La Kanzlei

Französische Datenschutzbehörde verhängt Bußgeld von 400.000 € gegen die RATP

Datenschutz / IT

Die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) hat am 29. Oktober 2021 aufgrund mehrerer Verstöße gegen die Datenschutzgrundverordnung (DSGVO) eine Geldstrafe in Höhe von 400.000 Euro gegen den Betreiber des öffentlichen Personennahverkehrs in Paris und Umgebung RATP (Régie Autonome des Transports Parisiens) verhängt. Die Entscheidung der CNIL wurde veröffentlicht.

Ursprung der Überprüfung durch die CNIL war eine Beschwerde der Gewerkschaftsorganisation CGT-RATP aus Mai 2020. Der Vorwurf: die Bewertungsdateien einzelner RATP-Buszentren, die der Vorbereitung der Einstufungskommissionen für Beförderungen dienten, enthielten die durch die Beschäftigten ausgeübten Streiktage. Diese Praxis konnte durch die CNIL bezüglich drei Buszentren der RATP bestätigt werden. Zudem stellte die CNIL datenschutzrechtliche Verstöße in Bezug auf die Speicherdauer und Datensicherheit fest.

Die Entscheidung der CNIL vom 29. Oktober 2021 im Einzelnen:

Verstoß gegen die Pflicht zur Datenminimierung (Artikel 5 Absatz 1 Buchstabe c DSGVO):

Gemäß Artikel 5 Absatz 1 Buchstabe c DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung"). Die betroffenen Buszentren der RATP hatten nach den Feststellungen der CNIL jedoch in den zur Vorbereitung von Einstufungen und Beförderungen erstellten Dateien auch die Anzahl der Streiktage pro Mitarbeiter im bewerteten Zeitraum aufgeführt. Die CNIL befand, dass diese Daten keine angemessenen, relevanten und notwendigen Daten für die Beurteilung der Beschäftigten und mithin für die Erreichung des Verarbeitungszwecks darstellten. Nach Auffassung der Datenschutzbehörde hätte es ausgereicht, in den Beurteilungsdateien lediglich die Gesamtzahl der Abwesenheitstage der Beschäftigten anzugeben. Es sei für die Beurteilung hingegen nicht notwendig gewesen, die Kategorie der Anzahl der Streiktage unter den erfassten Abwesenheiten zu individualisieren.

Die CNIL hat bei ihrer Entscheidung zweifellos den äußerst sensiblen Charakter der verarbeiteten Datenkategorie und deren möglichen sozialen und politischen Auswirkungen berücksichtigt. Denn sie unterstrich zumindest en passant den besonderen Charakter der das Streikrecht betreffenden Daten und wies darauf hin, dass die Verarbeitung dieser Datenkategorie durch den Arbeitgeber auf bestimmte legitime Zwecke beschränkt sein müsse.

Verstoß gegen die Pflicht zur Begrenzung der Speicherdauer (Artikel 5 Absatz 1 Buchstabe e DSGVO):

Gemäß Artikel 5 Absatz 1 Buchstabe e DSGVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Die RATP verwendet eine Anwendung namens DORA zur Visualisierung und Extraktion von Daten aus verschiedenen IT-Anwendungen für die Verarbeitung und Verwaltung von Personalressourcen ihrer Buszentren. Nach Angaben der RATP hat diese Anwendung insbesondere den Zweck, operative Daten zu erforschen. Die verarbeiteten personenbezogenen Daten wurden für sechs Jahre in der aktiven Datenbank der Anwendung aufbewahrt. Die CNIL erinnerte zunächst daran, dass die Speicherdauer personenbezogener Daten nach dem Verarbeitungszweck zu bestimmen sei. Wenn dieser Zweck erreicht sei, müssten die Daten grundsätzlich gelöscht, anonymisiert oder zwischenarchiviert werden, sofern ihre Speicherung für die Erfüllung gesetzlicher Pflichten oder für (vor)prozessuale Zwecke erforderlich sei.

Nach den Feststellungen der CNIL konnte die Speicherdauer von sechs Jahren durch die RATP im Hinblick auf die Zwecke der Anwendung DORA hingegen nicht gerechtfertigt werden. Beispielsweise sei nicht ersichtlich, warum in der Anwendung enthaltene Daten, die für die Berechnung der Bemessungsgrundlage für die Lohn- und Gehaltsabrechnung sowie für Sozialversicherungsbeiträge relevant seien, für eine Dauer von sechs Jahren aufbewahrt werden sollten, obwohl für die Erstellung der Lohnabrechnung eine deutlich kürzere Speicherdauer ausreichend wäre.

