

Datentransfer International

Mit der Entsendung von Mitarbeitern ins Ausland ist oftmals auch die Notwendigkeit des Abschlusses personengebundener Versicherungen für den entsandten durch den Arbeitgeber verbunden. Werden solche Versicherungen im Zielland abgeschlossen, oder sind diese dort obligatorisch, müssen dazu in der Regel personenbezogene Daten des entsandten Mitarbeiters in das Zielland übermittelt werden. Nicht erst seit der Anwendbarkeit der EU-DSGVO im Mai 2018 stellt sich damit die Frage, inwieweit solche Datentransfers datenschutzrechtlich zulässig sind.

Innerhalb des europäischen Binnenmarktes gilt der Grundsatz des freien Datenverkehrs. Sofern für die Verarbeitung personenbezogener Daten – d.h. auch: für deren Übermittlung – eine Rechtsgrundlage gegeben ist, dürfen solche Daten ohne Einschränkungen transferiert werden, weil in allen Mitgliedsstaaten ein angemessenes Datenschutzniveau unterstellt wird. ¹

Für Länder außerhalb der Union geht das EU-Recht davon aus, dass diese den Schutz personenbezogener Daten nicht in ausreichendem Maße gewährleisten. Personenbezogene Daten dürfen nur dann in ein solches Drittland übermittelt werden, wenn

- Der empfangende Staat ein angemessenes Datenschutzniveau gewährleistet; oder
- Das empfangende Unternehmen ein angemessenes Niveau durch entsprechende Garantien sicherstellt; oder
- Die Übermittlung der personenbezogenen Daten auf der Basis einer der Ausnahmeregelungen der DSGVO erfolgt.

Alle sonstigen Übermittlungen personenbezogener Daten in Drittländer sind untersagt.

Durch Beschluss kann die Europäische Kommission einem Drittland attestieren, ein der EU gleichwertiges Datenschutzniveau zu gewährleisten. Mit diesem Angemessenheitsbeschluss unterliegen Datentransfers in dieses Drittland keinen weiteren Beschränkungen. Die Kommission hat solche Beschlüsse für Andorra, Argentinien, Färöer, Guernsey, Isle of Man, Israel, Jersey, Neuseeland, und Uruguay erlassen.²

¹ Mit Beschluss des gemeinsamen EWR-Ausschusses vom 06.06.2018 wurde die EU-DSGVO in das EWR-Abkommen übernommen; sie gilt damit auch in Norwegen, Liechtenstein und Island.

² Mit Japan und Südkorea werden Beschlüsse verhandelt; mit Indien, Brasilien und Paraguay sollen Dialoge aufgenommen werden.

Für Kanada hat die Kommission ihren Angemessenheitsbeschluss auf Privatunternehmen eingeschränkt; an diese dürfen personenbezogene Daten übermittelt werden. Für die USA gibt es nur einen sektorenspezifischen Angemessenheitsbeschluss; personenbezogene Daten dürfen nur an Unternehmen übermittelt werden, die eine gültige Zertifizierung nach den EU-US Privacy Shield nachweisen.^{3 4}

Durch den Austritt des Vereinigten Königreichs aus der Union wird dieses zu einem datenschutzrechtlichen Drittland ohne angemessenes Schutzniveau; personenbezogene Daten dürfen also ab dem März

2019 nicht mehr nach dort übermittelt werden.⁵

Globaler Handel sowie Digitalisierung und Vernetzung der Wirtschaft setzen gleichwohl grenzüberschreitenden Datenverkehr voraus. Deshalb sieht die DSGVO Alternativen vor, auf deren Grundlage personenbezogene Daten übermittelt werden dürfen:

- Standarddatenschutzklauseln
- Verbindliche Unternehmensrichtlinien
- Genehmigte Verhaltensregeln
- Genehmigte Zertifizierungen

Sofern das Daten empfangende Unternehmen selbst durch geeignete Garantien sicherstellt, dass Betroffenen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen, kann damit das nicht angemessene Datenschutzniveau einer Landesgesetzgebung ausgeglichen werden.

Standarddatenschutzklauseln existierten bereits vor Inkrafttreten der DSGVO. Es handelt sich um von der EU Kommission vorgegebene Datenschutzverträge, die zwischen einem Datenexporteur in der EU und einem Datenimporteur außerhalb der Union geschlossen werden können, um so Datentransfers in ein Drittland zu legalisieren.⁶ Diese vorformulierten Verträge müssen von den Parteien ergänzt, dürfen jedoch nicht abgeändert werden.

³ Solche Zertifikate können einschränkt sein; gültige Zertifikate sind auf <https://www.privacyshield.gov> abrufbar.

⁴ Die Arbeitsgruppe der europäischen Datenschutzbehörden hat im Dezember 2017 erhebliche Zweifel an der Gleichwertigkeit des Schutzniveaus geäußert und von der EU Kommission Nachbesserungen gefordert. ⁵ Es sei denn, in den Brexit-Verhandlungen sollten entsprechende Vereinbarungen erzielt werden.

⁴ 001/497/EG v. 15. Juni 2001;

Download: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:DE:PDF>

⁷ Diese sog. Binding Corporate Rules sind für Datentransfers außerhalb des Konzerns ungeeignet. ⁸

Ein darauf gestützter Datentransfer in ein Drittland setzt eine rechtsverbindliche Erklärung des Daten empfangenden Unternehmens voraus, die darin geforderten Verpflichtungen zu erfüllen.

