Kurzpapier Nr. 2 Aufsichtsbefugnisse/Sanktionen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DSGVO) im praktischen Vollzug angewendet werden sollte.

Die DSGVO stellt den Aufsichtsbehörden einen umfassenden Katalog von Untersuchungs- und Abhilfebefugnissen zur Verfügung, um die Einhaltung datenschutzrechtlicher Bestimmungen durchzusetzen.
Zu beachten ist, dass sich die in Art 58 Abs. 2 DSGVO genannten behördlichen Befugnisse nicht nur gegen den Verantwortlichen selbst, sondern auch gegen Auftragsverarbeiter und in bestimmten Fällen gegen Vertreter (Art. 4 Nr. 17 DS-GVO) sowie Zertifizierungs- und Überwachungsstellen richten können.

Untersuchungs- und Abhilfebefugnisse im Verwaltungsverfahren (Art. 58 DSGVO)

Gegenüber Verantwortlichen und Auftragsverarbeitern können vorsorgliche Warnungen ausgesprochen werden, wenn eine beabsichtigte Datenverarbeitung voraussichtlich gegen die DSGVO verstoßen würde. Wurde durch eine Datenverarbeitung bereits gegen die DSGVO verstoßen, kann eine Verwarnung ausgesprochen werden. Darüber hinaus können Verantwortliche und Auftragsverarbeiter im Rahmen eines förmlichen Verwaltungsaktes von den Aufsichtsbehörden angewiesen werden, Betroffenenrechten zu entsprechen, Datenverarbeitungen mit der DSGVO in Einklang zu bringen sowie von einem Datenschutzverstoß betroffene Personen entsprechend zu benachrichtigen. Des Weiteren ist 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 seit Inkrafttreten der DSGVO Zertifizierungen seitens der Aufsichtsbehörden selbst widerrufen oder Zertifizierungsstellen angewiesen werden, erteilte Zertifizierungen zu widerrufen oder neue Zertifizierungen nicht zu erteilen.

Eine Geldbuße kann je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle anderer Abhilfemaßnahmen verhängt werden. Mehrere Maßnahmen können miteinander verbunden werden, wenn dies zur wirksamen Beseitigung oder Ahndung eines Verstoßes erforderlich und insgesamt verhältnismäßig ist.

Die Aufsichtsbehörden haben umfassende Untersuchungsbefugnisse, wobei Verantwortliche und Auftragsverarbeiter sowie deren Vertreter zur Mitwirkung verpflichtet sind (Art. 31 DSGVO). 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. Gegen rechtsverbindliche Entscheidungen der Aufsichtsbehörden steht nach Art. 78 DSGVO der Rechtsweg offen.

Verhängung von Geldbußen (Art. 83 DSGVO)

Geldbußen müssen nach Art. 83 Abs. 1 DSGVO in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Eine Geldbuße ist weder zwingende Folge jedes festgestellten Verstoßes noch auf außergewöhnliche Fälle beschränkt. Maßgeblich sind die konkreten Umstände des Einzelfalls.

Für die in Art. 83 Abs. 4 DSGVO genannten Verstöße (z. B. gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten) beträgt der Höchstbetrag einer Geldbuße 10 Millionen Euro oder im Fall eines Unternehmens zwei Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres.
Für die in Art. 83 Abs. 5 und 6 DSGVO genannten Verstöße (darunter Verstöße gegen die Datenverarbeitungsgrundsätze und gegen die Betroffenenrechte oder im Falle einer Verarbeitung ohne Rechtsgrundlage sowie im Falle der Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 DSGVO) beträgt der Höchstbetrag 20 Millionen Euro oder vier Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres. Bezugspunkt des „vorangegangenen Geschäftsjahres“ ist das letzte Jahr vor Erlass des Geldbußenbescheids (Europäischer Datenschutzausschuss – EDSA – Leitlinien 04/2022 Rn. 121). In allen drei Fallgestaltungen richtet sich der gesetzliche Höchstbetrag für die Geldbuße danach, welcher der Beträge höher ist.

