



Bußgelder bei Datenschutzverstößen

Einleitung

Verstöße gegen das Datenschutzrecht sorgen regelmäßig für Schlagzeilen in den Medien. Für die Übermittlung von personenbezogenen Daten in die USA musste [Adobe unlängst ein Bußgeld von 8.000 Euro zahlen. Gegen Punica und Unilever wurden durch die zuständige Aufsichtsbehörde Bußgelder in Höhe von 9.000 Euro bzw. 11.000 Euro verhängt](#). Eines der höchsten bisher in Deutschland verhängten Bußgelder traf die Supermarktkette Lidl. Sie musste bereits im Jahre 2010 insgesamt fast 1,5 Mio. Euro für die unerlaubte Videoüberwachung ihrer Mitarbeiter bezahlen. Die private Krankenversicherung Debeka einigte sich mit der Aufsichtsbehörde im Wege der Verständigung auf ein [Bußgeld von 1,3 Mio. Euro sowie eine Sonderzahlung von 600.000 Euro für eine Stiftungsprofessur zur Forschung an Datenschutzthemen](#). Anlass für die Untersuchung der Aufsichtsbehörde war hier der Ankauf von Listen mit personenbezogenen Daten potentieller Kunden und die datenschutzwidrige Nutzung dieser Daten. Die [Drogeriemarktkette Müller musste schließlich 137.500 Euro Bußgeld zahlen](#), weil sie unter anderem keinen Datenschutzbeauftragten bestellt hatte und Mitarbeiter über mehrere Jahre unzulässig nach den Gründen für krankheitsbedingte Abwesenheit befragt hatte.

Trotz dieser Beispiele besteht eine große Verunsicherung, in welchen Fällen tatsächlich Bußgelder verhängt werden und wie die Bemessung der Bußgeldhöhe erfolgt. Die nachfolgenden Ausführungen sollen daher als erste Orientierung dienen, können aber eine Beratung im Einzelfall nicht ersetzen.

Welche Bußgelder können aktuell verhängt werden?

Die europäische Datenschutzrichtlinie gibt vor, dass alle Mitgliedstaaten der Europäischen Union Bußgeldbestimmungen erlassen müssen, mit denen Verstöße gegen die nationalen Datenschutzbestimmungen sanktioniert werden (Art. 24 der Richtlinie 95/46/EG). Für Verstöße gegen datenschutzrechtliche Bestimmungen in Deutschland können aktuell gemäß § 43 Abs. 3 S. 1 BDSG Bußgelder in einer Höhe bis zu 300.000 Euro pro Verstoß verhängt werden.

Zuletzt wurde der Bußgeldrahmen moderat von 250.000 Euro auf 300.000 Euro angehoben. Außerdem ist jetzt vorgesehen, dass die Geldbuße ausdrücklich den wirtschaftlichen Vorteil, der dem Täter aus dem Verstoß gegen die Datenschutzbestimmungen zufließt, abschöpfen soll. Zur Erreichung dieses Ziels kann das Bußgeld auch über den eigentlich vorgesehenen Rahmen erhöht werden (§ 43 Abs. 3 S. 3 BDSG). Außerdem können verschiedene Bußgelder wegen des gleichen rechtswidrigen Vorgehens gegen verschiedene Konzerngesellschaften verhängt werden. Faktisch kann es so im Einzelfall zu einer Kumulation mehrerer Bußgelder kommen. Dies geschah beispielsweise im Fall von Lidl. Dort wurden zahlreiche Bußgelder zwischen 10.000 und 310.000 Euro verhängt, die sich letztlich für den Konzern auf insgesamt 1,46 Mio. Euro summierten.

Was ändert sich mit der Datenschutzgrundverordnung?

