E07040003. Juli 2023

WIESBADEN

Eg: 28.06.2023

über
Herrn Oberbürgermeister
Gert-Uwe Mende

über
Magistrat

und
Herrn Stadtverordnetenvorsteher
Dr. Gerhard Obermayr

an die Fraktion

Der Magistrat

Dezernat für Finanzen, Schule und Kultur

Stadtrat Axel Imholz

26. Juni 2023

Anfrage der DIE LINKE.- Fraktion vom 08.05.2023, Nr. 122/2023 nach § 45 der Geschäftsordnung der Stadtverordnetenversammlung 23-V-03-0006

Anfrage:

Berücksichtigung des Datenschutzes bei der Ausstattung von Wiesbadener Schüler*innen mit iPads

1. Ist für die iPads, die im Zuge der „1:1 Ausstattung mit iPads für alle 5. Klassen der weiterführenden Schulen“ besorgt werden, eine Nutzung des Mobile Device Mangementssystems (MDM) „jamf“ geplant?

2. Falls nein, welches Managementsystem soll bei den genannten Geräten zum Einsatz kommen? Ist es konform mit dem in der EU geltenden Datenschutzrecht?

3. Falls ja, welche Maßnahmen werden ergriffen, um sicherzustellen, dass eine Nutzung von „jamf“, das auf Amazon Web Service-Diensten (AWS) basiert, konform mit dem in der EU-geltenden Datenschutzrecht ist?

4. Falls ja, wurde die Nutzung von alternativen Managementsystemen geprüft, die konform mit dem in der EU geltenden Datenschutzrecht sind?

Die Anfrage beantworte ich wie folgt:

Die Anfrage 122/2023 bezog sich auf das Mobile Device Management (MDM) der iPads, die im Zuge der 1:1 Ausstattung mit iPads für alle 5. Klassen der weiterführenden Schulen besorgt werden sollen. Das erforderliche MDM geschieht mit der Software Jamf School. Jamf School ist eine MDM-Plattform, die es ermöglicht, mobile Geräte effizient zu verwalten und zu kontrollieren. Das Medienzentrum Wiesbaden übernimmt die Administration der iPads unter Verwendung von Jamf School. Diese Stellungnahme untersucht die

Schillerplatz 1 - 2
65185 Wiesbaden
Telefon: 0611 31-4285
Telefax: 0611 31-4299
E-Mail: Dezernat.III@wiesbaden.de

datenschutzrelevanten Aspekte im Zusammenhang mit der Nutzung von Jamf School an Schulen.

1. Datenschutz bei Jamf

Um einen angemessenen Schutz für die Übermittlung von personenbezogenen Daten zu gewährleisten hat Jamf umfangreiche Sicherheitsvorkehrungen vorgenommen. Die **Standardvertragsklauseln** (SCC) der europäischen Kommission von 2021 wurden in den **Auftragsverarbeitungsvertrag** aufgenommen und auch mit Unterauftragsverarbeitern vereinbart.
Jamf School Management System erfasst laut Aussage von Jamf lediglich ein Minimum an Kundendaten, das zur Bereitstellung unserer Dienste (Jamf) erforderlich ist. Darunter fällt unter Umständen auch die IP-Adresse der Schule oder des Standorts, wo der Nutzer sein Gerät benutzt. Jamf und seine Partner können keine Dokumente, Bilder oder In-App-Daten der Schüler in Apps oder auf Apple-Geräten sehen. (https://www.jamf.com/de/trust-center/privacy/). Wenn es sich der amerikanischen Amazon Web Services-Cloud (AWS) bedient, werden höchstens diese Daten dort gehostet. Die Privatsphäre der Nutzer bleibt gewahrt.
Darüber hinaus hat sich Jamf verpflichtet, geeignete **technische und organisatorische Maßnahmen** zum Schutz personenbezogener Daten zu ergreifen (https://www.jamf.com/de/trust-center/information-security/). JAMF ist außerdem sowohl ISO27001 als auch ISO27701 zertifiziert. Diese Zertifikate ermöglichen ein Datenschutzmanagement zum erweiterten Schutz personenbezogener Daten.

2. Auftragsverarbeitungsvertrag

Zwischen dem Medienzentrum und Jamf ist ein Auftragsverarbeitungsvertrag (AV-Vertrag) abgeschlossen worden. Dieser Vertrag regelt die vertraglichen Pflichten und Verantwortlichkeiten der Parteien im Hinblick auf den Datenschutz und definiert die Rollen und Verantwortlichkeiten der beteiligten Parteien. Er stellt sicher, dass der Auftragnehmer (=Jamf) die personenbezogenen Daten gemäß den Anweisungen des Auftraggebers und den Anforderungen der Datenschutzgesetze verarbeitet.

3. Einsichtnahme in personenbezogene Daten

Über Jamf School sind durch die Voreinstellungen zunächst keine personenbezogenen Daten einsehbar. Allerdings besteht die Möglichkeit für Nutzer, ihren Geräten einen Namen zuzuweisen, und dieser Name wäre über Jamf School einsehbar. Außerdem wird die IP-Adresse erhoben. Es wird daher empfohlen, bei der ersten Installation darauf hinzuweisen, keine Klarnamen als Gerätenamen einzusetzen, um die Privatsphäre zu schützen. Das könnte von Seiten des Medienzentrums während der Erstkonfiguration über einen angezeigten Hinweis an den Nutzer geschehen und sollte auch in den Informationen an die Lehrkräfte, Eltern, Schülerinnen und Schüler über die Verwendung der Geräte enthalten sein

4. Metadaten

Bei der Verwendung von Jamf School sind unter Umständen Metadaten einsehbar. Die eingesehenen Metadaten umfassen unter anderem die hinzugefügten privaten Apps, die letzte IP-Adresse, mit der das Gerät das letzte Mal im WLAN der Schule, am Wohnort oder an anderen Orten angemeldet war, die Zeit der letzten Netzwerkanmeldung und Akkudaten. Es werden keine GPS-Daten erfasst, und die Landkarten-Funktion wurde bei Jamf School von Seiten des Medienzentrums deaktiviert.

