STADTBÜCHEREIKAPPELN

Stellungnahme datenschutzkonformer Einsatz von OverDrive, 5. Dezember 2022

A. Ausgangssituation

Der Büchereiverein ist in folgender Angelegenheit Konsortialführer:

Den Büchereien soll es (weiterhin) ermöglicht werden, E-Hörbücher anzubieten.

Da das deutsche Unternehmen divibib GmbH als Anbieter der „Onleihe“ erhebliche technische Probleme hat, die auch über einen längeren Zeitraum nicht behoben werden konnten, kommt mangels weiterer Auswahlmöglichkeit nur noch der US-Anbieter OverDrive in Betracht. Die Bibliotheken des Verbundes „Onleihe zwischen den Meeren“ haben sich auf der Verbundkonferenz im September 2022 einstimmig für die Zurverfügungstellung der OverDrive-Dienstleistung ausgesprochen.

B. Situation hinsichtlich OverDrive im Einzelnen

Da es sich bei OverDrive um einen US-Anbieter handelt, war zu überprüfen, ob und wie eine Zusammenarbeit mit OverDrive datenschutzkonform möglich ist.

Mit Blick auf die im Schweben befindliche Rechtslage steht der eventuellen Gefahr einer (rechtswidrigen) Übermittlung personenbezogener Daten in die USA der Gedanke gegenüber, den Nutzenden Hörbücher anzubieten, die sie sonst nicht (mehr) erhalten würden.

Ausführungen zur derzeitigen Rechtslage in Bezug auf den Drittstaatentransfer in die USA befinden sich unten unter C..

Aufgrund der Rechtslage waren folgende Überlegungen anzustellen und zu dokumentieren:

- *eine systematische Beschreibung des geplanten Datentransfers samt Zweck und berechtigter Interessen, die der Verantwortliche verfolgt*
- *eine Bewertung der Notwendigkeit und der Verhältnismäßigkeit des Datentransfers in Bezug auf den Zweck*
- *eine Bewertung der Sensibilität der übermittelten Daten und der entstehenden Risiken für die Betroffenen*
- *die zur Bewältigung der Risiken geplanten zusätzlichen Maßnahmen*

I. Datenübermittlung Stadtbücherei – OverDrive?

Die Fahrbüchereien übermitteln an OverDrive mittels einer Schnittstelle nur, ob es sich bei einer Anmeldung über die LibbyApp oder über die Webanwendung um einen Nutzenden mit gültigem Bibliotheksausweise handelt. Darüber erhält OverDrive nur Kenntnis von der Ausweisnummer des jeweiligen Nutzenden.

Die Ausweisnummer wird von der Bibliothek verifiziert, nachdem der/die Nutzende sich in der App/Webanwendung damit angemeldet hat.

Eine Fahrbücherei authentifiziert damit als einziges personenbezogenes Datum die Ausweisnummer des/der jeweiligen Nutzenden.

Die Übermittlung aller anderen personenbezogenen Daten erfolgt durch den/die Nutzenden selbst, wobei eine Nennung des Klarnamens nicht vorgesehen ist.

Die Aufklärung der Sachlage erfolgte unter Einbezug von OverDrive unter Zuhilfenahme der Kriterien für ein Transfer Impact Assessment (TIA) nach Rosenthal.

Fazit zu I.

=> Zweck und berechtigtes Interesse liegen in der Zurverfügungstellung einer Anwendung zur Ausleihe von Hörbüchern im Rahmen der Bibliotheksmitgliedschaft durch den Büchereiverein als Träger der Fahrbüchereien

=> Die Notwendigkeit ergibt sich aus einer fehlenden europäischen Alternative eines Hörbuchanbieters. Für die Nutzenden wird das Angebot der Büchereien /Fahrbüchereien in diesem Bereich aufrechterhalten.

=> Seitens der Fahrbüchereien handelt es sich nicht um eine Datenübermittlung in die USA, sondern nur um eine Authentifizierung der Zugangsberechtigung Ausweisnummer. **Es werden von den Fahrbüchereien keine personenbezogenen Daten übermittelt. Damit ist seitens der Fahrbüchereien hinsichtlich der Erfüllung der Datenschutzkonformität nichts weiter zu beachten.** Ein SCC-Vertrag (Standard Contractual Clauses) im Sinne der DSGVO zwischen OverDrive und den Fahrbüchereien in Trägerschaft des Büchereivereins ist deshalb nicht notwendig. Die Daten der Ansprechpartner in den Büchereien, die in den Anmeldeformularen für die Nutzung der Schnittstelle enthalten sind, sind vertraglicher Bestandteil und nicht im Sinne des Drittstaatentransfers relevant, weshalb dafür nach momentaner Einschätzung kein SCC abgeschlossen werden muss.

=> **Die Lesenden nutzen den Dienst von OverDrive in eigener Verantwortung, die Datenübermittlung erfolgt damit auf Initiative des Lesenden selbst.** Hier bietet es sich für die Fahrbüchereien als Vermittler des Dienstes an, im Vorwege eine entsprechende Information bereitzustellen und die Lesenden über die Rechtslage und eventueller Risiken der Datenübermittlung aufzuklären.

