Neue Leitlinien zur Berechnung von Bußgeldern bei Datenschutzverstößen

Der Europäische Datenschutzausschuss (EDSA) hat am 12. Mai 2022 Leitlinien zur Harmonisierung der Berechnung von Bußgeldern durch die Datenschutzbehörden zur Konsultation veröffentlicht. Die vom EDSA vorgeschlagene Berechnungsmethode dient der Vereinheitlichung der Bußgeldpraxis in den Mitgliedstaaten und soll weitere Rechtsklarheit und Transparenz hinsichtlich der Anwendung der Kriterien des Art. 83 DSGVO schaffen. Welche Auswirkungen die neue Leitlinie auf die Bußgeldpraxis konkret haben wird, ist noch nicht abzusehen. Für große und umsatzstarke Unternehmen könnte dies im europaweiten Durchschnitt jedoch zukünftig zu höheren Geldbußen führen.

Das Fünf-Schritte-Modell

In der Leitlinie schlägt der EDSA ein Fünf-Schritte-Modell zur Bestimmung der Höhe von Bußgeldern vor. Hierbei soll es sich jedoch nicht um ein starres mathematisches Vorgehen handeln. Die individuelle Festsetzung eines Bußgeldes bleibt im Wesentlichen von der Beurteilung aller Umstände des Einzelfalls abhängig.

1. Ermittlung der Anzahl der Verstöße
2. Bestimmung des Ausgangsbetrages
   a. Ermittlung der Art des Verstoßes (Art. 83 Abs. 4-6 DSGVO)
   b. Prüfung der Schwere des Verstoßes (Art. 83 Abs. 2 DSGVO)
   c. Bestimmung des Jahresumsatzes des Unternehmens
3. Bewertung aller erschwerenden und mildernden Umstände
4. Bestimmung der Bußgeldobergrenze
5. Finale Evaluation

1. **Ermittlung der Anzahl der Verstöße**

Im ersten Schritt ermittelt die Datenschutzbehörde die relevanten Datenschutzverletzungen und prüft, ob diese jeweils einen oder mehrere einzeln zu ahndende Verstöße gegen das Datenschutzrecht begründen.

1. **Bestimmung des Ausgangsbetrages**

Anschließend ist der Ausgangsbetrag für die weitere Berechnung der Geldbuße zu ermitteln. Hierzu sind (i) die Art des Verstoßes, (ii) die Schwere des Verstoßes und (iii) der Jahresumsatz des Unternehmens zu bestimmen.

a. Zunächst sind die Verstöße den beiden in Art. 83 DSGVO bestimmten Kategorien zuzuordnen. Hiernach bestimmt sich der gesetzliche Höchstbetrag des zu verhängenden Bußgeldes. Verstöße nach Abs. 4 werden mit einer Maximalstrafe von 10 Mio. Euro bzw. 2 % des weltweiten Vorjahresumsatzes und Verstöße nach

Abs. 5 und 6 mit einer Höchststrafe von 20 Mio. Euro bzw. 4 % des weltweiten Vorjahresumsatzes geahndet.

b. Sodann ist die Schwere des jeweiligen Verstoßes zu bewerten. Verstöße sollen nach einer umfassenden Gesamtbetrachtung des Einzelfalls als gering, mittel oder hoch eingestuft werden. Dabei sind insbesondere die in Art. 83 Abs. 2 DSGVO aufgezählten Kriterien einzubeziehen. So können etwa Verstöße im Rahmen der Verarbeitung von Daten besonders schutzbedürftiger Personen (wie z.B. Arbeitnehmer oder Kinder), besonderer Kategorien personenbezogener Daten (wie z.B. Gesundheitsdaten), Verstöße, die die Kerntätigkeit des Verantwortlichen berühren, oder eine hohe Anzahl Betroffener besonders schwer wiegen. Zudem ist der Grad des Verschuldens zu berücksichtigen. Abhängig von der Schwere des Verstoßes ist ein angemessener Ausgangsbetrag zu bestimmen. Hierbei sehen die Leitlinien folgende Abstufung vor:

- Schwere des Verstoßes: Gering; Ausgangsbetrag: 0 – 10 % der gesetzlichen Höchstsumme
- Schwere des Verstoßes: Mittel; Ausgangsbetrag: 10 – 20 % der gesetzlichen Höchstsumme
- Schwere des Verstoßes: Schwer; Ausgangsbetrag: 20 – 100 % der gesetzlichen Höchstsumme

c. Der konkreten Berechnung des Ausgangsbetrages soll die Datenschutzbehörde auch den weltweiten Jahresumsatz des Unternehmens zugrunde legen. Hierbei können entsprechend der Schwere des Datenschutzverstoßes für Unternehmen mit geringerem Jahresumsatz Anpassungen an dem Ausgangsbetrag vorgenommen werden. Hierbei schlägt der EDSA folgende Abstufung vor:

- Jährlicher Umsatz in EUR: ? 2 Mio.; maximale Reduktion auf: 0,2 % des Ausgangsbetrages
- Jährlicher Umsatz in EUR: ? 10 Mio.; maximale Reduktion auf: 0,4 % des Ausgangsbetrages
- Jährlicher Umsatz in EUR: ? 50 Mio.; maximale Reduktion auf: 2 % des Ausgangsbetrages
- Jährlicher Umsatz in EUR: 50 Mio. – 100 Mio.; maximale Reduktion auf: 10 % des Ausgangsbetrages
- Jährlicher Umsatz in EUR: 100 Mio. – 250 Mio.; maximale Reduktion auf: 20 % des Ausgangsbetrages
- Jährlicher Umsatz in EUR: ? 250 Mio.; maximale Reduktion auf: 50 % des Ausgangsbetrages

In der Regel gilt: Je höher der Umsatz des Unternehmens innerhalb der jeweiligen Stufe, desto höher ist der Ausgangsbetrag. Die Datenschutzbehörde ist jedoch nicht verpflichtet, diese Anpassung vorzunehmen, wenn sie für eine abschreckende Wirkung nicht erforderlich ist.

1. **Bewertung aller erschwerenden und mildernden Umstände**

Im dritten Schritt wird der ermittelte Ausgangsbetrag unter Berücksichtigung der verbleibenden erschwerenden und mildernden Faktoren angepasst (Art. 83 Abs. 2 DSGVO).

Dabei ist vor allem das Verhalten des Unternehmens in der Vergangenheit und im Laufe des Bußgeldverfahrens zu betrachten. Insbesondere können dabei Maßnahmen des Verantwortlichen zur Schadensminderung für die Betroffenen, frühere Datenschutzverstöße des Verantwortlichen, die Art und Weise, wie der Verstoß der Datenschutzbehörde bekannt wurde, der Grad der Kooperation mit den Datenschutzbehörden oder die Erzielung eines wirtschaftlichen Gewinns aus dem Verstoß berücksichtigt werden.

1. **Bestimmung der Bußgeldobergrenze**

Im vierten Schritt ermittelt die Datenschutzbehörde die Höchstbeträge für die Datenschutzverletzung und legt die Obergrenze für die Geldbußen fest. Maßgeblich ist der weltweite Jahresumsatz des Unternehmens bezogen auf die gesamte Wirtschaftseinheit. Entsprechend dem so ermittelten Gesamtjahresumsatz kann entweder die statische Höchstsumme von 10 Mio. bzw. 20 Mio. Euro oder die dynamische Höchstsumme von 2 % bzw. 4 % des weltweiten Jahresumsatzes relevant werden, je nachdem, welcher Betrag höher ist.

1. **Finale Evaluation**

Abschließend wird evaluiert, ob das ermittelte Bußgeld wirksam, verhältnismäßig und abschreckend ist. Dieser Schritt stellt ein letztes Korrektiv im Sinne einer abschließenden Gesamtbetrachtung dar. Sollte die Datenschutzbehörde zu dem Schluss kommen, dass z.B. der ermittelte Gesamtbetrag nicht hinreichend geeignet ist, die genannten Ziele zu erreichen, oder die Geldbuße über das hinaus geht, was zur Erreichung der mit der DSGVO verfolgten Ziele erforderlich ist, kann der Betrag noch entsprechend korrigiert werden. Hierbei kann in begründeten Ausnahmefällen auch die wirtschaftliche Leistungsfähigkeit des Unternehmens berücksichtigt werden, etwa wenn das Unternehmen darlegt und beweist, dass das Bußgeld die wirtschaftliche Leistungsfähigkeit des Unternehmens nachhaltig beeinträchtigt.

Auswirkungen der Leitlinie

Nachdem der EDSA bis zum 27. Juni 2022 Gelegenheit gegeben hatte, zu der Leitlinie Stellung zu nehmen, wird erwartet, dass der Leitlinienentwurf im 4. Quartal dieses Jahres fertig gestellt und offiziell angenommen wird.

Das vorgestellte Berechnungsmodell bietet eine einheitliche Basis für die Berechnung von Bußgeldern bei Datenschutzverstößen und trägt damit zu einer Harmonisierung der Bußgeldpraxis auf europäischer Ebene bei. Es löst auch das bisher bestehende Berechnungsmodell der deutschen Behörden ab. Durch den strukturierten Berechnungsansatz wird die Transparenz der Bußgeldfestsetzung erhöht. Verantwortliche in der gesamten Union werden damit in die Lage versetzt, das jeweilige Bußgeldrisiko anhand der konkretisierten Bemessungskriterien und aufgezeigten Beispiele besser einordnen zu können. Es verbleibt jedoch ein erheblicher Ermessensspielraum für die Datenschutzbehörden, sodass genaue Vorhersagen weiterhin nicht möglich sind. Ob das neue Berechnungsmodell in Deutschland im Vergleich zur bisherigen Berechnungsmethode generell zu höheren oder niedrigeren Bußgeldern führen wird, kann daher nicht mit Sicherheit bestimmt werden. Die Kriterien der Bußgeldbemessung zu kennen ist jedoch der Schlüssel für Verantwortliche, um durch geeignete Gegenmaßnahmen auf möglichst geringe Bußgelder hinzuwirken.

Ansprechpartner:

Francois Heynike, LL.M. (Stellenbosch)
Tel: +49-69-951195770
fheynike@kpmg-law.com