5. Administratorenrechte

Die Administratoren des Medienzentrums können die verwalteten Apps sehen und verwalten. Das heißt, sie können sie aktualisieren, löschen und hinzufügen. Sie haben keinen Zugriff auf die Inhalte der Apps. Die von Lehrkräften geladenen fremden Apps können die Administratoren lediglich sehen, jedoch nicht verwalten.
Sie haben darüber hinaus keinen Zugriff auf Nutzungsdaten, Statistiken, Verläufe oder Login-Daten der Nutzer. Im Fall eines verlorenen Geräts besteht die Möglichkeit, es vollständig zu deaktivieren. Die Administratoren können den Code ggfs. entfernen und die Vergabe eines neuen Codes ermöglichen, ohne dass vorhandene Daten verloren gehen. Sie können ebenfalls anweisen, dass ein neuer Code eingegeben werden muss, haben jedoch keinen Zugriff auf den Code selbst.

6. Schulzugriff auf Jamf

Die meisten Schulen haben keinen direkten Zugriff auf Jamf School. Einige Schulen bzw. IT-Beauftragte haben über Jamf School Zugriff auf die Schülergeräte ihrer Schule, jedoch nicht auf Leihgeräte von Lehrkräften und dem 1:1 Projekt. Schülern ist es standardmäßig nicht gestattet sich mit ihrer Apple-ID anzumelden, um eigene Apps hochzuladen. Einige wenige Schulen können dies jedoch erlauben. Sollte dies in einer Schule der Fall sein, muss immer auch über die datenschutzrechtlichen Konsequenzen informiert werden. Lehrkräften ist es gestattet, sich mit einer eigenen Apple ID (dienstlich oder privat) anzumelden. Die Verwaltung der Geräte und die Durchführung von technischen Maßnahmen erfolgen durch die Administratoren des Medienzentrums.

Zu Ihren Fragen:

Ist für die iPads, die im Zuge der „1:1 Ausstattung mit iPads für alle 5. Klassen der weiterführenden Schulen" besorgt werden, eine Nutzung des Mobile Device Managementsystems (MDM) „Jamf" geplant?
Ja, es wird das Mobile Device Managementsystems (MDM) „Jamf School" benutzt.

Falls ja, welche Maßnahmen werden ergriffen, um sicherzustellen, dass eine Nutzung von „Jamf", das auf Amazon Web Service-Diensten (AWS) basiert, konform mit dem in der EU-geltenden Datenschutzrecht ist?

Folgende Maßnahmen wurden ergriffen:

- Ein AVV wurde abgeschlossen
- Alle Grund- und Ersteinstellungen werden datenschutzkonform im Sinne der gesetzlichen Vorgaben vorgenommen.
- Es werden über Jamf nur wenige Metadaten erhoben
- Es wird von Seiten des Medienzentrums angeregt, Nutzer darüber zu informieren, den Geräten keine Klarnamen zu geben. Sollten Lehrkräfte oder auch Schülerinnen und Schüler mit einer Apple-ID eigene Apps laden dürfen, sollte darauf hingewiesen werden, dass die Administratoren des Medienzentrums diese sehen können und dass dadurch unter Umständen ein Zugriff Dritter ermöglicht wird. Ein inhaltlicher Zugriff auf die Apps ist nicht möglich.

Fazit:

Die datenschutzkonforme Verwendung von Jamf für das Mobile Device Management an Schulen erfordert die Einhaltung bestimmter Richtlinien. Durch den Abschluss eines

Auftragsverarbeitungsvertrags und die Berücksichtigung empfohlener Maßnahmen, wie das Vermeiden von Klarnamen als Gerätenamen und die Verhinderung, dass einzelne Nutzer sich mit einer Apple-ID anmelden, kann der Schutz personenbezogener Daten gewährleistet werden. Die Erfassung von Metadaten beschränkt sich auf erforderliche technische Informationen, während der Zugriff auf Nutzungsdaten und private Informationen der Nutzer nicht ermöglicht wird.

Werden IP-Adressen des MDM auf den Servern gespeichert, besteht keine Möglichkeit, einen Personenbezug herzustellen, da die Netzbetreiber der Schulen (Witcom) und bei den Nutzern zu Hause andere deutsche oder europäische Netzbetreiber (beispielsweise Telekom oder Vodafone) sind. Diese können mangels Rechtsgrundlage nicht durch US-Behörden zur Preisgabe von Identitäten hinter IP-Adressen gezwungen werden.

Selbst wenn es also eine Anordnung von US-Behörden auf Herausgabe gespeicherter Daten an Jamf oder seinen Subunternehmer AWS geben würde, so würden diese keinen Personenbezug liefern können.

Nach alledem ist die Verwendung des MDM mit Hilfe des Anbieters Jamf datenschutzkonform möglich.

Mit freundlichen Grüßen

Imholz
Stadtrat