

## EuGH bestimmt neue Compliance-Pflichten nach der DSGVO

**Der Europäische Gerichtshof (EuGH) hat sich in einer neuen Entscheidung zu wesentlichen Fragen der DSGVO erneut sehr verbraucherfreundlich positioniert (Urteil vom 27. Oktober 2022, [C-129/21](#)). Das Urteil hat für Unternehmen weitreichende Folgen.**

### Eckpunkte:

- Der EuGH stellt neue Compliance-Pflichten für datenschutzrechtlich Verantwortliche auf, die klar über die in der DSGVO geregelten Vorgaben hinausgehen.
- Die erweiterten Compliance-Pflichten werden voraussichtlich zu einer deutlichen Ausdehnung der Haftung von Verantwortlichen führen.
- Verantwortliche können gegebenenfalls auch für mögliche Datenschutzverstöße durch Dritte haften (etwa im Rahmen sogenannter Einwilligungsketten).

Der EuGH schafft mit dieser Entscheidung einen Präzedenzfall. Er begründet nicht nur einen — in der DSGVO nicht vorgesehenen — weitreichenden Haftungsverbund im Rahmen von Verarbeitungsketten. Vor allem schafft der EuGH neue Compliance-Pflichten im Datenschutz. Denn er stellt klar, dass die in Art. 5 Abs. 2 DSGVO geregelte Rechenschaftspflicht datenschutzrechtlich Verantwortliche allgemein dazu verpflichtet, „geeignete Maßnahmen zu ergreifen, um etwaigen Verstößen gegen die Vorschriften der DSGVO vorzubeugen.“ Die Datenschutzaufsichtsbehörden könnten diese Aussage zum Anlass nehmen, um für Verantwortliche noch weitergehende Handlungspflichten zu begründen, die über den Wortlaut der DSGVO hinausgehen. Entsprechende könnten dann Geldbußen, Schadensersatzforderungen und andere Risiken nach sich ziehen.

### Sachverhalt des EuGH- Verfahrens

Die Klägerin betreibt als Telekommunikationsanbieter öffentlich zugängliche digitale Telefonverzeichnisse. Diese Verzeichnisse enthalten unter anderem Adressdaten und Telefonnummern von Nutzern. Die Klägerin erhielt die entsprechenden Daten unter anderem von Drittanbietern, die ebenfalls Telefonverzeichnisse führten. Diese Anbieter hatten die Datensätze auf Basis von Einwilligungen der betroffenen Nutzer erhoben. Die entsprechende Einwilligung diente auch als Rechtsgrundlage für die Weiterleitung der Daten an die Klägerin. Diese Daten gab die Klägerin wiederum an andere Anbieter von Telefonverzeichnissen weiter.

Im streitigen Fall hatte ein Nutzer eines Drittanbieters die Klägerin aufgefordert, seine Kontaktdaten in ihrem Verzeichnis und in Verzeichnissen Dritter nicht mehr aufzuführen. Dieser Aufforderung kam die Klägerin zunächst nach. Aufgrund eines technischen Fehlers wurden die Daten des betreffenden Nutzers

aber erneut in das Verzeichnis der Klägerin aufgenommen. Auf Aufforderung des Nutzers hin löschte die Klägerin den Datensatz erneut aus ihrem Verzeichnis. Sie teilte dem Nutzer zudem mit, dass sie auch andere Anbieter von Verzeichnissen, die seine Daten erhalten hatten, über seinen Antrag auf Löschung informiert hatte.

Der Nutzer wandte sich dennoch mit einer Beschwerde an die zuständige Datenschutzaufsichtsbehörde in Belgien (Gegevensbeschermingsautoriteit). Die Behörde verhängte gegen die Klägerin eine Geldbuße in Höhe von 20.000€ wegen eines Verstoßes gegen Art. 6 i.V.m. Art. 7 DSGVO sowie gegen Art. 5 Abs. 2 i.V.m. Art. 24 DSGVO. Zudem verpflichtete die Datenschutzaufsichtsbehörde die Klägerin zu weitergehenden Abhilfemaßnahmen. Die Klägerin erhob gegen den entsprechenden Bescheid Klage vor dem Hof van beroep te Brussel (Appellationshof Brüssel). Das Gericht legte dem EuGH einige Vorlagefragen zur Vorabentscheidung vor, unter anderem zur Auslegung von Art. 17 DSGVO und Art. 5 DSGVO.

