La Kanzlei

Kommerzielle Werbung und Datenschutz: Strafe von 600.000 € gegen den französischen Energieversorger EDF

IP- / IT-Recht



Mélanie Allemand

Die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) hat am 24. November 2022 nach Beschwerden von Privatpersonen aufgrund mehrerer Verstöße gegen die Datenschutzgrundverordnung (DSGVO) eine Geldbuße in Höhe von 600.000 € gegen EDF (Électricité de France), den größten Stromversorger in Frankreich, verhängt. Die Entscheidung der CNIL wurde veröffentlicht.

Hintergrund der Entscheidung der CNIL

Nachdem sich Betroffene an die Aufsichtsbehörde aufgrund von Schwierigkeiten bei der Ausübung ihrer Rechte gegenüber EDF gewandt hatten, wurde seitens der CNIL eine Überprüfung durchgeführt. Bei Missachtung der gesetzlich vorgeschriebenen Pflichten drohen hohe Bußgelder. Die Höhe der verhängten Geldbuße wurde von der zuständigen Kommission der CNIL unter Berücksichtigung der festgestellten Verstöße sowie der im Laufe des Verfahrens ergriffenen Maßnahmen seitens EDF festgelegt.

Die sanktionierten Verstöße im Einzelnen

Verstoß gegen die Verpflichtung, die Zustimmung von Personen zum Erhalt von kommerzieller Werbung auf elektronischem Wege einzuholen (Art. L. 34-5 CPCE und Artikel 7 DSGVO)

Zwischen 2020 und 2021 führte EDF eine **Werbekampagne auf elektronischem Wege** durch. Das Unternehmen konnte jedoch nicht nachweisen, dass es **zuvor eine wirksame Einwilligung** gemäß Art. L. 34-5 des französischen Gesetzbuches über das Postwesen und elektronische Medien (Code des postes et des communications électroniques) und Art. 7 DSGVO von den betroffenen Personen eingeholt hatte. Das Unternehmen konnte zwar zwei Beispiele für ein Standardformular zur Erfassung von Daten potenzieller Kunden vorlegen, welches EDF von einem Datenvermittler

(Englisch: data broker) zur Verfügung gestellt worden war. Die CNIL bemängelte jedoch **das Fehlen einer Liste der Empfänger der Daten**, obwohl eine solche Liste den Personen bei der Erteilung ihrer Zustimmung zur Verfügung gestellt werden muss. Die CNIL befand, dass die Maßnahmen, die EDF getroffen hatte, um sicherzustellen, dass die Einwilligung von den Personen wirksam erteilt wurde, bevor sie umworben wurden, unzureichend waren. EDF räumte ein, dass das Unternehmen die verwendeten **Standardformulare nicht überprüfte und keine Audits bei den Datenbrokern** durchführte.

Verstöße gegen die Informationspflicht (Artikel 13 und 14 DSGVO) und die Wahrung der Rechte der Betroffenen (Artikel 12, 15 und 21 DSGVO)

Die von der CNIL durchgeführten Überprüfungen ergaben weitere Verstöße, die in der Sanktionsentscheidung festgehalten wurden.

Die auf der Webseite des Unternehmens vorhandene **Datenschutzrichtlinie enthielt keine ausreichenden Informationen zu verschiedenen Aspekten der Datenverarbeitung** (Aufbewahrungsfrist für personenbezogene Daten) und gab nicht die Rechtsgrundlage an (Artikel 13 DSGVO). Darüber hinaus gab EDF im ersten Werbebrief lediglich an, dass die "Daten von einer auf Datensammlung spezialisierten Organisation gesammelt wurden", ohne genau anzugeben, woher die Daten stammten (Artikel 14 DSGVO). Auch auf eine Reihe von Anfragen Betroffener hatte das Unternehmen nicht rechtzeitig innerhalb der dafür vorgesehenen Monatsfrist geantwortet (Artikel 12 DSGVO). Ein weiterer Verstoß betraf das Auskunftsrecht (Artikel 15 DSGVO) und das Widerspruchsrecht der betroffenen Personen (Artikel 21 DSGVO). EDF gab nicht nur ungenaue Informationen über die Herkunft der gesammelten Daten, sondern ignorierte den Widerspruch gegen den Erhalt von kommerzieller Werbung.

Die Überprüfung seitens der Behörde ergab schließlich einen **Verstoß gegen die Gewährleistung der Datensicherheit** (Artikel 32 DSGVO), da das Unternehmen keine ausreichenden technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten ergriffen hatte. Zum einen waren die Passwörter für den Zugang zum Kundenbereich des Portals "Energieprämie" von mehr als 25.000 Konten bis Juli 2022 unsicher gespeichert und aufbewahrt. Zum anderen waren die Passwörter für den Zugang zum EDF-Kundenbereich von mehr als 2,4 Millionen Konten nur durch **Hashing** (eine Reihe von Zeichen, die anstelle des Passworts ermittelt werden) und nicht durch **Salting** (Hinzufügen von zufälligen Zeichen vor dem Hashing, um zu verhindern, dass ein Passwort durch den Vergleich von Hashes gefunden wird) gesichert, wodurch sie einem Risiko ausgesetzt waren.

Praxistipps

- Besonders auf **eine rechtzeitige und verständliche Information der betroffenen Personen** ist zu achten. Die Information der betroffenen Personen muss hinreichend klar über die geplante Verarbeitung unterrichten und umfasst auch die Belehrung über das Recht, eine erteilte Einwilligung jederzeit zu widerrufen. Die entsprechenden Hinweise sollten **auf der Unternehmens-Webseite stets aktuell und vollständig** zu finden sein.

- Sowohl die **Einwilligung als auch ein etwaiger Widerspruch** sollten **sachgerecht dokumentiert**

werden.

- Unternehmen sollten auf **funktionierende Prozesse zur Beantwortung von Betroffenenrechten** achten.

- Ebenso ist auf **ausreichende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten**, wie etwa in Bezug auf Passwörter, besonders Acht zu nehmen.

2022-12-08

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