orka Newsletter | IT-, KI- & Datenrecht

Haftung bei Auftragsverarbeitung: BGH verschärft Pflichten von Verantwortlichen

Der Bundesgerichtshof (BGH) hat sich in einer aktuellen Entscheidung (*Urteil vom 11.11.2025 – VI ZR 396/24*) mit den **Pflichten von datenschutzrechtlich Verantwortlichen im Zusammenhang mit der Beendigung von Auftragsverarbeitungsverhältnissen** beschäftigt. Die Entscheidung hat erhebliche praktische Bedeutung für Unternehmen.

In seiner Entscheidung stellte der BGH klar, dass Verantwortliche ihre datenschutzrechtlichen Pflichten nicht bereits mit dem Abschluss eines Auftragsverarbeitungsvertrags erfüllen. Vielmehr tragen sie auch bei Beendigung der Zusammenarbeit eine **eigenständige Verantwortung** dafür, **dass personenbezogene Daten tatsächlich gelöscht oder zurückgegeben werden**. Unterbleibt dies und kommt es infolgedessen zu Datenmissbrauch, kann dem Verantwortlichen ein eigener DSGVO-Verstoß mit haftungsrechtlichen Konsequenzen anzulasten sein.

Die Entscheidung zeigt damit deutlich, dass das Auftragsende eine besonders haftungsträchtige Phase im Datenschutzmanagement darstellt.

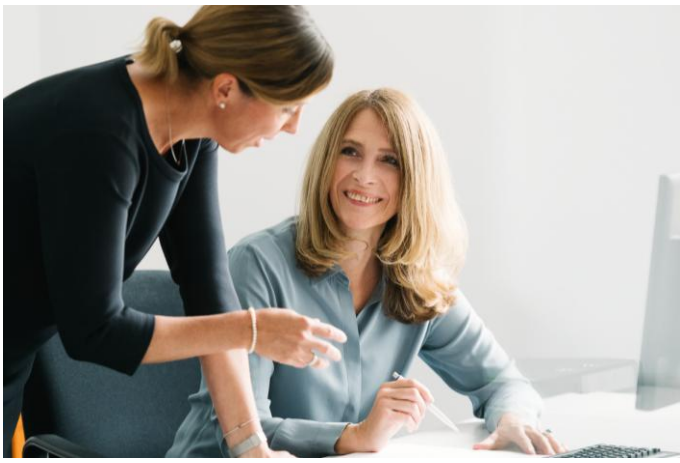
Der Sachverhalt

Der BGH befasste sich mit einer Klage einer betroffenen Person, deren personenbezogene Daten von der Beklagten, einem Online-Musikstreamingdienst mit Sitz in Frankreich, verarbeitet worden waren. Der Kläger war Nutzer dieses Online-Musikstreamingdienstes. Er nahm den beklagten Online-Musikstreamingdienst wegen **behaupteter Verstöße gegen die Datenschutz-Grundverordnung (DSGVO)** auf **immateriellen Schadenersatz** sowie auf Feststellung der Ersatzpflicht für künftige materielle Schäden in Anspruch.

Der beklagte Online-Musikstreamingdienst bediente sich eines externen Dienstleisters für die Verarbeitung personenbezogener Nutzerdaten. Der externe Dienstleister war als sogenannter Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO für den Online-Musikstreamingdienst tätig.

Im Jahr 2019 beendete der Online-Musikstreamingdienst als datenschutzrechtlich Verantwortlicher die Zusammenarbeit mit dem Auftragsverarbeiter. Einen Tag vor dem Ende der Zusammenarbeit teilte der Auftragsverarbeiter dem Online-Musikstreamingdienst mit, dass die Webseite des Online-Musikstreamingdienstes sowie die dort befindlichen Daten am Folgetag gelöscht würden. Eine **Bestätigung, dass die Löschung tatsächlich und vollständig erfolgt sei**, erhielt der beklagte Online-Musikstreamingdienst jedoch erst wesentlich später, nämlich im Februar 2023.

Zuvor war bekannt geworden, dass seit November 2022 **Datensätze von Nutzern** des Online-Musikstreamingdienstes **im Darknet zum Verkauf angeboten** wurden. Die betroffenen Daten stammten aus dem Jahr 2019 und waren von dem Auftragsverarbeiter nach der Beendigung der Zusammenarbeit nicht wie vereinbart gelöscht worden. Vielmehr waren die Nutzerdaten des Online-Musikstreamingdienstes von Mitarbeitern des Auftragsverarbeiters von der Produktiv- in eine Testumgebung überführt und anschließend entweder von Hackern erlangt oder unbefugt weitergegeben worden.



