Kapellmann
Rechtsanwälte

Praxisinfo Datenschutz: Erste DS-GVO-Millionengeldbuße in Frankreich – und auch deutsche Aufsichtsbehörden sind aktiv!

24. Januar 2019

Die seit dem 25. Mai 2018 geltende Europäische Datenschutz-Grundverordnung („DS-GVO") hat Zähne bekommen: Die französische Datenschutzbehörde CNIL hat am 21. Januar 2019 gegen den Internetgiganten Google eine **Rekordgeldstrafe in Höhe von 50 Millionen Euro** wegen Verstößen gegen die DS-GVO verhängt. Auch deutsche Aufsichtsbehörden sind in den vergangenen Monaten aktiv geworden.

Zum Hintergrund

Sowohl die österreichische Verbraucherschutzorganisation „None Of Your Business" („NOYB"), die sich der Durchsetzung des Datenschutzrechts verschrieben hat, als auch die französische

Netzbürgerrechtsorganisation „La Quadrature du Net“ („LQDN“) hatten gleich im Mai 2018 Beschwerden gegen Google wegen rechtswidriger Datenverarbeitungsvorgänge u.a. im Bereich der personalisierten Werbung eingelegt. Nach eigenen Angaben leitete die CNIL daraufhin Online-Recherchen ein und prüfte die Benutzeroberfläche von Google-Konten im Registrierungsprozess.

Die CNIL stellte dabei zwei wesentliche Verstöße fest:

- Zum einen rügte sie die fehlende Transparenz und Benutzerfreundlichkeit. Die **Datenschutzhinweise** u.a. zu den Zwecken der Datenverarbeitung und zur Speicherdauer seien **nicht leicht zugänglich**, sondern über mehrere Dokumente verteilt und die Nutzer müssten sich diese über verschiedene Verlinkungen und Buttons selbst zusammensuchen. Darüber hinaus seien die von Google bereitgestellten Informationen teils **nur schwer verständlich**, **zu abstrakt und ungenau** formuliert. Darin sieht die Behörde einen schwerwiegenden Verstoß gegen die DS-GVO. Denn diese schreibt zwingend vor, dass jeder Person, deren Daten erhoben werden, bestimmte Mindestinformationen über die Datenverarbeitung in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache bereitgestellt werden.
- Zum anderen hält die CNIL die **datenschutzrechtliche Einwilligung**, die Google für Datenverarbeitungen zu Zwecken der personalisierten Werbung bei Usern einholt, wegen mangelhafter Transparenz für **ungültig**. Daneben bemängelt sie, dass die Einwilligung durch die Nutzer entgegen den Vorgaben der DS-GVO nicht unmissverständlich abgegeben werde, da das **Kontrollkästchen** für die Erteilung der Einwilligung **bereits vorausgewählt** sei. Diese sog. Opt-Out-Lösung widerspricht Erwägungsgrund 32 der DS-GVO.

Die enorme Sanktionshöhe begründet die CNIL mit der **besonderen Schwere der Verstöße**: Google habe fortlaufend im gravierenden Maße grundlegende Datenschutzprinzipien verletzt. Mit Blick auf die großen Datenmengen, die Google über seine Nutzer erfasst, sowie die Vielzahl und Komplexität der Dienste und Anwendungen seien die Nutzer in ihren Rechten stark beeinträchtigt. Google beabsichtigt jüngsten Berichten zufolge, sich gegen den Bescheid vor dem höchsten französischen Verwaltungsgericht Conseil d’Etat zu Wehr zu setzen.

Aufatmen für den Mittelstand und Kleinstunternehmen?

Dass die großen US-Tech-Giganten schnell ins Kreuzfeuer der europäischen Aufsichtsbehörden geraten würden, stand zu erwarten. Und auch die Höhe der Geldbuße scheint Google – Berichten von › ***ZEIT online*** zufolge – angesichts jährlicher Umsatzzahlen in dreistelliger Milliardenhöhe wenig beeindruckt zu haben, zumal die französische Aufsichtsbehörde den Sanktionsrahmen bei weitem nicht ausgeschöpft hat. Die DS-GVO sieht bei schweren Verstößen etwa gegen die Transparenz- und Informationspflichten Geldbußen von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs eines Unternehmens vor – bei Google also bis zu 4-5 Mrd. Euro.

