September 2020

Newsletter Nr. 145

Swiss-US Privacy Shield bietet nach Auffassung des EDÖB kein angemessenes Datenschutzniveau:

Der EDÖB folgt damit – wenig überraschend – den Erwägungen des EuGH zum EU-US Privacy Shield im Urteil «Schrems II». Auch Standardvertragsklauseln stellen in vielen Fällen keine ausreichende Grundlage für Datenübermittlungen in Drittländer dar. Schweizer Unternehmen sollten deshalb prüfen, wie sie künftig personenbezogene Daten in Drittländer ohne angemessenes Datenschutzniveau datenschutzkonform übermitteln können.

walderwyss rechtsanwälte

Von Jürg Schneider
Dr. iur., Rechtsanwalt
Partner
Telefon direkt: +41 58 658 55 71
juerg.schneider@walderwyss.com

und David Vasella
Dr. iur., Rechtsanwalt
Partner
Telefon direkt: +41 58 658 52 87
david.vasella@walderwyss.com

und Lena Götzinger
Rechtsanwältin (Rechtsanwaltskammer Frankfurt am Main)
Associate
Telefon direkt: +41 58 658 56 63
lena.goetzinger@walderwyss.com

Mit Mitteilung vom 8. September 2020 hat der EDÖB die USA aus der von ihm geführten Liste mit Staaten, die ein angemessenes Datenschutzniveau bieten, entfernt. Datenübermittlungen aus der Schweiz in die USA allein auf Basis des Privacy Shield sollten deshalb im Regelfall nicht mehr durchgeführt werden. Auch auf Standardvertragsklauseln können sich Schweizer Unternehmen nicht unbesehen verlassen. Das führt zu Handlungsbedarf für Unternehmen in der Schweiz

Im Ergebnis wenig Überraschendes

Die Stellungnahme des Eidgenössischen Datenschutz- und Informationsbeauftragten (EDÖB), wonach für unter dem Swiss-US Privacy Shield in die USA übermittelte Daten kein angemessenes Datenschutzniveau mehr besteht, ist nach dem Urteil «Schrems II» des Europäischen Gerichtshofs (EuGH) nicht überraschend. Mit diesem hat der EuGH den EU-US Privacy Shield mit sofortiger Wirkung für unwirksam erklärt und an den Einsatz von Standardvertragsklauseln bei Datentransfers zusätzliche Anforderungen gestellt.

Seine Einschätzung begründet der EDÖB (dem EuGH folgend) im Wesentlichen mit weitreichenden Zugriffsmöglichkeiten der US-Nachrichtendienste auf die übermittelten Daten und mit dem Fehlen eines ausreichenden Rechtsschutzes der Betroffenen. Entsprechend hat der EDÖB die Vereinigten Staaten von der Liste mit Staaten gestrichen, die ein angemessenes Datenschutzniveau gewährleisten. Zwar hat der Swiss-US Privacy Shield rechtlich weiterhin Bestand. Die Staatenliste stellt lediglich eine widerlegbare Vermutung auf, ob (und ggf. unter welchen Voraussetzungen) ein angemessenes Datenschutzniveau im Zielland besteht. In praktischer Hinsicht ist ein Datentransfer in die USA auf Basis des Swiss-US Privacy Shield jedoch nicht mehr zu empfehlen.

Stattdessen sind Datentransfers in die USA zukünftig anders abzusichern. Zumindest für grosse Datenbestände und für regelmässige Übermittlungen stehen dabei die in Art. 6 Abs. 2 lit. a DSG genannten Garantien im Fokus, vor allem die EU-Standardvertragsklauseln. Auch Standardvertragsklauseln bieten nach Ansicht des EDÖB «in vielen Fällen» aber kein angemessenes Datenschutzniveau, weil sie nicht in der Lage sind, den Zugriff auf Personendaten durch ausländische Behörden zu verhindern. Einen echten «Standard» stellen diese so betrachtet nicht mehr dar; vielmehr seien sie je nach Umständen zu ergänzen (auf welche Weise, lässt der EDÖB freilich offen).

Handlungsbedarf für Schweizer Unternehmen

Standardvertragsklauseln – und ggf. auch «Binding Corporate Rules» (BCR) – sind deshalb darauf zu prüfen, ob diese im Einzelfall einen angemessenen Schutz für die Übermittlung von Daten ins Zielland gewährleisten. Dies gilt für bereits geschlossene als auch neu zu verwendende Standardvertragsklauseln - nicht nur bei Datentransfers in die USA. Vielmehr sind die Einschätzungen des EDÖB zu vertraglichen Garantien für alle Staaten relevant, die in der Staatenliste als solche ohne ein angemessenes Datenschutzniveau geführt sind.

Sollen sich Übermittlungen auf vertragliche Garantien stützen, hat der Übermittler nach der EDÖB-Stellungnahme im Einzelfall zu prüfen (durch eine Risikoanalyse), ob zusätzliche Massnahmen zum angemessenen Schutz der exportierten Personendaten erforderlich sind. Dabei ist laut EDÖB besonders zu berücksichtigen, ob der Datenimporteur einer Gesetzgebung unterliegt, die ausländischen Behörden erlaubt, auf die ihm übermittelten Daten zuzugreifen.

Entscheidend ist allein, ob der Empfänger einer entsprechenden Gesetzgebung unterfällt. Wünschenswert wäre diesbezüglich eine Differenzierung gewesen. Es sollte nicht nur das theoretische Risiko des Datenzugriffs durch ausländische Behörden massgeblich sein für die Frage, ob eine Übermittlung datenschutzkonform ist. In tatsächlicher Hinsicht werden einige Anbieter – je nach Geschäftsmodell – eher mit einem Zugriff von Behörden rechnen müssen als andere, obwohl all diese Anbieter gleichermassen in den Anwendungsbereich der entsprechenden Gesetzgebung fallen; Datenexporteure dürfen und sollen diese Eintretenswahrscheinlichkeit berücksichtigen.

