DSGVO-Megastrafe gegen „1&1“ wegen telefonischer Auskunft!

Praxistipps zur Vermeidung des bestraften Verhaltens!

Knapp vor Weihnachten wurde bekannt gegeben, dass gegen das deutsche **Telekommunikationsunternehmen „1&1“** wegen DSGVO-Verletzung eine **extrem hohe Geldstrafe,** konkret in Höhe **von EUR 9,55 Mio.,** verhängt wurde.

Wir sehen uns in diesem **Praxistipp das Urteil näher an,** weil der bei „1&1“ gemachte Fehler bei jedem anderen Unternehmen ebenfalls passieren kann. **Daher sollten wir daraus lernen!**

Was war passiert?
Bei „1&1“ war es in der Vergangenheit offensichtlich üblich, dass man Anrufern, **wenn sie Namen und Geburtsdatum eines Kunden nennen konnten, Auskünfte erteilte,** die „weitreichende Informationen zu weiteren personenbezogenen Kundendaten“ enthalten konnten. Daher wurde vom deutschen „Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“ (kurz BfDI) diese Megastrafe verhängt. Die Höhe überrascht vor allem deshalb, weil das Unternehmen beim Verfahren kooperativ war und zwischenzeitlich auch den Prozess datenschutzkonform abgeändert hat.
Auf der eigenen Homepage **begründet der BfDI die Strafe wie folgt:** „In diesem Authentifizierungsverfahren sieht der BfDI einen Verstoß gegen Artikel 32 DSGVO, nach dem das Unternehmen verpflichtet ist, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Verarbeitung von personenbezogenen Daten systematisch zu schützen.“

Und weiter: „Das Unternehmen hatte keine hinreichenden technisch-organisatorischen Maßnahmen ergriffen, um zu verhindern, dass Unberechtigte bei der telefonischen Kundenbetreuung Auskünfte zu Kundendaten erhalten können.“

Und der **Bundesbeauftragte Ulrich Kelber** wird wie folgt zitiert: „Datenschutz ist Grundrechtsschutz. Die **ausgesprochenen Geldbußen sind ein klares Zeichen, dass wir diesen Grundrechtsschutz 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.“
Der BfDI bestätigte in seiner Pressemeldung, dass sich die „1&1 Telecom GmbH einsichtig und äußerst kooperativ“ zeigte. So würde in einem ersten Schritt der **Authentifizierungsprozess durch die Abfrage zusätzlicher Angaben** stärker abgesichert. Und in einem weiteren Schritt werde bei der 1&1 Telecom GmbH nach Absprache mit dem BfDI ein neues, technisch und datenschutzrechtlich deutlich **verbessertes Authentifizierungsverfahren eingeführt.** So der BfDI.

Und weiter: **Dank des „kooperativen Verhaltens“** von 1&1 Telecom GmbH während des gesamten Verfahrens sei die Strafe „im unteren Bereich des möglichen Bußgeldrahmens“, so der Datenschutzbeauftragte. Aber der **Verstoß** sei „nicht nur auf einen geringen Teil der Kunden begrenzt (gewesen), sondern **stellte ein Risiko für den gesamten Kundenbestand dar“,** so die Begründung der Megastrafe durch den BfDI.
Wir erinnern uns: **DSGVO-Strafen können Existenz bedrohende Ausmaße** annehmen, weil sie am Umsatz des Unternehmens bemessen werden. Bis zu 20 Mio. Euro oder 4 % des Konzernumsatzes sind möglich.

Die Höhe der Strafe unter diesen beschriebenen Umständen kann man also so interpretieren, dass die **Datenschutzbehörde hier ein grobes Versäumnis** erkannt hat und **eine Art Musterurteil zur Abschreckung** bzw. zum Schaffen von Problembewusstsein erlassen wollte. Zwar handelt es sich hier um eine deutsche Entscheidung, aber da das **nationale Datenschutzrecht europaweit auf der DSGVO basiert,** der ersten europaweit gültigen Verordnung in diesem Bereich, ist das ein klares Ausrufezeichen auch für die anderen nationalen Datenschutzbehörden. Und diese werden sich – bei ähnlichen Anlässen – an der Argumentation, aber auch an der Strafhöhe der Deutschen orientieren.

Also kann man nur dringend davor warnen, sorglos am Telefon Auskünfte zu erteilen.
Überlegen Sie sich einen Prozess, der weitestgehend sicherstellt, dass der Anrufer tatsächlich der ist, als der er sich ausgibt und somit berechtigt ist, die Info zu erhalten.

Tipp: Etwa durch Vereinbarung eines eigenen Kundenkennworts, das nur die Kundin/der Kunde selbst wissen kann.
Wie oben von der Datenschutzbehörde definiert: Name und Geburtsdatum alleine reichen nicht.

Noch ein Praxis-Tipp: Und auch von einer **Nutzung der Sozialversicherungsnummer muss man DRINGEND abraten.** Einerseits, weil die Sozialversicherungsnummern unter die Kategorie „sensible Daten" fallen, andererseits weil die Verarbeitung aus datenschutzrechtlicher Sicht besonders heikel ist und man die Zustimmung des Betroffenen braucht.

Nehmen wir an, diese Zustimmung gibt der Kunde. Trotzdem darf man die Soz.Vers.Nr. nicht als „Kundenkennwort" verwenden. Grund ist, dass bereits die **„alte" Datenschutzkommission** mehrmals entschieden hat (zuletzt am 23.5.2014, nachzulesen im RIS unter GZ DSB-D213.131/0002-DSB/2014), dass die **Sozialversicherungsnummer nicht als „genereller Identifikator"** verwendet werden darf „in Zusammenhängen, die mit sozialversicherungsrechtlichen Sachverhalten nichts zu tun haben".

RA Mag. Stephan Novotny
Weihburggasse 4/2/26
1010 Wien
kanzlei@ra-novotny.at

Mag. Stephan Novotny, Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungswirtschaft

Quellen: Homepage des BfDI, dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Deutschland, RIS (Rechtsinformationssystem des Bundes), Homepage von Meineberater.at