Hierbei geht die DSGVO von einem gegenüber Art. 4 Nr. 18 DSGVO erweiterten Unternehmensbegriff aus. Wie der Begriff „Unternehmen“ im Zusammenhang mit dem datenschutzrechtlichen Geldbußenverfahren zu verstehen ist, ist Erwägungsgrund (ErwGr.) 150 der DSGVO 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 eher als wirtschaftliche und weniger als rechtliche Einheit betrachtet werden (Europäischer Datenschutzausschuss – EDSA – Leitlinien 04/2022 Rn. 121), sodass bei der Bestimmung des gesetzlichen Höchstbetrages der Gesamtumsatz der Unternehmensgruppe zugrunde gelegt wird (EuGH, Urt. vom 13. Februar 2025, Rechtssache C-383/23 – „ILVA“ Rn. 36).

Nach dem Wortlaut der DSGVO sowie der Rechtsprechung des EuGH (Urt. vom 5. Dezember, 2023 Rechtssache C-807/21 – „Deutsche Wohnen“) reicht es für die Zurechnung eines Verstoßes zu einem Unternehmen aus, dass ein Beschäftigter des Unternehmens oder auch jede andere Person im Rahmen der unternehmerischen Tätigkeit und im Namen der juristischen Person gehandelt hat (EuGH aaO Rn. 44). Die Zurechnung ist damit nicht mehr wie bisher (vgl. § 30 Gesetz über Ordnungswidrigkeiten – OWiG) auf Handlungen gesetzlicher Vertreter oder anderer Leitungspersonen des Unternehmens begrenzt.

Geldbußen müssen wirksam, verhältnismäßig und abschreckend sein. Artikel 83 Abs. 2 Satz 2 DSGVO 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) im Einzelfall gebührend berücksichtigt werden sollen. Neben Art, Schwere und Dauer des Verstoßes ist unter anderem auch in die Bewertung einzubeziehen, welche Art von Daten verarbeitet wurde sowie ob früher angeordnete Maßnahmen vom Verantwortlichen eingehalten wurden. Zu berücksichtigen ist 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 beachtendes Kriterium. Mithin ist im Einzelfall zu überprüfen, 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.

Der EDSA hat mit den Leitlinien 04/2022, die seit dem 24. Mai 2023 in ihrer endgültigen Fassung vorliegen, eine unionsweit abgestimmte Methodik für die Bemessung von Geldbußen in fünf Schritten entwickelt:

1. Ermittlung der sanktionierbaren Verhaltensweisen: Hierbei wird festgestellt, welche Handlungen oder Unterlassungen Gegenstand des Verfahrens sind. Bei mehreren Verstößen sind insbesondere Art. 83 Abs. 3 DSGVO sowie mögliche Konkurrenzverhältnisse zu prüfen.
2. Bestimmung des Ausgangsbetrags: Den Ausgangspunkt bilden der einschlägige Höchstbetrag der Geldbuße, die Schwere des Verstoßes und im Falle von Unternehmen der Umsatz. Die Leitlinien unterscheiden Verstöße niedriger, mittlerer und hoher Schwere und sehen hierfür Orientierungskorridore vor. Diese entsprechen keinen starren Katalogen für Geldbußen.
3. Berücksichtigung erschwerender und mildernder Umstände: Der Ausgangsbetrag ist anhand der weiteren Kriterien des Art. 83 Abs. 2 DSGVO anzupassen. Dazu gehören insbesondere frühere Verstöße, Maßnahmen zur Schadensminderung, der Grad der Verantwortung, die Zusammenarbeit mit der Aufsichtsbehörde sowie erlangte finanzielle Vorteile oder vermiedene Verluste.
4. Prüfung der gesetzlichen Höchstgrenze: Der errechnete Betrag darf die nach Art. 83 Abs. 4 bis 6 DSGVO geltende Höchstgrenze nicht überschreiten.
5. Abschließende Gesamtprüfung: Die Geldbuße ist daraufhin zu überprüfen, ob sie im konkreten Fall wirksam, verhältnismäßig und abschreckend ist. Dabei ist sowohl eine unverhältnismäßige Belastung als auch eine Geldbuße zu vermeiden, die ihre sanktionierende und präventive Wirkung verfehlt.

Die Leitlinien 04/2022 des EDSA sind keine mathematische Berechnungsformel. Sie bilden den methodischen Rahmen für die Bemessung von Geldbußen.

****

Anmerkung zur Nutzung dieses Kurzpapiers: