Zulässigkeit der Nutzung von Chromebooks und G Suite for Education nach dem Urteil des Europäischen Gerichtshofes vom 16. Juli 2020 – C-311/18 („Schrems II“)

Das sog. Schrems II-Urteil des Europäischen Gerichtshofs (EuGH) hat viele Frage über die Zulässigkeit von Datentransfers in die USA aufgeworfen. Google ist daran interessiert, dass Sie Chromebooks und G Suite for Education ohne rechtliche Bedenken verwenden. Google hat daher die Anwaltskanzlei Osborne Clarke PartmbB gebeten, zu einigen relevanten Fragen in Gestalt dieser Q&A Stellung zu nehmen. In diesem Dokument erklären wir Ihnen, warum, die Nutzung von Chromebooks und G Suite for Education an deutschen Schulen nach wie vor datenschutzkonform und im Einklang mit der DSGVO erfolgen kann. Diese Q&A sind nur eine unverbindliche Richtschnur und stellen keine Rechtsberatung gegenüber den Lesern dar.

1. Was hat der EuGH entschieden?

Der EuGH hatte sich im Urteil C-311/18 („Schrems II“) mit der Frage auseinanderzusetzen, unter welchen Umständen personenbezogene Daten aus der EU an einen Empfänger in den USA übermittelt werden dürfen.

Der Gerichtshof hat entschieden, dass eine Übermittlung in die USA auf Grundlage des sogenannten „EU-US-Privacy Shield“, einem Abkommen zwischen der Europäischen Union und den USA, nicht mehr möglich ist. Der Grund hierfür besteht im Wesentlichen darin, dass nach Auffassung des Gerichts US-Amerikanische Behörden theoretisch umfangreiche Zugriffsrechte auf solche Daten haben und keine ausreichenden Rechtsmittel für Nicht-US-Bürger bestehen.

Der Gerichtshof hat aber auch bestätigt, dass die von der EU Kommission erlassenen, sogenannten „Standarddatenschutzklauseln“ (oder auch „Standardvertragsklauseln“) nach Art. 46 Abs. 2 lit. c DSGVO weiterhin Gültigkeit besitzen. Bei Verwendung dieser Klauseln muss jedoch sichergestellt werden, dass ein der EU vergleichbares Datenschutzniveau in dem Empfängerstaat gewährleistet ist – gegebenenfalls, indem zusätzliche Maßnahmen ergriffen werden (s. auch den FAQ des Europäischen Datenschutz-Ausschusses, abrufbar hier https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf).

2. Können Chromebooks und G Suite for Education weiterhin an Schulen genutzt werden?

Ja. Die Nutzung von G Suite for Education und von Chromebooks ist weiterhin zulässig, wenn die genannten Standarddatenschutzklauseln mit Google abgeschlossen werden. Zusätzlich sollten entweder Maßnahmen zur Pseudonymisierung der Schülerdaten getroffen werden (s. Ziffer 2.1) oder die „Managed Guest Session“ genutzt werden (s. Ziffer 2.2).

2.1. Pseudonymisierung von Schülerdaten

Zum einen kann die erforderlich Sicherheit der Schülerdaten durch eine strikte Pseudonymisierung, wie sie z.B. der Landesbeauftragte für den Datenschutz und die Informationsfreiheit des Landes Rheinland-Pfalz vorgeschlagen hat (abrufbar unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/anforderungen-google-classroom.pdf) erreicht werden. Diese Lösungsmöglichkeit hat auch nach dem Schrems II-Urteil Bestand, und wurde ganz aktuell ausdrücklich durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg bestätigt (Orientierungshilfe vom 25.08.2020, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf, Abschnitt III Nr. 1). Diese Maßnahmen sollen sicherstellen, dass die Daten für andere Stellen als die Schule und für Google nicht personenbezogen sind, so dass der Datenschutz vollumfänglich gewährleistet ist.

Konkret können zur Pseudonymisierung der Daten die folgenden Maßnahmen ergriffen werden:

a. **Anlage von Google Accounts durch die Schule:** Alle Google Accounts, die zur Nutzung der Chromebooks und G Suite for Education durch die Schüler genutzt werden sollen, müssen zentral durch die Schule erstellt werden. Die Schüler sollten ihre Google Accounts gerade nicht selbst erstellen und auch keine sonstigen privaten Google Accounts für schulische Zwecke benutzen.

b. **Nutzung von Pseudonymen:** Die Google Accounts können so benannt werden, dass diese nicht die Identität eines Schülers erkennen lassen oder Rückschlüsse auf diese zulassen. Hierfür können die Google Accounts so gewählt werden, dass für Außenstehende nicht erkennbar ist, welcher Schüler welchen Google Account nutzt. Hierbei kann es sich zum Beispiel um eine Reihe von Buchstaben und Zahlen handeln anstelle der Nutzung der Namen der Schüler oder der Klasse als (Teil des) Google Accounts.

c. **Verbot der Privatnutzung:** Die private Nutzung (einschließlich der Nutzung außerhalb der Schule) von schulischen Chromebooks und G Suite for Education, jedenfalls bei Nutzung der schulischen Google Accounts, sollte (bspw. durch die Schulordnung) untersagt werden. Durch die private Nutzung könnten andernfalls Daten anfallen, die es erlauben, Rückschlüsse auf die Identität des Schülers zu ziehen und diese mit dem schulischen Google Account zu verbinden. Das Verbot sollte Schülern und Lehrern klar kommuniziert werden.

d. **Information von Schülern und Lehrern:** Schüler und Lehrer sollten über die bestehenden Risiken und wie diese vermieden werden können, aufgeklärt werden. Hierzu gehört auch, dass in den genutzten Inhalten und der Kommunikation keine identifizierenden Daten angegeben werden sollten.

e. **Getrennte Aufbewahrung der Pseudonym-Listen:** Jede Liste oder andere Quelle, über die herausgefunden werden kann, welches Pseudonym (also welcher Google Account) von welchem Schüler genutzt wird, sollte getrennt von allen Google-Services aufbewahrt werden. Zum Beispiel können diese Quellen auf einem lokalen PC oder einer externen Festplatte abgespeichert werden.

Werden diese Maßnahmen befolgt, sollte eine US-amerikanische Behörde keinen Rückschluss auf die Identität eines Schülers (oder Lehrers) ziehen können. Aus Sicht einer solchen Behörde handelt es sich dann gerade nicht mehr um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO. Diese Pseudonymisierung stellt damit also sicher, dass ein mit der EU vergleichbares Schutzniveau gewährleistet werden kann, sollte Google Daten in den USA verarbeiten.

2.2. Nutzung von „Managed Guest Sessions“

Außerdem können die sogenannten „Managed Guest Sessions“ der Chromebooks genutzt werden. In diesem Modus melden sich die Schüler nicht mit eigenen Google Accounts an und es werden keine Nutzerdaten während des Starts aus der Cloud geladen, so dass das so eingerichtete Chromebook von einer Vielzahl von Personen genutzt werden kann. Da sich die Schüler nicht mit eigenen Google Accounts anmelden, werden bei der Nutzung auch keine personenbezogenen Account-Daten an Google gesendet, insbesondere keine identifizierenden Merkmale wie Namen von Accountinhabern. Insofern ist es auch nicht erforderlich, dass Pseudonyme genutzt und Pseudonym-Listen getrennt aufbewahrt werden. Weiter können, wenn viele Schüler die gleiche „Managed Guest Session“ nutzen, die einzelnen Aktivitäten nicht mehr den einzelnen Schülern zugeordnet werden. Wenn die „Managed Guest Session“ endet, wird der Benutzer automatisch abgemeldet und alle lokalen Benutzerdaten werden vom Gerät gelöscht.

Als zusätzliche Maßnahmen sollten aber auch bei der Nutzung von „Managed Guest Sessions“ die Privatnutzung, einschließlich der Anmeldung mit einem privaten Google Account, untersagt werden (s.o. lit. c) sowie Schüler und Lehrer entsprechend über die Regeln zur Nutzung der Chromebooks unterrichtet werden (s.o. lit. d). Weiter sollte die „Managed Guest Session“ so konfiguriert werden, dass das Chromebook automatisch in der „Managed Guest Session“ startet und eine Anmeldung mit einem anderen Google Account nicht möglich ist. Auch der Gast Modus sollte abgestellt werden.

Bitte beachten Sie, dass bei „Managed Guest Sessions“ manche Funktionen nicht zur Verfügung stehen. Mehr Informationen zum Einrichten und Nutzen von „Managed Guest Sessions“ finden Sie hier: https://support.google.com/chrome/a/answer/3017014?hl=de.

3. Müssen Auftragsverarbeitungsverträge abgeschlossen werden?

Ja. Google wird als Dienstleister bei der Datenverarbeitung tätig, weswegen ein sogenannter Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO abgeschlossen werden muss.

Der Auftragsverarbeitungsvertrag zu G Suite for Education ist hier abrufbar: https://gsuite.google.com/terms/dpa_terms.html. Der Auftragsverarbeitungsvertrag für Google Chrome ist hier abrufbar: https://www.google.com/chrome/terms/dpa_terms.html.

4. Was müssen Schulen außerdem tun?

Schulen sollten die folgenden Schritte ergreifen, um weiterhin eine datenschutzkonforme Nutzung von Chromebooks sowie G Suite for Education zu gewährleisten:

- Abschluss der Standarddatenschutzklauseln: Schulen müssen die sogenannten Standarddatenschutzklauseln mit Google abschließen. Die Standarddatenschutzklauseln für das Chrome Education Upgrade sind bereits im Chrome Auftragsverarbeitungsvertragt enthalten, so dass die Standardvertragsklauseln, abrufbar unter https://cloud.google.com/terms/chrome-enterprise/mcc_terms, automatisch gelten. Für G Suite for Education bestehen die Standarddatenschutzklauseln ebenfalls bereits, da diese stets zusammen mit den entsprechenden Nutzungsverträgen abgeschlossen werden. Die Standardvertragsklauseln für G Suite for Education sind hier abrufbar: https://gsuite.google.com/intl/de/terms/mcc_terms.html
- Zusätzlich kann eine der folgenden Sicherheitsmaßnahmen ergriffen werden:
  - ✓ Umsetzung der Pseudonymisierung: Schulen können die unter Ziffer 2.1 dargestellten Maßnahmen zur Pseudonymisierung der Google Accounts und der übermittelten Daten umsetzen. Diese stellen sicher, dass anhand der im Schulunterricht produzierten Daten, kein Schüler identifiziert werden kann, so dass eventuelle Verarbeitungen in den USA abgesichert sind.
  - ✓ Nutzung von „Managed Guest Sessions“: Alternativ können Schulen die „Managed Guest Sessions“ nutzen, bei denen Schüler keine eigenen Accounts nutzen, so dass in dieser Hinsicht auch keine personenbezogenen Daten anfallen (s. Ziffer 2.2). Auch hierbei sollten Lehrer und Schüler aber entsprechend informiert werden und eine Privatnutzung der Chromebooks sollte ausgeschlossen sein. Eine Nutzung anderer Google Accounts sollte durch die Konfiguration der „Managed Guest Session“ ausgeschlossen werden.

✸ ✸ ✸ ✸ ✸