Kurzpapier Nr. 2
Aufsichtsbefugnisse/Sanktionen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Die DS-GVO stellt den Aufsichtsbehörden einen umfassenden Katalog von Untersuchungs- und Abhilfebefugnissen zur Verfügung, um die Einhaltung datenschutzrechtlicher Bestimmungen durchzusetzen. Neben diesen verwaltungsrechtlichen Maßnahmen können Verstöße auch mit hohen Geldbußen sanktioniert werden.

Untersuchungs- und Abhilfebefugnisse im Verwaltungsverfahren (Art. 58 DS-GVO)

Gegenüber Verantwortlichen und Auftragsverarbeitern können vorsorgliche Warnungen ausgesprochen werden, wenn diese Datenverarbeitungen beabsichtigen, die voraussichtlich einen Verstoß gegen die Grundverordnung darstellen, bzw. Verwarnungen, wenn mit Datenverarbeitungen bereits gegen die Grundverordnung verstoßen wurde. Darüber hinaus können Verantwortliche und Auftragsverarbeiter künftig im Rahmen eines förmlichen Verwaltungsaktes von den Aufsichtsbehörden angewiesen werden, Betroffenenrechten zu entsprechen, Datenverarbeitungen mit der Grundverordnung in Einklang zu bringen sowie von einem Datenschutzverstoß betroffene Personen entsprechend zu benachrichtigen. Des Weiteren ist künftig auch die Anordnung der Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation möglich. Die Befugnis der Aufsichtsbehörden, Beschränkungen und Verbote von Datenverarbeitungen und die Berichtigung oder Löschung bestimmter Daten sowie eine Einschränkung der Verarbeitung solcher Daten anzuordnen, bleibt unberührt. Nicht zuletzt können mit Inkrafttreten der Grundverordnung Zertifizierungen seitens der Aufsichtsbehörden selbst widerrufen oder Zertifizierungsstellen angewiesen werden, erteilte Zertifizierungen zu widerrufen oder neue Zertifizierungen nicht zu erteilen.

Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden.

Zu beachten ist, dass sich die genannten behördlichen Maßnahmen zukünftig nicht nur gegen den Verantwortlichen selbst, sondern auch gegen Auftragsverarbeiter richten können.

Die Aufsichtsbehörden haben umfassende Untersuchungsbefugnisse, wobei den Verantwortlichen und auch Auftragsverarbeiter Mitwirkungspflichten treffen. Insbesondere können die Aufsichtsbehörden den Verantwortlichen und Auftragsverarbeiter sowie deren Vertreter anweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind.

Alle Anordnungen können mit Zwangsmitteln, wie Zwangsgeldern, durchgesetzt werden. Rechtsschutz bei Zweifeln an der Rechtmäßigkeit der Anordnungen der Aufsichtsbehörde ist wie bisher auch im verwaltungsgerichtlichen Verfahren gewahrt.

Verhängung von Geldbußen (Art. 83 DS-GVO)

Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden.

Der Rahmen für die Geldbußen wird mit der DS-GVO deutlich erhöht. Dies trägt der gestiegenen Bedeutung des Datenschutzes Rechnung. So können Geldbußen von bis zu 10.000.000 € bzw. bei Unternehmen bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden (z. B. ist eine weitere erwähnenswerte Neuerung gegenüber der aktuellen Rechtslage, dass unter dem Regime der DS-GVO auch ein Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten mit einer Geldbuße geahndet werden kann). Bei bestimmten, besonders schwerwiegenden Verstößen, darunter Verstöße gegen die Datenverarbeitungsgrundsätze und gegen die Betroffenenrechte oder im Falle einer Verarbeitung ohne Rechtsgrundlage, sind Geldbußen von bis zu 20.000.000 € möglich. Gegen Unternehmen kann diese Grenze sogar noch überschritten werden, nämlich bis zu 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres. Für den Fall der Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO ist ebenfalls die Verhängung einer Geldbuße von bis zu 20.000.000 € oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vorgesehen. In allen drei Fallgestaltungen richtet sich die maximale Obergrenze für die Geldbuße danach, welcher der Beträge höher ist.

Hierbei geht die DS-GVO von einem gegenüber Art. 4 Nr. 18 DS-GVO erweiterten Unternehmensbegriff aus. Wie der Begriff „Unternehmen“ im Zusammenhang mit dem Bußgeldverfahren zu verstehen ist, ist Erwägungsgrund (ErwGr.) 150 der DS-GVO zu entnehmen. Danach gilt der aus dem Kartellrecht entlehnte weite, funktionale Unternehmensbegriff nach Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Dies hat zur Folge, dass Mutter- und Tochtergesellschaften als wirtschaftliche Einheit betrachtet werden, so dass bei der Bemessung des Bußgeldes der Gesamtumsatz der Unternehmensgruppe zu Grunde gelegt wird.

Nach dem Wortlaut der DS-GVO reicht es für die Zurechnung eines Verstoßes zu einem Unternehmen aus, dass ein Beschäftigter des Unternehmens oder auch ein für das Unternehmen agierender externer Beauftragter gehandelt hat. Die Zurechnung ist damit nicht mehr wie bisher (vgl. § 30 OWiG) auf Handlungen gesetzlicher Vertreter oder anderer Leitungspersonen des Unternehmens begrenzt.

Für die Zumessung der Geldbußen gilt zuvörderst der Grundsatz, dass die Geldbußen wirksam, verhältnismäßig und abschreckend sein müssen. Art. 83 Abs. 2 S. 2 DS-GVO enthält eine Auflistung von Kriterien, die bei der Entscheidung über die Verhängung und die Höhe einer Geldbuße (ggf. auch einem Absehen davon, vgl. ErwGr. 148) gebührend im Einzelfall berücksichtigt werden sollen. Neben Art, Schwere und Dauer des Verstoßes ist unter anderem auch zu berücksichtigen, welche Art von Daten verarbeitet wurde sowie ob früher angeordnete Maßnahmen vom Verantwortlichen eingehalten wurden. Zu berücksichtigen ist künftig auch die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere, ob und wie die Verantwortlichen mit den Aufsichtsbehörden zusammengearbeitet haben, um Verstößen abzuhelfen und ihre möglichen nachteiligen Auswirkungen zu mindern, und ob sie die Verstöße eigenständig mitgeteilt haben. Ferner ist auch der Grad der Verantwortung des Verantwortlichen bzw. Auftragsverarbeiters unter Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen ein zu berücksichtigendes Kriterium. Mithin wird im Einzelfall zu überprüfen sein, inwieweit ein Unternehmen im Rahmen seiner internen Organisation, etwa durch Ausgestaltung seiner Strukturen, Arbeitsprozesse und Kontrollmechanismen, Vorkehrungen getroffen hat, die dazu dienen, die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen, bzw. inwieweit die interne Organisation diesbezüglich Mängel aufweist. Zudem

können jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste, Berücksichtigung finden.

Abzuwarten bleibt, in welcher Form der Europäische Datenschutzausschuss seinen Auftrag aus Art. 70 Abs. 1 lit. k DS-GVO umsetzen wird. Danach obliegt ihm die Aufgabe, Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Art. 58 Abs. 1, 2 und 3 DS-GVO und die Festsetzung von Geldbußen gemäß Art. 83 DS-GVO zu erlassen.