MANDANTEN
INFORMATION

SZA
SCHILLING, ZUTT & ANSCHÜTZ

Dezember 2020

UPDATE BUßGELDPRAXIS BEI VERSTÖßEN GEGEN DIE DSGVO

Im Oktober 2020 hat der Hamburgische Landesdatenschutzbeauftragte gegen die Einzelhandelskette H&M ein Bußgeld in Höhe von über 35 Mio. € verhängt. Vorangegangen war dem ein Ermittlungsverfahren, das eine jahrelange unzulässige Verarbeitung von Beschäftigtendaten aufdeckte. Führungskräfte des Unternehmens hatten über längere Zeiträume persönliche Informationen über Beschäftigte erhoben, gespeichert und zur Profilbildung genutzt. Mit Urteil vom 11.11.2020 hat nun das LG Bonn (Az.: 29 OWi 1/20 LG) als erstes deutsches Gericht die Rechtmäßigkeit eines solchen Bußgeldbescheides überprüft. Dies ist Anlass genug, die Bußgeldpraxis der Datenschutzbehörden genauer zu analysieren und Potentiale zur Vermeidung oder zumindest Verminderung von Bußgeldrisiken aufzuzeigen.

I. Einführung

Das zunehmende Verhängen von Bußgeldern ist Teil einer beachtenswerten Entwicklung: Seit Inkrafttreten der DSGVO im Mai 2018 stieg die Zahl erlassener Bußgeldbescheide auf weit über 200 an. Davor waren es nur etwa 40. Auch die Bußgeldhöhe steigt: Neben H&M waren etwa die 1&1 Telecom GmbH (9,55 Mi-o.€), die Deutsche Wohnen SE (14,5 Mio.€) und die AOK Baden-Württemberg (1,24 Mio. €) Adressaten entsprechender Bescheide in mindestens siebenstelliger Höhe.

Fast schon axiomatische Folge dieser Entwicklung ist, dass sich zunehmend auch Gerichte mit der Rechtmäßigkeit der Bußgeldforderungen auseinanderzusetzen haben. Mit Urteil vom 11.11.2020 hat nun das LG Bonn (Az.: 29 OWi 1/20 LG) die Rechtmäßigkeit eines solchen Bußgeldbescheides überprüft. Die schriftlichen Urteilsgründe liegen noch nicht vor, das Ergebnis ist indes bekannt: Das Gericht entschied, dass der Bußgeldbescheid gegen 1&1 von 9,55 Mio.€ auf nunmehr 900.000 € herabzusetzen sei.

Die große Divergenz der einzelnen Bußgeldhöhen sowie die deutliche Herabsetzung durch das LG Bonn werfen die Frage auf, anhand welcher Kriterien solche Bußgelder bemessen werden.

II. Rechtlicher Rahmen der Bußgeldbemessung

Wird ein Verstoß gegen datenschutzrechtliche Regelungen festgestellt, kann der zuständige Datenschutzbeauftragte Abhilfeanordnungen nach Art. 58 Abs. 2 DSGVO treffen. Hierzu gehört insbesondere nach Art. 83 Abs. 1 – 3, 58 Abs. 2 i) DSGVO die Verhängung eines angemessenen Bußgeldes gegen die betroffenen Unternehmen, das alternativ oder kumulativ mit weiteren Maßnahmen nach Art. 58 Abs. 2 DSGVO angeordnet werden kann.

Die Höchstgrenze eines Bußgeldes richtet sich nach der Art des festgestellten Verstoßes:

- Verstöße gegen administrative Pflichten: 10 Mio. € oder bis zu 2% des weltweiten Umsatzes, Art. 83 Abs. 4 DSGVO
- Verstöße bei besonderer Gefährdung personenbezogener Daten: 20 Mio. € oder bis zu 4% des weltweiten Umsatzes, Art. 83 Abs. 5 DSGVO

- Nichtbefolgung von Abhilfeanordnungen: 20 Mio. € oder bis zu 4% des weltweiten Umsatzes, Art. 83 Abs. 6 DSGVO

Dies sind die maximal möglichen Bußgeldrahmen. Es handelt sich hierbei ausdrücklich um Ermessensvorschriften.

