La Kanzlei

Datenschutz Frankreich: 1,5 Millionen Euro Geldstrafe wegen Gesundheitsdatenleck

IP- / IT-Recht

Die Affäre war im Februar 2021 in aller Munde, nachdem die französische Presse über ein massives Datenleck berichtet hatte, von dem fast 500.000 Personen betroffen waren. Im Mittelpunkt: ein Anbieter von Softwarelösungen für medizinische Analyselabore, bei dessen Tätigkeit hochsensible Gesundheitsdaten durchgesickert und zeitweise im Internet abrufbar waren.

Zwar wurden die Internetseite und damit der Zugriff auf die Daten schnellstmöglich durch Gerichtsentscheidung blockiert. Für das Unternehmen hatte die Sache nun jedoch noch ein Nachspiel. Die französische Datenschutzbehörde CNIL hat mit Entscheidung vom 15. April 2022 mehrere gravierende Verstöße gegen die Datenschutzgrundverordnung (DS-GVO) festgestellt und ein hohes Bußgeld gegen den Auftragsverarbeiter verhängt.

Keine ausreichenden Sicherheitsvorkehrungen

Das Unternehmen hat laut der CNIL bei der Datenverarbeitung im Auftrag der Labore keine ausreichenden Sicherheitsvorkehrungen getroffen. Nach Artikel 32 DS-GVO sind der Verantwortliche und der Auftragsverarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei sind insbesondere die Wahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

Die CNIL stellte jedoch insbesondere fest, dass der Auftragsverarbeiter – trotz des hochsensiblen Charakters und der großen Anzahl der verarbeiteten Gesundheitsdaten - kein spezifisches Verfahren für Datenmigrationsvorgänge eingerichtet hatte, die Daten unverschlüsselt gespeichert wurden und auch keine automatische Löschung der Daten nach dem Transfer erfolgte. Mehrere Sicherheitswarnungen im Vorfeld des Datenlecks hätten das Unternehmen zudem zu einer Überprüfung seiner Sicherheitsvorkehrungen veranlassen müssen.

Weisungen der Auftraggeber überschritten

Nach den Feststellungen der CNIL extrahierte das Unternehmen im Rahmen der Migration von Daten von einer Software zu einem anderen Tool auch ein größeres Datenvolumen als erforderlich gewesen wäre und überschritt dadurch die Weisungen der auftraggebenden Labore. Darin liegt ein Verstoß gegen Artikel 29 DS-GVO, weil nach dieser Vorschrift im Rahmen einer Auftragsverarbeitung die Daten durch den Auftragnehmer ausschließlich auf Weisung des Verantwortlichen verarbeitet werden dürfen.

Fehlen einer formalisierten Grundlage für die Auftragsverarbeitung

Eine Auftragsverarbeitung ist nach der DS-GVO zudem nur dann rechtmäßig, wenn sie auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments erfolgt. Artikel 28 Absatz 3 DS-GVO enthält insofern eine Aufzählung bestimmter Regelungen, die der Auftragsverarbeiter und der Verantwortliche in der Rechtsgrundlage treffen müssen. Da im Streitfall weder die Allgemeinen Geschäftsbedingungen noch die Wartungsverträge des Unternehmens diese verpflichtenden Hinweise enthielten, stellte die CNIL auch einen Verstoß gegen Artikel 28 DS-GVO fest.

Bemessung der Geldstrafe

Die Entscheidung war schließlich Gelegenheit für die CNIL, die in Artikel 83 DS-GVO genannten Kriterien für die Verhängung von Geldbußen zu veranschaulichen. Die zahlreichen Sicherheitsmängel, die große Menge an durchgesickerten Daten sowie der Umstand, dass die Rechtsverletzung für die Betroffenen besonders intensiv war, da es sich um sehr sensible Daten (neben Daten zum Personenstand beispielsweise auch genetische Daten und Angaben zu Krankheiten und Behandlungen) gehandelt hatte, rechtfertigten nach Auffassung der Datenschutzbehörde unter Berücksichtigung der finanziellen Situation des Unternehmens eine Geldstrafe in Höhe von 1,5 Millionen Euro.

Sie haben Fragen zu Ihren Pflichten nach der DS-GVO und möchten mehr zu diesem Thema erfahren?

Sprechen Sie uns gerne an

Weitere grundlegende Informationen zum Datenschutz in Frankreich finden Sie auch in unserem Merkblatt Datenschutz in Frankreich nach der DSGVO.

2022-05-16

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]
4 Pl. Amédée Bonnet
F – 69002 Lyon
T + 33 (0) 4 27 46 51 50
F + 33 (0) 4 27 46 51 51
lyon@qivive.com

Strasbourg[F]
10 Pl. Gutenberg
F – 67000 Straßburg
T + 33 (0) 3 92 12 02 20
F + 33 (0) 3 92 12 02 21
strasbourg@qivive.com