BGH verschärft Datenschutz-Haftung bei Datenlecks

04.02.2026, 07:54 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *MTR Legal Rechtsanwälte Pressearchiv*

Datenschutz-Grundverordnung (DSGVO) – Grundlagen und Pflichten für Unternehmen

Ziel und Anwendungsbereich der DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist das zentrale Regelwerk der Europäischen Union zum Schutz personenbezogener Daten. Sie trat am 24. Mai 2016 in Kraft und ist seit dem 25. Mai 2018 verbindlich für alle Mitgliedstaaten der EU. Ziel der Verordnung ist es, ein einheitliches Datenschutzniveau zu schaffen und die Rechte der betroffenen Personen zu stärken. Die DSGVO regelt die Verarbeitung personenbezogener Daten durch Unternehmen, Organisationen und öffentliche Stellen – unabhängig davon, ob diese ihren Sitz innerhalb oder außerhalb der EU haben, solange sie Daten von EU-Bürgern verarbeiten.

Die Verordnung besteht aus 11 Kapiteln und 99 Artikeln, die sämtliche Aspekte des Datenschutzrechts abdecken. Zu den wichtigsten Grundlagen zählen die Definition personenbezogener Daten, die Grundsätze der Datenverarbeitung sowie die Rechte der betroffenen Personen. Personenbezogene Daten sind nach der DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen – dazu gehören etwa Name, Adresse, E-Mail-Adresse, Telefonnummer oder IP-Adresse.

Rechte der Betroffenen und Pflichten der Verantwortlichen

Unternehmen und Organisationen sind verpflichtet, die Verarbeitung personenbezogener Daten transparent zu gestalten und die Betroffenen umfassend über die Erhebung, Nutzung und Speicherung ihrer Daten zu informieren. Die DSGVO sieht vor, dass betroffene Personen ein Recht auf Auskunft, Berichtigung, Löschung und Widerspruch gegen die Verarbeitung ihrer Daten haben. Darüber hinaus müssen Unternehmen geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ergreifen und die Einhaltung der Vorschriften jederzeit nachweisen können. Verstöße gegen die DSGVO können erhebliche Sanktionen nach sich ziehen.

Kontrollpflichten enden nicht mit Ende des Auftragsverarbeitungsvertrags

Auftragsverarbeitungsverträge nach Art. 28 DSGVO

Streaming-Dienste arbeiten häufig auch mit externen Dienstleistern zusammen, die personenbezogene Daten der Nutzer verarbeiten. Dazu werden sog. Auftragsverarbeitungsverträge geschlossen. Datenschutzverstöße bei der Auftragsverarbeitung können zu Schadenersatzansprüchen der Nutzer gemäß Art. 82 DSGVO (Datenschutzgrundverordnung) führen. Die einzelnen Artikel der DSGVO bilden dabei die rechtlichen Rahmenbedingungen und enthalten umfassende Regelungen zur Auftragsverarbeitung. Das gilt auch, wenn das Vertragsverhältnis zwischen Unternehmen und Dienstleister bereits beendet wurde, wie ein Urteil des Bundesgerichtshofs vom 11. November 2025 (Az. VI ZR 396/24) zeigt.

Der BGH machte in seiner Entscheidung deutlich, dass der Streaming-Dienstleiter auch bei Beendigung der Auftragsverarbeitung den Schutz der Daten gewährleisten und dafür sorgen muss, dass keine personenbezogene Daten mehr beim Auftragsverarbeiter verbleiben. Zu den Aufgaben des Unternehmens gehört es, die Einhaltung der datenschutzrechtlichen Regelungen sicherzustellen, während die Aufsichtsbehörden die Kontrolle und Durchsetzung dieser Vorgaben übernehmen. Ist das nicht sichergestellt und es kommt z.B. zu einem Datenleck, kann das zu Schadenersatzansprüchen wegen Verstoßes gegen die DSGVO führen, so die Wirtschaftskanzlei MTR Legal Rechtsanwälte , die u.a. im Datenschutz berät.

