Übersetzung Artikel Lexblog vom 27.12.2018:
CNIL Fines Uber for Data Security Failure Related to 2016 Data Breach

CNIL verhängt Geldbußen gegen Uber wegen Datensicherheitsfehlers im Zusammenhang mit Datenverletzung 2016

Am 20. Dezember 2018 teilte die französische Datenschutzbehörde (die "CNIL") mit, dass sie gegen Uber France SAS, die französische Niederlassung von Uber B.V. und Uber Technologies Inc., eine Geldbuße in Höhe von 400.000 € erhoben hat, weil sie einige grundlegende Sicherheitsmaßnahmen nicht umgesetzt hat, die die Verletzung der Uber-Daten von 2016 ermöglicht haben.

Hintergrund

Am 21. November 2017 veröffentlichte Uber Technologies Inc. auf seiner Website einen Artikel, der enthüllte, dass zwei externe Personen Ende 2016 weltweit auf die personenbezogenen Daten von 57 Millionen Uber-Fahrgästen und -Fahrer zugegriffen hatten.
Am 28. November 2017 sandte Uber B.V. ein Schreiben an den Vorsitzenden der Artikel-29-Arbeitsgruppe ("Arbeitsgruppe"), um die Umstände der Datenschutzverletzung darzulegen und ihre Bereitschaft zur Zusammenarbeit mit allen zuständigen Datenschutzbehörden zum Ausdruck zu bringen.
Am 29. November 2017 richtete die Arbeitsgruppe eine Sondereinheit ein, die die Vielzahl der nationalen Untersuchungen in der gesamten EU zu Ubers Datenschutzverletzung 2016 koordinieren sollte. Diese Taskforce besteht aus Vertretern der niederländischen, spanischen, französischen, belgischen, italienischen, britischen und slowakischen Datenschutzbehörden ("DPAs").

Am 22. Dezember 2017 sandte die CNIL einen Fragebogen an Uber Technologies Inc. und Uber B.V., der sich auf die Umstände der Datenschutzverletzung und die von diesen Unternehmen ergriffenen Sicherheitsmaßnahmen bezog. Uber antwortete auf den Fragebogen und erklärte, dass die Datenschutzverletzung in drei Schritten erfolgte: (1) zwei externe Personen haben es geschafft, Zugang zu Anmeldeinformationen zu erhalten, die im Klartext auf der kollaborativen Entwicklungsplattform "GitHub" gespeichert sind, die von den Uber-Softwareingenieuren verwendet wird; (2) die Hacker haben dann diese Anmeldeinformationen verwendet, um sich mit GitHub zu verbinden, und einen im Klartext aufgezeichneten Zugangsschlüssel in einer Quellcode-Datei gefunden, so dass die Hacker aus der Ferne auf einen Server zugreifen konnten, auf dem die Daten der Uber-Benutzer gespeichert sind; und (3) sie haben persönliche Daten von 57 Millionen Benutzern heruntergeladen, darunter 1.4 Millionen in Frankreich (1,2 Millionen Fahrgäste und 163.000 Fahrer).

Die Entscheidung der CNIL

Vor diesem Hintergrund erließ die CNIL eine Entscheidung, in der sie unter anderem (1) die Datenkontrolle von Uber Technologies Inc. und Uber B.V., (2) die Anwendbarkeit des französischen Datenschutzrechts, (3) das Versäumnis von Uber, angemessene Garantien zu ergreifen, um unbefugte Dritte am Zugriff auf die Daten zu hindern, und (4) die Verhängung einer Sanktion gegen Uber France SAS, die französische Niederlassung von Uber Technologies Inc. und Uber B.V. behandelte.

Uber Technologies Inc. und Uber B.V. als gemeinsame Datenverantwortliche: Die CNIL wies Ubers Argumente zurück, dass ihre niederländische Tochtergesellschaft Uber B.V. der alleinige Datenverantwortliche sei und dass Uber Technologies Inc. als reiner Datenverarbeiter von Uber B.V. fungierte, als (1) Richtlinien für den Umgang mit personenbezogenen Daten herausgegeben wurden, (2) Schulungen für neue Mitarbeiter der Uber-Gruppe angeboten wurden, (3) Vereinbarungen mit Drittunternehmen abgeschlossen wurden und (4) die Folgen des Datenverstoßes behandelt wurden.

Insbesondere vertrat die CNIL die Auffassung, dass der letzte Punkt - die Behandlung des Falles der Datenschutzverletzung - keine rein technische oder organisatorische Frage ist, die von einem Datenverarbeiter im Rahmen des dem Datenverarbeiter überlassenen Handlungsspielraums behandelt werden kann. Nach Ansicht der CNIL ist die Art und Weise, wie mit einer Datenschutzverletzung umgegangen wird, eine Frage, die sich auf die wesentlichen Elemente der Mittel der Datenverarbeitung bezieht und nur vom für die Datenverarbeitung Verantwortlichen festgelegt werden kann. Nach Ansicht der CNIL ist die Tatsache, dass Uber Technologies Inc. (1) entworfene Datenschutzrichtlinien, die von allen Unternehmen der Uber-Gruppe angewendet werden, (2) für die Schulung neuer Mitarbeiter der Gruppe verantwortlich waren und (3) Vereinbarungen mit Drittunternehmen (einschließlich der Bereitstellung von Tools, die für das reibungslose Funktionieren der Uber-Dienste erforderlich sind) auch zeigen, dass Uber Technologies Inc. eine Schlüsselrolle bei der Festlegung der Zwecke und Mittel der Datenverarbeitung spielt. Infolgedessen stellte die CNIL fest, dass Uber Technologies Inc. ein gemeinsamer Datenverantwortlicher mit Uber B.V. ist.

