Datenablage bei Amazon Web-Services (AWS) und Schrems II – eine Entscheidung des Conseil d´etat in Frankreich zum Thema

Am 12. März 2021 hat der **Conseil d´etat** (Frankreich; höchstes Verwaltungsgericht) in einem Verfahren bei dem es um die **möglichen Zugriff von US-Behörden auf Daten geht** (Stichwort: Schrems II), eine **Entscheidung** gefällt.

Die Verfahrensgrundlage

In Frankreich ist die **Anmeldung zu COVID-19 Tests** über das Internet möglich, und die Daten werden von Doctolib verarbeitet. Doctolib verwendet **Amazon Web-Services (AWS) als Hostingdienstleister**.

Dagegen wendeten sich einige Organisationen, die darlegten, dass dies gegen die **Grundsätze**, die im **Schrems II – Urteil des EuGH vom 16.7.2020 verstößt**, da es zu einem **Datenzugriff durch US-Behörden** käme bzw. eine **Weiterleitung der Daten in die USA** möglich sei.

Die Entscheidung

Das Conseil d´etat hat jedoch dargelegt, dass die Verwendung von AWS als Hosting-Provider nicht unmittelbar dazu führt, dass die Verarbeitung der personenbezogenen Daten (auch wenn es sich um Gesundheitsdaten handelt) gegen die DSGVO verstößt,

da zusätzliche Maßnahmen implementiert wurden, die das Datenschutzniveau (das in den USA nicht ausreichend ist) auf ein angemessenes Maß anzuheben.

Es sei zwar nach den **US-amerikanischen Bestimmungen** (Article 702 of the Foreign Intelligence Surveillance Act or Executive Order 12333) ein **Zugriff der US-Behörden** auf die Daten möglich, das **AWS eine Tochtergesellschaft eines amerikanischen Konzerns** und noch dazu eines Internetdiensteanbieters sei, aber die Parteien hätten ausreichende zusätzliche Maßnahmen getroffen, nämlich:

Die zusätzlichen Maßnahmen der Parteien

Rechtliche Maßnahmen:
Das Gericht hat anerkannt, dass im Vertrag zwischen Doctolib und AWS Sarl, Vorsorge getroffen wurde, wenn es zu einer Anforderung des Zugriffes auf die personenbezogenen Daten durch eine ausländische Behörde kommt. Im Vertrag ist vereinbart, dass **AWS Sarl mit dem Sitz in der EU die Anordnung der Behörden bekämpfen** wird.

Technische Maßnahmen:
Die Daten wurden **verschlüsselt** abgelegt, und **der Schlüssel wird bei einer dritten Partei als Treuhänder verwahrt**, sodass AWS selbst keinen direkten Zugriff auf die gehosteten (Inhaltsdaten) hat. Dies verhindert, dass die Daten von Dritten ausgelesen werden können.

Weitere Maßnahmen:
Überraschenderweise stellte das Conseil d´etat auch fest, dass es sich bei den Daten **nicht um Gesundheitsdaten** handelt, da es nur „**Terminvereinbarungen**“ seien, die gespeichert werden. Der Zusammenhang mit der COVID-19 Impfung spielte für die Richter dabei keine Rolle. Anders sieht das mE die Österreichische Datenschutzbehörde bei der Frage der Gästeregistrierung in Wien.

Die **Speicherfrist (Löschfrist)** wurde mit **drei Monaten** festgelegt, und die betroffenen Personen haben überdies die Möglichkeit, die **Daten selbst unmittelbar und jederzeit zu löschen**.

Schlussfolgerung:

Die Folgen dieser Entscheidung sind mE sehr weitreichend, da zwar festgestellt wird, dass bei Tochtergesellschaften von US-amerikanischen Unternehmen ein Zugriff der US-Behörden möglich ist, aber ein Weg mit technischen und rechtlichen Maßnahmen aufgezeigt wird, Daten dennoch durch diese Unternehmen verarbeiten zu lassen, wobei der Verschlüsselung der Daten mE eine entscheidende Rolle zukommt.

Diese (technische) Maßnahme (Encyrption) hat auch der Europäische Datenschutzausschuss in den Empfehlungen 1/2020 (10.11.2020) zu Maßnahmen in Zusammenhang mit Schrems II als eine der möglichen Mittel genannt.