BGH-Urteil vom 11.11.2025 – Datenleck trotz beendeter Auftragsverarbeitung

Sachverhalt: Streamingdienst und externer Auftragsverarbeiter

In dem zugrunde liegenden Fall vor dem BGH arbeitete ein Streamingdienst mit einem externen Auftragsverarbeiter zusammen. Der Auftragsverarbeitungsvertrag endete am 1. Dezember 2019. Am 30. November 2019 teilte der Auftragsverarbeiter mit, dass „die Website und alle Daten auf der Seite“ am nächsten Tag gelöscht würden. Der Streamingdienst verzichtete auf eine verbindliche Bestätigung, dass die Löschung der Daten wie angekündigt erfolgt ist.

Datenmissbrauch und Veröffentlichung im Darknet

Tatsächlich wurden die Daten nicht gelöscht, sondern nur von der Produktiv- in eine Testumgebung überführt. Dort wurden sie entweder gehackt oder unbefugt weitergegeben, so dass es im November 2022 zu einem Datenleck bei dem Auftragsverarbeiter kam. Die Hacker erbeuteten Daten aus dem Jahr 2019 von den Nutzern des Streamingdienstes und boten diese im Darknet zum Verkauf an. Zu den Daten, die die Kriminellen erbeuteten, gehörten u.a. Name, Geschlecht, E-Mail-Adresse, Sprache und Registrierungsdatum.

Die Auswirkungen dieses Datenlecks waren erheblich: Für die betroffenen Nutzer bestand ein erhöhtes Risiko von Identitätsdiebstahl und Missbrauch, während das Unternehmen mit möglichen Bußgeldern und Schadensersatzforderungen rechnen musste. Die Information der Betroffenen über das Datenleck erfolgte unter besonderer Beachtung der Transparenz, wie sie als Grundsatz im Datenschutz gefordert wird. Das Gericht betrachtete den Vorfall als Einzelfall, da besondere Umstände und individuelle Aspekte bei der Bewertung berücksichtigt wurden.

Klage auf immateriellen Schadenersatz nach Art. 82 DSGVO

Anspruchsvoraussetzungen für immateriellen Schadensersatz

Ein betroffener Nutzer klagte daher auf immateriellen Schadensersatz sowie Feststellung der Ersatzpflicht für künftige materielle Schäden. Er argumentierte, dass der Streamingdienst die nach der DSGVO gebotenen technischen und organisatorischen Sicherheitsmaßnahmen nicht ergriffen habe. Aufgrund des Datenlecks befürchte er den Missbrauch seiner Daten, z.B. in Form von Identitätsdiebstahl, Phishing-Versuchen oder Werbe-Mails.

Sowohl das Landgericht als auch Oberlandesgericht Dresden haben die Klage zurückgewiesen. Das OLG begründete dies

im Berufungsverfahren u.a. damit, dass die bloße Befürchtung eines Missbrauchs nicht für den Anspruch auf immateriellen Schadenersatz ausreiche.

Abweichende Bewertung durch den Bundesgerichtshof

Der BGH sah dies im Revisionsverfahren jedoch anders und hält einen Anspruch auf immateriellen Schadensersatz nach Art. 82 Abs. 1 DSGVO zumindest für möglich. In seiner entscheidungsfindung zur Auslegung von Art. 82 DSGVO betonte der BGH, dass die Anforderungen an den Nachweis eines Schadens nicht überspannt werden dürfen.

In seinem Leitsatz stellte der BGH klar, dass der Verantwortliche auch nach Beendigung einer Auftragsverarbeitung für den Schutz der Rechte der betroffenen Personen verantwortlich bleibt und sicherstellen muss, dass — wenn keine gesetzliche Speicherpflicht besteht — keine personenbezogenen Daten mehr beim Auftragsverarbeiter verbleiben, die ihm zwecks Auftragserfüllung überlassen wurden.

