Geräterichtlinie

Stand: 20.01.2020

Um die HPI Schul-Cloud möglichst effizient nutzen zu können, sollte den Nutzer*innen der Zugriff von diversen (mobilen) Endgeräten (Tablets, Smartphones, Laptops usw.) ermöglicht werden. Sinn der HPI Schul-Cloud ist es gerade, die in der Cloud bereitgestellten Dokumente und Funktionen geräteübergreifend zur häuslichen Nacharbeit verwenden zu können.

Mit der Nutzung mobiler Geräte ergeben sich jedoch auch spezielle Anforderungen und Herausforderungen an den Datenschutz und die Datensicherheit. Diese Richtlinie zeigt den Schulen, Lehrkräften und Schüler*innen daher Wege auf, um die Risiken für personenbezogene Daten bei der Nutzung mobiler Endgeräte zu reduzieren. Diese Richtlinie ist als nicht abschließende und nicht verpflichtende Orientierungshilfe zu verstehen.

1. Anschaffung

Notwendige Voraussetzung für die Nutzung der HPI Schul-Cloud außerhalb und innerhalb der Schulen ist zunächst, dass geeignete (mobile) Endgeräte vorhanden sind. Um dies sicherzustellen, bestehen insbesondere die nachfolgend kurz beschriebenen Optionen.

1.1. Bring Your Own Device (BYOD)

Im Rahmen von BYOD-Konzepten wird auf bereits bei den Schüler*innen vorhandene, private Geräte zurückgegriffen. Dies hat den Vorteil, dass für die Schulen zunächst keine Anschaffungskosten entstehen. Auch kann eine hohe Vertrautheit der Schüler*innen mit der Bedienung der Geräte vorausgesetzt werden.

Auf der anderen Seite ist nicht sichergestellt, dass alle Schüler*innen über entsprechende Geräte verfügen. Zusätzlich führen BYOD-Konzepte stets zu einer großen Anzahl an verschiedenen technischen Plattformen durch eine Vielzahl von Herstellern und Systemen. Aus Perspektive des Datenschutzes und der Datensicherheit stellt diese Vielfalt an technischen Lösungen einen zusätzlichen Risikofaktor dar.

1.2. Übereignung durch die Schule

Alternativ dazu hat die Schule die Möglichkeit, gesammelt eine große Anzahl baugleicher Geräte anzuschaffen und diese an die Schüler*innen zu übereignen. In diesem Fall besteht eine einheitliche technische Basis und die Anschaffung stellt keine finanzielle Mehrbelastung für die Erziehungsberechtigten dar.

Jedoch ist hier mit hohen, auch wiederholten Kosten für die Schulen zu rechnen, da in großem Umfang Geräte angeschafft werden müssen. Auch administrativ müssen Regelungen getroffen werden, um dem Verlust einzelner Geräte und Fällen der missbräuchlichen Nutzung adäquat zu begegnen.

1.3. Klassensätze

Eine Anschaffung durch die Schule kann auch ohne anschließende Übereignung an die Schüler stattfinden. Bei einem solchen Konzept werden die mobilen Geräte in der Schule vorgehalten und dann jeweils nach Bedarf an die Schüler*innen herausgegeben. Hierbei teilen sich zumeist mehrere Schüler*innen in verschiedenen Klassen ein Gerät. Die Kosten sind dadurch geringer als bei der Übereignung der Geräte an jeweils nur eine*n Schüler*in. Auch kann die Wartung und Pflege der Geräte besser gewährleistet werden, da diese ständig in der Schule verbleiben und von den Schuladministratoren überprüft werden können.

Jedoch ist zu berücksichtigen, dass dieses Modell dazu führt, dass Schüler*innen die Geräte in der Regel nur in der Schule verwenden können. Eine Nutzung der Geräte außerhalb der Schule ist allenfalls kurzzeitig möglich, da hier jeweils mehrere Schüler*innen Bedarf an einem einzigen Gerät haben.