Anwendbarkeit des französischen Datenschutzrechts: Uber hat eine Niederlassung in Frankreich - Uber France SAS -, die Marketingkampagnen zur Förderung der Dienstleistungen von Uber durchführt und Uber-Fahrgäste und -Fahrer in Frankreich unterstützt. Unter Bezugnahme auf die Entscheidung des Europäischen Gerichtshofs ("EuGH") in der Rechtssache Google v. Costeja hielt die CNIL die Verarbeitung der personenbezogenen Daten von Uber-Fahrgästen und Fahrern für im Rahmen der Tätigkeit der französischen Niederlassung der für die Datenverarbeitung für verantwortlich, Uber B.V. und Uber Technologies Inc.

Versäumnis, angemessene Sicherheitsmaßnahmen zu ergreifen: Die CNIL kam zu dem Schluss, dass die Datenschutzverletzung vermeidbar gewesen wäre, wenn Uber bestimmte grundlegende Sicherheitsmaßnahmen getroffen hat, darunter:

- Das Unternehmen hätte von seinen Ingenieuren verlangen sollen, dass sie sich mit einer starken Authentifizierungsmaßnahme (z.B. Benutzername und Passwort und dann ein Geheimcode auf dem Handy des Ingenieurs) mit der Plattform "GitHub" verbinden.
- Das Unternehmen sollte keine Zugangsdaten - im Klartext im Quellcode der Plattform "GitHub" - gespeichert haben, die den Zugriff auf den Server ermöglichen.
- Das Unternehmen hätte ein IP-Filtersystem implementieren sollen, um auf die Server "Amazon Web Services S3" zuzugreifen, die personenbezogene Daten seiner Benutzer enthalten.

Uber France SAS als Adressat der Entscheidung der CNIL: Die CNIL hat unter Berufung auf die Entscheidung des EuGH vom 5. Juni 2018 zur Wirtschaftsakademie Schleswig-Holstein GmbH die Argumentation von Uber zurückgewiesen, dass die CNIL eine Sanktion nur gegen einen Datenverantwortlichen (und nicht gegen eine bloße Einrichtung des für die Datenverarbeitung Verantwortlichen) verhängen könne. In dieser Entscheidung stellte der EuGH fest, dass, wenn ein außerhalb der EU niedergelassenes Unternehmen mehrere Niederlassungen in verschiedenen EU-Mitgliedstaaten hat, die Aufsichtsbehörde eines Mitgliedstaats seine aus der EU-Datenschutzrichtlinie abgeleiteten Befugnisse in Bezug auf eine Niederlassung im Hoheitsgebiet dieses Mitgliedstaats ausüben kann, auch wenn dies aufgrund der Aufgabenverteilung innerhalb der Gruppe der Fall ist, (1) diese Einrichtung ausschließlich für den Verkauf von Werbeflächen und andere Marketingaktivitäten im Hoheitsgebiet des betreffenden Mitgliedstaats zuständig ist und (2) die ausschließliche Zuständigkeit für die Erhebung und Verarbeitung personenbezogener Daten für das gesamte Hoheitsgebiet der EU zu einer Einrichtung mit Sitz in einem anderen Mitgliedstaat gehört. Die CNIL beschloss daher, eine Sanktion gegen Uber France SAS zu verhängen. Da die allgemeine Datenschutzverordnung der EU zum Zeitpunkt der Datenschutzverletzung nicht anwendbar war, verhängte die CNIL eine Geldbuße von 400.000 € gegen Uber France SAS. Bei der Festsetzung der Höhe der Geldbuße berücksichtigte die CNIL die Tatsache, dass Hacker Zugang zu den Daten erhielten, wodurch sie möglicherweise die Möglichkeit hatten, die Daten weiter zu nutzen. Die CNIL betonte, dass, obwohl bisher kein Schaden für die betroffenen Personen gemeldet wurde, der Nachweis der völligen Abwesenheit eines Schadens von Uber nicht erbracht werden kann.

Dies ist die dritte Geldbuße, die von einem EU-DPA gegen Uber im Zusammenhang mit seiner Datenverletzung im Jahr 2016 verhängt wurde. Am 6. November 2018 verhängte das niederländische DPA eine Geldstrafe von 600.000 € gegen Uber, weil Uber den Verstoß nicht gemeldet hatte. Am 26. November 2018 verhängte das ICO außerdem eine Geldbuße für Uber in Höhe von 385.000 Pfund wegen Nichteinhaltung geeigneter Sicherheitsmaßnahmen.