Datenschutz

Bußgeldverfahren

Das Landgericht Bonn hat ein entscheidendes Urteil gegen den Telekommunikationsdienstleister 1&1 Telecom GmbH in der noch jungen Geschichte der Datenschutzgrundverordnung (DSGVO) gesprochen. Das Urteil stellt insbesondere die Frage nach einer angemessenen Bußgeldfestsetzung.

Im Dezember 2019 verhängte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ein Bußgeld in Höhe von 9,55 Millionen Euro gegen 1&1 wegen eines Verstoßes gegen die DSGVO. Daraufhin legte das Telekommunikationsunternehmen Einspruch gegen den Bußgeldbescheid ein. Schließlich bestätigte das LG Bonn den Datenschutzverstoß aufgrund unzureichender Sicherheitsmaßnahmen und folgte außerdem der Auffassung, dass das Unternehmen nach den Maßstäben der DSGVO dafür zu haften hat. Allerdings empfand das LG Bonn das ursprüngliche Bußgeld als unangemessen hoch und setzte es auf 900.000 Euro herab.

Das Urteil bildet einen Meilenstein in der Rechtsprechung zu den DSGVO-relevanten Bußgeldern. Einerseits wird deutlich, welche Maßstäbe die Gerichte an die erforderlichen Schutzmaßnahmen stellen. Andererseits wird ersichtlich, welche Maßgaben bei der Bemessung von Bußgeldern berücksichtigt werden.

Solch unmittelbare Haftung des Unternehmens stellt bis dato ein Novum im deutschen Sanktionsrecht dar. Nach § 41 des Bundesdatenschutzgesetzes (BDSG) gelten die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß. Für Ordnungswidrigkeitentatbestände in Art. 83 Abs. 4 bis 6 DSGVO gelten wiederum die Grundsätze des supranationalen Kartellrechts. Dieses geht bei Verstößen gegen Art. 101 und 102 AEUV von einer unmittelbaren Verantwortlichkeit der Unternehmen aus.

Der zugrundeliegende Sachverhalt

2018 reichte ein Kunde des Telekommunikationsunternehmens Beschwerde ein. Seine ehemalige Lebensgefährtin gab sich gegenüber dem 1&1-Callcenter als dessen Ehefrau aus und konnte so die neue Telefonnummer erfragen. Mit bloßer Angabe des Namens und des Geburtsdatums des Kunden konnte sich die Anruferin als Berechtigte authentifizieren und personenbezogene Daten in Erfahrung bringen. Dem Kunden wurde daraufhin durch seine Ex-Lebensgefährtin in strafrechtlich relevanter Weise nachgestellt.

1&1 reagierte auf die Beschwerde unmittelbar mit der Einführung einer angepassten Authentifizierungsmethode – bestehend aus Kunden-/Vertrags- oder Auftragsnummer, Geburtsdatum bzw. E-Mail-Adresse und den letzten vier Ziffern der IBAN. Ende 2019 stellte 1&1 auf eine fünfstellige Service-PIN zur Authentifizierung um.

Der Bußgeldbescheid des BfDI

Als der Bundesdatenschutzbeauftragte (BfDI) von dem Vorfall Kenntnis erlangte, warf er 1&1 einen Verstoß gegen Art. 32 DSGVO vor. Die Abfrage von Name und Geburtsdatum zur Authentifizierung gewährleiste keinen ausreichenden Schutz der Kundendaten. Deshalb handele es sich in diesem Fall um einen schwerwiegenden Verstoß.

Diesen Datenschutzverstoß ahndete der BfDI mit einer Geldbuße in Höhe von 9,55 Millionen Euro. Bei der Bemessung des Bußgeldes sieht Art. 83 DSGVO Abs. 4 Geldbußen von bis zu 2 % des Jahresumsatzes des vorangegangenen Geschäftsjahrs vor. Im Falle von 1&1 wäre somit bei einem Umsatz von 3,63 Milliarden Euro im Jahr 2018 eine Geldbuße von bis zu 72,6 Millionen Euro möglich. Aufgrund des kooperativen Verhaltens von 1&1 blieb der BfDI im unteren Bereich des möglichen Bußgeldrahmens.