II. Datenübermittlung Nutzenden - OverDrive

1) Verlinkung auf deutsche DSE von OverDrive bzw. Nennung des Links

OverDrive stellt eine ausführliche Datenschutzerklärung (DSE) in Deutsch aus der Perspektive der DSGVO zur Verfügung.

Hierbei muss deutlich gemacht werden, dass OverDrive den Bestimmungen der DSGVO nicht unterliegt, auch wenn die DSE entsprechend ausgestaltet ist.

Zu der Datenschutzerklärung in Deutsch besteht allerdings kein direkter Zugang über die App oder die Webseite. Die dort genannte Datenschutzerklärung verlinkt auf die englische Version.

Entsprechend müsste bei einer Information für Nutzende durch die Fahrbüchereien auf die deutsche Version verlinkt werden.

2) Zusätzliche Datenverarbeitungsinformation /Einwilligungserklärung für unter-16-Jährige

Ferner soll die Information enthalten:

- Erläuterung, warum die Wahl auf OverDrive fiel
- Hinweis auf die Rechtslage in den USA (anlasslose Massenüberwachung)
- Hinweis, dass der/die Nutzende selbst über die Übermittlung seiner/ihrer Daten in die USA als unsicheres Drittland entscheidet; Minderjährige bzw. unter-16-Jährige können dies nicht rechtswirksam entscheiden und benötigen die Einwilligung der Sorgeberechtigten
- Hinweis, dass OverDrive angibt, bislang noch nicht zur Herausgabe von Daten an Sicherheitsbehörden aufgefordert worden zu sein

(Antwort von OverDrive in der Mail von F. Graul vom 6.10.2022: OverDrive wurde noch nie von US-Behörden zur Mitarbeit gezwungen oder zur freiwilligen Mitarbeit aufgerufen oder von US-Behörden um den Erhalt personenbezogener Daten gebeten oder die Überwachung der Kommunikation durchzuführen. Falls es in der Zukunft dazu kommt, dass wir nach geltendem US-Recht zur Zusammenarbeit verpflichtet werden würden, würde OverDrive versuchen, den Umfang einer erzwungenen Offenlegung anzufechten und einzuschränken.)

- Übersicht über die erhobenen personenbezogenen Daten mit Verweis auf die Ziffern in der DSE
- Hinweis, dass OverDrive zur genauen Dauer der Aufbewahrung keine Angaben macht
- Deshalb Empfehlung, das Konto bei nicht-mehr-Benutzung aktiv zu löschen und im Anschluss eine Anfrage auf Auskunft zu stellen.
- Beschwerderecht: Hier muss der/die Nutzende sich im Klaren sein, dass eine Beschwerde bei einer deutschen Aufsichtsbehörde nutzlos ist, da es sich um einen US-Anbieter handelt, der nicht dem deutschen Recht unterliegt.

Fazit zu II.

- ist umgesetzt in dem Dokument „OverDrive – Hinweise für Lesende“

C. Datenschutz - Allgemeine Rechtslage bei sog. Drittstaatentransfers zur Verdeutlichung der angestellten Überlegungen

(Bezugnehmend und Textauszüge übernommen aus: Kommt bald "Schrems III"?, Gastbeitrag von Jens Nebel, 29.10.2022 https://www.lto.de/recht/hintergruende/h/eu-usa-daten-transfer-eugh-schrems-datenschutz-geheimdienste-unternehmen/)

Bei der Nutzung von Online-Diensten werden immer personenbezogenen Daten an den Anbieter übermittelt.

- Dies sind zum einen die Daten des technischen Gerätes des Nutzers, die zur Darstellung des Angebots notwendig sind.
- Zum anderen sind dies inhaltliche Daten, die im Rahmen der Verwendung der Anwendung übermittelt werden.

Handelt es sich bei dem Anbieter des Online-Dienstes um eine Firma mit Sitz in Deutschland oder in einem EU-Mitgliedsstaat, unterliegt die Firma den gesetzlichen Vorgaben der EU-DSGVO und hat für die Datenschutzkonformität zu sorgen oder kann bei einem Verstoß dagegen vom Nutzer oder von einer Datenschutz-Aufsichtsbehörde in Anspruch genommen werden.

Anbieter in sogenannten Drittstaaten, wie die USA, unterliegen nicht der EU-DSGVO.

In USA gelten außerdem Bestimmungen, die es den dortigen Sicherheitsbehörden ermöglichen, Daten von EU-Bürgern massenhaft und anlasslos auszuwerten und diese Daten auch gegen sie zu verwenden, ohne dass die EU-Bürger Rechtsschutzmöglichkeiten haben. In den USA gibt es damit kein den EU-Regeln entsprechendes Datenschutzniveau. Durch das sog. Schrems II-Urteil des EuGH im Juli 2020 wurden Datentransfers in die USA, die nicht auf einer gesetzlichen Grundlage oder auf einer Einwilligung beruhen, deshalb zum Datenschutzverstoß erklärt.

