SCHINDLER
ATTORNEYS

Datenschutzrechtliche Implikationen im Zusammenhang mit Dienstreisen und Remote Work von Mitarbeitern in Drittstaaten

In vielen Branchen gehören Dienstreisen von Mitarbeitern zur Tagesordnung, aber auch die Möglichkeit des Remote Workings wird seit der Pandemie immer häufiger genutzt. Doch ob und welche datenschutzrechtlichen Implikationen damit möglicherweise verbunden sein können, ist oft nicht bekannt.

Wenn nämlich ein Mitarbeiter von einem Drittland aus (außerhalb der EU oder des EWR) auf personenbezogene Daten von Kunden, Kollegen, Bewerbern und anderen Personen zugreift, stellt sich die Frage, ob dieser Zugriff als eine „Datenübermittlung“ im Sinne der DSGVO zu betrachten ist.

Eine Übermittlung personenbezogener Daten in Länder außerhalb der EU oder des EWR (*Drittstaatentransfer*) ist nämlich nur in den in Kapitel 5 (*Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen)* der DSGVO genannten Fällen zulässig. Dies ist vor allem dann der Fall, wenn ein Angemessenheitsbeschluss der europäischen Kommission vorliegt oder Standardvertragsklauseln, verbindliche Unternehmensregeln oder Zertifizierungen verwendet werden.

Bei der Verwendung von Standardvertragsklauseln muss der Datenexporteur gemeinsam mit dem Datenimporteur überprüfen, ob im Drittland tatsächlich ein angemessener Schutz der personenbezogenen Daten gewährleistet werden kann. Es darf insbesondere kein Grund zur Annahme bestehen, *„dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten den Datenimporteur an der Erfüllung seiner Pflichten gemäß der Standardvertragsklauseln hindern.*“

Vor kurzem hat die Belgische Datenschutzbehörde (kurz *DPA*) die Ansicht vertreten, dass ein Mitarbeiter nicht als Verantwortlicher oder Auftragsverarbeiter gilt, da er dem Arbeitgeber direkt

unterstellt ist und nur im Rahmen der Weisungen, Befugnisse und der Aufsicht des Arbeitgebers Daten verarbeiten darf. Demgemäß geht die DPA davon aus, dass die Verpflichtungen im Sinne des Kapitel 5 der DSGVO nicht anwendbar sind.

Der Arbeitgeber ist somit nicht verpflichtet, die im dritten Absatz genannten Maßnahmen zu implementieren, selbst wenn im jeweiligen Drittland, in dem sich der Mitarbeiter befindet, kein angemessenes Schutzniveau besteht. Sehr wohl hat er jedoch als Verantwortlicher oder Auftragsverarbeiter dafür zu sorgen, dass die allgemeinen Grundsätze der DSGVO eingehalten werden.

Das bedeutet, dass der Arbeitgeber insbesondere technische und organisatorische Maßnahmen (kurz TOMs) implementieren muss, um die Sicherheit der Verarbeitung personenbezogener Daten sicherzustellen. Solche TOMs sind beispielsweise die Verschlüsselung oder Pseudonymisierung von personenbezogenen Daten. Ferner wird empfohlen, interne Vorgaben für den Fall zu haben, dass ein Mitarbeiter in einem Drittland arbeitet oder eine Dienstreise in ein solches unternimmt. Dadurch können Mitarbeiter über potentielle Risiken aufgeklärt werden, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten in Drittländern bestehen. Dazu gehört vor allem, dass nicht über ungesicherte öffentliche Internetverbindungen auf das Unternehmensnetzwerk zugegriffen werden soll.

Wir erachten die Auffassung der DPA für richtig, weshalb zuvor Gesagtes auch für Österreich zu beachten ist. Somit sollten auch österreichische Arbeitgeber im Auge behalten, von wo aus Mitarbeiter Zugriff auf personenbezogene Daten haben, falls diese „aus der Ferne“ arbeiten.

DR. PHILIPP SPRING
PARTNER
LEITER IP/IT