EU-Datenschutz-Grundverordnung (DS-GVO)

Das BayLDA auf dem Weg zur Umsetzung der Verordnung

Wichtiger Hinweis zu diesem Dokument:
Die DS-GVO wird nach der Übergangsphase von zwei Jahren am 25. Mai 2018 wirksam. Die Aufsichtsbehörden sind aktuell bemüht, durch intensive Abstimmungsrunden eine einheitliche Sichtweise der neu geregelten Grundlagen und Anforderungen an den Datenschutz auf europäischer Ebene zu erzielen. Das BayLDA beteiligt sich deshalb an verschiedenen Arbeitskreisen, die sich dieser Herausforderung auch in Deutschland stellen. In der Zwischenzeit möchte das BayLDA Interessierten einen Einblick gewähren, welche Themenkomplexe der DS-GVO derzeit auch in der bayerischen Aufsichtsbehörde intensiv diskutiert werden. Das BayLDA veröffentlicht deshalb in regelmäßigen Abständen (geplant: zweimal im Monat) ein kurzes Papier zu einem ausgewählten Schwerpunkt. Das BayLDA weist ausdrücklich darauf hin, dass es sich hierbei um keine verbindlichen Auffassungen handelt, sondern um gegenwärtige Interpretationen und Meinungen zur DS-GVO. Kommentare zum dargestellten gegenwärtigen Verständnis nimmt das BayLDA gerne entgegen.

XI Datenübermittlungen in Drittstaaten nach der DS-GVO

Vieles bleibt beim Alten

Die Anforderungen an Übermittlungen personenbezogener Daten nach der DS-GVO decken sich in vielen Teilen mit dem derzeit noch geltenden Recht. Eine Übermittlung darf grundsätzlich erfolgen, wenn für das Drittland durch Entscheidung der Europäischen Kommission ein angemessenes Datenschutzniveau anerkannt ist. Fehlt es hieran, kommt eine Übermittlung in Betracht, wenn *„geeignete Garantien“* – etwa Standarddatenschutzklauseln oder verbindliche interne Datenschutzvorschriften (Binding Corporate Rules / BCR) – verwendet werden oder ein Ausnahmetatbestand wie etwa die Einwilligung greift.

Neu: Codes of Conduct und Zertifizierung als Grundlage für Übermittlungen

Die DS-GVO bringt jedoch für Datenübermittlungen in Nicht-EU-Staaten mehr Flexibilität. Künftig kommen auch genehmigte Verhaltensregeln (Codes of Conduct, CoC) sowie genehmigte Zertifizierungsmechanismen als Grundlage für solche Übermittlungen in Betracht. Diese Instrumente können auch Übermittlungen aus mehreren Mitgliedstaaten abdecken. Für diesen Fall sind sie mit den Datenschutzbehörden aller Mitgliedstaaten im Kohärenzverfahren abzustimmen. Es darf vermutet werden, dass CoC und Zertifizierungen als Instrumente für Datentransfers in Nicht-EU-Staaten auf erhebliches Interesse der Wirtschaft stoßen werden. Was die inhaltlichen Anforderungen betrifft, müssen solche CoC und Zertifizierungen die wesentlichen Bestimmungen des europäischen Datenschutzrechts abbilden und wirksamen Rechtsschutz für die Betroffenen bieten – vergleichbar etwa mit BCR.

Standarddatenschutzklauseln

Standarddatenschutzklauseln (bisher: Standardvertragsklauseln) kommen auch künftig grundsätzlich als geeignete Garantien für Übermittlungen in Nicht-EU-Staaten in Betracht. Die drei bislang von der Kommission beschlossenen Standardverträge bleiben in

Kraft, bis sie *„erforderlichenfalls“* durch die Kommission geändert, ersetzt oder aufgehoben werden.

Die DS-GVO eröffnet grundsätzlich auch die Möglichkeit von Standarddatenschutzklauseln für Übermittlungen durch Auftragsverarbeiter. Ein Standardvertrag dieser Art existiert bislang nicht und war auf Grundlage der noch geltenden Datenschutzrichtlinie wohl auch nicht möglich.

Zudem können nach der DS-GVO auch Datenschutzaufsichtsbehörden Standarddatenschutzklauseln vorschlagen. Diese sind mit den anderen Aufsichtsbehörden im Kohärenzverfahren abzustimmen und werden anschließend von der Kommission mit Zustimmung eines Ausschusses der Regierungen der Mitgliedstaaten erlassen.

Binding Corporate Rules

Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) werden in der DS-GVO (anders als in der noch geltenden Datenschutzrichtlinie) als Möglichkeit zur Erbringung *„geeigneter Garantien“* für Datentransfers in Drittstaaten ausdrücklich anerkannt. Das Gesetz übernimmt weitgehend die in den Arbeitspapieren der Artikel-29-Gruppe definierten Anforderungen an BCR. Bisherige BCR müssen nur in wenigen Punkten an die DS-GVO angepasst werden. Von den Aufsichtsbehörden sind bis zum Mai 2018 Informationen zu diesen (überschaubaren) Anpassungen zu erwarten.

Datenanforderungen durch Behörden aus Drittstaaten

Im Gesetzgebungsverfahren hatte das Europäische Parlament eine Regelung vorgeschlagen, wonach Anforderungen personenbezogener Daten durch Behörden oder Gerichte eines Drittstaates nur noch dann „anerkannt“ werden, wenn sie auf einer internationalen Übereinkunft (z.B. Rechtshilfeabkommen) beruhen. Dieser Vorschlag hat sich jedoch nicht durchgesetzt. Vielmehr ist nun aus Art. 48 DS-GVO zu entnehmen, dass auch andere Rechtsgrundlagen (etwa Ausnahmen nach Art. 49) für solche Datenübermittlungen in Betracht kommen. Die DS-GVO hat damit in dieser sehr praxisrelevanten Frage leider keinen Beitrag für mehr Rechtsklarheit gebracht. Es wird abzuwarten sein, wie Artikel 48 in der Praxis ausgelegt wird. Wünschenswert sind Hinweise der Aufsichtsbehörden.

Problem der Datenzugriffsbefugnisse von Behörden in Drittstaaten

Des Weiteren sind die Konsequenzen des Urteils des EuGH vom 06.10.2015 in der Sache „Schrems“ (Rs. C-362/14) zu beachten. Aufgeworfen ist die Frage, ob und ggf. unter welchen Voraussetzungen die Aufsichtsbehörden eine Übermittlung in einen Drittstaat aussetzen können, weil Zugriffsbefugnisse dortiger Behörden zu einer Gefahr der Verletzung von Grundrechten Betroffener führen. Es geht somit um die Balance zwischen der Bindungswirkung etwa von Angemessenheitsbeschlüssen der Kommission und den Befugnissen der Aufsichtsbehörden. Die Aufsichtsbehörden werden diese - bislang noch nicht befriedigend geklärte - Problematik, die sich auch unter der DS-GVO stellt, weiter intensiv beraten müssen.

Fazit

Die Systematik der DS-GVO hinsichtlich von Datenübermittlungen in Drittstaaten deckt sich weitgehend mit dem derzeit noch geltenden Recht. Das neue Recht bringt jedoch mehr Flexibilität, u.a. durch neue Instrumente wie Codes of Conduct und Zertifizierungen. Unabhängig davon bedarf das Problem von Datenzugriffen ausländischer Behörden weiterer Klärung, auch seitens der Aufsichtsbehörden.