Stellen sich die Standardvertragsklauseln nach der Risikoanalyse als unzureichend heraus, seien diese durch weitere Klauseln zu ergänzen. Der EDÖB lässt aber offen, um welche Klauseln es sich dabei handeln könnte. Erweisen sich auch ergänzende vertragliche Garantien als ungeeignet, das vom Exporteur einzuschätzende Risiko ausreichend zu senken, sind gemäss der EDÖB-Stellungnahme technische Massnahmen zu ergreifen, um den Behördenzugriff faktisch zu verhindern oder zu erschweren.

Zu diesem Zweck ist laut EDÖB eine Verschlüsselung von zu übermittelnden Daten denkbar – nach den Prinzipien BYOK (bring your own key) und BYOE (bring your own encryption) –, wenn diese beim Empfänger lediglich gespeichert werden. So liegen im Zielland keine Klardaten vor. Bei über die reine Datenhaltung hinausgehenden Dienstleistungen im Zielland gestalten sich technische Massnahmen nach Ansicht des EDÖB jedoch «anspruchsvoll», was sicher keine Untertreibung ist. Kann der Zugriff von ausländischen Behörden durch technische Massnahmen nicht verhindert werden, empfiehlt der EDÖB, auf die Übermittlung von Personendaten in den nicht gelisteten Staat gestützt auf vertragliche Garantien zu verzichten.

Was zu tun ist

Wir empfehlen Schweizer Unternehmen, zunächst ein Verzeichnis aller Datentransfers in ihrem Verantwortungsbereich zu erstellen, sofern ein solches nicht bereits vorliegt (z.B. als Teil eines Verfahrensverzeichnisses oder im Rahmen eines Vendor bzw. Third Party Management). So kann ermittelt werden, ob Daten an den eigenen Vertragspartner in Drittstaaten ohne angemessenes Schutzniveau übermittelt oder an in solchen Staaten tätige Subunternehmer des eigenen Vertragspartners weitergeleitet werden. Trifft dies zu, sollten Schweizer Unternehmen anschliessend in Betracht ziehen, die entsprechenden Vertragspartner im Ausland zu kontaktieren, sie über die Stellungnahme des EDÖB und die daraus folgenden Konsequenzen informieren und sich – bei grösseren Anbietern – nach Abhilfemassnahmen des Anbieters erkundigen.

Auf Basis des Verzeichnisses kann im nächsten Schritt eine Risikoanalyse durchgeführt werden. Dabei wird der Dienstleister bzw. Vertragspartner gegebenenfalls unterstützen können – etwa bei Klärung der Frage, welche Verwaltungspraxis Behörden im Zielland verfolgen oder welche Rechtsschutzmöglichkeiten Betroffenen zur Verfügung stehen. Werden Daten nicht nur aus der Schweiz, sondern auch aus dem übrigen Europäischen Wirtschaftsraum in Länder ohne angemessenes Datenschutzniveau übermittelt, ist es sinnvoll, im gleichen Zug zu prüfen, ob nach den Vorgaben des EuGH und den zuständigen Datenschutzbehörden Anpassungen der bisherigen Übermittlungspraxis geboten sind.

Das weitere Handeln hängt von den Risiken ab. Kann eine Ergänzung der Standardvertragsklauseln die Risiken ausreichend mitigieren, sollten sich Schweizer Unternehmen mit dem Datenempfänger über eine Änderung der Bestimmungen der Standardvertragsklauseln verständigen.

Die vom Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg veröffentlichte Orientierungshilfe kann hierzu Hinweise geben.

Stellen sich vertragliche Anpassungen als unzureichend heraus, können unter Umständen technische Massnahmen zur Risikosenkung beitragen. Bei vielen Diensten – insbesondere SaaS-und PaaS-Diensten – ist eine Verschlüsselung faktisch jedoch kaum möglich. Alternativen sind unter Umständen eine Anonymisierung oder Pseudonymisierung von übermittelten Daten.

Können weder vertragliche Ergänzungen noch technische Massnahmen den Risiken ausreichend begegnen, bleibt nur zu prüfen, ob ein Dienstleister in einem Land mit angemessenem Datenschutzniveau in Frage kommt. Dies werden insbesondere Länder des Europäischen Wirtschaftsraums sein (wobei in diesem Fall zu prüfen ist, ob und unter welchen Umständen ein Datenzugriff von einem anderen Standort aus möglich ist und welche Risiken sich aus dieser Möglichkeit ergeben).

Der EuGH und die Behörden haben ein politisches Problem den Unternehmen zugespielt. Es ist aber offensichtlich, dass sich dieses Problem – das auf einem unterschiedlichen Verständnis des Datenschutzes und seiner Bedeutung beruht – nicht durch eine Anpassung der Unternehmenspraxis lösen lässt. Die Datenschutzbehörden werden ihr Vorgehen daher am Grundsatz der Verhältnismässigkeit auszurichten haben, soll der Unternehmensdatenschutz glaubwürdig bleiben. Immerhin sind die EU und die USA im Gespräch. Vorderhand darf man also auf einen «Privacy Shield Plus» und auf die bereits angekündigten, an «Schrems II» angepassten Standardvertragsklauseln hoffen.

Zudem hat der EDÖB angekündigt, beizeiten weitere Hinweise zum datenschutzverträglichen Export von Personendaten in die USA und anderen nicht gelisteten Drittstaaten zu geben – wir hoffen, dass diese Hinweise rasch verfügbar und inhaltlich gehaltvoll sein werden.