## **Einwilligung als Rechtsgrundlage**

Der EuGH geht in seiner Entscheidung davon aus, dass die von einem Anbieter eingeholte Einwilligung auch die Weitergabe der hiervon umfassten personenbezogenen Daten an Drittanbieter rechtfertigen könne (Rn. 75 des Urteils). Wenn die entsprechende Datenübermittlung von den in der Einwilligung genannten Verarbeitungszwecke umfasst sei, müsse der Drittanbieter keine separate Einwilligung von der betroffenen Person einholen.

Diese Aussagen des EuGH sind zu begrüßen. Das Urteil ermöglicht es Verantwortlichen innerhalb von Verarbeitungsketten, ihre Datenverarbeitungen auf bereits durch andere Anbieter eingeholte Einwilligung zu stützen. Hierdurch wird zusätzlicher organisatorischer Aufwand vermieden. Allerdings wird dieser Vorteil durch die weitreichenden Folgerungen des EuGH zu allgemeinen Compliance-Pflichten von Verantwortlichen mehr als ausgeglichen.

## **Haftung für die Handlungen Dritter**

Der EuGH stellt in seinem Urteil weitreichende Compliance-Pflichten für datenschutzrechtlich Verantwortliche auf. Diese gehen über die in der DSGVO ausdrücklich geregelten Vorgaben deutlich hinaus. Nach Auffassung des EuGH soll die in Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO geregelte Rechenschaftspflicht eine Form von Haftungsverbund zwischen Verantwortlichen begründen. Dies gelte auch dann, wenn es an den Voraussetzungen für eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO fehlt. Nach Ansicht des EuGH seien Verantwortliche auf Basis dieser allgemeinen Compliance-Pflicht unter anderem dazu verpflichtet, die Einhaltung datenschutzrechtlicher Vorgaben auch durch Dritte durch entsprechende eigene Maßnahmen sicherzustellen.

Das Urteil führt damit die in weiten Teilen sehr weitgehende und verbraucherfreundliche Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit weiter, vgl. etwa die Rechtssachen Wirtschaftsakademie Schleswig-Holstein (Rs. C-210/16) und Zeugen Jehovas (Rs. C-25/17).

## **Informationspflichten bei widerrufenen Einwilligungen**

Der EuGH zeigt in seiner Entscheidung ein Beispiel für eine konkrete Ausprägung der von ihm propagierten erweiterten allgemeinen Compliance-Pflicht. Danach muss ein Verantwortlicher andere Verantwortliche, die ihm personenbezogene Daten zur Verfügung stellen oder von ihm erhalten, über den Widerruf einer Einwilligung durch die betroffene Person informieren.

Der EuGH geht mit dieser Vorgabe weit über den klaren Wortlaut von Art. 19 DSGVO hinaus. Nach dieser Vorschrift muss der Verantwortliche sämtliche Empfänger, denen er personenbezogene Daten offengelegt hat, unter anderem über die Löschung von personenbezogenen Daten nach Art. 17 DSGVO informieren. Der EuGH entfernt sich von diesem Wortlaut, indem er auch sonstige Verantwortliche dazu verpflichtet, umfassende technische und organisatorische Maßnahmen zu ergreifen. Unter anderem sollen Empfänger von Daten etwa auch Dritte, mit denen sie Daten austauschen, über einen nur an sie selbst gerichteten Widerruf einer Einwilligung informieren (Rn. 83 des Urteils). Nur eine entsprechende Informationspflicht könne die Wirksamkeit des in Art. 7 Abs. 3 DSGVO geregelten Rechts auf Widerruf einer erteilten Einwilligung sicherstellen. Den betroffenen Personen stehe damit ein Wahlrecht zu, an welchen Verantwortlichen sie innerhalb einer Verarbeitungskette den Widerruf ihrer Einwilligung richten.

