

von **Dr. Bea Brünen**

DSGVO: DSK stellt Konzept zur Bußgeldbemessung bei Verstößen vor

Der Bußgeldrahmen für DSGVO-Verstöße sieht Bußgelder von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Vorjahresumsatzes eines Unternehmens vor. Wie hoch DSGVO-Bußgelder aufgrund dieses sehr weitreichenden Rahmens konkret ausfallen, war bis dato weitgehend unklar. Die Datenschutzkonferenz (DSK) hat nun ein Bußgeld-Konzept vorgestellt, das Licht in die dunkle Bußgeldberechnung bringt. Wie hoch Bußgelder danach künftig ausfallen werden, zeigen wir Ihnen im Folgenden.

A. Der Bußgeld-Katalog der DSGVO

Wie hoch ein Bußgeld bei einem Verstoß gegen die DSGVO ausfällt, entscheiden die Landesbeauftragten der Datenschutzbehörden im Einzelfall. Der Bußgeldrahmen wird dabei von Art. 83 DSGVO vorgegeben. Danach können etwa Verstöße gegen Pflichten bei der Auftragsdatenverarbeitung oder Verstöße gegen bestimmte Zertifizierungspflichten mit einem Bußgeld von bis zu 10 Millionen Euro oder von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden (vgl. Art. 83 Abs. 4 DSGVO).

Bei bestimmten (schwerwiegenderen) Verstößen, etwa bei der Nichtbefolgung einer Anweisung der Aufsichtsbehörde, ermöglicht der Bußgeldrahmen die Festsetzung einer Geldbuße von bis zu 20 Millionen Euro oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Die konkrete Bußgeldhöhe bemisst sich innerhalb des von der DSGVO vorgegebenen Rahmens anhand unterschiedlicher Faktoren, die in Art. 83 Abs. 2 DSGVO aufgelistet sind. Unter anderem hängt die Höhe des Bußgeldes danach von

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- etwaigen einschlägigen früheren Verstößen des Verantwortlichen oder des Auftragsverarbeiters

ab.

Doch wie lassen sich Bußgelder anhand dieser Faktoren konkret berechnen? Die DSK will mit ihrem Bußgeldkatalog Antworten auf diese Frage geben.

B. Das Bußgeldkonzept der DSK im Fokus

Das von der DSK entwickelte Bußgeldkonzept orientiert sich in erster Linie am Umsatz eines Unternehmens. Laut DSK stellt dies eine geeignete, sachgerechte und faire Anknüpfung zur Sicherstellung der Wirksamkeit der DSGVO, Verhältnismäßigkeit und Abschreckung dar. Vor diesem Hintergrund erfolgt die Bußgeldzumessung im Verfahren gegen Unternehmen in fünf Schritten:

1. Das betroffene Unternehmen wird einer Größenklasse zugeordnet
2. Der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse wird bestimmt
3. Ein wirtschaftlicher Grundwert wird ermittelt
4. Der wirtschaftliche Grundwert wird mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert
5. Der ermittelte Wert wird anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst.

Die Verfahrensschritte sind dabei konkret folgendermaßen ausgestaltet:

I. Schritt

Das betroffene Unternehmen wird anhand seiner Größe **einer von vier Größenklassen** (A bis D) zugeordnet. Zudem gibt es innerhalb der jeweiligen Größenklasse noch drei bis sieben **Untergruppen**.

Die Größenklassen richten sich dabei nach dem gesamten weltweit erzielten Vorjahresumsatz der Unternehmen (vgl. Art. 83 Abs. 4 bis 6 DSGVO) und sind unterteilt in Kleinstunternehmen, kleine und mittlere Unternehmen (KMU) sowie Großunternehmen.

Dabei erfolgt die grundsätzliche Zuordnung folgendermaßen:

- **Kleinstunternehmen:** Unternehmen mit einem Jahresumsatz von bis zu 2 Millionen €; dabei erfasst die kleinste Untergruppe (A.I) etwa Unternehmen mit einem Jahresumsatz von bis zu 700.000 €
- **kleines Unternehmen:** Unternehmen mit einem Jahresumsatz von über 2 Millionen bis 10 Millionen Euro
- **mittleres Unternehmen:** Unternehmen mit einem Jahresumsatz von über 10 Millionen bis 50 Millionen Euro
- **Großunternehmen:** Unternehmen mit einem Jahresumsatz von über 50 Millionen Euro

II. Schritt

Im Anschluss daran wird der **mittlere Jahresumsatz** der Untergruppe, in die das Unternehmen eingeteilt wurde, bestimmt. Dieser beträgt bei Kleinstunternehmen der Untergruppe A.I 350.000 €.