Die Nutzerdaten des Klägers gehörten zu den Datensätzen, die nach dem Vorfall im Darknet veröffentlicht und dort zum Verkauf angeboten wurden; betroffen waren unter anderem Vor- und Nachname, Geschlecht, E-Mail-Adresse, die verwendete Sprache sowie das Registrierungsdatum des Klägers.

Der Kläger war der Auffassung, er habe durch die Veröffentlichung seiner Daten im Darknet einen **immateriellen Schaden erlitten**, denn seit Kenntnis des Datenlecks befürchte er einen **Missbrauch seiner Daten**, insbesondere in Form von Identitätsdiebstahl, Phishing sowie unzulässiger Werbekontakte.

Das Landgericht Dresden hat die Klage abgewiesen (Urteil vom 18.06.2024 – 3 O 1284/23), ebenso das Oberlandesgericht

Dresden die Berufung des Klägers (Urt. v. 05.11.2024 – 4 U 999/24). Mit der vom Berufungsgericht zugelassenen Revision verfolgte der Kläger seine Ansprüche vor dem BGH weiter.

Das DSGVO-Haftungsregime

Nach der DSGVO ist ein Auftragsverarbeiter jede natürliche oder juristische Person oder sonstige Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Verantwortliche bleibt dabei „Herr der Verarbeitung" und trägt die primäre Verantwortung dafür, dass die Datenverarbeitung im Einklang mit den rechtlichen Vorgaben erfolgt.

Zu den **wesentlichen Pflichten im Rahmen einer Auftragsverarbeitung** gehört, dass die Verarbeitung personenbezogener Daten auf einer vertraglichen Grundlage erfolgt (sog. Auftragsverarbeitungsvertrag), die den Auftragsverarbeiter rechtlich bindet und klare Vorgaben für die Datenverarbeitung enthält.

Zu den zwingenden Vertragsinhalten eines Auftragsverarbeitungsvertrags zählt insbesondere, dass der Auftragsverarbeiter personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen verarbeitet und **nach Abschluss der Auftragsverarbeitung sämtliche personenbezogenen Daten löscht** oder, sofern es der Verantwortliche verlangt, zurückgibt und dem Verantwortlichen die Einhaltung dieser Pflichten nachweist.

Hinsichtlich der **Haftung für Datenschutzverstöße** gegenüber betroffenen Personen sieht die DSGVO eine weitreichende Verantwortlichkeit vor. Jede Person, der aufgrund eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, kann Schadensersatz grundsätzlich sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter verlangen.

Dabei trägt der Verantwortliche allerdings die primäre Haftung für Schäden, die durch eine nicht DSGVO-konforme Datenverarbeitung verursacht wurden. **Die Haftung des Auftragsverarbeiters gegenüber betroffenen Personen ist demgegenüber regelmäßig nachrangig** und greift nur dann ein, wenn er gegen speziell ihm auferlegte Pflichten verstoßen oder entgegen rechtmäßigen Weisungen des Verantwortlichen gehandelt hat.

Eine **Haftungsbefreiung** ist **für Verantwortliche und Auftragsverarbeiter** nur unter engen Voraussetzungen möglich. Sie setzt voraus, dass der jeweilige Beteiligte nachweist, in keinerlei Hinsicht für den Umstand verantwortlich zu sein, durch den der Schaden eingetreten ist. Damit macht die DSGVO deutlich, dass sich Verantwortliche im Außenverhältnis gegenüber betroffenen Personen regelmäßig nicht allein mit dem Hinweis auf ein Fehlverhalten des Auftragsverarbeiters entlasten können.

Pflichten bei Auftragsende

Der BGH entschied, dem Kläger sei ein **immaterieller Schaden** entstanden, weil seine personenbezogenen Daten nach Beendigung der Auftragsverarbeitung nicht nur unbefugt zugänglich waren, sondern anschließend **im Darknet veröffentlicht und dort zum Verkauf angeboten** wurden. Spätestens mit dieser missbräuchlichen Verwendung der Daten habe ein immaterieller Schaden vorgelegen.

Darüber hinaus könne ein immaterieller Schaden auch durch eine begründete Befürchtung eintreten, die im Darknet veröffentlichten Daten könnten missbräuchlich verwendet werden, insbesondere etwa durch die Versendung von Spam-Mails.