## Relevanz für die Praxis

Das Urteil betrifft zunächst nur Unternehmen, welche die Verarbeitung personenbezogener Daten in erster Linie auf Einwilligungen der betroffenen Personen stützen. Hierzu zählen insbesondere Onlinehändler und Werbeagenturen. Aber auch andere Unternehmen sollten ihre Datenschutzstrukturen und vor allem ihr Einwilligungsmanagement überprüfen, um die vom EuGH aufgestellten Anforderungen zeitnah umzusetzen. Das vorliegende Urteil könnte sich auch auf die Anforderungen an Einwilligungen im Rahmen der geplanten ePrivacy-Verordnung und des Digital Markets Act (DMA) auswirken. Denn auch nach diesen EU-Regelwerken sind Einwilligungen für Marktteilnehmer von hoher praktischer Bedeutung.

Zudem könnten die Datenschutzaufsichtsbehörden die vom EuGH angenommenen erweiterten Compliance-Pflichten dazu nutzen, um für Verantwortliche über die Regelungen der DSGVO hinausgehende Anforderungen zu begründen. Insbesondere sind für Unternehmen weitreichende Haftungsrisiken bei Datenschutzverstößen möglich — selbst wenn diese durch Dritte begangen wurden.

## Fazit

Die Rechtsprechung des EuGH zu allgemeinen Compliance-Pflichten von datenschutzrechtlich Verantwortlichen zeigt eine bedenkliche Tendenz auf. Der EuGH entfernt sich weit von einer am Wortlaut orientierten Auslegung der DSGVO und schafft somit neue Herausforderungen. Verantwortliche müssen nun damit rechnen, dass Datenschutzbehörden auf der Basis dieser Entscheidung künftig Anforderungen aufstellen, die vom Wortlaut der DSGVO abweichen. Zur Vermeidung von Risiken sollten Unternehmen ihre bestehenden Prozesse umfassend überprüfen und gegebenenfalls anpassen. Das Urteil ist Ausdruck einer problematischen Rechtsfortbildung. Der EuGH könnte diesen Ansatz auch im Rahmen anderer Datenschutzgesetze, wie etwa der e-Privacy-Verordnung oder dem DMA fortführen.

---

Wenn Sie Fragen zu diesem Client Alert haben, wenden Sie sich bitte an einen der unten aufgeführten Verfasser oder an den Latham-Anwalt, mit dem Sie normalerweise Kontakt aufnehmen:

**Tim Wybitul**

tim.wybitul@lw.com  
+49.69.6062.6560  
Frankfurt

**Dr. Wolf-Tassilo Böhm**

wolf.boehm@lw.com  
+49.69.6062.6558  
Frankfurt

**Dr. Isabelle Brams**

isabelle.brams@lw.com  
+49.69.6062.6559  
Frankfurt

**Das könnte Sie auch interessieren**

[Neue Leitlinien zur Bußgeldberechnung für DSGVO-Verstöße: Welche Risiken drohen \(vor allem größeren\) Unternehmen in der Praxis?](#)

---

Der Client Alert wird von Latham & Watkins LLP für Mandanten und andere Geschäftspartner herausgegeben. Die hierin enthaltenen Informationen dienen nicht als konkreter Rechtsrat. Bei weitergehendem Bedarf an Ausführungen oder Beratung über ein hier dargestelltes Thema wenden Sie sich bitte an Ihren üblichen Ansprechpartner in unserem Hause. Eine Übersicht aller Client Alerts finden Sie unter <http://www.lw.com/>. Falls Sie eine Aktualisierung Ihrer Kontaktdaten oder eine Anpassung der Informationsmaterialien wünschen, besuchen Sie bitte die Seite <https://www.sites.lwcommunicate.com/5/2399/forms-english/subscribe.asp> für das weltweite Mandanten-Mailing-Programm von Latham & Watkins.