Die Sanktionen unter der Datenschutzgrundverordnung (DSGVO) sind deutlicher härter als unter den bisher geltenden nationalen Bestimmungen in Deutschland. Bußgelder für Datenschutzverstöße gegen Unternehmen können zukünftig gemäß Art. 83 Abs. 5 DSGVO bis zu 20 Mio. Euro oder bis zu 4 % des gesamten weltweiten erzielten Konzernumsatzes des letzten Jahres betragen, je nachdem welcher Wert höher ist. Gerade für größere Unternehmen stellt die Anknüpfung der Bußgeldhöhe an den Konzernumsatz eine deutliche Erhöhung des Risikos dar. Die gewählte Umsetzung in der DSGVO orientiert sich dabei an der Forderung des LIBE-Ausschusses des EU-Parlaments, dass Datenschutzverstöße unter der DSGVO [„weh tun“ sollen, also für ein Unternehmen auch spürbar sein müssen](#).

Bußgelder können voraussichtlich außerdem direkt gegen verantwortliche Mitarbeiter oder Auftragsdatenverarbeiter in einer Größenordnung von bis zu 300.000 Euro verhängt werden (§ 40 BDSG-Entwurf). Auch im Hinblick auf die Bußgelder, die gegen das Unternehmen verhängt werden, wird sich zukünftig noch häufiger die Frage stellen, ob verantwortliche Mitarbeiter im Innenverhältnis von ihrem Unternehmen in Regress genommen werden können, wenn ein vorsätzliches oder fahrlässiges Verhalten vorliegt. Besonders relevant wird die Frage, wenn – was nach der

Datenschutzgrundverordnung ausdrücklich zulässig ist – ein externer Datenschutzbeauftragter als Dienstleister beauftragt ist. Während interne Mitarbeiter häufig nicht in Regress genommen werden können, gelten derartige Regelungen für Dienstleister nicht. Insoweit kann ein externer Datenschutzbeauftragter auch bewusst als „Haftungspuffer“ genutzt werden, was allerdings dessen ordnungsgemäße Einbeziehung voraussetzt.

Wie ist die bisherige Praxis der Aufsichtsbehörden und was ändert sich?

Maßgebliche Bemessungsfaktoren für die Höhe eines Bußgeldes sind die Bedeutung des Datenschutzverstoßes und der Vorwurf, der den Täter trifft. Außerdem sind auch die wirtschaftlichen Verhältnisse des Täters zu berücksichtigen (§ 17 Abs. 3 OWiG). Es ist also nicht damit zu rechnen, dass auch gegen kleinere Unternehmen Bußgelder in einer Höhe verhängt werden, die die Existenz des Unternehmens gefährden würden.

Die in der Einleitung genannten Beispiele haben gezeigt, dass in der Vergangenheit vor allem Bußgelder für Verhaltensweisen verhängt wurden, die – bei genauerer Betrachtung – eindeutig und offensichtlich als Datenschutzverstöße erkennbar waren. In Zweifelsfällen oder bei Auslegungsfragen wird eine Aufsichtsbehörde dagegen eher das Gespräch mit dem Unternehmen suchen und nicht sofort ein Bußgeld verhängen. Es ist daher von großer Wichtigkeit, vor allem bei Standardthemen und wesentlichen Pflichten keine Schwächen zu zeigen. Außerdem sollte unbedingt mit der Aufsichtsbehörde kooperiert werden, da dies ebenfalls bei der Bemessung des Bußgeldes berücksichtigt wird.

Wenn ein qualifizierter Datenschutzbeauftragter bestellt ist und dieser ordnungsgemäß in Entscheidungsprozesse einbezogen wurde, werden in der Regel kaum Bußgelder verhängt. Dies gilt jedenfalls dann, wenn der Datenschutzbeauftragte eine angemessene Beratung vornimmt und das Unternehmen sich an den Empfehlungen seines Datenschutzbeauftragten orientiert. In diesen Fällen ist eher damit zu rechnen, dass die Aufsichtsbehörde mit Weisungen arbeitet, wenn die Auffassung des Datenschutzbeauftragten nicht geteilt wird. Von dem betroffenen Unternehmen kann kaum verlangt werden, die Tätigkeit des eigenen Datenschutzbeauftragten ohne Anlass noch weiter zu überprüfen.