Im Ausgangspunkt bestätigte der BGH die rechtliche Würdigung des Berufungsgerichts, **der beklagte Online-Musikstreamingdienst sei für den Umstand haftbar, dass die Daten** des Klägers bei dem Auftragsverarbeiter **nach Beendigung des Auftragsverarbeitungsverhältnisses nicht gelöscht wurden** und dadurch die Möglichkeit bestand, dass sie – sei es durch einen Hacking-Angriff oder infolge unbefugter Weitergabe durch Mitarbeiter des Auftragsverarbeiters – abgegriffen und anschließend im Darknet zum Verkauf angeboten werden konnten.

Dabei ging der BGH nicht nur von einem Verstoß des Auftragsverarbeiters aus, für den der Verantwortliche gemäß Art. 82 Abs. 2 Satz 1 DSGVO einzustehen habe. **Vielmehr nahm der BGH zugleich einen eigenständigen Verstoß des Online-Musikstreamingdienstes als Verantwortlichem an.** Der Verstoß des Verantwortlichen liege darin, dass sich der Online-Musikstreamingdienst bei Beendigung der Zusammenarbeit mit dem Auftragsverarbeiter **mit der bloßen Ankündigung einer Datenlöschung begnügte** und keine Bestätigung einer tatsächlich erfolgten umfassenden Datenlöschung einforderte.

Zur Begründung führte der BGH aus, dass ein Verantwortlicher sich durch die Einschaltung eines Auftragsverarbeiters nicht von seinen datenschutzrechtlichen Pflichten befreien könne. Er bleibe „Herr der Verarbeitung“ und gegenüber betroffenen Personen für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich.

Soweit der Auftragsverarbeiter – etwa im Sinne eines Auftragsverarbeiterexzesses – selbst Zwecke und Mittel der Verarbeitung bestimmt, könne dies zwar zu einer eigenständigen Verantwortlichkeit des Auftragsverarbeiters führen; gleichwohl komme auch dann eine **Haftung des Verantwortlichen** in Betracht, wenn er es versäumt, mit den Mitteln des Vertragsrechts **auf ein vertragskonformes Verhalten des Auftragsverarbeiters hinzuwirken**.

Besonders hob der BGH die **Pflichten des Verantwortlichen im Zusammenhang mit der Beendigung des Auftragsverhältnisses** hervor. Es sei – vorbehaltlich etwaiger gesetzlicher Speicherpflichten – auch und gerade durch den Verantwortlichen sicherzustellen, dass beim Auftragsverarbeiter keinerlei personenbezogene Daten verbleiben, die diesem zur Auftragserfüllung überlassen wurden.

Der Verantwortliche dürfe sich dabei grundsätzlich nicht darauf beschränken, im Auftragsverarbeitungsvertrag eine Löschungs- bzw. Rückgabepflicht und einen Nachweis hierüber vorzusehen, so der BGH. Vielmehr müsse er bei Auftragsende das nach den Umständen des Einzelfalls **Erforderliche dazu beitragen, dass die vertragliche Verpflichtung tatsächlich erfüllt wird und die Daten nicht weiter gespeichert bleiben**, sodass dem Auftragsverarbeiter der Zugriff ab Auftragsende tatsächlich entzogen ist.

In diesem Zusammenhang stellte der BGH klar, dass das **Risiko eines unbefugten Zugriffs auf gespeicherte Daten** nicht erst bei einem Cyberangriff durch außenstehende Dritte entsteht, sondern bereits dann, wenn Daten nach Beendigung des Auftragsverhältnisses beim Auftragsverarbeiter gespeichert bleiben, obwohl dessen Zugriffsrecht erloschen ist. **Dieses Risiko habe der Verantwortliche durch geeignete Maßnahmen *„so weit wie möglich“* zu verhindern, so der BGH.** Der Verantwortliche könne sich seiner Verantwortung nicht dadurch entziehen, dass er sich auf einen „Auftragsverarbeiterexzess“ des Auftragsverarbeiters berufe, wenn er selbst seine Pflicht, auf eine vertragskonforme Datenlöschung bei Auftragsende hinzuwirken, verletzt hat.

Schließlich bestätigte der BGH, dass sich der beklagte Online-Musikstreamingdienst **nicht durch den Hinweis auf ein weisungs- oder vertragswidriges Verhalten des Auftragsverarbeiters** oder auf einen Hacking-Angriff durch unbefugte Dritte nach Art. 82 Abs. 3 DSGVO entlasten kann. Eine Entlastung des Verantwortlichen setze den Nachweis voraus, dass er in keinerlei Hinsicht für den schadensbegründenden Umstand verantwortlich ist.

