht selten sind.

Gerade das Anpassen von Einschränkungen in Profilen eines MDM ist wenig aufwändig. Haken werden gesetzt oder entfernt. Es sind Kleinigkeiten, doch sie können enorme Unterschiede machen. Deshalb sollte es nach einer verabredeten Zeit eine **Evaluation** geben, in welcher die Alltagserfahrungen der Lehrkräfte bei der Arbeit mit den verwalteten iPads erhoben werden, um daraus resultierend die Maßnahmen nachzujustieren.

Verarbeitung und Speicherung - auf dem Gerät & online

In NRW schließt die Verarbeitung von personenbezogenen Daten aus der Schule auf einem dienstlichen Endgerät auch die Speicherung auf dem Endgerät selbst mit ein. Anders als in in Niedersachsen, ist eine Speicherung von personenbezogenen Daten auf einem dienstlich genutzten iPad in NRW zulässig[5]. Diesem muss bei der Einrichtung und Verwaltung dieser Geräte (in beiden Bundesländern) Rechnung getragen werden. Entsprechend müssen getroffene Schutzmaßnahmen die Verarbeitung und Speicherung auf dem Gerät selbst berücksichtigen wie auch die Verarbeitung von Daten, welche nicht auf dem Gerät selbst gespeichert werden. Letzteres meint die Verarbeitung in Online Plattformen, auf die entweder über einen Browser zugegriffen wird oder über ein App, welches keine lokale Datenspeicherung vorsieht.

[5] Auf privaten Mobilgeräten mit nicht technisch intervenierbaren Betriebssystemen (iOS, iPadOS, Android, ChromeOS), ist in Niedersachsen die Speicherung dienstlicher Daten untersagt. Diese dürfen lediglich als Zugangsgeräte zu speziell gesicherten Plattformen verwendet werden. Auf Geräten, die durch z.B. den Schulträger extern gemanaged werden, ist eine lokale Speicherung zulässig. Es gibt in Niedersachsen noch keine behördlich abgesicherten Aussagen dazu, wie ein solche abgesicherte Konfiguration gestaltet sein muss.

Risikoszenarien

Bei der Nutzung von dienstlichen iPads muss von mehreren Risikoszenarien ausgegangen werden.

Unbefugter Zugriff auf Daten

Nicht berechtigte Personen erlangen Zugriff auf personenbezogene Daten, welche auf oder über das dienstliche iPad verarbeitet werden. Dieses kann erfolgen, wenn der Zugriff auf das Gerät nicht gesichert ist oder es gelingt, den bestehenden Zugriffsschutz zu überwinden. In Folge können sie

- unbefugt Kenntnis erhalten von diesen Daten,
- Daten stehlen,
- Daten verändern,
- Daten löschen.

Unbefugte Übermittlung von Daten

Eine unbefugte Übermittlung findet statt, wenn auf oder über das Dienstgerät verarbeitete und gespeicherte personenbezogene Daten an Personen oder Dienste übermittelt werden, welche keine Berechtigung dafür besitzen. Dazu gehören:

- die Speicherung von Daten in Clouds, mit denen die Schule keinen Vertrag zur Auftragsverarbeitung abgeschlossen hat,
- die Speicherung in Clouds, deren Nutzung als nicht DS-GVO konform eingestuft wird,
- das Auslesen von Daten vom Gerät durch unbefugte Dritte,
- die Übermittlung von Daten an nicht berechtigte Dienste oder Personen durch Nutzerfehler/ Fehlbedienung

Verlust von Daten

Zu einem Verlust von Daten kann es durch verschiedene Szenarien kommen. Ein Verlust kann entstehen durch

- den Verlust des Gerätes selbst durch Diebstahl oder Fahrlässigkeit des Benutzers, sofern die darauf gespeicherten Daten nicht außerhalb des Gerätes gesichert werden,
- die Zerstörung des Gerätes,
- eine Fehlbedienung des Benutzers,
- unbefugten Zugriff durch Dritte auf
    - das Gerät selbst, wo sie gezielt Daten löschen oder das Gerät komplett zurücksetzen,
    - das Apple Konto des Gerätebenutzers, um es aus der Ferne zurückzusetzen

Schutzgut

Die personenbezogenen Daten, welche auf dienstlichen iPads durch das Personal der Schule verarbeitet werden dürfen, umfassen grundsätzlich sämtliche in VO-DV I & II aufgeführten Daten, sofern diese nicht explizit von einer digitalen Verarbeitung ausgeschlossen sind. Diese Daten lassen sich grob in drei Kategorien einteilen, die sich

durch die Verarbeitungszwecke unterscheiden, und aus denen sich unterschiedliche Schutzbedarfe ergeben. Aus diesen Schutzbedarfen ergeben sich dann die Schutzstufen, anhand derer die erforderlichen Einschränkungen bestimmt werden.

Pädagogische Daten

Hierzu gehören alle personenbezogenen Daten, die im Unterricht entstehen. Es geht dabei vor allem um von Schülerinnen und Schülern erzeugte Artefakte, zugewiesene Aufgaben, erledigte Aufgaben, um Kommunikationsdaten, Kommentare und Feedback, um Tests und Klassenarbeiten.

Schutzbedarf

normal

Pädagogische Dokumentation

Es geht um die personenbezogenen Daten, welche aus der Dokumentation von Schülerleistungen und -verhalten entstehen. Dazu gehören Noten, Auswertungen von Tests, Arbeiten und anderen Diagnoseinstrumenten, Notizen über Schüler, Gutachten, Protokolle von Gesprächen und ähnlich.

Schutzbedarf

normal bis sehr hoch - in Abhängigkeit von den zur Aufgabenerfüllung der Lehrkraft erforderlichen personenbezogenen Daten. Bei

- Fachlehrkräften
    - normal
- Klassenlehrkräften
    - normal bis hoch,
- Klassenlehrkräften mit Schülern mit sonderpädagogischem Förderbedarf
    - normal bis sehr hoch
- Förderschulpädagogen
    - hoch bis sehr hoch
- Schulsozialpädagogen
    - hoch bis sehr hoch

Schulinterne Verwaltung

Zu diesem Bereich gehören alle Daten, die in der Schulverwaltung verarbeitet werden, von den Stammdaten bis zu den Leistungsdaten und Zeugnissen, dem Schriftverkehr mit Erziehungsberechtigten, den Protokollen von Konferenzen, Klassenbüchern und Kursheften mit Absenzen.

Schutzbedarf

hoch bis sehr hoch - in Abhängigkeit von den zur Aufgabenerfüllung der Lehrkraft erforderlichen personenbezogenen Daten. Bei

- Fachlehrkräften
    - normal
- Klassenlehrkräften

    - normal bis hoch,
- Klassenlehrkräften mit Schülern mit sonderpädagogischem Förderbedarf
    - normal bis sehr hoch
- Förderschulpädagogen
    - hoch bis sehr hoch
- Schulsozialpädagogen
    - hoch bis sehr hoch
- Lehrkräften mit Funktionsstellen, die die Verarbeitung der personenbezogenen Daten von vielen Schülern beinhaltet
    - hoch bis sehr hoch
- Mitgliedern der Schulleitung
    - hoch bis sehr hoch

Nutzung von iCloud

iCloud ist ein für Schulen attraktives Angebot. Jeder managed Apple ID stehen 200 GB Online Speicher zur Verfügung, die über digitale Endgeräte und den Browser zugänglich sind. Für Nutzer von managed Apple IDs und privaten Apple IDs stellt iCloud neben dem Online Speicher eine Reihe von weiteren Funktionalitäten für angebundene Endgeräte zur Verfügung. Mit der Anmeldung an einem iOS oder mac OS Gerät wird dieses mit den Diensten der iCloud verbunden. Die auf iPads vorinstallierten System-Apps, die Apple als built-in Apps bezeichnet, synchronisieren ihre Inhalte in der Standardeinstellung automatisch in die iCloud, um sie dem Benutzer auf anderen von ihm genutzten Apple Geräten zur Verfügung zu stellen. Dieses ermöglicht auch die Continuity Funktion, über welche mittels Handoff die Arbeit in einem App wie Notes von einem Apple Gerät, etwa einem iPad, auf einem anderen, z.B. einem Mac, lückenlos fortgesetzt werden kann. Auch die Apple eigenen Apps Pages, Numbers und Keynote, sowie zahlreiche Apps von Drittanbietern unterstützen diese Funktionen.

iCloud ist auch Voraussetzung für die gemeinsame Arbeit verschiedener Nutzer an einem geteilten Dokument (engl. collaboration). Dabei hält iCloud die Eingaben der verschiedenen Mitarbeiter und den gemeinsamen Bearbeitungsstand für alle Mitarbeitenden synchron.

Über iCloud können auch die auf einem Endgerät im Schlüsselbund hinterlegten Nutzerdaten (engl. credentials) für verschiedene Websites, Apps, Wifi-Netzwerke gesichert und mit anderen Geräten des Nutzers synchron gehalten werden.

Apple sichert die Übermittlung und Speicherung von Daten in iCloud im Minimum durch eine starke 128-bit AES Verschlüsselung. Die Schlüssel speichert Apple in gesicherten Datenzentren und sichert zu, diese Schlüssel niemals an Dritte weiterzugeben. Passwörter und Anmeldedaten der schulischen Nutzer werden nach Apples Angaben so gespeichert, dass selbst der Anbieter sie nicht lesen kann.

Viele der Funktionen von iCloud wurden speziell mit Blick auf private Nutzer entwickelt. Sie können in Schule durchaus einen Nutzen haben, bringen jedoch mit Blick auf die Daten, welche auf dienstlichen iPads verarbeitet werden, auch datenschutzrechtliche Risiken mit sich.

Risiken

Für eine Speicherung, Backup und Synchronisation von auf dienstlichen iPads verarbeiteten personenbezogenen Daten sollte iCloud nicht genutzt werden, da aufgrund der aktuellen US amerikanischen Rechtslage nicht auszuschließen ist, dass US Ermittlungsbehörden Zugriff auf diese Daten erhalten. Zwar sichert Apple zu, die Schlüssel, mit welchen diese Daten verschlüsselt gespeichert werden, nicht an Dritte weiterzugeben, doch dieses schließt eine Übermittlung der Inhalte selbst nicht aus, nachdem Apple sie für US Ermittlungsbehörden entschlüsselt hat. Dass Apple Ermittlungsersuchen dieser Art nachkommt, ist aus verschiedenen Fällen der Vergangenheit belegt.

Steuerungsmöglichkeiten

Es gibt zwei Orte, an denen der Zugriff auf iCloud gesteuert werden kann. Über das MDM kann ein Administrator Funktionen der iCloud sowohl für verwaltete als auch nicht verwaltete Apps aktivieren und deaktivieren. Am iPad angemeldete Benutzer können iCloud Funktionen für verwaltete Apps, eigenständig abschalten, solange sie nicht über das MDM deaktiviert wurden. Außerdem können sie diese Funktionen für von ihnen installierte, nicht verwaltete Apps steuern.

Über das MDM ist es möglich,

- die folgenden Funktionen von iCloud für verwaltete und nicht verwaltete Apps zu aktivieren/ deaktivieren
    - “Sichern in iCloud erlauben”
    - “iCloud Dokumente und Daten erlauben” *(erforderlich für Continuity)*
    - “iCloud Schlüsselbund erlauben”
    - “iCloud Fotomediathek erlauben”
    - “Synchronisieren verwalteter Apps mit iCloud erlauben”
    - “Fotostream erlauben”
    - “Gemeinsamen Fotostream erlauben”
- durch Deaktivierung von “*Änderungen der Accounteinstellungen*” die Anmeldung von Nutzern am iPad zu verhindern, wodurch die iCloud deaktiviert bleibt.

Über das MDM ist es nicht möglich,

- die Funktionen von iCloud für System-Apps zu aktivieren/ deaktivieren, wenn iCloud auf dem Gerät aktiv ist.

Über das iPad kann

- eine managed Apple ID die iCloud gezielt für alle System-Apps aktivieren/ deaktivieren,
- eine private Apple ID die iCloud gezielt für alle manuell installierten Apps sowie die System-Apps aktivieren/ deaktivieren,
- eine private Apple ID iCloud Drive aktivieren/ deaktivieren,

sofern iCloud auf dem Gerät durch das MDM zugelassen ist.

Maßnahmen

Verzicht auf Apple IDs

Werden die dienstlichen iPads komplett ohne Apple IDs genutzt, das meint sowohl ohne managed Apple IDs als auch ohne private Apple IDs, dann sind auf dem iPad keine iCloud Funktionen verfügbar. Es können keine personenbezogenen Daten vom dienstlichen iPad in die iCloud abfließen, auch nicht durch Bedienfehler des Benutzers.

Um die Anmeldung am dienstlichen iPad auszuschließen, wird die Einschränkung "*Ändern der Accounteinstellungen (E-Mail. Kontakte, Kalender, iCloud und iTunes Store)*" genutzt. Mit dieser Einschränkung verlieren Nutzer auch die Möglichkeit, eigene Apps zu installieren. Funktionen für den Unterricht, welche eine Verbindung zu Apple Diensten voraussetzen, können nicht genutzt werden.

Bei Nutzung von Apple IDs

Benutzeranmeldung am Gerät

Bei einer Nutzung der dienstlichen iPads mit managed wie auch privaten Apple IDs, wird die iCloud durch die entsprechenden Einschränkungen im MDM für alle verwalteten Apps komplett deaktiviert. Es geht dabei sowohl um den Schutz der auf dem dienstlichen iPad verarbeiteten personenbezogenen Daten wie auch die Daten des Nutzers selbst. Da diese Einschränkungen nicht die System-Apps einschließen, müssen die Lehrkräfte über eine Dienstanweisung angewiesen werden, die iCloud für alle System-Apps manuell zu deaktivieren.

Eingeschränkter Schutz

Soll die iCloud für pädagogische Zwecke genutzt werden, darf die Funktion "iCloud Dokumente und Daten erlauben" nicht deaktiviert sein. Lehrkräfte müssen dann angewiesen werden, iCloud manuell für alle Apps (einschließlich System-Apps) zu deaktivieren, mit denen personenbezogene Daten, die zur pädagogischen Dokumentation und schulinternen Verwaltung gehören, verarbeitet werden. iCloud darf nur bei Apps aktiv bleiben, welche für pädagogische Zwecke benötigt werden.

Nutzeranmeldung am App Store

Ist am Gerät noch keine Apple ID angemeldet und Nutzer melden sich mit einer privaten Apple ID am App Store an, so wird iCloud dabei nicht automatisch mit aktiviert. Es besteht die Möglichkeit, iCloud über einen separaten Dialog zu aktivieren. Solange dieses unterbleibt, sind auf dem Gerät keine iCloud Funktionen verfügbar, weder für die über das MDM installierten Apps, noch für die System-Apps. Nutzer haben die Möglichkeit, eigene Apps zu installieren und zu nutzen, ohne dass diese auf iCloud zugreifen können. Um diese Maßnahme umzusetzen, braucht es eine entsprechende Nutzungsvereinbarung oder Dienstanweisung.

Apps

Mit Blick auf in einem MDM verwaltete dienstliche iPads kann man drei Gruppen von Apps unterscheiden. Über Einschränkungen können die verschiedenen Gruppen angesprochen und in ihren Funktionen gesteuert werden. So ist es unter anderem auch möglich, die Daten von verwalteten und nicht verwalteten Apps von einander getrennt zu halten.

System-Apps

Diese Apps sind auf jedem iOS Gerät im Auslieferungszustand vorhanden. Sie unterscheiden sich von den anderen beiden Gruppen durch höhere Berechtigungen. So zählen sie nicht zu den verwalteten Apps und können dadurch im MDM nicht mit den gleichen Einschränkungen gesteuert werden wie verwaltete Apps. Mit Blick auf iCloud gelten diese Apps als nicht verwaltet und iCloud ist für standardmäßig aktiviert.

Verwaltete Apps (managed Apps)

Diese Apps werden durch die Institution im VPP (Volume Purchase Program) gekauft und über das MDM Geräten oder Nutzern zugewiesen. Bei ihnen greifen alle Einschränkungen des MDM, auch wenn diese nicht speziell als für verwaltete Apps gekennzeichnet sind. Für verwaltete Apps können keine in App Käufe getätigt werden.

Nicht verwaltete Apps (unmanaged Apps)

Von Nutzern einer privaten Apple ID auf einem verwalteten iPad installierte Apps werden als nicht verwaltete Apps bezeichnet. In App Käufe sind hier möglich. Sie unterliegen den Einschränkungen, welche als für verwaltete Apps gekennzeichnet sind, nicht. Diese Einschränkungen können jedoch indirekt auf sie wirken.

Nutzung von Apple IDs

Die Nutzung von managed Apple IDs und/ oder privaten Apple IDs auf einem dienstlichen iPad muss unter verschiedenen Gesichtspunkten betrachtet werden.

Erfordernis

- Um ein Dienst iPad zu verwalten, braucht es weder eine managed Apple ID noch eine private Apple ID.
    - Moderne MDM können iPads als Geräte verwalten und diesen über Profile Apps und Einschränkungen zuweisen.
    - Von Nachteil ist dabei, dass über den **VPP Store keine in App Käufe** getätigt werden können. Apps, die es nicht als Paket gibt, in denen alle in App Käufe bereits enthalten sind, können nur in der oft kostenlosen Basisversion genutzt werden.
- Einige Funktionen, die von iOS bereitgestellt werden, benötigen eine Apple ID.

    - Mit **Apple Classroom** haben Lehrkräfte die Möglichkeit, die iPads der Schüler zu kontrollieren. So können sie beispielsweise den Bildschirm einsehen und iPads in einen Single App Modus versetzen.[6]
        - Werden die Klassen in Apple Classroom über Apple School Manager (ASM) verwaltet, erfordert Apple Classroom zwingend die Nutzung von managed Apple IDs, sowohl bei Lehrkräften wie auch Schülern.
        - Alternativ können die Klassen über das MDM verwaltet werden. Managed Apple IDs sind dann optional. Sind Lehrer mit einer managed Apple ID am Gerät angemeldet, können sie auch die Passwörter von Schülern zurücksetzen, die auf shared iPads angemeldet sind.
        - Alternativ kann Apple Classroom genutzt werden, ohne dass die Klassen über ASM oder das MDM verwaltet werden. Dann dürfen auf den Geräten keine managed Apple IDs angemeldet sein.
    - **Apple Schoolwork** stellt Funktionen für den Unterricht bereit, mit welchen Lehrkräfte Schülern Aufgaben geben und ihre Fortschritte bei der Bearbeitung dieser Aufgaben einsehen können.[7]
        - Zur Nutzung werden bei Schülern und Lehrkräften managed Apple IDs benötigt, die über den ASM der Schule verwaltet und Klassen zugeordnet werden.

- iOS erlaubt die Zusammenarbeit (**Kollaboratives Arbeiten**) an Dokumenten und anderen Inhaltsformaten, wenn die entsprechenden Apps dieses unterstützen.[8] In unterrichtlichen Kontexten ist diese Art der Zusammenarbeit durchaus sinnvoll. Lehrkräfte können so Dokumente bereitstellen, an denen die ganze Klasse mitarbeiten kann.
    - Voraussetzung für die Nutzung der Funktion zur Zusammenarbeit ist iCloud, über welche die von verschiedenen Personen getätigten Bearbeitungen abgeglichen werden. iCloud setzt die Nutzung von managed Apple IDs oder privaten Apple IDs voraus, um andere zur Zusammenarbeit einzuladen. Neben den Apple eigenen Apps wie Pages, Keynote, Numbers und Notes unterstützen auch die Apps einiger Drittanbieter diese Funktionen.

Funktionalität

Ohne Einschränkungen durch das MDM steht managed Apple IDs und privaten Apple IDs die iCloud für verschiedene Funktionen zur Verfügung. Die meisten Prozesse laufen dabei automatisch und für den Nutzer unsichtbar im Hintergrund ab. Auch wenn Nutzer nicht aktiv Inhalte in iCloud speichern, werden viele Inhalte und Metadaten in die iCloud übertragen, über die Backup Funktion, die Funktion zur Zusammenarbeit, die iCloud Speicherfunktion

[6] "App „Classroom“ – Voraussetzungen - Apple Support." https://support.apple.com/de-de/guide/classroom/clac1b9b4dx8/mac. Abgerufen 10 Mai. 2021.
[7] "Voraussetzungen für Schoolwork - Apple Support." https://support.apple.com/de-de/guide/schoolwork-teacher/phxa5a248e65/ios. Abgerufen 10 Mai. 2021.
[8] "Informationen zur Zusammenarbeit in Pages ... - Apple Support." 14 Apr. 2021, https://support.apple.com/de-de/HT206181. Abgerufen 10 Mai. 2021.

wie auch eine Funktion, über welche diese Daten für iCloud und andere Geräte des gleichen Nutzers zur Verfügung gestellt werden (Continuity). Voraussetzung dafür ist, dass Apps diese Funktionen unterstützen. Bei vielen Apps ist das der Fall.

Datenschutz

Mit Blick auf Datenschutz sollten weder Inhalte mit personenbezogenen Daten aus der Schule noch Daten, welche personenbezogene oder -beziehbare Daten des schulischen iPad Nutzers enthalten, in der iCloud verarbeitet und/ oder gespeichert werden. Während es in der Verantwortung der Schule liegt, die personenbezogenen Daten eines Nutzers mit einer schulischen managed Apple ID zu schützen, liegt die Verantwortung für den Schutz und die Sicherheit der eigenen personenbezogenen Daten im Zusammenhang mit der Nutzung einer privaten Apple ID auf einem Dienstgerät beim Benutzer selbst. In der Verantwortung des Benutzers liegt außerdem die Umsetzung der von der Schule vorgegebenen Schutzmaßnahmen zum Schutz der von ihm auf dem Dienstgerät verarbeiteten schulischen personenbezogenen Daten, soweit diese durch die Nutzung einer privaten Apple ID auf dem Dienstgerät zusätzlich erforderlich sind.

Private Apple IDs - Vorteile

Lehrkräfte können

- Apps installieren, die ihnen von der Schule über das MDM nicht bereitgestellt werden.
- Apps installieren, die in App Käufe zulassen und keine VPP Version bieten, die alle diese Extras inkludiert.
- Apps nutzen, die sie bereits privat erworben haben.
- die Funktion zur Zusammenarbeit bei Inhalten nutzen, die keine personenbezogenen Daten enthalten.

Private Apple IDs - Nachteile

Aus Nutzersicht hat die Anmeldung über eine private Apple ID mehr Vorteile als Nachteile. Von vielen Nutzern wird jedoch als Nachteil wahrgenommen, dass sie für privat installierte Apps eigenständig Einstellungen vornehmen müssen, um Datenschutz und -sicherheit für damit verarbeitete personenbezogene Daten (sofern zulässig) zu gewährleisten.

Aus Sicht der Schule ergeben sich zusätzliche Risiken bei der Verarbeitung von personenbezogenen Daten, wenn die Nutzung von privaten Apple IDs zugelassen wird.

Private Apple IDs - Risiken

Risiken können entstehen, wenn der Nutzer sich mit seiner private Apple ID am Gerät anmeldet (und nicht nur am App Store). Ist eine private Apple ID nicht ausreichend abgesichert (schwaches Passwort), können sich Dritte eventuell unberechtigt Zugriff auf die iCloud und Kontoverwaltung der privaten Apple ID verschaffen und darüber

- auf in iCloud gespeicherte bzw. synchronisierte Daten zugreifen,
- auf ein in iCloud gespeichertes Backup zugreifen und dieses auf einem fremden Gerät wiederherstellen und dadurch an auf dem iPad verarbeitete Daten gelangen,

- den Zugriff auf das iPad, die darauf gespeicherten Daten und das Nutzerkonto unterbinden,
- das iPad aus der Ferne löschen.

Risiken können bereits entstehen, wenn der Nutzer sich lediglich am App Store anmeldet, ohne dass ein Nutzer am Gerät angemeldet ist, und zusätzlich die iCloud für sich aktiviert. Diese Risiken entstehen auch, wenn der Nutzer sich direkt am Gerät anmeldet, da er dann auch zum App Store Nutzer wird. Apps, die durch eine private Apple ID installiert werden, unterliegen bezüglich iCloud nicht automatisch den Einschränkungen von verwalteten Apps. Datenflüsse zu anderen mit privat installierten Apps verbundenen Online-Diensten lassen sich nicht durch Einschränkungen steuern. Risiken können entstehen, wenn

- mit diesen nicht verwalteten Apps personenbezogene Daten aus der Schule verarbeitet werden und eine Speicherung in iCloud nicht durch den Nutzer unterbunden wird,
- verwaltete Apps, mit denen personenbezogene Daten verarbeitet werden, Daten an nicht verwaltete Apps weitergeben können, bzw. nicht verwaltete Apps, Zugriff auf die in verwalteten Apps verarbeiteten personenbezogenen Daten haben,
- personenbezogene Daten aus nicht verwalteten Apps an mit diesen verbundene Online-Dienste abfließen.

Eine Quelle weiterer Risiken ist die Installation von Apps, welche die Sicherheit und den Schutz der auf dem Gerät verarbeiteten Daten gefährden,

- wenn sie Schadcode enthalten, der es ihnen ermöglicht, auf von anderen Apps verarbeitete Daten zuzugreifen und sie zu manipulieren, zu löschen oder an Dritte zu übermitteln,
- wenn Benutzer ihnen durch Fehleinschätzungen Berechtigungen geben, welche ihnen Zugriff auf von anderen Apps verarbeitete Daten geben.

Managed Apple IDs - Vorteile

Managed Apple IDs haben Vorteile in zwei Bereichen. Auf der einen Seite sind spezielle Funktionen wie Apple Schoolwork und ein Speicherkontingent von 200 GB in iCloud, die nur managed Apple IDs zur Verfügung stehen. Und auf der anderen Seite sind es Einschränkungen, welchen managed Apple IDs durch iOS unterworfen sind. Diese erhöhen die Sicherheit und reduzieren das Missbrauchspotential. Deshalb können managed Apple IDs im App Store und in iTunes keine Käufe tätigen und es stehen ihnen Dienste wie “Find my” und “Apple Pay” nicht zur Verfügung. Im App Store können sie lediglich verfügbare Apps installieren und aktualisieren, soweit der App Store nicht unterdrückt ist. Der Login an iCloud ist von **jedem Gerät** aus möglich, setzt aber einen sechsstelligen, von der Schule bereitgestellten Bestätigungscode voraus. Dieser Code ist ein Jahr lang gültig. Gibt der User beim Login an einem Browser an, dem Browser zu vertrauen, muss der Bestätigungscode für diesen Browser auf dem Gerät erst wieder eingegeben werden, wenn sich die öffentliche IP ändert. Mit der managed Apple ID, Passwort und Bestätigungscode können Nutzer sich auch an einem nicht-schulischen Apple Gerät anmelden.

Managed Apple IDs - Nachteile

Ähnlich wie bei privaten Apple IDs haben managed Apple IDs ohne entsprechende Einschränkungen vollen Zugriff auf die Funktionen der iCloud (Synchronisation, Backup, Speicherung, Zusammenarbeit). Anders als private Apple IDs können sie weder Apps im App Store kaufen, noch zu vorhandenen Apps in App Käufe tätigen. Eine Ausnahme besteht nur für managed Apple IDs, die über ASM eine Funktion zugewiesen bekommen haben, welche ihnen App Käufe im VPP Store der Schule erlauben. In iCloud ist kein iCloud Mail verfügbar.[9] Ohne Bestätigungscode ist eine Anmeldung in iCloud oder an nicht-schulischen Geräten nicht möglich. Bei schulischen Geräten wird ein Bestätigungscode für die Anmeldung benötigt, sobald sich seine öffentliche IP Nummer ändert. Einschränkungen der iCloud durch das MDM wirken ähnlich wie auch bei Anmeldung mit einer privaten Apple ID nicht auf die System-Apps. Diese nutzen die Funktionen der iCloud, solange die managed Apple ID iCloud nicht manuell für jedes System-App deaktiviert.

