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.

X Auftragsverarbeitung nach der DS-GVO

Vergleich: Altes Recht - neues Recht

Die nach dem BDSG privilegierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 3 Abs. 8 Satz 3 und § 11 BDSG), wonach der per Auftrag eingesetzte Dienstleister nicht Dritter ist, sondern sozusagen ein „Innenverhältnis“ ohne Prüfschranken für eine Datenübermittlung gesetzlich bestimmt wird, findet sich in vergleichbarer Weise auch in der DS-GVO wieder. Nach Art. 4 Nr. 10 DS-GVO ist ein Auftragsverarbeiter nicht Dritter. Die DS-GVO enthält aber keine Beschränkung der Privilegierung der Auftragsverarbeitung auf den EU-/EWR-Raum mehr, wie sich dies bisher aus der Eingrenzung in § 3 Abs. 8 Satz 3 BDSG ergab. Allerdings legt die DS-GVO den Auftragsverarbeitern künftig *mehr Verantwortung* und *mehr Pflichten* auf.

Statt § 11 BDSG künftig Art. 28 DS-GVO

Die zentrale Vorschrift für Auftragsverarbeiter in der DS-GVO ist Art. 28, wo in Absatz 1 zunächst die Prüfung der Geeignetheit eines Auftragsverarbeiters eingefordert wird. Der Verantwortliche darf danach nur Auftragsverarbeiter einsetzen, die hinreichend Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz haben. Als Beleg solcher Garantien können auch genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DS-GVO oder Zertifizierungen nach Art. 42 DS-GVO herangezogen werden.

Vertrag mit Maßnahmen zur Sicherheit

Wie bisher muss mit dem Auftragsverarbeiter im Regelfall ein Vertrag über die weisungsgebundene Tätigkeit geschlossen werden, der schriftlich oder -neu- in elektronischer Form abgefasst sein kann. Für den notwendigen Inhalt des Vertrags gilt *weitestgehend* das Gleiche wie bisher. Ein wichtiger Bestandteil wird jedoch vor allem die Darstellung der erforderlichen Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO. Gerade hier mangelte es bislang häufig bei Datenschutzkontrollen.

Subunternehmer-Einsatz

Will der Auftragsverarbeiter Subunternehmen als weitere Auftragsverarbeiter bei der Erbringung der vereinbarten Dienstleistung einsetzen, so bedarf dies der vorherigen (schriftlichen oder elektronischen) Genehmigung durch den Verantwortlichen. Später beabsichtigte Änderungen bei den eingesetzten Subunternehmen muss der Auftragsverarbeiter dem Auftraggeber als Verantwortlichen vorher mitteilen, wobei der Verantwortliche dann bei Bedarf Einspruch gegen die geplante Einbeziehung des neuen Subunternehmers einlegen kann. Kann zu dem Einspruch keine Einigung zwischen dem Verantwortlichen und dem Auftragsverarbeiter gefunden werden, wird das zur Beendigung des Vertrags mit dem Auftragsverarbeiter führen.

Neue Verantwortlichkeiten und Pflichten

Verstößt ein Auftragsverarbeiter gegen die Pflicht zur weisungsgebundenen Verarbeitung, indem er die Daten des Auftraggebers für eigene Zwecke oder Zwecke Dritter verarbeitet, gilt er nach Art. 28 Abs. 10 DS-GVO insoweit *selbst als Verantwortlicher* – mit allen rechtlichen Folgen, z. B. auch zur Erfüllung der Betroffenenrechte. Neu hinzugekommen sind in der DS-GVO auch spezielle Haftungsregelungen für Auftragsverarbeiter bei Datenschutzverletzungen in Art. 82 DS-GVO. Demnach drohen Auftragsverarbeitern bei Verstößen auch Schadensersatzforderungen von Betroffenen.

Desweitern besteht für Auftragsverarbeiter die neue Pflicht, künftig auch ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO für alle Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führen. Diese müssen der Aufsichtsbehörde auf Anfrage, z. B. bei Kontrollen, zur Verfügung gestellt werden.

Wartung und Fernzugriffe

Weil die DS-GVO einschließlich der Erwägungsgründe keine § 11 Abs. 5 BDSG vergleichbare Regelung enthält, wird zu diskutieren sein, wie im Falle einer allgemeinen Möglichkeit des Zugriffs auf personenbezogene Daten durch Dienstleister umgegangen werden muss. Dies könnte bei bestimmten Tätigkeiten, wie bei einer rein technischen Wartung, unter Umständen nicht zu einer Qualifikation als Auftragsverarbeiter und einer Anwendung von Art. 28 DS-GVO führen. Ist Auftragsgegenstand der (Fern-)Wartung allerdings gerade der Umgang mit Datensätzen mit personenbezogenen Daten, so handelt es sich weiter um eine Auftragsverarbeitung nach Art. 28 DS-GVO.

Datenpannen und Folgen bei Verstößen

In der Praxis nicht unerhebliche Relevanz dürfte Art. 33 Abs. 2 DS-GVO besitzen: Demnach muss ein Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten nach Bekanntwerden unverzüglich dem Verantwortlichen melden. Ebenso sind die umfassenden Bußgeldvorschriften des Art. 83 Abs. 4, 5 und 6 DS-GVO zu berücksichtigen: Diese können bei Verstößen durchaus auch bei einem Auftragsverarbeiter zur Anwendung kommen.

Ausblick: Auftragsverarbeitung mit Standardvertragsklauseln

Die DS-GVO ermächtigt in Art. 28 Abs. 7 und 8 jeweils die EU-Kommission und (im Einklang mit dem Kohärenzverfahren) jede Aufsichtsbehörde, Standardvertragsklauseln für die Vertragsregelungen zwischen Verantwortlichen und Auftragsverarbeitern festzulegen. Gleiches gilt für das Verhältnis zwischen Auftragsverarbeitern und Subunternehmern. Wie schnell solche Standardvertragsklauseln geschaffen werden, ist derzeit noch nicht abzusehen.