III. Schritt

Im dritten Schritt wird der **wirtschaftliche Grundwert** ermittelt. Dafür wird der mittlere Jahresumsatz durch 360 (Tage) geteilt und so ein durchschnittlicher, auf die Vorkammastelle aufgerundeter Tagessatz errechnet. Bei der Untergruppe A.I beträgt dieser bspw. 972 € (350.000/360).

IV. Schritt

Im Anschluss daran erfolgt anhand der konkreten **tatbezogenen Umstände des Einzelfalles** (vgl. Art. 83 Abs. 2 Satz 2 DSGVO) eine Einordnung des Schweregrades der Tat in leicht, mittel, schwer oder sehr schwer.

Dafür werden unter Berücksichtigung der Umstände des Einzelfalles anhand des Kriterienkatalogs des Art. 83 Abs. 2 DSGVO der **Schweregrad des Tatvorwurfs** und der jeweilige Faktor ermittelt, mit dem der Grundwert multipliziert wird. An dieser Stelle werden also etwa Art, Schwere und Dauer des Verstoßes sowie der Verschuldensgrad (fahrlässig oder vorsätzlich) berücksichtigt. Anhand dieser Faktoren wird der jeweilige Verstoß in einen der vier Schweregrade eingeteilt. Dem Schweregrad des Verstoßes ist jeweils ein bestimmter Faktor zugeordnet, welcher im nächsten Schritt mit dem Tagessatz multipliziert wird. Dabei differenziert das Bußgeldkonzept zusätzlich danach, ob ein formeller oder ein materieller Verstoß vorliegt.

Schweregrad des Verstoßes	Formeller Verstoß	Materieller Verstoß
Leicht	1 bis 2	1 bis 4
Mittel	2 bis 4	4 bis 8
Schwer	4 bis 6	8 bis 12
Sehr <u>Schwer</u>	6 <	12 <

Als **formelle Verstöße** sind alle in Art. 83 Abs. 4 DSGVO genannten Verstöße anzusehen, also etwa Verstöße bei der Auftragsverarbeitung sowie Verstöße gegen bestimmte Zertifizierungspflichten. Als **materielle Verstöße** werden solche nach Art. 83 Abs. 5, 6 DSGVO eingestuft, also etwa eine unrechtmäßige Datenverarbeitung sowie Verstöße gegen die Bedingungen der Einwilligung.

V. Schritt

Im letzten Schritt wird der so errechnete Betrag schließlich an den „Täter“ angepasst. Dafür werden alle für und gegen den Betroffenen sprechenden Umstände ermittelt, soweit sie nicht bereits im vierten Schritt berücksichtigt wurden. Hierzu zählen sämtliche **täterbezogenen Umstände**, die sich aus dem Kriterienkatalog des Art. 83 Abs. 2 DSGVO ergeben sowie sonstige Umstände, wie z.B. eine lange Verfahrensdauer oder eine drohende Zahlungsunfähigkeit des Unternehmens.

C. Beispiel für eine Bußgeldberechnung

Zur Veranschaulichung des Konzepts sei abschließend folgendes Beispiel angeführt: Verstößt ein kleines Unternehmen mit einem Jahresumsatz von bis zu 700.000 € in geringem Umfang gegen seine Pflichten bei der Auftragsdatenverarbeitung, führt dies – ohne die Berücksichtigung sonstiger Einzelfallumstände – nach dem Bußgeldkonzept der DSK zu einem Bußgeld in Höhe von 972 €.

Denn: Das Unternehmen ist im ersten Schritt der Untergruppe A.I. zuzuordnen. Im zweiten Schritt wird der mittlere Jahresumsatz des Unternehmens bestimmt, dieser beträgt im Beispiel 350.000€. Im dritten Schritt wird der wirtschaftliche Grundwert ermittelt, indem man den mittleren Jahreswert durch 360 (Tage) teilt. Dieser beträgt im Beispiel somit 972 €. Im vierten Schritt wird der Verstoß schließlich in das oben dargestellte Faktorensystem eingeordnet. Da es sich bei dem im Beispiel genannten Verstoß um einen nur leichten Verstoß handelt und dieser als „formeller“ Verstoß anzusehen ist, ist der Faktor 1 einschlägig. Mit diesem wird der wirtschaftliche Grundwert (972 €) multipliziert, also $972 \cdot 1$, wodurch sich letztlich ein Bußgeld in Höhe von 972 € ergibt.

Autor:

Dr. Bea Brünen

(freie jur. Mitarbeiterin der IT-Recht Kanzlei)