Managed Apple IDs - Risiken

Ohne Setzen der entsprechenden Einschränkungen im MDM können von Lehrkräften verarbeitete personenbezogene Daten aus der Schule von allen verwalteten Apps, welche die iCloud Funktionen (Synchronisation, Backup, Speicherung, Zusammenarbeit) unterstützen, in iCloud gespeichert werden. Das gilt auch für die System-Apps, solange der Nutzer der managed Apple ID die iCloud für diese Apps nicht manuell deaktiviert.

Durch die Einschränkungen, welchen managed Apple IDs unterliegen, sind sie auch ohne zusätzliche Maßnahmen etwas besser abgesichert als private Apple IDs. Ein Zugriff auf iCloud und appleid.apple.com (Kontoverwaltung) ist nur mit dem von der Schule vergebenen sechsstelligen Bestätigungscode möglich und die Funktionen von iCloud sind reduziert. Meldet sich eine managed Apple ID über den Browser auf einem beliebigen Computer in iCloud an und speichert dort die Zugangsdaten oder meldet sich nach der Sitzung nicht wieder ordnungsgemäß ab, ist es auch für Dritte möglich, auf die Inhalte der iCloud zuzugreifen, diese herunterzuladen, zu verändern oder zu löschen. Je nach Einstellung auf dem iPad wirkt sich dieses dann auch auf die dort gespeicherten Daten aus.

Unter appleid.apple.com kann das Passwort des Kontos geändert werden. Damit Dritte dieses tun können, benötigen sie neben der managed Apple ID, deren Passwort und den Bestätigungscode, um sich dort anzumelden. Vergisst der Nutzer, sich von appleid.apple.com abzumelden, wird er nach wenigen Minuten Inaktivität automatisch abgemeldet. Ein Löschen des Gerätes über iCloud oder Apple Konto ist für Dritte, die sich unberechtigt Zugang verschafft haben, nicht möglich, da die Funktion “Find my”, die dafür erforderlich ist, für managed Apple IDs nicht zur Verfügung steht.

Empfehlung - Apple IDs

Vielfach steht bei Schulen und Schulträgern die Frage im Raum, ob es Gründe gibt, die gegen eine Nutzung von Apple IDs sprechen. Die Antwort darauf ist kurz - nein. Mit Blick auf den Schutz und die Sicherheit der auf dienstlichen iPads verarbeiteten personenbezogenen Daten spricht zumindest nichts gegen die Nutzung von Apple IDs auf dienstlichen iPads, solange der Nutzer des Gerätes darauf keine personenbezogenen Daten mit sehr hohem

[9] Das Mail App selbst steht Nutzern einer managed Apple ID auf dem iPad zur Verfügung.

Schutzbedarf verarbeitet. Durch geeignete technische und organisatorische Maßnahmen lassen sich Datenabflüsse gut kontrollieren und mögliche Risiken dadurch ausreichend begrenzen. Für die Nutzung von privaten Apple IDs spricht vor allem, dass Lehrkräfte dadurch auch Apps für ihre Arbeit einsetzen können, welche die Schule nicht über VPP bereitstellt. Apps, die in App Käufe erfordern, lassen sich so von Lehrkräften ebenfalls auf den Dienstgeräten nutzen. Aus datenschutzrechtlicher Sicht von Vorteil ist auch, dass die Verarbeitung der im Zusammenhang mit der Nutzung von iCloud anfallenden Nutzerdaten in die Verantwortung der Lehrkraft selbst fällt, da es sich um ein privates Konto handelt.

Anmeldung mit Apple IDs

Bei der Anmeldung an einem iPad ist zwischen zwei Anmeldungen zu unterscheiden, der Anmeldung am Gerät und der Anmeldung am App Store.

Anmeldung am Gerät

Die Anmeldung am Gerät erfolgt über “Einstellungen”. Damit erhält die angemeldete Apple ID automatisch Zugriff auf alle Apple Dienste auf dem Gerät, sofern diese nicht durch Einschränkungen im MDM unterbunden sind. Mit der Anmeldung am Gerät ohne Einschränkungen ist die Apple ID auch direkt an iCloud angemeldet und kann den App Store aktivieren und iTunes.

Eine komplette Deaktivierung der iCloud durch den Nutzer ist bei dieser Art der Anmeldung nur durch ein Abmelden vom Gerät möglich. Alternativ muss die iCloud Einbindung für jedes App einzeln deaktiviert werden. In dem Fall muss der Nutzer auch iCloud Drive und die Backup Funktion manuell deaktivieren.

Anmeldung im App Store und bei iTunes

Keine managed Apple IDs am Gerät angemeldet

Alternativ zur Anmeldung am Gerät über die “Einstellungen” besteht die Möglichkeit, sich mit einer privaten Apple ID direkt am “App Store” anzumelden. Im Unterschied zu einer Anmeldung am Gerät ist in diesem Fall die iCloud noch nicht aktiviert und erfordert eine manuelle Aktivierung durch den Nutzer. Angezeigt werden dazu beim ersten Anklicken des Menüpunkts iCloud die Optionen “Aktivieren” und “Später”. Die Aktivierung ist durch Eingabe eines Passwortes geschützt. Funktionen der iCloud stehen für die vom Nutzer installierten Apps wie auch die System-Apps und verwaltete Apps erst dann zur Verfügung, wenn dieser die iCloud aktiviert. Bis dahin findet kein Datenaustausch dieser Apps mit iCloud statt.

Managed Apple ID bereits am Gerät angemeldet

Eine direkte Anmeldung am App Store ist auch dann möglich, wenn der Nutzer bereits mit seiner managed Apple ID am Gerät angemeldet ist. Die managed Apple ID kann vom App Store dazu abgemeldet werden und der Nutzer meldet sich mit einer privaten Apple ID dort an. Über diese private Apple ID lassen sich dann Apps installieren und kaufen. Durch die managed Apple ID ist die iCloud bereits belegt. Dadurch können die vom Nutzer der privaten Apple ID installierten Apps nicht auf die iCloud Funktionen der eigenen iCloud zugreifen. Bei aktivierter iCloud der am Gerät angemeldeten managed Apple ID ist es jedoch möglich, dass die Daten aus den nicht verwalteten Apps in die iCloud der managed Apple ID synchronisiert

werden, wenn die dafür erforderlichen Einschränkungen (engl. payloads) zugelassen sind. Nutzer sollten deshalb die iCloud für die von ihnen installierten Apps auf jeden Fall deaktivieren. Gleiches gilt für die der managed Apple ID zugeordneten System-Apps. Hier muss die iCloud manuell durch den Nutzer deaktiviert werden. Hinweis: werden in dieser Konstellation von managed Apple ID und privater Apple ID Apps privat installiert, kann das MDM diese zwar in Bezug auf die Berechtigungen für verwaltete und nicht verwaltete Apps unterscheiden, wird aber bei einer Neuinstallation durch das MDM nicht verwaltete Apps "überschreiben" (bzw. in verwaltete Apps umwandeln) und dabei bestehende Inhalte übernehmen.

Um den Abfluss von personenbezogenen Daten in die iCloud zu unterbinden, ist die direkte Anmeldung über den App Store ohne anschließende Aktivierung der iCloud der einfachste Weg, dieses Ziel zu erreichen.

Schutzstufen und Maßnahmen

Ausgehend von den bisherigen Überlegungen empfiehlt es sich, bei der Einrichtung und Verwaltung von dienstlichen iPads von drei verschiedenen Schutzstufen auszugehen, die drei unterschiedlich hohe Schutzziele verfolgen und technische Maßnahmen (Einschränkungen) und organisatorische Maßnahmen (Nutzungsvereinbarung/ Dienstanweisung) sinnvoll kombinieren.

Alle definierten Schutzstufen gehen von einer zusätzlichen Nutzung der dienstlichen iPads für pädagogische Zwecke aus. Sie gehen bis auf die höchste Schutzstufe immer davon aus, dass eine Anmeldung mit einer managed oder privaten Apple ID vorgesehen oder möglich ist.

Schutzstufe - normal

Nutzungszweck

Verarbeitung von personenbezogenen Daten für

- pädagogische Zwecke,
- pädagogische Dokumentation,
- schulinterne Verwaltung (stark eingeschränkt oder gar nicht wie Fachlehrer).

Apple ID

- Private Apple IDs zugelassen.

App Store

- Installation von privat erworbenen Apps und in App Käufe zugelassen.

iTunes Store

- Download und Zugriff auf privat erworbene Inhalte zugelassen.

Technische Maßnahmen

- siehe Kapitel "Technische Maßnahmen"

Organisatorische Maßnahmen

Lehrkräfte erhalten über Nutzungsvereinbarung/ Dienstanweisung folgende Vorgaben:

- In System-Apps (Notes, Kalender, Kontakte, Erinnerungen) dürfen keine personenbezogenen Daten verarbeitet werden.
- In privaten Cloud Speichern (z.B. Dropbox) dürfen keine personenbezogenen Daten aus der Schule gespeichert werden.
- Personenbezogene Daten, die dem Bereich pädagogische Dokumentation zuzurechnen sind, dürfen in privat installierten Apps verarbeitet werden.
- Für privat installierte Apps, in denen personenbezogene Daten aus der Schule verarbeitet werden, muss iCloud deaktiviert werden.
- Regelmäßiges Backup der auf dem iPad verarbeiteten Daten durch den Nutzer mittels einer von der Schule vorgegebenen Lösung.

Schutzstufe - hoch

Nutzungszweck

Verarbeitung von personenbezogenen Daten für

- pädagogische Zwecke,
- pädagogische Dokumentation,
- schulinterne Verwaltung (umfangreicher, z.B. Klassenlehrer oder Stufenleitung).

Apple ID

- Private Apple IDs zugelassen.

App Store

- Installation von privat erworbenen Apps und in App Käufe zugelassen.

iTunes Store

- Download und Zugriff auf privat erworbene Inhalte zugelassen.

Technische Maßnahmen

- siehe Kapitel “Technische Maßnahmen”

Organisatorische Maßnahmen

Lehrkräfte erhalten über Nutzungsvereinbarung/ Dienstanweisung Vorgaben der “Schutzstufe - normal”. Eine Vorgabe wird in abgeänderter Form gegeben:

- Personenbezogene Daten, die dem Bereich schulinterne Verwaltung zuzurechnen sind, dürfen ausschließlich in verwalteten Apps oder von der Schule offiziell genutzten Cloud Plattformen und **nicht** in privat installierten Apps verarbeitet werden.

Schutzstufe - sehr hoch

Nutzungszweck
Verarbeitung von personenbezogenen Daten für

- pädagogische Zwecke,
- pädagogische Dokumentation (auch bezüglich AO-SF Verfahren),
- schulinterne Verwaltung (ohne Einschränkung, auch bezüglich AO-SF Verfahren).

Apple ID
- private Apple IDs nicht zugelassen

App Store
- keine Installation von privat erworbenen Apps und in App Käufe

iTunes Store
- kein Download und Zugriff auf privat erworbene Inhalte

Technische Maßnahmen
- siehe Kapitel "Technische Maßnahmen"

Organisatorische Maßnahmen
Lehrkräfte erhalten über Nutzungsvereinbarung/ Dienstanweisung folgende Vorgaben:

- Eine Anmeldung mit privater Apple ID ist auf dem Dienstgerät nicht zulässig.
- In System-Apps (Notes, Kalender, Kontakte, Erinnerungen) dürfen keine personenbezogenen Daten verarbeitet werden, wenn die Geräte mit einer managed Apple ID ausgegeben werden.
- Die Installation privat erworbener Apps ist nicht zulässig.

Technische Maßnahmen
Folgende technische Maßnahmen müssen zusätzlich über die Einschränkungen umgesetzt sein.

- Sperrung der Möglichkeiten, sich am Gerät oder App Store anzumelden *(Hinweis: von der Deaktivierung von **Ändern der Accounteinstellungen (E-Mail. Kontakte, Kalender, iCloud und iTunes Store)** sind auch Anmeldungen an anderen E-Mail Konten über das Mail App unterbunden.)*
- Deaktivierung des App Stores, so dass dort keine Anmeldung möglich ist.
- siehe außerdem Kapitel "Technische Maßnahmen"

Zuordnung von Schutzstufen

Welches Profil für ein dienstliches iPad erforderlich ist, sollte sich letztlich am geplanten Nutzungszweck orientieren. Eine Schulleitung, die ihr iPad lediglich wie eine Fachlehrkraft einsetzen möchte und nicht beabsichtigt, darauf sensible personenbezogene Daten aus der schulinternen Verwaltung zu verarbeiten, benötigt kein Profil, welches einem sehr hohen Schutzbedarf Rechnung trägt. Gleiches gilt für eine Förderschullehrkraft, die für die

Bearbeitung von personenbezogenen Daten im Zusammenhang mit AO-SF Verfahren ein anderes Endgerät nutzt. Die Zuordnung zu einer Schutzstufe erfolgt anhand der personenbezogenen Daten mit dem höchsten Schutzbedarf, die auf dem Dienstgerät verarbeitet werden sollen.

Beispiele für die Zuordnung von Schutzstufen

Fachlehrkraft - Schutzstufe normal

Verarbeitet werden: Daten zur Erreichbarkeit von Schülern und Erziehungsberechtigten, Kommunikation mit Schülern und Erziehungsberechtigten, Fotos von Schülerinnen und Schülern, von Schülern erstellte Artefakte, Auswertungen von Tests und Klassenarbeiten, Noten, Förderempfehlungen des Faches, Notizen über Schüler, Zuteilung von Aufgaben und Feedback, Absenzen.

Klassenlehrkraft (1) - Schutzstufe hoch

Verarbeitet werden: alle personenbezogenen Daten wie auch durch die Fachlehrkraft und außerdem: Notenlisten für Zeugnisse, Klassenübersichten, Zeugnisse, Protokolle über Elterngespräche und Konferenzen, Elternschreiben zu Ordnungsmaßnahmen (§53 SchulG NRW) und “blaue Briefe.”

Klassenlehrkraft (2) - Schutzstufe sehr hoch

Verarbeitet werden: alle personenbezogenen Daten wie auch durch die Klassenlehrkraft (1) und außerdem: Unterlagen im Zusammenhang mit Durchführung eines AO-SF Verfahrens.