III. Rechtlicher Rahmen der Ermessensbetätigung

Ob überhaupt und – wenn ja – **wie hoch** ein Bußgeld ausfällt, liegt im Ermessen der Aufsichtsbehörde. Eine pflichtgemäße Ausübung dieses Ermessens liegt aber nur vor, wenn sie sich an den Kriterien des Art. 83 Abs. 2 S. 2 DSGVO orientiert. Bei der Erfüllung dieser Kriterien besteht für Unternehmen **Vor- und Nachsorgebedarf**. Die berücksichtigungsfähigen Maßnahmen lassen sich systematisch in drei Kategorien unterteilen:

1. In der Regel **nicht beeinflussbar** durch das betroffene Unternehmen sind:

- Art, Schwere und Dauer des Verstoßes (lit. a)
- Eine vorsätzliche oder fahrlässige Begehung (lit. b)
- Die Art der betroffenen Daten (lit. g), also ob der Verstoß etwa sensible Daten iSd Art. 9 und 10 DSGVO betrifft
- Ob durch den Verstoß finanzielle Vorteile entstanden oder Verluste vermieden wurden (lit. k)

2. Als direkte **Reaktion** auf die Aufnahme von Ermittlungen durch die Aufsichtsbehörde, können Unternehmen:

- Maßnahmen zur **Minderung des entstandenen Schadens** ergreifen (lit. c); hierzu zählt insbesondere die Zusage, den Betroffenen unbürokratisch Schadensersatz zu gewähren, damit diese ihren Anspruch aus Art. 82 DSGVO nicht erst einklagen müssen; auch wird eine umgehende Entschuldigung bei den Betroffenen honoriert genauso wie die Ermöglichung, entsprechende Daten einsehen zu können und anschließend umgehend zu löschen;
- Mit den Behörden **umfangreich kooperieren** (lit. f); dahingehend, dass die Kooperation über das gesetzlich vorgeschriebene Maß hinausgeht; z.B. neben dem Nachkommen der Herausgabeverpflichtungen zusätzliche Informationen – etwa über Organisation und Umsatz des Unternehmens – offenzulegen, die für das weitere Verfahren von Bedeutung sein können;
- Die strikte **Einhaltung aller Anordnungen** der Aufsichtsbehörden (lit. i); dies verhindert eine negative Berücksichtigung bei einem potentiellen erneuten Verstoß.

3. Präventiv Strukturen zu schaffen, die Verstöße zu verhindern suchen und – wenn diese dennoch auftreten – den Aufsichtsbehörden zeigen können, dass man bemüht war, im Sinne einer "**best practice**" Datenschutzverstößen Einhalt zu gebieten.

Umfasst sind damit folgende Maßnahmen:

- Schaffung von Systemen des Datenschutzes durch **Technikgestaltung** und **datenschutzfreundliche Voreinstellungen** nach Art. 25 und 32 DSGVO (lit. d); ersteres meint hierbei Datenminimierung und Zweckbindung durch z.B. Pseudonymisierung der Daten, möglichst strikte Zugriffsberechtigungen für die zuständigen MitarbeiterInnen und das Festlegen von Speicherfristen mit automatisierten Löschungen; letzteres bezieht sich auf technische Sicherheitsvorkehrungen wie ausreichende Verschlüsselung, abgesichert etwa durch regelmäßige Datenschutzaudits;
- Berücksichtigt wird die **Art und Weise**, wie der Verstoß **bekannt wurde** (lit. h); honoriert wird, wenn es das Unternehmen selbst ist, welches den Verstoß bei den Aufsichtsbehörden anzeigt; empfehlenswert ist je-

denfalls das Einrichten eines unternehmensinternen, anonymen Hinweisgebersystems ("Whistleblowerschutz"), damit das Unternehmen und nicht ein Dritter zuerst von dem potentiellen Verstoß erfährt und entsprechend agieren kann und nicht reagieren muss;

- Die Einhaltung von **genehmigten Verhaltensregeln** und **Zertifizierungsverfahren** als Maßnahme der Selbstregulierung (lit. j); prämiert wird hiermit, dass sich Unternehmen überhaupt den Aufwand machen, interne Verfahrensregeln auszuarbeiten, die die Anwendung der DSGVO innerhalb des Unternehmens erleichtern soll;
- Abschließend wird klargestellt, dass **jegliche mildernden Umstände** des Einzelfalles berücksichtigungsfähig sind (lit. k); diese **Generalklausel** eröffnet Unternehmen die Möglichkeit, durch alternative – also nicht ausdrücklich in Art. 83 Abs. 2 S. 2 DSGVO genannte – Schutzmechanismen eine Bußgeldforderung abzusenken; denkbar sind hierbei etwa regelmäßige **Datenschutzfortbildungen** der verantwortlichen MitarbeiterInnen, die Einrichtung eines **Datenschutzkoordinators** im Unternehmen, regelmäßige **Datenschutz-Statusupdates**, ein ausreichendes **Compliance-System**, **Löschroutinen** sowie die Möglichkeit der MitarbeiterInnen, durch ein verlässliches **Auskunftssystem** die über sie gespeicherten Daten einzusehen