Was bedeutet die Entscheidung für **mittelständische und kleinere Unternehmen** anderer Branchen? Ist die Entscheidung der CNIL als bloßer Warnschuss für große Technologiekonzerne zu verstehen? Gilt für mittelständische und kleinere Unternehmen derzeit noch eine Schonfrist?

Laut jüngsten Berichten des › ***Handelsblatts*** und der **Thüringischen Landeszeitung** hat eine Umfrage bei den deutschen Aufsichtsbehörden ergeben, dass seit Geltung der DS-GVO bereits **64 Bußgeldbescheide in Deutschland u.a. auch gegen kleinere Unternehmen** erlassen worden sind. 33 Bußgelder sollen dabei in Nordrhein-Westfalen verhängt worden sein, 23 in Thüringen, drei weitere in Hamburg, jeweils zwei in Baden-Württemberg und Berlin sowie ein Bußgeld im Saarland. Laut *Handelsblatt* sind die Bußgelder dabei ihrer Höhe nach bislang eher gering ausgefallen. In Hamburg sollen Bußgelder in Höhe von insgesamt nur 25.000 Euro, in Nordrhein-Westfalen sogar von nur 15.000 Euro verhängt worden sein. In Thüringen belief sich das höchste zu zahlende Bußgeld auf 12.000 Euro. Die mit 80.000 Euro bislang höchste bekannte Einzelstrafe in Deutschland wurde durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI Baden-Württemberg) verhängt.

Die bislang erlassenen Bußgelder erwecken den Eindruck, dass die Aufsichtsbehörden derzeit noch eine Art inoffizielle Schonfrist gewähren. Laut *Handelsblatt* laufen allerdings derzeit noch „**sehr viele" weitere Bußgeldverfahren**. Allein in Bayern sollen 85 Bußgeldverfahren nach der DS-GVO anhängig sein. Bereits in den vergangenen Monaten hatte die für den nicht-öffentlichen Bereich zuständige bayerische Datenschutzbehörde dabei immer wieder angekündigt, neben anlassbezogenen auch stichprobenartige Prüfungen in allen Regionen Bayerns durchführen und sich an überregionalen Prüfungen beteiligen zu wollen. Von solchen Prüfungen betroffen sind private Wirtschaftsunternehmen aller Branchen ebenso wie freiberuflich Tätige, Vereine und Verbände. Und auch die Datenschutzaufsicht in Niedersachsen führt laut *Handelsblatt* derzeit eine „Querschnittsprüfung" von 50 niedersächsischen Unternehmen zur Umsetzung der DS-GVO durch. Die Aufsichtsbehörde in Brandenburg gab zwar an, in der „**Umstellungsphase**" Beratungen für zielführender zu halten, von Bußgeldern aber „künftig Gebrauch machen" zu wollen.

Sanktionierte Verhaltensweisen

Im genannten Fall des LfDI Baden-Württemberg wurden **Gesundheitsdaten im Internet** aufgrund unzureichender interner Kontrollmechanismen veröffentlicht. Weitere Fälle betrafen die versehentliche Ausgabe eines Schwerbehindertenausweises an den falschen Patienten durch ein Krankenhaus, die **Offenlegung von Kontoauszügen** an unberechtigte Bankkunden beim Online-Banking sowie das **unbefugte Abgreifen von Kundendaten** im Rahmen eines Hackerangriffs aufgrund unzureichender Sicherheitsvorkehrungen. Neben solchen Fällen **mangelhafter Datensicherheit** waren ferner der **unzulässige Versand von Werbe-E-Mails**, der unzulässige **Einsatz von Videoüberwachungssystemen** zu Zwecken der Kunden- und Mitarbeiterüberwachung, die unzulässige **Dashcam-Nutzung**, die unzulässige **Datenweitergabe an einen Geschäftsnachfolger** ohne Einwilligung der Betroffenen und

offene E-Mail-Verteiler Gegenstand von Bußgeldverfahren.