Für die Zukunft ist allerdings zu erwarten, dass generell Anzahl und Höhe der Bußgelder tatsächlich steigen werden. Auch die Erfahrung in anderen Rechtsbereichen hat gezeigt, dass die europäische Harmonisierung von Bußgeldtatbeständen häufig einen derartigen Effekt hat. Die Aufsichtsbehörden können insbesondere zukünftig auch Präzedenzentscheidungen aus anderen Staaten zur Rechtfertigung von verhängten Bußgeldern heranziehen.

Welche weiteren Folgen drohen im Zusammenhang mit dem Bußgeldverfahren?

Die Verhängung eines Bußgeldes geht regelmäßig mit Weisungen der Aufsichtsbehörden einher, das datenschutzwidrige Verhalten einzustellen. Auf ein Unternehmen kommen so

neben dem eigentlichen Bußgeld regelmäßig Kosten und Mühen für die Umsetzung der erforderlichen Datenschutzmaßnahmen, die Kommunikation mit der Aufsichtsbehörde und eine etwaige Nachprüfung durch die Aufsichtsbehörde zu. Außerdem kann es vorkommen, dass die Aufsichtsbehörde einen festgestellten Datenschutzverstoß zum Anlass für eine gründlichere Prüfung des Unternehmens nimmt.

Zudem wird die Verhängung des Bußgeldes regelmäßig öffentlich bekannt, sodass Unternehmen für ihren pflichtwidrigen Umgang mit personenbezogenen Daten einen Imageschaden erleiden. Die Aufsichtsbehörden berichten in ihren Tätigkeitsberichten über derartige Verfahren und geben teilweise auch Pressemitteilungen unter voller Namensnennung der betroffenen Unternehmen heraus. Nach [einer internationalen Umfrage der Beratungsagentur Boston Consulting](#) führen derartige Bekanntmachungen zu merkbareren Umsatzverlusten von bis zu 8 % des Jahresumsatzes.

Fazit

Mit Hinblick auf die 2018 in Kraft tretende DSGVO ist für Unternehmen vor allem die starke Erhöhung der Bußgelder auf bis zu 20 Mio. Euro bzw. 4 % des Konzernumsatzes bedeutend. Alle Unternehmen sollten diese Veränderung zum Anlass für eine neue Einschätzung der Datenschutzrisiken nehmen und über die Einführung neuer Strategien zur Risikovermeidung nachdenken. Damit sich Unternehmen im Zweifelsfall vom Fehlverhalten ihrer Mitarbeiter distanzieren können, wird zukünftig die Bedeutung von Datenschutzkonzepten und die Einführung von Datenschutz-Management-Systemen an Bedeutung gewinnen.

Da bei Datenschutzverstößen vergleichbare Bußgelder auch bei Tochtergesellschaften im EU-Ausland drohen, sollten Unternehmen den Datenschutz in EU-Konzerngesellschaften ebenfalls prüfen. Insoweit hat die DSGVO allerdings den Vorteil, dass Datenschutzkonzepte und ein Datenschutz-Management-System künftig einfacher auf Gesellschaften in anderen EU-Staaten ohne eine nationale Anpassung übertragen werden können, soweit die nationalen Öffnungsklauseln der DSGVO beachtet werden.

Robert Bommel, LL.M. / Dr. Sebastian Meyer, LL.M.

Kontakt:

BRANDI Rechtsanwälte Partnerschaft mbB
Dr. Sebastian Meyer, LL.M.
 Rechtsanwalt
 Fachanwalt für Informationstechnologierecht (IT-Recht)
 Datenschutzauditor (TÜV)

Adenauerplatz 1, 33602 Bielefeld
 T +49 521 96535 - 812
 F +49 521 96535 - 115
sebastian.meyer@brandi.net
www.brandi.net