Präsident Joe Biden hat am 7. Oktober 2022 eine "Excecutive Order" erlassen, die den Datenschutz von Europäern gegen Abhöraktivitäten der US-Geheimdienste verbessern soll.

Neben den quasi schrankenlosen Befugnissen der US-Geheimdienste monierte der EuGH die fehlenden Rechtsschutzmöglichkeiten für betroffene EU-Bürger. Beide Punkte werden in dem neuen Präsidialerlass jetzt adressiert: So ist die Auswertung nur noch auf Basis bestimmter festgelegter legitimer Zwecke zulässig und muss verhältnismäßig sein. Zudem erhalten EU-Bürger die Möglichkeit, einen eigens hierfür eingerichteten "Data Protection Review Court" in den USA anzurufen.

Nach mehr als einem halben Jahr am Verhandlungstisch ist nun die EU-Kommission am Zug: Sie muss den Erlass formal bewerten und kann die USA per Angemessenheitsbeschluss wieder zum "sicheren Drittland" erklären. Beobachter erwarten, dass dies in etwa einem halben Jahr der Fall sein könnte.

Auch nach einer positiven Bewertung der EU-Kommission steht dann noch nicht abschließend fest, dass diese neu geschaffene Lage einer sehr wahrscheinlichen Überprüfung durch den EuGH standhält.

„Jedenfalls bis zu einem Angemessenheitsbeschluss bleibt Unternehmen, die sich mit über die Cloud angebotenen digitalen Produkten und Services befassen, nur der Weg über die von der EU- Kommission freigegebenen sog. "Standardvertragsklauseln". Dieser Weg allerdings bleibt rechtlich unsicher. Denn der EuGH schrieb den Verwendern der Standardvertragsklauseln in der "Schrems II"-Entscheidung zusätzliche Pflichten ins Stammbuch: Betreibt das Zielland – wie die USA – rechtsstaatlich fragwürdige Überwachungsprogramme, sind die Musterklauseln allein nicht ausreichend.

Vielmehr müssen die datenexportierenden EU-Unternehmen zusätzliche Maßnahmen treffen, um die personenbezogenen Daten zu schützen. Beispielsweise kann dies eine wirksame Verschlüsselung der Daten notwendig machen. Eine solche Verschlüsselung kollidiert jedoch mit vielen Cloud-Anwendungen. Denn um

die Daten in der Cloud-Software verarbeiten zu können, müssen sie entschlüsselt werden – was sie wiederum dem technischen Zugriff der NSA und anderen Geheimdiensten aussetzt.

Viele europäische Unternehmen flüchten sich bei der Nutzung von Cloud-Anwendungen daher derzeit in zusätzliche (gegen staatliche Zugriffe aber nicht wirksame) vertragliche Maßnahmen. Zudem kommen sie in einer schriftlichen Risikoabschätzung – meist als Transfer Impact Assessment (TIA) bezeichnet – zum Ergebnis, dass sich der Datentransfer noch im vertretbaren Bereich bewege. Dabei argumentieren die Unternehmen im TIA meist risikobasiert: Weil es beim konkreten ausländischen Anbieter in der Vergangenheit nie oder nur selten zu einem Datenzugriff staatlicher Stellen gekommen ist, sei die Gefahr eines solchen Zugriffs auch in der Zukunft gering.

Allerdings haben die Datenschutzbehörden einem solchen "risikobasierten Ansatz" eine Absage erteilt. Eine gerichtliche Klärung der Frage steht zwar noch aus. Die Gefahr ist aber groß, dass der "risikobasierte Ansatz" für unzulässig befunden wird. Das Risiko für Unternehmen ist beträchtlich: So entfielen bei einem Bußgeld von mehr als acht Millionen Euro, das die spanische Aufsichtsbehörde 2021 gegen Vodafone verhängte, allein zwei Millionen Euro auf den Verstoß gegen die internationalen Datentransfervorschriften der DSGVO. Theoretisch kann sich ein Bußgeld sogar auf bis zu 20 Millionen EUR oder vier Prozent des weltweiten Jahresumsatzes belaufen.

Auch deutsche Unternehmen können dabei in den Fokus der Aufsichtsbehörden geraten. So haben Datenschutzbehörden – beispielsweise aus Bayern, Berlin oder Baden-Württemberg – bereits etliche deutsche Unternehmen, beispielsweise aus den Bereichen Bewerberportale und Webhoster, ins Visier genommen. Alle angeschriebenen Unternehmen müssen zunächst einen Fragebogen ausfüllen, der es in sich hat: So müssen Unternehmen beispielsweise selbst einschätzen, ob sie Section 702 des Foreign Intelligence Surveillance Act (FISA) der USA unterfallen. Ohne die Hilfe eines amerikanischen Anwaltes dürfte das für viele Unternehmen kaum zu beantworten sein. Die Stoßrichtung der peniblen Nachfragen ist klar: Deutsche Unternehmen sollen dazu gebracht werden, sich von US-Anbietern zu trennen und auf europäische Anbieter auszuweichen. Umso wichtiger ist es, dass die Datenschutztransfers zum wichtigen Handelspartner USA nun wieder auf ein sichereres Fundament gestellt werden.“ (Quelle unter C.)