Handlungsempfehlung

Die Entscheidung des BGH verdeutlicht, dass Unternehmen als datenschutzrechtlich Verantwortliche ihre Pflichten nicht bereits mit dem Abschluss eines Auftragsverarbeitungsvertrags erfüllen. Vielmehr bestehen diese Pflichten bis zur tatsächlichen und vollständigen Beendigung der Datenverarbeitung fort.

Unternehmen müssen daher **sicherstellen, dass nach Beendigung eines Auftragsverhältnisses keine personenbezogenen Daten mehr beim Auftragsverarbeiter verbleiben**, sofern nicht ausnahmsweise gesetzliche Aufbewahrungspflichten eingreifen.

Wie die Entscheidung des BGH deutlich macht, genügt es hierfür nicht, den Auftragsverarbeiter lediglich vertraglich zur Löschung oder Rückgabe der Daten zu verpflichten. Verantwortliche müssen vielmehr **aktiv darauf hinwirken**, dass die vertraglich geschuldete **Löschung oder Rückgabe tatsächlich und vollständig** erfolgt.

Vor diesem Hintergrund sollten Unternehmen bei der Beendigung einer Auftragsverarbeitung konkrete organisatorische Maßnahmen vorsehen, um den Vollzug der Löschung oder Rückgabe zu überprüfen. Dazu gehört insbesondere, eine **ausdrückliche und belastbare Bestätigung des Auftragsverarbeiters einzufordern**, aus der hervorgeht, dass sämtliche personenbezogenen Daten – einschließlich aller Kopien sowie etwaiger Datenbestände in Test- oder Sicherungsumgebungen – gelöscht oder zurückgegeben wurden. Bleibt eine solche Bestätigung aus, sollten Verantwortliche **zeitnah nachfassen und auf die Erfüllung der Löschungspflichten hinwirken**.

Besonders haftungsträchtig ist schließlich der Umstand, dass sich Verantwortliche im Schadensfall nicht mit dem bloßen Hinweis auf ein Fehlverhalten des Auftragsverarbeiters entlasten können, wenn ihnen selbst ein eigener Pflichtverstoß vorzuwerfen ist. Unternehmen sollten ihre internen Prozesse daher so ausgestalten, dass sie im Streitfall **darlegen und nachweisen können, alles Erforderliche unternommen zu haben**, um eine ordnungsgemäße Beendigung der Auftragsverarbeitung sowie die vollständige Löschung oder Rückgabe aller personenbezogenen Daten sicherzustellen. Eine sorgfältige und nachvollziehbare **Dokumentation der ergriffenen Maßnahmen** ist dabei unerlässlich.

Insgesamt zeigt die Entscheidung, dass die Beendigung von Auftragsverarbeitungen eine **kritische Phase des Datenschutzmanagements** darstellt. Unternehmen, die sich hierbei auf formale Regelungen oder bloße Ankündigungen des Auftragsverarbeiters verlassen, setzen sich einem relevanten Haftungsrisiko aus. Nur ein aktives, überprüfbares und dokumentiertes Vorgehen bei Auftragsende kann das Risiko datenschutzrechtlicher Haftung wirksam reduzieren.

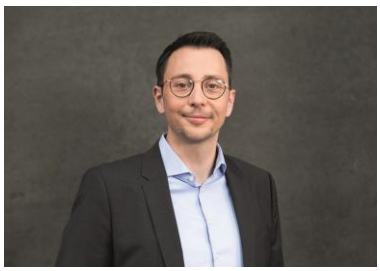
Ihre Ansprechpartner

Dr. Ulla Kelp, LL.M.
Rechtsanwältin, Partnerin

T +49 211 60035-176
ulla.kelp@orka.law

Dr. Philipp Mels
Rechtsanwalt, Partner

T +49 211 60035-180
philipp.mels@orka.law



Dr. Michael Grobe-Einsler
Rechtsanwalt, Salary Partner

T +49 211 60035-450
michael.grobe-einsler@orka.law

Felix Meurer
Rechtsanwalt, Salary Partner

T +49 30 509320-117
felix.meurer@orka.law

Prof. Dr. Michael Bohne
Of Counsel

T +49 211 60035-174
michael.bohne@orka.law


One Team.
One Goal.