IV. Erwägungen der Datenschutzbehörden

Von welchen Erwägungen sich die Datenschutzbeauftragten bei der Bemessung der Bußgeldhöhe leiten lassen, kann zumindest indiziell den jeweiligen Pressemitteilungen entnommen werden:

Im Fall von H&M wurden ausdrücklich Maßnahmen positiv hervorgehoben, die das Unternehmen beschlossen hatte und die im Rahmen eines umfassenden **Compliance-Systems** für die Zukunft etabliert werden sollten. Bei dem Verfahren gegen die Deutsche Wohnen SE hingegen wurde gerade das **Fehlen eines solchen Konzepts** negativ berücksichtigt: Zum einen hatte die Deutsche Wohnen offensichtlich keinerlei Datenschutzkonzepte, nach denen Zulässigkeit oder Erforderlichkeit der Datenspeicherungen bei der Erhebung geprüft wurden. Zum anderen wurde Aufforderungen des Datenschutzbeauftragten nur unzureichend nachgekommen. Im Fall der AOK Baden-Württemberg hingegen lag die umgekehrte Situation vor: Die AOK hatte Vorsichtsmaßnahmen getroffen, welche die Verarbeitung von Daten ohne Einwilligung der Kunden verhindern sollten. Diese entsprachen aber nicht den gesetzlichen Mindestanforderungen. Trotzdem führte die **bloße Existenz** eines solchen Systems zu einem im Vergleich zu den anderen Fällen erheblich geringeren Bußgeld. Auch im Verfahren gegen 1&1 betonte der Bundesdatenschutzbeauftragte ausdrücklich die positive Gewichtung der Kooperation sowie der Bereitschaft des Unternehmens, für die Zukunft ein **anspruchsvolles, rechtskonformes Datenschutzkonzept** zu etablieren.

V. Erwägungen des LG Bonn

Dass bereits das ehrliche Bemühen um eine datenschutzkonforme Ausgestaltung honoriert werden kann, zeigt die Pressemitteilung des LG Bonn im Verfahren um 1&1. Die im Unternehmen etablierte Authentifizierungspraxis war datenschutzrechtlich unzureichend, über lange Zeit aber beanstandungslos geblieben. Berücksichtigt wurde also, dass dem Unternehmen in Bezug auf systemische Mängel das Problembewusstsein gefehlt habe; dieser Rechtsirrtum sei zwar vermeidbar gewesen, aber auch verständlich. Unter anderem diese Erwägung führte zu einer Herabsetzung des Bußgeldes um rund 90%.

VI. Fazit

Es gilt folglich die Prämisse "Aktion ist besser als Reaktion". Wenn es zu einem Verstoß

kommt und ein Bußgeldbescheid droht, sind jedenfalls umgehend alle Maßnahmen zu ergreifen, die eine Aufklärung des Sachverhalts befördern. Die gelebte Praxis der Datenschutzbeauftragten und nun auch des LG Bonn lassen hingegen darauf schließen, dass präventive Maßnahmen, die ein umsichtiges Unternehmen bereits im Vorfeld im Sinne eines **datenschutzrechtlichen Compliance-Management-Systems** etabliert hat oder für die Zukunft etablieren möchte, wesentlich positiveren Einfluss auf die Bußgeldhöhe haben. Der Aufbau eines solchen Instrumentariums ist daher dringend zu empfehlen.

MANDANTEN *INFORMATION*

SZA
SCHILLING, ZUTT & ANSCHÜTZ

Diese Mandanteninformation beinhaltet lediglich eine unverbindliche Übersicht über das in ihr adressierte Themengebiet. Sie ersetzt keine rechtliche Beratung. Als Ansprechpartner zu dieser Mandanteninformation und zu Ihrer Beratung stehen gerne zur Verfügung:

DR. GEORG JAEGER,
PARTNER
T +49 621 4257-208
F +49 621 4257-289
Georg.Jaeger@sza.de
www.sza.de

KATHARINA STEINBRÜCK, LL.M.
PARTNERIN
T +49 69 976 9601-270
F +49 69 976 9601-202
Katharina.Steinbrueck@sza.de
www.sza.de

DR. ANDRÉ REINHARD,
COUNSEL
T +49 621 4257-232
F +49 621 4257-289
Andre.Reinhard@sza.de
www.sza.de

DR. ALEXANDER HOFMANN,
ASSOCIATE
T +49 621 4257-206
F +49 621 4257-289
Alexander.Hofmann@sza.de
www.sza.de