Förderschullehrkraft - Schutzstufe sehr hoch

Verarbeitet werden: alle personenbezogenen Daten wie auch durch die Klassenlehrkraft (1) und außerdem: Unterlagen im Zusammenhang mit Durchführung eines AO-SF Verfahrens, Unterlagen im Zusammenhang mit der Erteilung von Unterricht für Schülerinnen und Schülern mit Förderbedarf.

Schulleitung - Schutzstufe sehr hoch

Verarbeitet werden: alle personenbezogenen Daten wie auch durch die Fachlehrkraft und außerdem: alle personenbezogenen Daten aus der schulinternen Verwaltung von Schülern, Erziehungsberechtigten und Lehrkräften, Beurteilungen, Dienstzeugnisse, disziplinarrechtliche Angelegenheiten, Einstellungsverfahren, Bewerbungen, Kommunikationsdaten mit Personen in der Schule sowie externen Stellen.

Technische Maßnahmen - Einschränkungen - Einstellungen

Alle im folgenden Teil beschrieben Einstellungen/ Einschränkungen gehen immer davon aus, dass eine Apple ID (managed Apple ID und/ oder private Apple ID) auf dem Dienstgerät genutzt wird. Auch wenn eine Anmeldung mit privaten Apple IDs untersagt ist, sollten die Einschränkungen vorgenommen werden, die auch für eine Nutzung mit privaten Apple IDs gelten, um Nutzern, welche sich nicht an die Vorgaben halten, eine missbräuchliche Nutzung zu erschweren.

Die im folgenden beschriebenen Profileinstellungen zur Wahrung des Schutzes und der Sicherheit der auf den dienstlichen iPads verarbeiteten personenbezogenen Daten sind kumulativ zu verstehen. Dem erhöhten Schutzbedarf der Schutzstufen *hoch* und *sehr hoch* wird durch weitere Maßnahmen Rechnung getragen. Für die “Schutzstufe - hoch” gelten auch die Empfehlungen der “Schutzstufe - normal”, sofern dort nicht explizit andere Empfehlungen ausgesprochen werden, die vorherige Empfehlungen aufheben. Entsprechend gelten für die “Schutzstufe - sehr hoch” auch die Maßnahmen der beiden darunter liegenden Stufen.

Aktualität und mögliche Fehler

Die folgenden Empfehlungen zur Konfiguration von iPads mittels eines MDM oder auch Apple Configurator orientieren sich an den Einstellmöglichkeiten und Einschränkungen (engl. payloads) in JamfSchool, welches die von Apple bereitgestellten Möglichkeiten sehr umfassend umsetzt. Bitte beachten Sie, dass sich die Empfehlungen am Stand orientieren, wie er zu dem im Fußteil der Seiten angegeben Datum aktuell war. Mit größeren Updates von iOS/ iPad OS ergeben sich oftmals auch Veränderungen bei den payloads. Neue kommen hinzu, alte verschwinden. JamfSchool kann Fehler bei der Umsetzung haben. Sobald sich größere Änderungen ergeben, spätestens mit der Veröffentlichung einer neuen Version von iOS/ iPad OS, sollte auch dieses Dokument aktualisiert werden. Im Fußteil unten rechts sehen Sie den Versionsstand des Dokuments.

Bei Schutzstufe - normal

Code (Zugriff schützen)

Für Code gibt es einen separaten Konfigurationsbereich, außerhalb von Einschränkungen.

- **Code-Richtlinie durchsetzen**
  - *Code erforderlich*
  - ***(Empfohlen)***
- **Code-Stärke**
  - *Einfachen Wert erlauben*
  - ***(Nicht empfohlen)***
  - *Alphanumerische Werte erforderlich*
  - ***(Empfohlen)***
- **Mindestlänge des Codes**
  - ***(8 Zeichen)***
- **Mindestanzahl komplexer Zeichen**
  - ***(2)***
- **Automatische Sperre (max.)**
  - *Maximale Zeit, die ein Gerät nach Eingabe des Passcodes entsperrt bleibt. Kann vom Nutzer reduziert werden.*
  - ***(5 min)***
- **Code-Gültigkeit (max.)**
  - Zeitraum, *wie lange ein Passcode genutzt werden kann, bevor der Nutzer einen neuen erstellen muss.*
  - ***(1 Jahr)***
- **Code-Verlauf**

    - *Gibt an, nach wie vielen anderen eindeutigen Codes ein einmal genutzter Code erneut genutzt werden kann.*
    - ***(3)***
- **Maximale Nachfrist**
    - Gibt vor, w*ie viel Zeit dem Nutzer bleibt, das Gerät zu entsperren, bevor zum Entsperren erneut der Code angefordert wird.*
    - ***(Sofort erforderlich)***
- **Maximale Anzahl von Fehlversuchen**
    - *Soll im Fall eines Geräteverlusts die Daten schützen, indem nach der maximal angelegten Anzahl von Fehlversuchen (ohne zwischenzeitlich erfolgreiche Logins), alle Daten vom Gerät gelöscht werden.*
    - ***(10)***

Einschränkungen (Zugriff Schützen)

- **Ändern des Codes erlauben**
    - *Nutzer können einen eigenen Code wählen. Die Einstellung ist erforderlich, um alle Code Vorgaben, die Aktionen des Nutzers erfordern, umzusetzen.*
    - ***(Empfohlen)***
- **Touch ID das Entsperren des Geräts erlauben**
    - *Die Nutzung biometrischer Merkmale zum Entsperren des dienstlichen iPads ist vor allem für Lehrkräfte wichtig, die ihr Gerät im Unterricht nutzen und darauf personenbezogene Daten verarbeiten. Damit wird es Schülern erschwert, den Code auszuspähen.*
    - ***(Empfohlen)***
- **Ändern von Touch ID Fingerabdrücken / Face ID Gesichtern erlauben**
    - *Setzt **Ändern des Codes erlauben** voraus.*
    - *Touch ID kann vom Nutzer auch konfiguriert werden für iTunes und App Store Käufe, sowie für andere Apps, die eine Sicherung des Zugriffs mit Touch ID erlauben. Ist das Entsperren des Gerätes mittels Touch ID deaktiviert, sind diese Funktionen trotzdem weiterhin verfügbar.*
    - ***(Empfohlen)***
- **Verwendung eines Passworts beim Erhalt von AirPlay Kopplungsanfragen von diesem Gerät auf anderen Geräten durchsetzen**
    - ***(Empfohlen)***

Einschränkungen (Verfügbarkeit gewährleisten)

- **Verschlüsselte Sicherungen erzwingen**
    - *Auf einem iPad sind die dort gespeicherten Daten automatisch verschlüsselt. Werden manuelle Backups über iTunes auf einem mac OS Computer angefertigt (sofern zugelassen), müssen auch diese verschlüsselt abgelegt werden.*
    - ***(Empfohlen)***
- **Verwenden der Einstellung "Alle Inhalte & Einstellungen löschen" erlauben** unter “Benutzeranpassungen”
    - *Der Nutzer selbst oder Dritte sollten bei einem unbefugten Zugriff nicht alle auf dem iPad befindlichen Daten löschen können.*

        - *Wenn die Einstellung vor Rückgabe eines Gerätes benötigt wird, kann vorab ein Profil aufgespielt werden, in welchem diese Funktion aktiviert ist. Der Nutzer kann dann eigenständig alle Inhalte und Einstellungen seines Leihgerätes löschen.*
    - ***(Nicht empfohlen)***

Einschränkungen (Übermittlung/Abfluss von Daten in iCloud kontrollieren)

Eine Speicherung von personenbezogenen Daten aus der Schule in iCloud ist aus verschiedenen Gründen nicht zulässig. Da iOS nicht unterscheiden kann zwischen personenbezogenen Daten und Daten ohne Personenbezug, betrifft die gewählte Einschränkung immer **alle Daten**.

Eine Speicherung von Daten in bzw. Synchronisation mit iCloud setzt die Anmeldung eines Nutzers mit einer **managed Apple ID** und/ oder **privaten Apple ID** voraus, da iCloud immer nutzerbezogen arbeitet. Solange kein Nutzer an einem Gerät angemeldet ist, werden keine (personenbezogenen) Daten in iCloud gespeichert.

Wichtig!
Einschränkungen der Funktionen von iCloud wirken sich bei Anmeldung eines Nutzers am Gerät **nicht** auf die **System-Apps** (*Kontakte, Kalender, Erinnerungen, Notizen, Safari*) aus! Nutzer der iPads müssen für diese Apps die iCloud jeweils manuell deaktivieren.

- **Sichern in iCloud erlauben**
    - *Wenn zugelassen, kann iCloud-Backup von Nutzern mit privater wie managed Apple ID manuell ein- und ausgeschaltet werden.*
    - *iCloud Drive ist nicht verfügbar, wenn ausschließlich "Sichern in iCloud erlauben" zugelassen ist. Nutzer können so keine Daten aus verwalteten und nicht verwalteten Apps manuell in iCloud sichern.*
    - ***(Nicht empfohlen)***
- **iCloud Dokumente und Daten erlauben**
    - *Wenn zugelassen, können Nutzer mit privater Apple ID die iCloud aktivieren und Inhalte von nicht verwalteten Apps dort ablegen. Für verwaltete Apps ist der Zugriff auf iCloud gesperrt.*
    - *Unverwaltete Apps synchronisieren Inhalte und Metadaten mit iCloud, um diese Daten in iCloud bzw. auf einem anderen Gerät zur Weiterarbeit bereitzustellen. Werden in einer nicht verwalteten App personenbezogene Daten verarbeitet, gelangen diese automatisch in die iCloud.*
        - *Die Einschränkung wirkt sich auch auf verwaltete Apps aus, wenn gleichzeitig **Synchronisieren verwalteter Apps mit iCloud erlauben** zugelassen ist.*
    - ***(Nicht empfohlen)***
- **iCloud Schlüsselbund erlauben**

    - *iOS speichert Passwörter (für Websites, Apps, Clouds, …) in einem Schlüsselbund auf dem Gerät. Mit einer Speicherung in iCloud werden sie auf andere Geräte des Nutzers synchronisiert.*
    - ***(Nicht empfohlen)***
- **iCloud Fotomediathek erlauben**
    - *iCloud wird zum primären Speicherort für mit dem iOS Gerät aufgenommene Fotos und Videos. Eine lokale Kopie wird auf dem Gerät gespeichert, bei Bedarf in reduzierter Auflösung. Fotos und Videos können immer auch personenbezogene Daten enthalten und sollten im schulischen Kontext nicht in iCloud landen.*
    - ***(Nicht empfohlen)***
- **Synchronisieren verwalteter Apps mit iCloud erlauben**
    - *In der Funktion ähnlich wie **iCloud Dokumente und Daten erlauben**, wirkt sich aber nur auf **verwaltete Apps** aus und ermöglicht, dass Inhalte und Einstellungen via iCloud abgeglichen werden, um sie auf einem anderen Gerät des Nutzers bereitzustellen.*
    - *Erlaubt kein aktives Speichern von Daten aus verwalteten Apps in iCloud.*
        - *Setzt "**iCloud Dokumente und Daten erlauben**" voraus.*
    - ***(Nicht empfohlen)***
- **Fotostream erlauben**
    - *Mit der Option Fotostream werden Fotos und Videos der letzten 30 Tage aus der lokalen Mediathek des Fotos App werden automatisch in iCloud geladen, um sie auf anderen Geräten über Fotostream ansehen zu können, ohne dass sie auf das Gerät heruntergeladen werden. Fotos und Videos können immer auch personenbezogene Daten enthalten und sollten im schulischen Kontext nicht in iCloud landen.*
    - ***(Nicht empfohlen)***
- **Gemeinsamen Fotostream erlauben**
    - *iOS ermöglicht es, den eigenen Fotostream mit anderen Nutzern über iCloud zu teilen. Diese können dann geteilte Fotos und Videos über ihr Fotos App ansehen und kommentieren.*
    - ***(Nicht empfohlen)***

Einschränkungen (Übermittlung/Abfluss von Daten kontrollieren - weitere)

- **Dokumente aus verwalteten Apps in nicht verwalteten Apps erlauben**
    - *Unter iOS können Apps untereinander Daten austauschen, entweder über den Teilen Dialog oder teilweise auch über das Dateien App. Vor allem dann, wenn personenbezogene Daten in verwalteten Apps verarbeitet werden, kann eine Verarbeitung dieser Daten in nicht verwalteten Apps ein Risiko darstellen.*
    - *Bei einer kompletten Deaktivierung aller iCloud Funktionen und einer manuellen Deaktivierung der iCloud für System-Apps, sollte das Risiko von Datenabflüssen gering sein. Eine Deaktivierung dieser Funktion würde eine unterrichtliche Nutzung deutlich einschränken.*
    - ***(Empfohlen)***
- **Dokumente aus nicht verwalteten Apps in verwalteten Apps erlauben**