Keine Selbstbelastungsfreiheit – „unverbindliche" Anfrage mündet in Geldbuße

Die Aufsichtsbehörden betonen immer wieder, insbesondere auch kleineren und mittelständischen Unternehmen bei der Umsetzung der DS-GVO Hilfestellung zu leisten und insoweit eine Beratungsfunktion wahrzunehmen. Beim **Bayerischen Landesamt** sollen laut *Handelsblatt* **mehr als 4.000 Beratungen** stattgefunden haben. Die frühzeitige freiwillige Einbeziehung von Aufsichtsbehörden kann bei komplexeren und datenschutzsensiblen Vorhaben je nach Fall durchaus sinnvoll sein. Bei Datenpannen muss sogar nach der DS-GVO unter bestimmten Voraussetzungen möglichst innerhalb von 72 Stunden eine Meldung an die zuständige Behörde erfolgen. Die **Kommunikation mit den Aufsichtsbehörden** sollte jedoch **stets mit Bedacht** geführt werden. Denn jedenfalls bei freiwilligen Anfragen kennt das Datenschutzrecht **keine Selbstbelastungsfreiheit**. Das bekam etwa ein Hamburger Unternehmen zu spüren, nachdem es bei einer Datenschutzaufsichtsbehörde eigeninitiativ um Rat gebeten und anfragt hatte, wie mit einem Dienstleister umzugehen sei, der trotz mehrfacher Aufforderung **keinen Auftragsverarbeitungsvertrag** übersendet habe. Die Behörde wies darauf hin, dass der Auftraggeber als „Verantwortlicher" selbst verpflichtet sei, eine entsprechende Vereinbarung zu erwirken und dem Dienstleister zur Unterschrift zu übersenden. Nachdem das Unternehmen dem nicht Folge leistete, verhängte die zuständige Hamburgische Datenschutzbehörde eine **Geldbuße in Höhe von 5.000 Euro** – dies obgleich das Unternehmen betont hatte, nur rein vorsorglich angefragt zu haben. Auskünfte gegenüber den Aufsichtsbehörden sollten also stets unter Konsultation des betrieblichen Datenschutzbeauftragten oder juristischer Berater eingeholt werden.

Bedeutung für die Unternehmenspraxis

Die genannten Fälle zeigen eines ganz deutlich: Versäumnisse im Datenschutz können – je nach Art und Schwere des Verstoßes, der damit einhergehenden Folgen für die betroffenen Personen sowie der Kooperationsbereitschaft des Verantwortlichen – durchaus mit empfindlich hohen Bußgeldern geahndet werden. Das betrifft private Wirtschaftsunternehmen aller Branchen und jeder Größe ebenso wie öffentliche Wettbewerbsunternehmen, freiberuflich Tätige, Vereine und Verbände. **Typische Datenschutzverstöße**, die immer wieder Gegenstand von Beschwerden der Betroffenen oder Verbraucherschutzverbänden sind, sind etwa

- eine Verletzung der **Informations- und Transparenzpflichten** gegenüber Kunden, Vertragspartnern, Mitarbeitern oder Bewerbern,
- eine Missachtung der **Betroffenenrechte**,
- unzureichende technische und organisatorische **Datensicherheitsmaßnahmen**,
- fehlerhafte **Einwilligungserklärungen**,
- der unzulässige Einsatz neuer Technologien oder von **Videoüberwachungssystemen**,

- unzulässige **Mitarbeiterüberwachungen** oder
- der **fehlende** Abschluss von **Auftragsverarbeitungsverträgen**.

Unternehmen sind daher gut beraten, sich die mit solchen Versäumnissen verbundenen Risiken klar vor Augen zu führen. Neben **Geldbußen** drohen auch **Schadensersatzansprüche** der Betroffenen für immaterielle Schäden („Schmerzensgeld") sowie **Reputationsverlust** bei Bekanntwerden solcher Verstöße. Um sich vor solchen Folgen zu schützen, sind insbesondere größere Unternehmen gut beraten, ein **effektives Datenschutzmanagementsystem** umzusetzen und geeignete Vorkehrungen zu treffen, um Missstände frühzeitig identifizieren und auf Beschwerden und behördliche Anfragen und Untersuchungen angemessen reagieren zu können.

Bei Rückfragen steht Ihnen unser Team für › **Datenschutzrecht** gerne zur Verfügung.