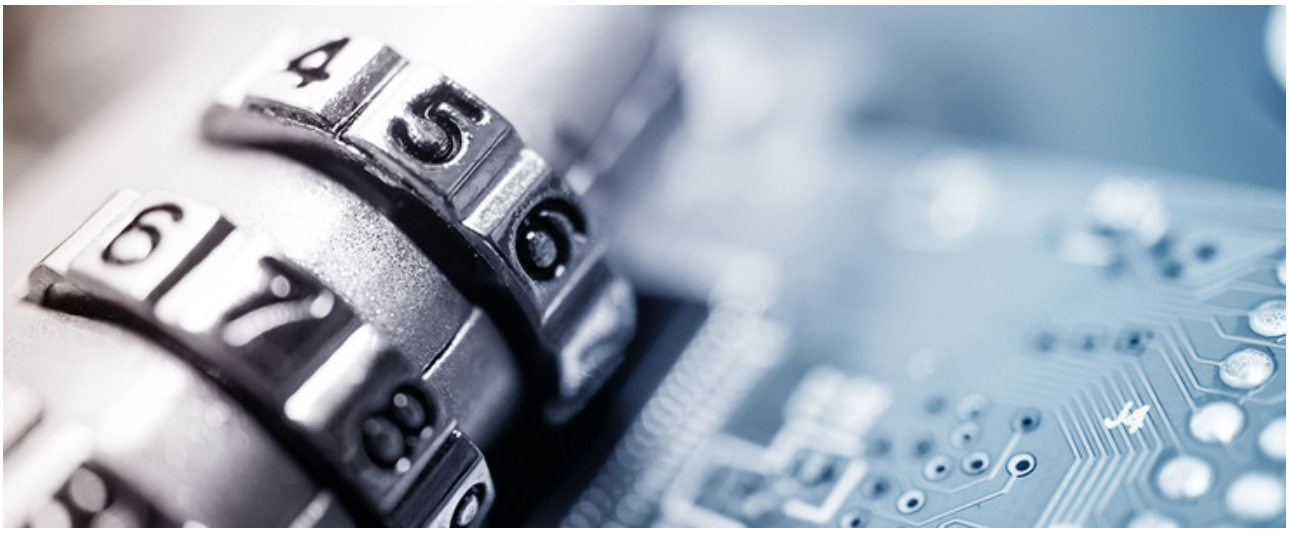
Kapellmann
Rechtsanwälte

Praxisinfo Datenschutzrecht: Aufsichtsbehörden verhängen erste Bußgelder nach Art. 83 DS-GVO

30. November 2018



Es ist so weit: Nachdem europäische Unternehmen zwei Jahre Zeit hatten, die neuen Datenschutzvorgaben der Europäischen Datenschutz-Grundverordnung (kurz „DS-GVO“) umzusetzen, sind die ersten Bußgelder durch europäische Datenschutzbehörden verhängt worden. Dies zeigt, dass die vielerorts verlautete „Schonfrist“ abgelaufen ist.

Zum Hintergrund

Nachdem die DS-GVO am 24. Mai 2016 in Kraft trat, gilt sie seit dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten der EU. Ergänzende Regelungen finden sich für die Privatwirtschaft im

Bundesdatenschutzgesetz (BDSG) in der ebenfalls seit dem 25. Mai 2018 geltenden Fassung. Zweck der novellierten datenschutzrechtlichen Regelungen ist, den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten. Um dieses Ziel zu erreichen, werden dem für die Datenverarbeitung Verantwortlichen u.a. erhebliche Organisations-, Transparenz- und Nachweispflichten auferlegt. Schlagworte wie Verarbeitungsverzeichnis, Datenschutzinformation, Betroffenenrechte, Auftragsverarbeitung, Joint Controllership, Löschkonzept, Datenschutz-Folgenabschätzung sowie technische und organisatorische Maßnahmen (kurz „TOM") sollten jedem Unternehmen inzwischen ein Begriff sein. Bei Verstößen gegen die datenschutzrechtlichen Vorschriften sieht die DS-GVO drastische Bußgelder vor, die je nach Schwere des Verstoßes und Auswirkungen für die Betroffenen bis zu 20 Mio. € oder 4 % des weltweit erzielten Vorjahresumsatzes eines Unternehmens oder gar des gesamten Konzerns betragen können, je nachdem, welcher Betrag höher ist.

Erstes bekannt gewordenes Bußgeld in Deutschland

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) hat am 21.11.2018 das erste in Deutschland bekannt gewordene Bußgeld nach Art. 83 DS-GVO gegen den Betreiber des Chat-Portals Knuddels.de verhängt. Nach einem Hackerangriff auf die Datenbank des Portals wurden Daten von etwa 330.000 Nutzern der Plattform Knuddels.de – darunter Pseudonyme, Passwörter und E-Mail-Adressen – veröffentlicht. Die Höhe des Bußgelds ist mit einem Betrag in Höhe von 20.000 € eher gering ausgefallen, was nach eigenen Angaben der Aufsichtsbehörde darauf zurückzuführen ist, dass der Betreiber des Chat-Portals den Vorfall selbst gemeldet sowie „in vorbildlicher Weise" eigene Versäumnisse offengelegt und sich bei der Aufarbeitung des Geschehens äußerst kooperativ gezeigt hatte.