    - *Auch umgekehrt können Risiken entstehen, wenn Daten von nicht verwalteten Apps an verwaltete Apps weitergegeben bzw. von diesen geöffnet werden können, etwa wenn die Lehrkraft die iCloud für dieses App nicht korrekt deaktiviert hat.*
    - *Bei einer kompletten Deaktivierung aller iCloud Funktionen und einer manuellen Deaktivierung der iCloud für System-Apps, sollte das Risiko von Datenabflüssen gering sein. Eine Deaktivierung dieser Funktion würde eine unterrichtliche Nutzung deutlich einschränken.*
    - ***(Empfohlen)***
- **Sichern unternehmenseigener Bücher erlauben**
    - *Auch schuleigene Bücher können verwaltet werden. Solange sie als selbst erstellte Bücher keine personenbezogenen Daten enthalten, können sie in iCloud gesichert werden.*
    - ***(Empfohlen)***
- **Synchronisieren von Notizen und Hervorhebungen in unternehmenseigenen Büchern erlauben**
    - *Notizen und Hervorhebungen in Büchern sind immer personenbeziehbar und können personenbezogene Daten enthalten, die nicht in iCloud landen sollten.*
    - *Eine Synchronisation mit iCloud ist vertretbar, wenn sich die Nutzung auf Unterricht beschränkt und dabei keine personenbezogenen Daten genutzt werden.*
    - ***(Empfohlen)***
- **AirDrop als nicht verwaltetes Ziel behandeln**
    - *Werden personenbezogene Daten in verwalteten Apps verarbeitet, besteht das Risiko, einer versehentlichen Weitergaben an unbefugte Dritte per AirDrop. Mit der Einschränkung kann dieses Risiko ausgeschlossen werden.*
        - *Die Einschränkung der Funktion von AirDrop ist nur verfügbar, wenn AirDrop selbst zugelassen ist (Einstellung - **AirDrop erlauben**), was bei einer unterrichtlichen Nutzung sinnvoll ist. Die Einschränkung ist nur wirksam, wenn auch **Dokumente aus verwalteten Apps in nicht verwalteten Apps erlauben** deaktiviert ist!*
    - *Das Risiko einer Fehlbedienung von AirDrop sollte insgesamt eher gering sein. Werden von Lehrkräften auf dem dienstlichen iPad nur personenbezogene Daten mit einem normalen Schutzbedarf verarbeiten, überwiegen die Vorteile der Funktion die Risiken. Ohne die Funktion könnten auch aus unterrichtlich genutzten verwalteten Apps keine Daten mit Schülern geteilt werden, etwa beim Verteilen von Materialien.*
    - ***(Nicht empfohlen)***
- **Einrichten neuer Geräte in der Nähe erlauben**
    - *Es ist unter iOS möglich, von einem Gerät aus, auf dem ein Nutzer angemeldet ist, ein weiteres Gerät für diesen Nutzer einzurichten. Dieses Gerät unterliegt dann im Fall einer Nutzung mit einer managed Apple ID nicht den Einschränkungen des verwalteten Geräts. (Bei Nutzung mit einer privaten Apple ID könnte der Nutzer ein privates Gerät einrichten.)*
    - ***(Nicht empfohlen)***

- **Fortsetzen von Aktivitäten (Handoff) erlauben**
  - *iOS Geräte lassen es mit einem mit Apple ID angemeldeten Nutzer zu, eine auf dem iPad begonnene Arbeit in einem App auf einem anderen Gerät des Nutzers im gleichen App fortzusetzen und umgekehrt. Wifi und Bluetooth müssen dafür aktiviert sein.*
  - *Risiko: Damit wird es möglich, personenbezogene Daten außerhalb des Dienst iPads zu verarbeiten.*
  - ***(Nicht empfohlen)***
- **Mitteilungszentrale auf Sperrbildschirm anzeigen**
  - *Auf dem Lockscreen lassen sich durch Wischen vom linken Bildschirmrand Informationen des Gerätes wie z.B. Kalendererereignisse, Erinnerungen und E-Mails anzeigen.*
  - *Risiko: Personenbezogene Daten können gegenüber unbefugten Dritten offenbart werden.*
  - ***(Nicht empfohlen)***
- **Ansicht "Heute" auf Sperrbildschirm anzeigen**)
  - *Nutzer können auf dem Sperrbildschirm nach unten wischen, um sich die Heute Informationen anzeigen zu lassen. In der Heute Ansicht können Informationen von vom Nutzer ausgewählten Apps wie Kalender, Erinnerungen, Notizen und anderen Apps, welche die Funktion unterstützen, angezeigt werden. Darunter können auch sensible Informationen sein.*
  - ***(Nicht empfohlen)***
- **Passbook Mitteilungen auf Sperrbildschirm anzeigen**)
  - *Im Zusammenhang mit managed Apple IDs nicht von Belang. Aus Sicherheitsgründen sollte eine Anzeige im Umfeld Schule auch bei privaten Apple IDs nicht erfolgen.*
  - ***(Nicht empfohlen)***
- **Ändern von Mitteilungseinstellungen erlauben**
  - *Nutzer können für einzelne Apps, die Mitteilungen anzeigen können, Ort und Art der Mitteilungen einstellen.*
  - ***(Nicht empfohlen)***
- **AirPrint erlauben**
  - *Drucken auf AirPrint fähigen Druckern, kann durch diese Option vereinfacht werden.*
  - *Sicherheitsrisiken: Je nach Drucker können Inhalte von Druckaufträgen, die personenbezogene Daten enthalten, dauerhaft auf dem internen Speicher des Druckers gespeichert werden. Das ist bei Nutzung von Druckern außerhalb der Schule von Bedeutung.*
  - *Ohne weitere Einschränkungen, kann vom Nutzer auf jedem beliebigen AirPrint fähigen Drucker gedruckt werden.*
  - *Schutzmaßnahme: nur auf Druckern der Schule und dem privaten Drucker zu Hause drucken zulassen.*
  - ***(Empfohlen)***
- **Speichern der Anmeldedaten für AirPrint im Schlüsselbund erlauben**
  - *Die Speicherung erfolgt im iCloud Schlüsselbund. Bei Deaktivierung der iCloud sollte dieses kein Problem sein. Sind Nutzer mit privaten Apple IDs an*

den Dienstgeräten angemeldet werden die Anmeldedaten im privaten Schlüsselbund gesichert.
    - *Risiko: sollte bei jedem Szenario begrenzt sein.*
    - ***(Empfohlen)***
- **Vertrauenswürdiges Zertifikat für TLS-Verbindung mit Druckern erzwingen**
    - *In Schulen dürfte diese Option kaum umzusetzen sein.*
    - *Risiko: sollte in Schulen keine Relevanz haben.*
    - ***(Nicht empfohlen)***
- **Suche nach AirPrint Druckern per iBeacon erlauben**
    - *Deaktivierung soll davor schützen, dass falsche AirPrint-Bluetooth-Beacons den Netzwerkverkehr ausschnüffeln können.*
    - *Risiko: sollte im schulischen Umfeld ohne Relevanz sein.*
    - ***(Empfohlen)***
- **Geräten nur den Beitritt zu WLAN-Netzwerken erlauben, die mit einem Profil konfiguriert wurden**
    - *Ermöglicht es, die Nutzung auf WLAN Netze zu beschränken, die als sicher gelten. Würde jedoch verhindern, dass Nutzer ihr heimisches WLAN nutzen können bzw. erfordern, dass dieses für jeden Nutzer speziell in ein Profil aufgenommen wird.*
    - *In Nutzungsvereinbarung/ Dienstanweisung sollte WLAN Nutzung geregelt sein - keine unsicheren WLAN, öffentliche Hotspots.*
    - ***(Nicht empfohlen)***
- **Nicht vertrauenswürdige TLS-Verbindungen mit Bestätigung erlauben**
    - *Wenn aktiviert, müssen Nutzer bei Verbindungen mit nicht vertrauenswürdigen HTTPS-Zertifikaten, die Verbindung aktiv bestätigen. Bei Deaktivierung werden diese Zertifikate automatisch zurückgewiesen und Verbindungen abgelehnt.*
    - ***(Empfohlen)***
- **Automatische Updates von Einstellungen für vertrauenswürdige Zertifikate erlauben**
    - ***(Empfohlen)***
- **Erstellen von VPN-Konfigurationen erlauben**
    - *Gibt Nutzern die Möglichkeit, sichere Verbindungen zu von der Schule genutzten Servern/ Diensten herzustellen. Wird im Umfeld Schule eher selten genutzt.*
    - *Risiko: sollte deaktiviert werden, wenn Schulen eine VPN-Verbindung für den Zugriff auf ein geschütztes Schulnetzwerk damit absichern wollen.*
    - ***(Empfohlen)***
- **Ändern von Bluetooth-Einstellungen (einschließlich Kopplung neuer Geräte) erlauben**
    - *Erlaubt Nutzern die Kopplung von Tastaturen, Mäusen, Lautsprechern, Kopfhörern, Mikrofonen, ...*
    - ***(Empfohlen)***
- **Zugriff auf USB-Laufwerke in Dateien App erlauben**

    - *Nutzer können über angeschlossene USB Festplatten, CD/DVD Laufwerke und USB Sticks, soweit kompatibel, über das Dateien App auf Daten zugreifen oder diese extern ablegen.*
    - ***(Empfohlen)***
- **Modus für eingeschränkten Zugriff über USB erlauben**
    - *Erlaubt die Kopplung mit USB Geräten auch wenn der Bildschirm gesperrt ist. Die Verbindung bleibt aufrechterhalten, wenn der Bildschirm gesperrt wird. Dieses kann sinnvoll sein, wenn Zubehör am iPad aufgeladen werden soll, etwa ein Stift oder eine Tastatur, die über USB/ Lightning angeschlossen wird.*
        - ***Damit der USB Port auch bei Bildschirmsperre offen bleibt, darf der Haken nicht gesetzt sein!!!** "Erlauben" ist hier im Sinne von Vorschreiben zu verstehen.*
    - ***(Empfohlen)***
- **Koppeln mit anderen Computern erlauben**
    - *Dem iPad kann erlaubt werden, sich mit beliebigen Computern zu verbinden. Zum Herstellen einer Verbindung ist dann noch immer die Eingabe des Code des iPads auf dem entsperrten iPad selbst erforderlich. Danach ist es möglich, auf Inhalte des iPads zuzugreifen und ein Backup des iPads auf dem Computer zu erstellen.*
    - *Wird eine Kopplung nicht zugelassen, lehnt das iPad Kopplungsanfragen ab. Es kann sich nur noch mit dem Computer verbinden, auf dem es ursprünglich mit Apple Configurator 2 (AC 2) konfiguriert wurde. Wurde es über MDM konfiguriert, gibt es diesen Computer nicht. Die Funktion ist von Bedeutung, wenn Einstellungen nicht mehr über das MDM auf ein iPad übertragen werden können.*
    - *Durch das Deaktivieren der Kopplung mit anderen Computern zur Konfiguration über AC 2 wird eine Vielzahl von hardwarebasierten Angriffen auf das Gerät blockiert.*
    - ***(Empfohlen)***
- **Automatisches Einfügen von Passwörtern erlauben**
    - *Die Funktion greift auf iCloud Schlüsselbund zu oder andere Passwort Manager Apps, sofern eingerichtet. Dem Nutzer werden bei Aktivierung in Safari und anderen Apps Passwörter vorgeschlagen.*
    - *Bei Deaktivierung steht auch die Funktion von iOS, dem Nutzer starke Passwörter vorzuschlagen, nicht mehr zur Verfügung.*
    - *Bei Nutzung eines sicheren Passwort Managers sollte die Funktion genutzt werden, da sie die Nutzung sicherer Passwörter erleichtert und dadurch zur Sicherheit insgesamt beiträgt.*
        - **Vor automatischem Einfügen Authentifizierung erforderlich** *muss unbedingt zusätzlich aktiviert werden.*
    - ***(Empfohlen)***
- **Vor automatischem Einfügen Authentifizierung erforderlich**
    - *Um den Missbrauch der Funktion zum automatischen Einfügen von Passwörtern zu verhindern, muss bei Aktivierung, diese Funktion ebenfalls aktiviert werden.*
    - ***(Empfohlen)***

- **Siri erlauben**
  - *Siri greift zum Umsetzen von Befehlen und Fragen zunächst auf die Ressourcen auf dem Gerät zurück. Reicht dieses nicht aus, greift Siri auf Apple Dienste in der Cloud zu. Das erfolgt mit einer anonymisierten ID, die regelmäßig wechselt.*
  - *Siri kann eine Hilfe für Nutzer mit Einschränkungen sein und sollte dort in Kopplung mit einer privaten Apple ID genutzt werden.*
  - *Risiko: ohne Diktieren ist das Risiko, dass über Siri personenbezogene Daten aus der Schule abfließen eher gering.*
  - ***(Empfohlen)***
- **Siri bei gesperrtem Gerät erlauben**
  - *Die Funktion ist sinnvoll für Nutzer mit entsprechenden Einschränkungen.*
  - *Informationen vom Gerät sollten durch Code geschützt sein, der benötigt wird, bevor Siri hier Antwort gibt. Wenn nicht benötigt, sollte die Funktion zur Sicherheit deaktiviert werden.*
  - ***(Nicht empfohlen)***
- **Serverseitige Protokollierung für Siri erlauben**
  - *Audiodateien werden auf Apple Server geladen, z.B. zur Qualitätskontrolle. Dabei können personenbezogene Inhalte dort verarbeitet und Personen potentiell an ihrer Stimme identifiziert werden.*
  - ***(Nicht empfohlen)***
- **Diktierfunktion erlauben**
  - *Es geht hier um die Diktierfunktion, welche ausschließlich Ressourcen nutzt, welche auf dem Gerät selbst verfügbar sind.*
  - ***(Empfohlen)***
- **Diktieren mit Siri verhindern**
  - *Wenn aktiviert, werden die zur Nutzung der Diktierfunktion erforderlichen Daten ausschließlich auf dem Gerät selbst verarbeitet.*
  - *Ohne Deaktivierung kann Siri beim Diktieren auch auf Apple Dienste zugreifen, um die Spracherkennung zu verbessern.*
  - ***(Empfohlen)***
    - *Bei Nutzern mit Einschränkungen muss hier eine Abwägung vorgenommen werden. Diktieren sollte dann nicht für Texte mit personenbezogenen Daten aus der Schule genutzt werden.*
  - ***(Nicht empfohlen)***
- **Verwenden von Safari erlauben**
  - *Die Nutzung von Safari kann zugelassen werden. Die nachfolgenden Einschränkungen sind zu berücksichtigen.*
  - *Nutzer müssen für Safari die iCloud Funktionen manuell deaktivieren.*
  - ***(Empfohlen)***
- **Automatisches Einfügen aktivieren**
  - *Die Deaktivierung verhindert, dass Safari Automatisches Einfügen für Kennwörter, Kontaktinformationen und Kreditkarten nutzt und verhindert auch, dass der Schlüsselbund für Automatisches Einfügen verwendet wird.*
  - *Passwort-Manager von Drittanbietern und Apps, die Automatisches Einfügen verwenden, unterliegen dieser Einschränkung nicht.*