1&1 erhob Einspruch mit der Begründung, das Bußgeld sei unverhältnismäßig und verstoße gegen das Grundgesetz.

Die Entscheidung des Landgerichts Bonn

Im November 2020 erklärte das LG Bonn 1&1 für schuldig im Sinne einer Ordnungswidrigkeit nach Art. 83 Abs. 4a DSGVO. Der Bußgeldbescheid wurde somit als berechtigt eingestuft. Aber das Bußgeld ist nach Ansicht des Landgerichts unverhältnismäßig hoch bemessen. >

Schuldhafter Verstoß gegen Art. 32 DSGVO

Das LG Bonn bestätigte den Verstoß gegen Art. 32 Abs. 1 DSGVO, wonach die Datenverantwortlichen keine geeigneten technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten ergriffen hatten.

Die Abfrage von Name und Geburtsdatum reichte sogar aus, wenn offensichtlich nicht der Vertragsinhaber, sondern eine dritte, möglicherweise nicht berechtigte Person in dessen Namen anrief. Besonders da sich Callcenter-MitarbeiterInnen und KundInnen in der Regel nicht persönlich kennen, muss eine sichere Authentifizierungsmethode zum Schutz der Kundendaten gewährleistet sein. Das Schutzniveau muss an die Eintrittswahrscheinlichkeit, die Schwere der Folgen und den Stand der Technik angepasst sein.

Es bestand somit ein erhebliches und reales Risiko für die Kunden, Opfer von Straftaten zu werden oder durch unberechtigten Datengebrauch geschädigt zu werden. Besonders die Daten Name und Geburtsdatum sind leicht von Dritten zu ermitteln. Daher eignen sich diese auch nicht zur Authentifizierung von Berechtigten und/oder Bevollmächtigten. Die Gefahr des Datenmissbrauchs ist somit deutlich erhöht und einfach möglich gewesen.

Mit geringem – personellem und finanziellem – Aufwand hätte, so das Gericht in seiner Urteilsbegründung, das Schutzniveau erhöht werden können. Schon die Abfrage von spezifischeren Daten hätte das Schutzniveau maßgeblich verbessert.

Das LG Bonn geht indes nicht davon aus, dass die Callcenter-Mitarbeiterin vorsätzlich gehandelt hat und sich über den Tatbestand bewusst war. Sie folgte dabei allen Vorschriften der damals gültigen Sicherheitsmaßnahmen. Ebenso ist zu berücksichtigen, dass die Callcenter-Mitarbeiterin keinen Zugriff auf besonders sensible oder schützenswerte Kundendaten hatte. Schlussendlich lag auch kein Massendiebstahl von Kundendaten vor und ein solcher sei auf diese Weise auch nicht möglich gewesen. Bis zu dem Zeitpunkt des Verstoßes war die Authentifizierungsstrategie des Callcenters nicht bemängelt worden. Zudem gibt es keine einheitlichen Richtlinien und Anforderungen an Authentifizierungsprozesse in Callcentern seitens des BfDI.

Nichtsdestotrotz ist der Datenverstoß vermeidbar gewesen. So ist es nötig, die Sicherheitsmaßnahmen der Datenverarbeitungsprozesse regelmäßig zu prüfen und an den Stand der Technik und etwaige Risiken anzupassen. Bei der Einführung der DSGVO hat die Rechtsabteilung des Unternehmens es versäumt, entsprechende Evaluierungen durchzuführen.

Eine Kernfrage war, ob eine Verbandshaftung in einem derartigen Fall überhaupt zulässig sei. § 41 BDSG verweist bei Bußgeldverfahren auf das Ordnungswidrigkeitengesetz (OWiG). Nach §§ 30 und 130 OWiG ist eine Verbandsgeldbuße nur dann möglich, wenn Betriebsinhaber, juristische Personen oder Personenvereinigungen eine Straftat oder Ordnungswidrigkeit ausüben. Das LG Bonn definiert den funktionalen Unternehmensbegriff des europäischen Kartellrechts nach Erwägungsgrund 150 DSGVO. Somit haftet das Unternehmen, woraus sich wiederum höhere Bußgelder ergeben.