Weitere Bußgelder durch die Datenschutzbehörde in Portugal und Österreich verhängt

Bereits zuvor hatte die portugiesische Datenschutzbehörde ein Bußgeld verhängt. Laut Presseberichten hatte ein Krankenhaus Patientenakten nicht ausreichend durch entsprechende Zugangsbeschränkungen geschützt, so dass nicht nur das behandelnde medizinische Personal in dem erforderlichen Umfang Zugang zu den Akten hatte, sondern auch beauftragte IT-Techniker auf die Inhalte der Patientenakten zugreifen konnten. Dies führte dazu, dass etwa dreimal so viele Systemnutzer wie notwendig Einblick in die vertraulichen Patientenakten nehmen konnten. Hierin sah die Aufsichtsbehörde einen Verstoß gegen den Grundsatz der Datenminimierung, den sie mit einem drastischen Bußgeld in Höhe von 400.000 € ahndete.

In Österreich wurde überdies ein Bußgeld in Höhe von 4.800 € gegenüber dem Betreiber eines Wettlokals wegen unzulässiger Videoüberwachung im öffentlichen Raum verhängt.

Stichprobenartige Datenschutzprüfungen durch deutsche Aufsichtsbehörden

In einer Pressemitteilung des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) hat die Aufsichtsbehörde angekündigt, seine Prüfaktivitäten wieder verstärkt aufzunehmen und flächendeckende Datenschutzkontrollen in Bayern vorzunehmen. Im Fokus der aktuellen Prüfungen stehen insbesondere der sichere Betrieb von Online-Shops, die Rechenschaftspflicht bei Großkonzernen, die Umsetzung der DS-GVO in kleinen und mittelständischen Unternehmen sowie die Erfüllung der Informationspflichten in Bewerbungsverfahren. Angesichts der personellen Aufrüstung deutscher Datenschutzbehörden ist davon auszugehen, dass auch andere Behörden dem bayerischen Beispiel folgen und ihre Kontrollaktivitäten ausweiten werden. Die Ankündigung des BayLDA zeigt, dass die Datenschutzbehörden durchaus gewillt sind, Kontrollen in Unternehmen nicht nur anlassbezogen, sondern auch stichprobenartig durchzuführen und die Einhaltung der vorgeschriebenen Standards nach der DS-GVO kritisch zu überprüfen. Wenngleich nicht jedes datenschutzrechtliches Versäumnis ein Bußgeld zur Folge haben wird, werden völliges Untätigbleiben und grobe Datenschutzverstöße sicherlich nicht ungeahndet bleiben.

Ausblick

Die vorgenannten Fälle zeigen, dass Versäumnisse im Datenschutz nicht folgenlos bleiben, sondern – je nach Art und Schwere des Verstoßes sowie der damit einhergehenden Folgen für die betroffenen Personen – durchaus mit empfindlich hohen Bußgeldern geahndet werden können. Bei der Bußgeldbemessung stellen die Aufsichtsbehörden dabei insbesondere auf die Kooperationsbereitschaft und die bei dem verantwortlichen Unternehmen vorhandenen Datenschutzstrukturen und -vorkehrungen ab. Für die Bußgeldhöhe ist es ebenfalls entscheidend, ob Unternehmen proaktiv Verstöße selbst melden oder diese vielmehr aufgrund von Hinweisen oder Beschwerden aufgedeckt werden; im letzteren Fall können weitaus höhere Geldbußen drohen. Daneben besteht künftig – anders als bislang – verstärkt das Risiko einer zivilrechtlichen Inanspruchnahme durch die Betroffenen. Denn die DS-GVO sieht Schadensersatzansprüche der Betroffenen für immaterielle Schäden bei Verstößen gegen die DS-GVO („Schmerzensgeld“) vor. Nicht zu unterschätzen sind auch reputative Schäden durch das Bekanntwerden solcher Verstöße. Um sich vor den möglichen Folgen zu schützen, sind Unternehmen gut beraten, die Anforderungen der DS-GVO möglichst effektiv umzusetzen und insbesondere geeignete Vorkehrungen zu treffen, um datenschutzrechtliche Risiken und Missstände frühzeitig identifizieren und minimieren zu können. Datenschutz ist schon lange kein „Nice-to-have“ mehr, sondern spätestens seit Geltung der DS-GVO für jedes Unternehmen eine unverzichtbare Compliance-Disziplin geworden.

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