1.4. Bring Your Own School Device (BYOSD)

Bei dieser Abwandlung des BYOD-Konzepts wird nicht auf bereits vorhandene Geräte der Schüler*innen zurückgegriffen. Vielmehr werden die Geräte durch die Schule oder einen Dritten (z.B. einen spezialisierten Service-Partner) angeschafft und für einen bestimmten Zeitraum an die Schüler*innen verliehen (das Konzept wird deshalb auch als „Bring Your Rented Device – BYRD" bezeichnet). Nach Ablauf dieses Zeitraums fallen die Geräte wieder an die Schule bzw. den Service-Partner zurück. Durch die gebündelte Anschaffung können durch die Schule einheitliche Standards und Anforderungen an die Geräte gestellt werden. Zudem werden einkommensschwächere Haushalte entlastet.

Die Schule trägt jedoch die Kostenlast. Auch müssen zusätzliche Regelungen zwischen Schule und Schüler*innen getroffen werden, insbesondere für den Fall des Verlustes oder der Beschädigung des Gerätes.

1.5. Mischkonzept

Ein Mischkonzept kann eine Vereinigung von BYOD und BYOSD darstellen. In diesem Fall nutzen die Schüler*innen, soweit möglich, bereits bei ihnen vorhandene Geräte. Die vorhandenen Geräte müssen auf dem aktuellen Stand der Technik sein und gewisse technische Mindeststandards erfüllen, um die Funktionsfähigkeit und Sicherheit des Konzepts zu gewährleisten. Schüler*innen, die über kein bzw. kein den Mindeststandards entsprechendes Gerät verfügen, wird ein Gerät aus einem von der Schule angeschafften Pool zur Verfügung gestellt. Dadurch ist gewährleistet, dass die erforderlichen Standards nicht unterschritten werden und Haushalte, welche die Anschaffungskosten nicht übernehmen können oder wollen, entlastet werden. Die Schule hingegen muss die verbleibenden Anschaffungskosten übernehmen und der bei BYOSD erwähnte organisatorische Mehraufwand bleibt auch in diesem Modell bestehen.

1.6. Empfehlung

Aus datenschutzrechtlicher Sicht kann keine eindeutige Empfehlung für eines der Modelle ausgesprochen werden. Im Hinblick auf den Datenschutz und die Datensicherheit sind grundsätzlich dieselben Anforderungen zu erfüllen, unabhängig davon, auf welchem Weg das Gerät angeschafft wurde. Fest steht allerdings, dass eine möglichst hohe Aktualität und Einheitlichkeit der verwendeten Geräte hilft, Datenrisiken zu minimieren. Die Frage, auf welchem Weg die Geräte angeschafft werden, muss jeweils von der Schule im Hinblick auf ihre spezifische Situation und ihre Anforderungen beantwortet werden.

2. Sicherheitsmaßnahmen

Die Schulen sind für die Verarbeitung personenbezogener Daten in der HPI Schul-Cloud datenschutzrechtlich verantwortlich. Auch bei der Nutzung mobiler Geräte müssen die Schule insofern **angemessene technische und organisatorische** Maßnahmen zur Datensicherheit treffen, vgl. Art. 32 Datenschutz-Grundverordnung (**DSGVO**).

Das größte Risiko für den Schutz der personenbezogenen Daten der Schüler*innen und der Lehrkräfte ist dabei die **Offenbarung der Daten gegenüber unberechtigten Personen**, sei es durch die unbeabsichtigte Offenlegung seitens der Schüler*innen oder durch den unbefugten Zugriff eines Dritten, z.B. durch einen Cyber-Angriff oder Schadsoftware.

Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgeschlagene Drei-Säulen-Strategie zur Umsetzung von BYOD-Konzepten sollte hierbei beachtet werden.[1] Zu berücksichtigen sind daneben die von den Datenschutzaufsichtsbehörden geäußerten Vorschläge zur sicheren Anwendung von Geräten im Rahmen mobiler Geräte und BYOD. Diese Aussagen beziehen sich zwar zumeist auf die Nutzung von mobilen Geräten im Beschäftigungsverhältnis, jedoch sind die Grundsätze auch auf das hier vorliegende Verhältnis zwischen Schüler*innen und Schule übertragbar.

Vor der Einleitung weiterer Maßnahmen ist durch die Schul-IT bzw. die Schuladministratoren zunächst festzulegen, welche **Mindeststandards** die verwendeten Geräte zu erfüllen haben. Insbesondere sollte eine Festlegung auf bestimmte **Betriebssysteme** und deren (Mindest-)Version erfolgen. Veraltete Betriebssysteme bergen vermehrt das Risiko, vom Entwickler keine regelmäßigen Updates mehr zu erhalten und dadurch Sicherheitslücken aufzuweisen. Zur Vermeidung dieser Problematik ist immer ein Betriebssystem von angemessener Aktualität einzusetzen.[2]

[1] Vgl. Michael Otter (BSI), „BYOD – Bring your own Disaster?, Die Sicht des BSI zu Sicherheit in Informationsverbünden mit BYOD“, Präsentation beim 22. EDV-Gerichtstag, 25. – 27.09.2013, S.22 abrufbar unter: https://edvgt.de/wp-content/uploads/2015/12/edvgt2013-AK-BYOD-Pr%C3%A4s.pdf.
[2] Vgl. XI. Tätigkeitsbericht des Landesbeauftragten für Datenschutz Sachsen-Anhalt vom 01.04.2011-31.03.2013, Ziffer 4.9.

2.1. Organisatorische Maßnahmen

Auf organisatorischer Ebene ist die Verpflichtung der Schüler*innen auf eine **Nutzungsordnung** zur Nutzung von mobilen Endgeräten im Rahmen der HPI Schul-Cloud zu empfehlen.[3] Dies kann durch ein separates Dokument oder im Rahmen der bereits vorgesehenen Nutzungsordnung (Anlage 15) geschehen.

Im Rahmen dieser Nutzungsordnung sind die Schüler*innen auf ein Verhalten zu verpflichten, dass das angemessene Maß an Datenschutz und Datensicherheit gewährleistet.

Diese Verpflichtung sollten u.a. umfassen:

- das Verbot an dem mobilen Gerät „Jailbreaks" oder „Rooting" durchzuführen;[4]
- die Zusage personenbezogene Daten aus dem Kontext der HPI Schul-Cloud nicht für andere Zwecke zu verwenden;
- ein verbindlich einzuhaltendes Verfahren bei Verlust und/oder Beschädigung des Gerätes (auch für eigene Geräte im Rahmen des BYOD);[5]
- eine Regelung, inwieweit das Gerät auch privat genutzt werden kann, sofern das Gerät durch die Schule angeschafft wurde (unabhängig, ob als BYOSD oder im Rahmen des Mischkonzeptes);[6]
- die Verpflichtung, regelmäßig Updates der relevanten Software durchzuführen (entweder selbst oder durch eine von der Schule benannte Stelle);
- die Löschung aller Daten bei Beendigung der Teilnahme an der HPI Schul-Cloud.

Neben diesen Verpflichtungen der Schüler*innen, sollte vor Nutzungsbeginn eine generelle **Sensibilisierung** der Schüler*innen und der Lehrkräfte zu den Thematiken Datenschutz und Datensicherheit stattfinden, beispielsweise durch eine Extra-Schulung durch die Schuladministratoren zur Nutzung der Geräte.