Bemessung des Bußgeldes

Die Bemessung des Bußgeldes richtet sich nach Art. 83 DSGVO nach dem Umsatz des letzten abgeschlossenen Jahres vor Erlass des Bußgeldbescheides. Demnach bemisst sich das Bußgeld an dem Umsatz von 3,63 Milliarden Euro aus dem Kalenderjahr 2018, woraus sich eine zweiprozentige Obergrenze von 72,6 Millionen Euro ergibt. Diese Grenze gilt dabei lediglich als erste

AUTOR UND ANSPRECHPARTNER

Michael Switalla
Leiter Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de

In 2020

283 Bußgelder

mit einem Gesamtbetrag von ca. 48 Mio. Euro

Anstieg um ca. 50 Prozent gegenüber dem Vorjahr*

Orientierung, denn eine Geldbuße muss stets wirksam, verhältnismäßig und abschreckend sein.

Bei leichten Datenschutzverstößen umsatzstarker Unternehmen muss daher besonders auf die Verhältnismäßigkeit der Buße geachtet werden. Dementsprechend sind Zumessungskriterien zu berücksichtigen wie „Art, Schwere und Dauer des Verstoßes, die Zahl der von der Verarbeitung betroffenen Personen, das Ausmaß des Schadens, die Kategorie der betroffenen personenbezogenen Daten, das Bemühen des Unternehmens, den Schaden zu begrenzen, Art und Umfang der Kooperation mit den Datenschutzbehörden und der Grad der Verantwortlichkeit".

In dem konkreten Fall sind nach Ansicht des LG Bonn mildernde Umstände zu berücksichtigen.

- Es waren keine sensiblen Daten betroffen. Es hat nur einen Fall gegeben und es handelte sich um die erste Geldbuße gegen 1&1 wegen eines Datenschutzverstoßes.
- Der Datenschutzverstoß wurde nicht bewusst oder vorsätzlich begangen. 1&1 empfand den Authentifizierungsprozess als rechtlich unbedenklich, zumal es bezüglich der Authentifizierung im Callcenter keine Vorgaben des BfDI gab. Außerdem bestand dieses niedrige Schutzniveau, um den Kunden die Kontaktaufnahme zu erleichtern.
- Schließlich zeigte sich das Unternehmen äußerst kooperativ, erhöhte umgehend das Schutzniveau und stellte letztendlich auf eine Service-PIN um.
- Theoretisch waren 7,4 Millionen Kunden betroffen; relativ betrachtet bestand das Risiko allerdings nur für eine geringe Kundenzahl.

Infolge des öffentlichkeitswirksamen Verfahrens ist ein Reputationsverlust entstanden, der aufgrund der vergleichsweise geringfügigen Straftat unbegründet ist. In Anbetracht der mildernden Gesichtspunkte reduzierte das LG Bonn das Bußgeld schließlich auf 900.000 Euro.

Fazit

Das Urteil des LG Bonn gegen den Telekommunikationsdienstleister 1&1 zeigt einmal mehr auf, dass Datenschutzverstöße nicht ohne Folgen bleiben.

Der Bundesdatenschutzbeauftragte Ulrich Kelber stellt klar: „Datenschutz ist Grundrechtschutz. Die ausgesprochenen Geldbußen sind ein klares Zeichen, dass wir diesen Grundrechtschutz durchsetzen werden. Die europäische Datenschutzgrundverordnung (DSGVO) gibt uns die Möglichkeit, die unzureichende Sicherung von personenbezogenen Daten entscheidend zu ahnden. Wir wenden diese Befugnisse unter Berücksichtigung der gebotenen Angemessenheit an."

Angesichts der unmittelbaren Verbandshaftung von Unternehmen bei Datenschutzverstößen einzelner Mitarbeiterinnen und Mitarbeiter wird die Notwendigkeit deutlich, sämtliche Prozesse der Datenverarbeitung an ein solch erhöhtes Haftungsrisiko anzupassen. ▬

*Quelle: https://dsgvo-portal.de/news/rueckblick_dsgvo_bussgelder_datenpannen_2020.php