        - *Hinweis: Wird diese Funktion nicht aktiviert, ist auch die Funktion* **Automatisches Einfügen von Passwörtern erlauben** nicht möglich.
        - *Die Funktion darf nur aktiviert werden, wenn* ***Vor automatischem Einfügen Authentifizierung erforderlich*** *zusätzlich aktiviert ist, um bei unbefugtem Zugang zum Gerät Missbrauch zu verhindern.*
    - ***(Empfohlen)***
- **JavaScript aktivieren**
    - *Erlaubt es Safari, JavaScript auszuführen.*
    - ***(Empfohlen)***
- **Deaktivieren des Pop-Up-Blockers durch Benutzer erlauben**
    - *Nutzer können bei Websites, die für ihre Funktionalität Pop-Ups nutzen, die standardmäßig bestehende Blockierung aufheben.*
    - ***(Empfohlen)***
- **Betrugswarnung erzwingen**
    - *Nutzer und Daten auf dem Gerät müssen vor unsicheren Websites geschützt werden. Tracking durch 3rd Party Cookies über Websites hinweg sollte deaktiviert werden und bleiben. Cookies sind für die Funktion von Websites oftmals erforderlich, um Einstellungen zu speichern.*
    - *Es gibt drei Optionen. Die Folgende wird empfohlen.*
    - ***Die Option "Website übergreifendes Tracking verhindern" ist aktiviert und kann vom Benutzer nicht deaktiviert werden. "Alle Cookies blockieren" ist nicht aktiviert.***
    - ***(Empfohlen)***
- **Bildschirmaufnahmen erlauben**
    - *iOS Geräte haben eine Funktion für Bildschirmfotos und -aufnahmen. Diese können ein Sicherheitsrisiko darstellen, da Dritte, denen es gelingt, unbefugt Zugriff auf das Gerät zu erhalten, so Inhalte mit personenbezogenen Daten aufnehmen und übertragen können. (Das wäre zwar auch mittels Abfotografieren/ -filmen möglich, dann jedoch auffälliger.) Die Deaktivierung ist vor allem bei Geräten zu empfehlen, auf denen sehr sensible Daten verarbeitet werden. Ohne solche, kann die Funktion aktiviert werden, um das Aufnehmen von Erklärvideos und ähnlich zu ermöglichen.*
    - ***(Empfohlen)***

Mitteilungen (Übermittlung/Abfluss von Daten kontrollieren - weitere)

Viele Apps sind in der Lage, Mitteilungen zu zeigen, beispielsweise Termine oder Erinnerungen. Je nach App können diese personenbezogene Daten enthalten. Werden diese Mitteilungen auf dem Sperrbildschirm angezeigt, können Dritte diese potentiell zur Kenntnis nehmen. Die unter Einschränkungen bereitgestellten Möglichkeiten reichen nicht aus, um diese Funktion ausreichend zu steuern. Für Mitteilungen gibt es einen separaten Konfigurationsbereich, außerhalb von Einschränkungen. Die Einstellung dort wirken nur auf Mitteilungen von verwalteten Apps und nicht auf von Nutzern privat installierte Apps. Entsprechende Einstellungen müssen von ihnen für jedes App manuell vorgenommen werden.

- **Vorschau anzeigen**

    - *Es kann für jedes App einzeln eingestellt werden, ob es Mitteilungen anzeigen darf und ob dieses auch auf dem Sperrbildschirm erfolgen soll oder ob keine Mitteilungen erfolgen sollen.*
    - *Von den drei Auswahlmöglichkeiten sollte entweder "Nie" oder "Wenn entsperrt" eingestellt werden.*
    - ***(Empfohlen)***
- **Anwendungen auswählen**
    - *Auswahl aller Apps, mit denen personenbezogene Daten verarbeitet werden.*
    - ***(Empfohlen)***
- **Ausgewählte Anwendungen**
    - *Für jede Anwendung muss noch einmal separat ausgewählt werden, ob sie auf dem Sperrbildschirm erscheinen darf oder nicht.*
    - ***(Empfohlen)***

Einschränkungen (Sicherheit des Gerätes)

- **Passwortfreigabe über AirDrop erlauben**
    - *Von einem iOS Gerät aus können Zugangsdaten zu Websites (Nutzername, Passwort und Website) per AirDrop mit Geräten in der Nähe (bis ca. 10m) teilen. Dazu wird eine Verbindung per Bluetooth zwischen den Geräten aufgebaut. Der Datenaustausch erfolgt dann über eine direkte Wifi-Verbindung.*
    - *Die Funktion setzt voraus, dass der Empfänger in den Kontakten des Absenders gespeichert ist. Der Empfänger muss dem Empfang zustimmen und die empfangenen Zugangsdaten werden in seinem Schlüsselbund für automatisches Ausfüllen gespeichert.*
    - *Die Funktion kann auch genutzt werden, um Zugangsdaten an ein App auf einem Apple TV zu senden.*
    - ***(Nicht empfohlen)***
- **Abfrage von Passwörtern auf Geräten in der Nähe erlauben**
    - *Wenn aktiviert, können andere Geräte (iOS/ mac OS/ TV OS) in unmittelbarer Nähe Passwortanfragen an das iPad senden. Damit können unter Umständen andere Sicherheitseinschränkungen umgangen werden.*
    - ***(Nicht empfohlen)***
- **Kontrollzentrum auf Sperrbildschirm anzeigen**
    - *Auf dem Sperrbildschirm kann das Kontrollzentrum angezeigt werden. Je nach Konfiguration können dadurch unter Umständen Sicherheitsrisiken entstehen, etwa weil Dritte Einstellungen verändern können z.B. für AirDrop.*
    - ***(Nicht empfohlen)***

Einschränkungen (Schutz der Konfiguration des Gerätes)

- **Installation von Konfigurationsprofilen erlauben**
    - *Die Konfiguration des iPads wird durch über das MDM aufgespielte Konfigurationsprofile gewährleistet. Sind Nutzer in der Lage, eigene Konfigurationsprofile zu installieren, können diese durch das MDM erzwungene Einstellungen und Einschränkungen außer Kraft setzen.*
    - ***(Nicht empfohlen)***

- **WLAN durchgehend aktiviert lassen**
  - *Verhindert, dass das Gerät nicht mehr über das MDM ansprechbar ist.*
  - ***(Empfohlen)***
- **Ändern des Gerätenamens erlauben**
  - *Wenn der Gerätename verändert werden kann, ist es möglich, dieses als das Gerät eines anderen Nutzers auszugeben, um dadurch an sensible Informationen zu gelangen.*
  - ***(Nicht empfohlen)***
- **Entfernen von System-Apps erlauben**
  - *Die Apps, welche auf auf einem unkonfigurierten iPad im Standard bereits vorhanden sind (System-Apps) können durch Nutzer deinstalliert werden, wenn zugelassen. Dazu gehören u.A. Notizen, E-Mail, Kalender, Erinnerungen. Bei Dienstgeräten sinnvoll, Lehrkräften die Möglichkeit zu geben.*
  - ***(Empfohlen)***
- **Ändern der Accounteinstellungen (E-Mail. Kontakte, Kalender, iCloud und iTunes Store)**
  - *Nutzer können sich mit privaten Apple IDs oder managed Apple IDs am Gerät anmelden und dann weitere E-Mail Adressen und Telefonnummern hinzufügen, die verwendet werden können, um den Nutzer bei iMessage, FaceTime, Game Center usw. zu erreichen, sofern diese Apps zugelassen sind. Das Passwort der (managed) Apple ID kann geändert werden. iCloud kann für die am Gerät angemeldete (managed) Apple ID für die System-Apps einzeln ein- und ausgeschaltet werden.*
  - *Wird diese Option deaktiviert, kann auch der App Store nicht genutzt werden, selbst wenn das App auf dem Gerät ist.*
  - ***(Empfohlen)***
- **Installation von Apps erlauben**
  - *Nutzer, die mit ihrer privaten Apple ID am Gerät oder am App Store angemeldet sind, können privat erworbene Apps installieren. Ist die Einschränkung "App-Installation über den App Store erlauben" deaktiviert, können Nutzer weiterhin Apps in Kopplung mit einem Rechner über iTunes installieren, sofern keine anderen Einschränkungen eine solche Kopplung unterbinden.*
  - ***(Empfohlen)***
- **In-App-Käufe erlauben**
  - *Diese Einschränkung ist nur wirksam, wenn die vorherige zugelassen ist.*
  - ***(Empfohlen)***
- **App-Installation über den App Store erlauben**
  - *Ist die "Installation von Apps erlauben" aktiviert, erscheint mit der Aktivierung dieser Einschränkung das App Store App auf dem Homescreen und der Nutzer kann direkt auf dem dienstlichen iPad auf den App Store zugreifen.*
  - ***(Empfohlen)***
- **Eingabe eines iTunes Store Passworts für alle Einkäufe durch den Benutzer durchsetzen**
  - ***(Empfohlen)***

- **Software-Updates zurückstellen für *15* Tage**
  - *In der Vergangenheit kam es immer wieder vor, dass iOS-Updates fehlerhaft waren und diese Fehler erst nach einigen Tagen bekannt wurden. Um die Sicherheit (und Funktion) des Gerätes und die Verfügbarkeit der darauf gespeicherten Daten zu gewährleisten, sollten Software-Updates um 15 Tage zurückgestellt werden.*
  - *Es ist weiterhin möglich iOS- und App Updates manuell auf dem iPad auszulösen.*
  - *Bei kritischen Sicherheits-Updates sollten diese manuell über das MDM ausgelöst werden.*
  - ***(Empfohlen)***
- **Starten von Geräten im Wiederherstellungsmodus mit einem nicht gekoppelten Gerät, das über ein Lightning Kabel angeschlossen ist, erlauben**
  - *Mit dieser Funktion können iPads, die lediglich über ein MDM eingerichtet wurden, mittels Lightning Kabel mit einem beliebigen Computer gekoppelt werden, um sie in den Wiederherstellungsmodus zu versetzen.*
  - *Bei Geräten, die mit Apple Configurator 2 eingerichtet wurden, ist eine Kopplung mit dem Computer, über den die ursprüngliche Einrichtung erfolgte, weiterhin möglich, wenn die Funktion deaktiviert ist.*
  - *Deaktiviert man diese Funktion, verliert man unter Umständen die Möglichkeit, Geräte, die über das MDM nicht mehr ansprechbar sind, "zu retten."*
  - *Sicherheitsrisiken: im Recovery Modus ist kein Zugriff auf Daten auf dem Gerät möglich, da sämtliche Daten bei diesem Prozess gelöscht werden. Ungesicherte Daten wären dabei jedoch unwiderruflich verloren. Mittels des Recovery Modus könnten Dritte nach erfolglosen Versuchen, sich Zugang zum Gerät zu verschaffen, es wieder in den Ausgangszustand versetzen, um weitere Versuche zu starten.*
  - ***(Nicht empfohlen)***
- **Koppeln mit Apple Watch erlauben**
  - *Über eine Kopplung des dienstlichen Gerätes können Nutzer Nachrichten des Gerätes, direkt auf der Apple Watch empfangen und darauf reagieren. Wird die Funktion zugelassen, **muss** sie jedoch zwingend durch die Handgelenkserkennung abgesichert werden, um Missbrauch der Zugriffsfunktionen zu verhindern.*
  - ***(Empfohlen)***
- **Handgelenkerkennung bei Apple Watch erzwingen**
  - *Sorgt dafür, dass die Funktionen der Apple Watch nur verfügbar sind, wenn sich diese am Handgelenk des Besitzers befindet.*
  - ***(Empfohlen)***
- **Einschränkungen/Bildschirmzeit erlauben**
  - *Nutzer können eigene zusätzliche Einschränkungen definieren.*
  - ***(Empfohlen)***

Einschränkungen (Schutz der Nutzerdaten)

Wenn Nutzer mit managed Apple IDs oder privaten Apple IDs an einem Dienstgerät angemeldet sind, sollten auch die Nutzerdaten nach Möglichkeit geschützt werden.

- **Senden von Diagnosedaten an Apple erlauben**
  - *Es sollten keine Diagnosedaten an Apple gesendet werden, da diese u. U. personenbezogene oder -beziehbare Daten enthalten könnten.*
  - ***(Nicht empfohlen)***
- **Beschränktes Ad-Tracking erzwingen**
  - *Soweit möglich, sollte Tracking durch Werbung unterbunden werden. Die Einschränkung bezieht sich aber vor allem auf Werbung, die nicht im Zusammenhang mit Apple selbst steht.*
  - ***(Empfohlen)***
- **Interessenbezogene Werbung von Apple erlauben**
  - *Apple sollte keine Nutzerdaten verwenden dürfen, um personalisierte Werbung zu erstellen. Falls es Werbung durch Apple gibt, ist diese dann unpersonalisiert.*
  - ***(Nicht empfohlen)***
- **FaceTime erlauben**
  - *Bei Anmeldung mit privaten Apple IDs am dienstlichen iPad fällt die mit der Nutzung verbundene Datenverarbeitung durch Apple in die eigene Verantwortung der Lehrkraft. Eine Nutzung mit dienstlichen Inhalten mit personenbezogenen Daten sollte per Dienstanweisung untersagt werden.*
  - ***(Empfohlen)***
- **iMessage erlauben**
  - *Bei Anmeldung mit privaten Apple IDs am dienstlichen iPad fällt die mit der Nutzung verbundene Datenverarbeitung durch Apple in die eigene Verantwortung der Lehrkraft. Eine Nutzung mit dienstlichen Inhalten mit personenbezogenen Daten sollte per Dienstanweisung untersagt werden.*
  - ***(Empfohlen)***

Nachricht für Sperrbildschirm

- Hier sollte ein Text mit Bitte um Rückgabe des Gerätes an die Schule mit Adresse ergänzt werden.
  - ***(Empfohlen)***

Bei Schutzstufe - hoch

Einschränkungen (Übermittlung/Abfluss von Daten kontrollieren - weitere)

- **Dokumente aus verwalteten Apps in nicht verwalteten Apps erlauben**
  - *Unter iOS können Apps untereinander Daten austauschen, entweder über den Teilen Dialog oder teilweise auch über das Dateien App. Vor allem dann, wenn personenbezogene Daten in verwalteten Apps verarbeitet werden, kann eine Verarbeitung dieser Daten in nicht verwalteten Apps ein Risiko darstellen. Verwaltete Apps sind alle Apps, die über das MDM installiert werden. Nicht verwaltete Apps sind aus dem App Store installierte Apps*