Konzerne dürfen verbindliche Unternehmensrichtlinien für grenzüberschreitende Transfers personenbezogener Daten festlegen. Diese müssen von der zuständigen Aufsichtsbehörde genehmigt werden.⁷

Wirtschaftsverbände dürfen für ihren jeweiligen Sektor datenschutzrechtliche Verhaltenskodizes erarbeiten.⁸ Auch diese bedürfen der Genehmigung durch die Aufsicht.

Auf der Basis einer anerkannten Datenschutzzertifizierung dürfen personenbezogene Daten grenzüberschreitend übermittelt werden.^{5 6}

Mit Ausnahme der Standarddatenschutzklauseln wird dem typischen Mittelstandsbetrieb regelmäßig wohl keines der oben beschriebenen Instrumente zur Verfügung stehen. Die DSGVO sieht deshalb für Fälle, in denen dennoch ein grenzüberschreitender Datentransfer erfolgen soll, zusätzlich einen Katalog von insgesamt sieben definierten Ausnahmeregelungen vor. Deren Inanspruchnahme wird jedoch von z.T. strikten Voraussetzungen abhängig gemacht.

Für die betriebliche Praxis des Mittelstandes werden dabei im Wesentlichen vier der definierten Ausnahmen eine Rolle spielen:

- Die Übermittlung erfolgt auf der Grundlage einer ausdrücklichen Einwilligung des Betroffenen;
- Die Übermittlung ist für die Vorbereitung oder Durchführung eines Vertrages zwischen dem Betroffenen und dem Verantwortlichen⁷ erforderlich;
- Die Übermittlung ist für die Vorbereitung oder Durchführung eines im Interesse des Betroffenen zwischen dem Verantwortlichen und einem Dritten geschlossenen Vertrages erforderlich;
- Die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

Zwar scheint die Einwilligung des Betroffenen zunächst das offenbar zweckmäßigste Instrument – die daran geknüpften Voraussetzungen aber sind hoch. Sie muss ausdrücklich erteilt werden, und muss Art, Umfang und Zweck der vorgesehenen Datenübermittlung präzise beschreiben. Darüber

⁵ Die Kriterien der Zertifizierung und der Akkreditierung von Zertifikaten befinden sich derzeit in den Abstimmungsverfahren der Aufsichtsbehörden.

⁶ Der auf eine Zertifizierung gestützte Datentransfer bedarf zusätzlich einer rechtsverbindlichen Selbstverpflichtung des Daten empfangenden Unternehmens zum Schutz der Daten.

⁷ i.e. dem Daten exportierenden Unternehmen

hinaus muss der Betroffene über sämtliche mit der Übermittlung verbundenen Risiken⁸ aufgeklärt werden. Im Übrigen sind Einwilligungen jederzeit widerruflich; eine weitere Verarbeitung ist dann unmöglich.

Im Zusammenhang mit der oben angesprochenen Entsendung von Mitarbeitern ins Ausland werden deshalb – oft allein in Ermangelung anderer Instrumente – für die Übermittlung personenbezogener Daten in ein Drittland in der Regel die Vertragserfüllung aus dem Beschäftigungsverhältnis¹³ oder die Erfüllung eines Vertrages im Interesse des Betroffenen⁹ als Rechtsgrundlage herangezogen.

Sollte sich für die Übermittlung personenbezogener Daten in ein Drittland auch unter den definierten Ausnahmeregelungen keine Rechtsgrundlage finden, bleibt nur, die Übermittlung auf ein berechtigtes eigenes Interesse zu stützen. Die daran geknüpften Bedingungen sind allerdings ausgesprochen restriktiv:

- Das berechtigte Eigeninteresse des Übermittelnden muss zwingend sein;
- Die Übermittlung darf nicht wiederholt erfolgen¹⁰; und sich nur auf eine begrenzte Anzahl Betroffener beziehen;
- Die einer Übermittlung entgegenstehenden Interessen oder Rechte und Freiheiten des Betroffenen dürfen nicht überwiegen;
- Alle Umstände der Übermittlung sind zu beurteilen, und es sind dem Ergebnis dieser Risikobeurteilung entsprechende Garantien zum Schutz der übermittelten personenbezogenen Daten vorzusehen.¹¹

Damit stehen zwar grundsätzlich insgesamt acht verschiedene Wege zur Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union zur Verfügung. In der betrieblichen Praxis werden solche Übermittlungen zur Zeit jedoch im Wesentlichen entweder auf der Grundlage eines Datenschutzvertrages erfolgen, oder auf die Ausnahmeregelungen zur Vorbereitung oder Durchführung eines Vertrages gestützt werden.

⁸ Viele solcher Einwilligungen scheitern bereits daran, dass der Verantwortliche gar nicht übersehen kann, an welche zusätzlichen Stellen im Empfängerland diese Daten mglw. weitergegeben werden (müssen oder können), und welche zusätzlichen Risiken damit verbunden sind (oder sein können). ¹³ i.d.R. der Arbeitsvertrag sowie die darauf beruhende Entsendevereinbarung

⁹ Das kann u.U. auf sämtliche, an die Personeneigenschaft des Betroffenen gebundenen betrieblichen oder vom Betrieb zu dessen Gunsten zu veranlassenden lokalen Versicherungen zutreffen.

¹⁰ Nach Auffassung der europäischen Aufsichtsbehörden kann schon eine etablierte Geschäftsbeziehung ausreichen, das Kriterium der „Nicht-Wiederholung“ zu Fall zu bringen.

¹¹ Zusätzlich ist die Aufsichtsbehörde von der beabsichtigten Übermittlung in Kenntnis zu setzen sowie der Betroffene von dem zwingenden berechtigten Interesse zu informieren; die ohnehin bereits bestehenden Informationsverpflichtungen des Verantwortlichen bleiben davon unberührt.