Ebenso sei es nicht gerechtfertigt, dass in einigen Buszentren der Vorbereitung der Einstufungsgremien dienende Dateien für mehr als drei Jahre nach Abhaltung des entsprechenden Gremiums gespeichert worden waren. Die CNIL stufte diese Speicherdauer als exzessiv ein und befand, dass damit die für den Verarbeitungszweck erforderliche Speicherdauer überschritten werde.

Mit dieser Entscheidung bleibt die CNIL ihrer Linie treu. In der Tat werden Verstöße gegen die Speicherbegrenzung durch die CNIL immer wieder zum Anlass für Sanktionen genommen. Die Behörde empfiehlt generell eine Speicherdauer von nicht mehr als drei Jahren.

Verstoß gegen die Pflicht zur Gewährleistung der Datensicherheit (Artikel 23 DSGVO):

Schließlich stellte die CNIL fest, dass es allen zugangsberechtigten Beschäftigten unabhängig von ihrem Aufgabenbereich möglich war, die im Tool DORA gespeicherten personenbezogenen Daten anzuzeigen sowie zu extrahieren. Sie konnten auf die gespeicherten Mitarbeiterdaten aller – nicht nur der eigenen – Geschäftseinheiten und somit auf Daten von über 16.000 Personen zugreifen, ohne dass die RATP die Notwendigkeit dieser Zugriffsmöglichkeit für alle Mitarbeiter rechtfertigen

konnte.

Nach Auffassung der CNIL erlaubte die Konfiguration der DORA-Anwendung mithin nicht, den Zugriff der Nutzer auf diejenigen Daten zu beschränken, die effektiv im Rahmen ihrer jeweiligen Aufgaben benötigt wurden. Dies sei datenschutzrechtlich jedoch erforderlich. Nach Artikel 32 DSGVO habe der für die Verarbeitung personenbezogener Daten Verantwortliche geeignete Maßnahmen zu ergreifen, um die Vertraulichkeit der Daten zu gewährleisten und zu verhindern, dass die Daten unrechtmäßig durch Personen verarbeitet werden, die nicht notwendigerweise Kenntnis von ihnen haben müssen. Es obliege dem Verantwortlichen, verschiedene Berechtigungsprofile für den Zugriff auf die gespeicherten Daten zu erstellen und im Rahmen der Zugriffsberechtigungen eine Trennung nach Aufgaben und Verantwortungsbereichen vorzunehmen, die der Bedeutung und der Sensibilität der verarbeiteten Daten sowie den Risiken für die betroffenen Personen angemessen sei.

Diese notwendigen und geeigneten technischen und organisatorischen Maßnahmen, um ein angemessenes Schutzniveau für die in der Anwendung DORA enthaltenen Daten zu gewährleisten, habe die RATP hingegen nicht ergriffen, wodurch ein Verstoß gegen Artikel 23 DSGVO begründet sei.

Praxistipp:

Die hier besprochene Entscheidung ist nur eines von vielen Beispielen für das strenge und entschiedene Eingreifen der CNIL bei Verstößen gegen die geltenden Datenschutzbestimmungen. Auch in diesem Jahr machte die Datenschutzbehörde wiederholt ernst und verhängte zahlreiche, teils sehr empfindliche Geldstrafen. Unternehmen sollten sich dessen bewusst sein und das Thema Datenschutz keinesfalls auf die leichte Schulter nehmen.

2021-12-22

Qivive
Rechtsanwalts GmbH

qivive.com

Köln[D]
Konrad-Adenauer-Ufer 71
D – 50668 Köln
T + 49 (0) 221 139 96 96 - 0
F + 49 (0) 221 139 96 96 - 69
koeln@qivive.com

Paris[F]
50 avenue Marceau
F – 75008 Paris
T + 33 (0) 1 81 51 65 58
F + 33 (0) 1 81 51 65 59
paris@qivive.com

Lyon[F]
10 –12 boulevard Vivier Merle
F – 69003 Lyon
T + 33 (0) 4 27 46 51 50
F + 33 (0) 4 27 46 51 51
lyon@qivive.com