(einschließlich der System-Apps) und Apps die zu manuell auf dem Gerät eingerichteten Konten gehören.
    - *Die Deaktivierung wirkt sich einschränkend auf die Funktion von iCloud bei nicht verwalteten Apps aus.*
    - *Bei einer kompletten Deaktivierung aller iCloud Funktionen und einer manuellen Deaktivierung der iCloud für System-Apps, sollte das Risiko von Datenabflüssen gering sein. Werden von Lehrkräften auf dem dienstlichen iPad jedoch personenbezogene Daten mit einem hohen Schutzbedarf verarbeiten, überwiegen die Risiken die Vorteile der Funktion.*
    - ***(Nicht empfohlen)***
- **Dokumente aus nicht verwalteten Apps in verwalteten Apps erlauben**
    - *Auch umgekehrt können Risiken entstehen, wenn Daten von nicht verwalteten Apps an verwaltete Apps weitergegeben bzw. von diesen geöffnet werden können, etwa wenn die Lehrkraft die iCloud für dieses App nicht korrekt deaktiviert hat.*
    - *Die Deaktivierung wirkt sich einschränkend auf die Funktion von iCloud bei nicht verwalteten Apps aus.*
    - *Bei einer kompletten Deaktivierung aller iCloud Funktionen und einer manuellen Deaktivierung der iCloud für System-Apps, sollte das Risiko von Datenabflüssen gering sein. Werden von Lehrkräften auf dem dienstlichen iPad jedoch personenbezogene Daten mit einem hohen Schutzbedarf verarbeiten, überwiegen die Risiken die Vorteile der Funktion.*
    - ***(Nicht empfohlen)***
- **AirDrop als nicht verwaltetes Ziel behandeln**
    - *Werden personenbezogene Daten in verwalteten Apps verarbeitet, besteht das Risiko, einer versehentlichen Weitergaben an unbefugte Dritte per AirDrop. Mit der Einschränkung kann dieses Risiko ausgeschlossen werden.*
    - *Die Einschränkung der Funktion von AirDrop ist nur verfügbar, wenn AirDrop selbst zugelassen ist (Einstellung - **AirDrop erlauben**), was bei einer unterrichtlichen Nutzung sinnvoll ist. Die Einschränkung ist nur wirksam, wenn auch die Einschränkung (Einstellung - **Dokumente aus verwalteten Apps in nicht verwalteten Apps erlauben**) deaktiviert ist!*
    - *Das Risiko einer Fehlbedienung von AirDrop sollte insgesamt eher gering sein. Werden von Lehrkräften auf dem dienstlichen iPad personenbezogene Daten mit einem hohen Schutzbedarf verarbeiten, überwiegen die Risiken die Vorteile der Funktion.*
    - ***(Empfohlen)***

Bei Schutzstufe - sehr hoch

Auch wenn für diese Schutzstufe die Nutzung für private Apple IDs nicht zugelassen wird, sollten zur Sicherheit Einstellungen, die erforderlich sind, um den Schutz bei Nutzung einer privaten Apple ID abzusichern, ebenfalls vorgenommen werden. Das ist vor allem dann von Bedeutung, wenn keine Einstellungen vorgenommen werden, mit denen die Anmeldung mit einer privaten Apple ID unterbunden werden kann.

Code (Zugriff schützen)

- **Automatische Sperre (max.)**
  - *maximale Zeit, die ein Gerät nach Eingabe des Passcodes entsperrt bleibt. Kann vom Nutzer reduziert werden.*
  - ***(1 min)***
- **Maximale Anzahl von Fehlversuchen**
  - *Soll im Fall eines Geräte Verlusts die Daten schützen, indem nach der maximal angelegten Anzahl von Fehlversuchen (ohne zwischenzeitlich erfolgreiche Logins), alle Daten vom Gerät gelöscht werden.*
  - ***(3)***

Einschränkungen (Zugriff Schützen)

- **Touch ID das Entsperren des Geräts erlauben**
  - *Da Touch ID mit etwas Aufwand manipuliert werden kann, Nachbau eines Fingerabdrucks und Entsperrung ohne vorherige Code Eingabe bis zu 48 Stunden möglich, entsteht hier laut BSI SYS_3_2_3_iOS_for_Enterprise_2021 ein hohes Risiko.*
  - *Mit dieser Einstellung ist das Gerät nicht mehr für einen Einsatz im Unterricht geeignet, da dann ein Entsperren nur noch mit Code möglich ist und dieser von Schülern ausgespäht werden könnte.*
  - ***(Nicht empfohlen)***
- **Ändern von Touch ID Fingerabdrücken / Face ID Gesichtern erlauben**
  - *setzt **Ändern des Codes erlauben** voraus*
  - *Touch ID kann vom Nutzer auch konfiguriert werden für iTunes und App Store Käufe sowie für andere Apps, die eine Sicherung des Zugriffs mit Touch ID unterstützen. Ist das Entsperren des Gerätes mittels Touch ID deaktiviert, sind diese Funktionen weiterhin verfügbar.*
  - ***(Empfohlen)***

Einschränkungen (Übermittlung/Abfluss von Daten kontrollieren - weitere)

- **Bildschirmaufnahmen erlauben**
  - *iOS Geräte haben eine Funktion für Bildschirmfotos und -aufnahmen. Diese können ein Sicherheitsrisiko darstellen, da Dritte, denen es gelingt, unbefugt Zugriff auf das Gerät zu erhalten, so Inhalte mit personenbezogenen Daten aufnehmen und übertragen können. (Das wäre zwar auch mittels Abfotografieren/ -filmen möglich, dann jedoch auffälliger.) Die Deaktivierung ist vor allem bei Geräten zu empfehlen, auf denen sehr sensible Daten verarbeitet werden. Ohne solche, kann die Funktion aktiviert werden, um das Aufnehmen von Erklärvideos und ähnlich zu ermöglichen.*
  - ***(Nicht empfohlen)***
- **Geräten nur den Beitritt zu WLAN-Netzwerken erlauben, die mit einem Profil konfiguriert wurden**
  - *Ermöglicht es, die Nutzung auf WLAN Netze zu beschränken, die als sicher gelten. Würde jedoch verhindern, dass Nutzer ihr heimisches WLAN nutzen können bzw. erfordern, dass dieses für jeden Nutzer speziell in ein Profil aufgenommen wird.*

    - *Wenn es vom Schulträger/ Admin zu leisten ist, sollte diese Absicherung genutzt werden.*
    - ***(Empfohlen)***
- **Modus für eingeschränkten Zugriff über USB erlauben** (i.S.v. vorschreiben)
    - *Erlaubt die Kopplung mit USB Geräten auch wenn der Bildschirm gesperrt ist. Die Verbindung bleibt aufrechterhalten, wenn der Bildschirm gesperrt wird. Dieses kann sinnvoll sein, wenn Zubehör am iPad aufgeladen werden soll, etwa ein Stift oder eine Tastatur, die über USB/Lightning angeschlossen wird.*
    - *Risiko: Unter Umständen könnte die Funktion ausgenutzt werden, um Zugriff auf das Gerät zu erlangen.*
        - ***Damit der USB Port bei Bildschirmsperre deaktiviert ist, darf der Haken nicht gesetzt sein!!!** "Erlauben" ist hier im Sinne von Vorschreiben zu verstehen.*
    - ***(Nicht empfohlen)***
- **Zugriff auf USB-Laufwerke in Dateien App erlauben**
    - *Nutzer können über angeschlossene USB Festplatten, CD/DVD Laufwerke und USB Sticks, soweit kompatibel, über das Dateien App auf Daten zugreifen oder diese extern ablegen.*
    - *Risiko: Die Funktion kann genutzt werden, um Daten vom Gerät zu entwenden.*
    - ***(Nicht empfohlen)***
- **Koppeln mit anderen Computern erlauben**
    - *Erlaubt es, dem iPad sich mit beliebigen Computern zu verbinden.*
    - *Risiko: Wenn Dritte den Code des iPad kennen und "Koppeln mit anderen Computern" zugelassen ist, können sie auf diesem Weg Daten des iPads auf einen Computer kopieren und ein Backup erstellen.*
    - *Bei Deaktivierung der Funktion lehnt das iPad Kopplungsanfragen ab, außer sie kommen von dem Computer mit dem es über AC2 konfiguriert wurde.*
    - ***(Nicht empfohlen)***
- **Synchronisieren von Notizen und Hervorhebungen in unternehmenseigenen Büchern erlauben**
    - *Notizen und Hervorhebungen können unter Umständen personenbezogene Daten enthalten, die nicht in iCloud landen sollten.*
    - ***(Nicht empfohlen)***
- **Siri erlauben**
    - *Siri greift zum Umsetzen von Befehlen und Fragen zunächst auf die Ressourcen auf dem Gerät zurück. Reicht dieses nicht aus, greift Siri auf Apple Dienste in der Cloud zu. Das erfolgt mit einer anonymisierten ID, die permanent wechselt.*
    - ***(Nicht empfohlen)***
- **FaceTime erlauben**
    - *Wegen der nicht auszuschließenden Risiken durch Fehler des Nutzers sollte die Funktion nicht zugelassen werden.*
    - ***(Nicht empfohlen)***
- **iMessage erlauben**

    - *Wegen der nicht auszuschließenden Risiken durch Fehler des Nutzers sollte die Funktion nicht zugelassen werden.*
    - ***(Nicht empfohlen)***
- **Nicht vertrauenswürdige TLS-Verbindungen mit Bestätigung erlauben**
    - *Wenn aktiviert, müssen Nutzer bei Verbindungen mit nicht vertrauenswürdigen HTTPS-Zertifikaten, die Verbindung aktiv bestätigen. Bei Deaktivierung werden diese Zertifikate automatisch zurückgewiesen und Verbindungen abgelehnt.*
    - ***(Nicht empfohlen)***
- **Automatisches Einfügen von Passwörtern erlauben**
    - *Die Funktion greift auf iCloud Schlüsselbund zu oder andere Passwort Manager Apps, sofern eingerichtet. Dem Nutzer werden dann in Safari und anderen Apps Passwörter vorgeschlagen, wenn aktiviert.*
    - *Bei Deaktivierung steht auch die Funktion von iOS, dem Nutzer starke Passwörter vorzuschlagen nicht mehr zur Verfügung.*
    - *Bei Nutzung eines sicheren Passwort Managers sollte die Funktion genutzt werden, da sie die Nutzung sicherer Passwörter erleichtert und dadurch zur Sicherheit insgesamt beiträgt.*
        - **Vor automatischem Einfügen Authentifizierung erforderlich** *muss unbedingt zusätzlich aktiviert werden.*
    - ***(Nicht empfohlen)***
- **Vor automatischem Einfügen Authentifizierung erforderlich**
    - *Um den Missbrauch der Funktion zu verhindern, muss bei Aktivierung, diese Funktion ebenfalls aktiviert werden.*
    - ***(Empfohlen)***
- **Verwenden von Safari erlauben**
    - *Die Nutzung von Safari kann zugelassen werden. Die nachfolgenden Einschränkungen sind zu berücksichtigen.*
    - *Nutzer müssen für Safari die iCloud Funktionen manuell deaktivieren.*
    - ***(Empfohlen)***
- **Automatisches Einfügen aktivieren**
    - *Die Deaktivierung verhindert, dass Safari Automatisches Einfügen für Kennwörter, Kontaktinformationen und Kreditkarten nutzt und verhindert auch, dass der Schlüsselbund für Automatisches Einfügen verwendet wird. Passwort-Manager von Drittanbietern und Apps, die Automatisches Einfügen verwenden, unterliegen dieser Einschränkung nicht.*
        - *Hinweis: Wird diese Funktion nicht aktiviert, ist auch die Funktion* **Automatisches Einfügen von Passwörtern erlauben** nicht möglich.
        - *Die Funktion darf nur aktiviert werden, wenn* ***Vor automatischem Einfügen Authentifizierung erforderlich*** *zusätzlich aktiviert ist, um bei unbefugtem Zugang zum Gerät Missbrauch zu verhindern.*
    - ***(Nicht empfohlen)***

Einschränkungen (Schutz der Konfiguration des Gerätes)

- **Ändern der Accounteinstellungen (E-Mail. Kontakte, Kalender, iCloud und iTunes Store)**

    - *Nutzer können sich mit privaten Apple IDs oder managed Apple IDs am Gerät anmelden und dann weitere E-Mail Adressen und Telefonnummern hinzufügen, die verwendet werden können, um den Nutzer bei iMessage, FaceTime, Game Center usw. zu erreichen, sofern diese Apps zugelassen sind. Das Passwort der (managed) Apple ID kann geändert werden. iCloud kann für die am Gerät angemeldete (managed) Apple ID für die System-Apps einzeln ein- und ausgeschaltet werden.*
    - *Wird diese Option deaktiviert, kann auch der App Store nicht genutzt werden, selbst wenn das App auf dem Gerät ist.*
    - ***(Nicht empfohlen)***
- **Installation von Apps erlauben**
    - *Nutzer, die mit ihrer privaten Apple ID am Gerät oder am App Store angemeldet sind, können privat erworbene Apps installieren.*
    - *Ist die Einschränkung "App-Installation über den App Store erlauben" deaktiviert, können Nutzer noch Apps in Kopplung mit einem Rechner über iTunes installieren, sofern keine anderen Einschränkungen eine solche Kopplung unterbinden. Auch die Installation über das MDM, sofern eingerichtet, wird hiervon nicht berührt.*
    - ***(Nicht empfohlen)***
- **In-App-Käufe erlauben**
    - *Diese Einschränkung ist nur wirksam, wenn die vorherige zugelassen ist.*
    - ***(Nicht empfohlen)***
- **App-Installation über den App Store erlauben**
    - *Ist die "Installation von Apps erlauben" aktiviert, erscheint mit der Aktivierung dieser Einschränkung das App Store App auf dem Homescreen und der Nutzer kann direkt auf dem dienstlichen iPad auf den App Store zugreifen.*
    - ***(Nicht empfohlen)***
- **Benutzer das Ändern des Hintergrundbilds erlauben**
    - *Kann zum Risiko werden, wenn Nutzer persönliche Hintergrundbilder verwenden, welche beispielsweise den Benutzer oder Teile seiner Familie darstellen.*
    - ***(Nicht empfohlen)***

Domänen

- **Verwaltete Safari Webdomänen**
    - *Es besteht die Möglichkeit, Webdomänen (URLs) als verwaltet zu behandeln. Sensible Dateien, die auf einer Website verfügbar sind, können standardmäßig in die nicht verwalteten App-Bereiche heruntergeladen werden. Durch die Konfiguration der spezifischen Domänen, die Safari als verwaltet betrachten soll, können Dateien von der Website nur an verwaltete Apps weitergegeben oder von diesen geöffnet werden.*
    - ***(Empfohlen)***

Organisatorische Maßnahmen

Welche Maßnahmen insgesamt getroffen werden müssen, um die Verarbeitung von personenbezogenen Daten auf dienstlich genutzten iPads abzusichern, hängt, wie oben beschrieben, von verschiedenen Faktoren ab. Sollen Lehrkräfte mit von der Schule zugewiesenen managed Apple IDs arbeiten? Möchte man Lehrkräften die Nutzung von privaten Apple IDs und die Installation von privat erworbenen Apps gestatten? Soll iCloud durch die Möglichkeiten des MDM maximal eingeschränkt bzw. deaktiviert werden oder soll iCloud für unterrichtliche Zwecke eingesetzt werden? Soll es möglich sein, auf den iPads dienstliche E-Mails lokal abzurufen?