Die Schule hat **Überwachungsmaßnahmen** an den mobilen Geräten grundsätzlich zu **unterlassen**. Dies gilt insbesondere dann, wenn es sich um von der Schule bereitgestellte Geräte handelt und auf diese Zugriff im Rahmen der lokalen oder Fernwartung besteht. In diesen Fällen darf nicht auf die privaten Daten der Schüler*innen zugegriffen werden.[7] Auch dürfen durch die Schule keine Analysen anhand von Bewegungsdaten oder anderer Gerätedaten, die sich auf einzelne Schüler*innen zurückführen lassen, durchgeführt werden.

Zusätzlich sollten die Schul-IT bzw. Schuladministratoren oder Service-Partner angemessenen **Support** für die Schüler*innen sicherstellen können, um auf etwaige Probleme bei der Nutzung der Geräte oder Sicherheitsvorfälle jederzeit schnell reagieren zu können.

---

[3] Vgl. Berliner Beauftragter für Datenschutz und Informationsfreiheit, Bericht 2012, S. 33.
[4] Vgl. LfD Sachsen-Anhalt, aaO; Der Bayerische Landesbeauftragte für Datenschutz, 25. Tätigkeitsbericht 2012, Ziffer 2.1.3.
[5] Vgl. BlnBDI, aaO, S. 35.
[6] Vgl. LfD Bayern, aaO.
[7] Vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 34. Tätigkeitsbericht 2011/2012, Ziffer 10.1.

Vor Übergabe der Geräte an eine*n neue*n Nutzer*in, müssen ggf. noch vorhanden personenbezogene Daten **vollständig gelöscht** werden. Nach Ende der Verwendung ist ein Prozess zur Entsorgung der genutzten Geräte zu schaffen, der sicherstellt, dass keine personenbezogenen Daten mehr auf den Geräten vorhanden sind.[8]

2.2. Technische Maßnahmen

Potenzielle Risiken für die personenbezogenen Daten lassen sich nicht alleine durch die Einhaltung organisatorischer Maßnahmen abwenden. Es bedarf zusätzlich auch der Umsetzung technischer Maßnahmen zur Sicherung der verwendeten Geräte.

Diese technischen Maßnahmen sind bei zentral administrierten Geräten einfacher umsetzen als bei einer Vielzahl von (BYOD-)Geräten, auf die Seitens der Schul-IT kein Zugriff besteht.

Die wichtigste Maßnahme für Geräte bei denen sowohl eine schulische als auch eine private Nutzung stattfindet, ist eine **strikte logisch-technische Trennung** zwischen diesen beiden Anwendungsarten. Hier bietet sich die Einrichtung eines eigenen Containers auf den Geräten, durch den die schulischen Inhalte im Rahmen der HPI Schul-Cloud technisch von den sonstigen privaten Inhalten getrennt werden.[9] Dies dient auch dazu, dass die übrigen auf dem mobilen Gerät verwendeten Applikationen keinen Zugriff auf die Daten der HPI Schul-Cloud erhalten, insbesondere da sich viele **Applikationen von Dritt-Anbietern** weitreichende Zugriffsrechte auf alle auf dem Gerät befindlichen Daten einräumen lassen und diese dann an Dritte übermitteln.

Sofern mehrere Schüler*innen sich ein Gerät teilen (vgl. das Anschaffungsmodell „Klassensätze", Ziffer 1.3), ist zum Beispiel durch die Einrichtung von User-Accounts sicherzustellen, dass auch die lokal gespeicherten personenbezogenen Daten strikt voneinander getrennt sind.

Zusätzlich sollte der Zugang zu den mobilen Geräten immer gesichert sein. Dazu ist hier ein sicheres Passwort oder eine technische Methode zum Freischalten des Gerätes, wie ein Fingerabdruckscanner, einzurichten. Auf als unsicher anzusehende Sperrmechanismen wie Entsperrmuster oder Facescan ist aus Sicherheitsgründen zu verzichten. Nach der **mehrfachen Falscheingabe** kann eine automatische Datenlöschung implementiert werden.[10]

Als Ergänzung zu diesen Freischaltmechanismen ist das Gerät von den Schuladministratoren so einzurichten, dass eine **automatische Sperrung** nach einer Phase der Inaktivität eintritt, um Personen, die das Gerät zufällig unbeaufsichtigt finden, keinen Zugriff zu gestatten. Hier wäre eine automatische Sperrung nach 5 Minuten Inaktivität angemessen.