Technische Maßnahmen alleine können eine sichere und datenschutzkonforme Verarbeitung von personenbezogenen Daten auf den dienstlichen Endgeräte nicht gewährleisten. Sie müssen immer auch von organisatorischen Maßnahmen ergänzt werden. Je weniger durch Einschränkungen über das MDM in die Funktionen des dienstlichen iPads eingegriffen wird, etwa um die pädagogische Nutzbarkeit der dienstlichen iPads nicht zu sehr einzuschränken, desto mehr Bedeutung gewinnen organisatorische Maßnahmen, um dadurch entstehende Risiken für die auf dem Gerät verarbeiteten personenbezogenen Daten einzuschränken. Dabei ergänzen sich verschiedene Formen von organisatorischen Maßnahmen.

Formen von organisatorischen Maßnahmen

Auch wenn viele Lehrkräfte privat ein iPhone oder iPad nutzen, so kann von durchschnittlichen Nutzern nicht erwartet werden, dass sie ausreichende Kenntnisse haben, wie ein iPad sicher genutzt wird. Lehrkräfte, die privat andere Smartphones oder Tablets nutzen, kennen sich mit iOS vielfach gar nicht aus. Deshalb sind Schulungen und praktische Unterstützung bei der Umsetzung der Vorgaben ein essentieller Bestandteil des gesamten Konzeptes zum Schutz und zur Sicherheit der Verarbeitung von personenbezogenen Daten auf dienstlichen iPads. Wer Lehrkräfte hier alleine stehen lässt, kann nicht erwarten, dass Lehrkräfte ihrer Verantwortung gerecht werden können. Eine Dienstanweisung alleine reicht nicht. Das sollte allen Beteiligten klar sein. Der Erfolg des Einsatzes von dienstlichen iPads im Sinne der Richtlinie wird nicht zuletzt auch wesentlich davon abhängen, wie gut Schule und Schulträger ihre Lehrkräfte hier unterstützen.

Schulungen

In Schulungen lernen Lehrkräfte, wie sie ein iPad sicher benutzen. Dazu gehören je nach zulässigem Nutzungsszenario:

- Sicherheitsfunktionen des iPads,
- iCloud und Datenschutz,
- Von Lehrkräften umzusetzende Maßnahmen zum Schutz und zur Sicherheit der Verarbeitung von personenbezogenen Daten auf dem Dienstgerät,
- Welche Daten dürfen auf dem dienstlichen iPad verarbeitet werden und wie müssen sie geschützt werden. Klassifizierung von Daten nach Schutzbedarf.
- Zulässige und unzulässige Verarbeitung von personenbezogenen Daten auf dem dienstlichen iPad,

- Trennung von Unterricht (pädagogische Daten) von pädagogischer Dokumentation und schulinterner Verwaltung,
- Schutz von privaten Apple Kontos, um schulische Daten zu schützen,
- Kriterien für die Auswahl von privat installierten Apps, mit denen personenbezogene Daten verarbeitet werden sollen.

Praxis Workshops

In Praxis Workshops werden die Lehrkräfte an die Hand genommen, welche praktische Hilfe bei der Umsetzung der Vorgaben zur Wahrung von Datenschutz und Datensicherheit für die auf den dienstlichen iPads verarbeiteten personenbezogenen Daten, benötigen.
Dazu gehören je nach zulässigem Nutzungsszenario folgende Inhalte:

- Erstanmeldung am Gerät,
- Abmeldung der managed Apple ID vom App Store und Anmeldung der privaten Apple ID,
- Anmeldung nur am App Store,
- Ändern des persönlichen Codes,
- Einrichten von Touch ID/ Face ID,
- Sperren und Entsperren des Gerätes,
- Deaktivierung von iCloud für System-Apps,
- Deaktivierung von iCloud für privat installierte Apps,
- Einrichtung eines dienstlichen E-Mail Kontos,
- Einrichtung eines privaten Apple Store Kontos,
- Anmelden am Apple Store auf dem iPad und Installation von Apps,
- Berechtigungen von Apps anpassen,
- Manuelles Auslösen von Updates für Apps,
- Manuelles Auslösen von System Updates,
- Sicherung von Daten außerhalb des iPads,
- Löschung von Daten vom iPad,
- Konfiguration von Mitteilungen für privat installierte Apps,
- Absichern eines privaten Apple Kontos.

Dienstanweisungen

Schulleitungen sollten über eine Dienstanweisung rechtlich verbindliche Vorgaben für die Nutzung der dienstlichen iPads machen. Damit ergänzen und präzisieren sie die Nutzungsvereinbarungen der Schulträger und sichern sich darüber hinaus in datenschutzrechtlicher Hinsicht als Verantwortliche zusätzlich ab. Mit einer Dienstanweisung werden den Lehrkräften verbindliche Vorgaben gemacht, welche Einstellungen sie als Nutzer der dienstlichen iPads treffen müssen, um die Vorgaben durch das MDM zu ergänzen, wo das MDM selbst keine Einflussmöglichkeiten hat. Bestimmt werden muss außerdem, welche Arten von personenbezogenen Daten in welchen Apps verarbeitet werden dürfen und, falls erforderlich, welche Daten in verwalteten und welche in nicht verwalteten Apps verarbeitet werden dürfen. Geregelt werden kann in einer Dienstanweisung auch, welche Apps Lehrkräfte zur Verarbeitung von personenbezogenen Daten installieren und nutzen dürfen bzw. über welches Verfahren eine Zulässigkeit bestimmt wird. Da das MDM keinen Einfluss auf Sicherheitsfunktionen von Apps selbst hat,

sind auch hier Vorgaben zu machen. Dazu gehört die Verpflichtung, den Zugriffsschutz zu den im App verarbeiteten Daten durch Passwort und/ oder Touch ID zu sichern.

Praktische Tipps

Kriterien für die Auswahl von Apps

Mit iOS 14.5 müssen Apps transparent angeben, auf welche Ressourcen auf dem Gerät sie zugreifen bzw. welche Berechtigungen sie benötigen. Die Angaben werden von den Entwicklern der Apps gemacht. Daher ist nicht zu 100% garantiert, dass diese Angaben auch stimmen. Trotzdem sollten sie bei der Auswahl von Apps berücksichtigt werden. Das gilt vor allem für Apps, die von Nutzern mit privaten Apple IDs installiert werden. Es gilt auch für Apps, die über das MDM aufgespielt werden. Das BSI gibt weitere nützliche Hinweise, worauf zu achten ist. Die folgenden Fragen orientieren sich daran.

- Wo speichert das App die App-Anwendungsdaten?
    - Speichert es sie auf dem Gerät oder außerhalb des Gerätes?
    - Falls die Speicherung außerhalb Deutschlands oder des EWR erfolgt, könnte das datenschutzrechtlich problematisch sein.
    - Werden vom App personenbezogenen Daten aus der Schule verarbeitet, muss ein Vertrag zur Auftragsverarbeitung mit dem Anbieter bestehen. Ohne diesen ist eine Speicherung auf den Servern des Anbieters nicht zulässig.
- Erfolgt die Speicherung von personenbezogenen Daten auf dem Server des Anbieters (unabhängig, wo dieser steht) automatisch oder kann der Nutzer die Speicherung beeinflussen? (Gefahr eines unkontrollierten Datenabflusses)
- Sammelt das App Nutzerdaten zur Erstellung eines Profils durch Tracker oder Werbung im App?
- Wie sind die Daten im App geschützt? Werden die Daten in der App beim Entsperren der App automatisch entschlüsselt oder können sie mit einem Passwort, TouchID oder FaceID vor unberechtigtem Zugriff geschützt werden?
- Bietet das App eigene Sharing-Dienste oder Netzwerkschnittstellen an?
- Benötigt das App Zugriff auf Daten, die auf dem Gerät gespeichert sind?
- Wird das App durch seine Entwickler regelmäßig aktualisiert?

Es kann für Lehrkräfte sehr hilfreich sein, wenn erfahrene Nutzer in der Schule eine Empfehlungsliste für Apps erstellen, die als gut, sicher und datenschutzkonform nutzbar gelten.

Eine Frage des MDM

Nicht jedes MDM greift alle von iOS bereitgestellten Einschränkungen vollumfänglich auf. Dadurch lassen sich die hier abgegebenen Empfehlungen auch nicht in Gänze umsetzen. Diese Nachteile muss man dann durch umfangreichere organisatorische Maßnahmen ausgleichen. Dazu könnte gehören, dass man die Einschränkungen, welche man nicht durch das MDM vornehmen kann, aber gerne umsetzen möchte, durch die Nutzer vornehmen lässt. Eine entsprechende Schulung und praktische Unterstützung wird dabei in der Regel erforderlich sein.

Schulen, die ihren Lehrkräften die Nutzung von privaten Apple IDs ermöglichen wollen, dabei aber in Bezug auf iCloud auf Nummer sicher gehen möchten, sollten die Anmeldung der Lehrkräfte auf den App Store beschränken, wie oben beschrieben. Die iCloud darf dann nicht aktiviert werden. Damit ist eine sehr sichere Nutzung möglich, da die durch iCloud entstehenden Risiken entfallen.

Umsetzung vor Ort - Bedarfsabfrage

Wenn Schulträger und Schulen sich entscheiden, mit den drei vorgeschlagenen oder daraus abgeleiteten Profilen zu arbeiten, empfiehlt es sich, die Bedarfe an den Schulen abzufragen. Dafür könnte eine Tabelle erstellt werden, in welcher die drei definierten Nutzungszwecke beschrieben werden. Die Lehrkräfte tragen sich dann in der Tabelle entsprechend des von ihnen geplanten Nutzungszwecks ein. Dafür muss ihnen vorab klar sein, welche Einschränkungen eventuell mit der Entscheidung für eine Stufe einhergehen. Lehrkräfte, welche ihr dienstliches iPad sehr stark im Unterricht einsetzen wollen und die Möglichkeit haben, personenbezogene Daten, die der Schutzstufe hoch zuzurechnen sind, auf anderen Endgeräten zu verarbeiten, sollten dann die “Schutzstufe normal” wählen.

Es empfiehlt sich von daher, vorab eine Veranstaltung durchzuführen, in welcher das Konzept der Schutzstufen erklärt und begründet wird. Soll die Nutzung privater Apple IDs zugelassen werden, muss auch hier erklärt werden, welchen Einschränkungen dieses unterliegen kann und welche Anforderungen dabei an Lehrkräfte gestellt werden.

	Schutzstufe - normal	**Schutzstufe - hoch**	**Schutzstufe - sehr hoch**
Nutzung für	• **pädagogische Zwecke** im Unterricht **mit Schülern** • **pädagogische Dokumentation**: z.B. Noten, Bemerkungen, Versäumnisse • **schulinterne Verwaltung** (*stark eingeschränkt oder gar nicht wie Fachlehrer*): z.B. Kontakte Eltern, Absenzen	• **pädagogische Zwecke** im Unterricht **mit Schülern** • **pädagogische Dokumentation**: wie Schutzstufe normal • **schulinterne Verwaltung** wie Schutzstufe normal **plus** Blaue Briefe, Zeugnisnoten, Zeugnisse, Protokolle Klassenkonferenzen, Elternschreiben Ordnungsmaßnahmen, …	• **pädagogische Zwecke** im Unterricht **mit Schülern** • **pädagogische Dokumentation**: wie Schutzstufe normal **plus** Dokumentation AO-SF Verfahren • **schulinterne Verwaltung**: ohne Einschränkung, auch bezüglich AO-SF Verfahren
Beispiele: in welcher Rolle werden die oben beschriebenen Daten auf dem iPad verarbeitet, wenn nicht ein Teil auf andere Geräte ausgelagert wird.	Fachlehrer*in	Klassenlehrer*in, Stufenleiter*in	Förderschulpädagog*in, Schulleitung, Schulsozialpädagog*in
Name			
Peter Lehrer	x		

Siglinde Lehrerin		x	
...			

Ressourcen

Empfehlungen des BSI

- Allgemein BSI-Grundschutz-Kompendium
- dazu - Umsetzungshinweis INF.9 Mobiler Arbeitsplatz (Edition 2020)
- BSI SYS.3.2.3 iOS (for Enterprise)
- und dazu UH_SYS_3_2_3_iOS_CD.pdf

Andere

- Apple Developer - Device Management Restrictions
- Apple - MDM restrictions for iPhone and iPad devices
- National Cyber Security Centre - End user device (EUD) security guidance
- CIS - CIS Apple iOS 12 Benchmark (für iOS 14 nach Anmeldung verfügbar)
- Jamf - iOS Security Checklist - Implementing the Center for Internet Security Benchmark for iOS
- UCF - Apple iOS/iPadOS 14 Security Technical Implementation Guide

Sonstiges

Mitarbeitende

Beigetragen haben zu diesem Dokument durch praktisches Austesten der Aktivierung und Deaktivierung von payloads in verschiedenen Kombinationen und kritisches Lesen:

- J. Marr

Versionshinweise

- Version 1.0
- Version 1.10 - Ergänzt bei *Schutzbedarf - normal*
    - **Siri bei gesperrtem Gerät erlauben**
    - **Serverseitige Protokollierung für Siri erlauben**
-