Grundsätzlich sollte für die Bereiche, in denen personenbezogene Daten lokal abgelegt werden können, eine **Verschlüsselung** eingerichtet werden.[11]

Das Gerät ist mit jeweils den aktuellsten Software-Versionen und einer aktuellen **Firewall** bzw. **Virenscanner** auszustatten.[12]

---

[8] Vgl. LfD Bayern, aaO.
[9] Vgl. LfD Sachsen-Anhalt, aaO; LfD Bayern, aaO.
[10] Vgl. LfD Bayern, aaO.
[11] Vgl. LfD Bayern, aaO.
[12] Vgl. LfD Bayern, aaO.

Auch sind regelmäßige **Datensicherungen** der lokal gespeicherten Daten durchzuführen. Dabei ist allerdings darauf zu achten, dass mobile Geräte häufig über eine automatische Back-Up-Funktion verfügen, bei der die Daten auf dem Gerät in der Cloud des Geräteherstellers bzw. Betriebssystemanbieters gesichert werden. Dadurch kann es zu einer Übermittlung personenbezogener Daten an Dritte kommen, in vielen Fällen auch verbunden mit einer Übermittlung in Nicht-EU-Länder wie die USA. Hier sind Maßnahmen zu treffen, um diese automatischen Back-Up-Übermittlungen zu unterbinden.

Wenn möglich sollte ein **Logging** der Zugriffe und Aktivitäten auf dem Gerät durchgeführt werden, um unberechtigte Zugriffe nachvollziehen zu können.[13] Bei Geräten der Schüler*innen kommt ein Logging typischerweise nicht in Frage, sondern nur bei von den Schule gestellten Geräten. Ein Logging darf zudem keinesfalls zur Überwachung oder ähnlichen Maßnahmen führen (s.o.). Daher dürfen nur ausgewählte, fachkundige geschulte Personen die Möglichkeit des Zugriffs auf die Logs erhalten. Der konkrete Zugriff auf die Gerätelogs darf nur in Beisein des Datenschutzbeauftragten, auf einen konkreten Anlass hin und nach entsprechend datenschutzkonformen Richtlinien erfolgen.

Für den Fall des Verlustes eines Gerätes sollte für die Schul-IT eine technische Möglichkeit zur **Fernlöschung** der Daten mit Bezug zur HPI Schul-Cloud implementiert werden.[14]

All diese Maßnahmen sind einfacher umzusetzen, wenn ein regelmäßiger (Fern-)**Zugriff für Wartungsmaßnahmen** durch die Schul-IT auf die Geräte besteht. Wo dies nicht möglich ist, z.B. da es sich um die privaten Geräte der Schüler*innen handelt, sind diese im Rahmen der Nutzungsordnung (siehe Ziffer 1.2) auf die Umsetzung dieser Maßnahmen zu verpflichten.

2.3. Maßnahmen zur Netzanbindung

Die Verwendung mobiler Geräte birgt generell die Gefahr, dass Daten während der **Übermittlung** zum Gerät abgefangen werden. Auf diese Gefahr ist ebenfalls mit technischen Maßnahmen zu reagieren.

Zu einen sollte hier eine automatische **Authentifizierung** des Gerätes eingerichtet werden, die vor Beginn der Datenübermittlung durch die HPI Schul-Cloud überprüft wird.

[13] Vgl. LfD Sachsen-Anhalt, aaO, BlnBDI, aaO, S. 37.
[14] Vgl. LfD Bayern, aaO.