Löschung aller personenbezogenen Daten nach Datenschutz Grundverordnung

Wurden dennoch personenbezogene Daten nach Beendigung des Auftrags beim Auftragsverarbeiter belassen und gelangten dort ins Darknet und wurden zum Verkauf angeboten, begründet dies einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO – und zwar unabhängig davon, ob die Daten zuvor bereits rechtswidrig abgegriffen worden waren.

Verantwortlichkeit des Auftraggebers als „Herr der Verarbeitung“

Zur Begründung führte der BGH im Wesentlichen aus, dass der Verantwortliche, in diesem Fall der Streamingdienst, seine datenschutzrechtlichen Pflichten nicht dadurch abwälzen kann, dass er lediglich einen Vertrag mit einem Auftragsverarbeiter geschlossen hat. Der „Verantwortliche“ bleibe auch nach Vertragsende „Herr der Verarbeitung“. Sobald das Auftragsverhältnis endet, entfalle jegliche Rechtfertigung dafür, dass der Auftragsverarbeiter weiterhin Zugriff auf die personenbezogenen Daten hat. Die gesetzlichen Beschränkungen gemäß Abschnitt 5 und Artikel 23 DSGVO regeln dabei, unter welchen Voraussetzungen personenbezogene Daten gespeichert oder gelöscht werden dürfen.

Der Vertrag müsse vorsehen, dass der Auftragsverarbeiter nach Ende der Verarbeitung alle Daten entweder zurückgibt oder löscht, inkl. aller Kopien und Backups und dies auf Verlangen auch nachweist; die Modalitäten der Datenlöschung und deren Nachweis sind dabei klar zu definieren. Die Aufsichtsbehörden besitzen in diesem Zusammenhang weitreichende Befugnisse, um die Einhaltung der Datenschutzvorgaben und insbesondere die ordnungsgemäße Datenlöschung zu kontrollieren. Zudem besteht eine Informationspflicht des Verantwortlichen gegenüber den betroffenen Personen, sie gemäß Artikel 13 und 14 DSGVO über die erfolgte Datenlöschung und deren Umfang zu informieren. Der Verantwortliche müsse sicherstellen, dass der Auftragsverarbeiter seine vertraglichen Pflichten erfüllt und keine personenbezogenen Daten mehr bei ihm gespeichert bleiben.

Verletzung von Sicherungs- und Kontrollpflichten

Warum bloße Löschzusagen nicht ausreichen

Dieser Verpflichtung sei der beklagte Streamingdienst nicht nachgekommen. Stattdessen habe er sich mit der Ankündigung, dass alle Daten gelöscht werden, begnügt und keine schriftliche Bestätigung der Löschung gefordert. Damit habe er seine Sicherungs- und Kontrollpflichten nicht eingehalten. Im Zusammenhang mit Datenschutzverletzungen ist besonders auf die Rechte der betroffenen Personen hinzuweisen, wie das Auskunftsrecht, das Beschwerderecht, Schadensersatzansprüche sowie das Widerspruchsrecht gegen die Verarbeitung ihrer Daten. Unternehmer tragen hierbei eine besondere Verantwortung, die gesetzlichen Vorgaben der DSGVO einzuhalten und Betroffenenanfragen fristgerecht zu beantworten.

Verlust der Kontrolle über personenbezogene Daten als Schaden

Weiter führte der BGH aus, dass der Verlust der Kontrolle über personenbezogene Daten und deren Veröffentlichung im Darknet einen immateriellen Schaden darstellen kann. Die abstrakte Gefahr künftigen Missbrauchs, z.B. durch Phishing, Identitätsdiebstahl oder unerwünschte Werbung, könne dafür schon genügen. Eine sog. Bagatellgrenze lehnt der BGH ab.

DSGVO-Haftung auch nach Vertragsende

Fortbestehende Haftung trotz beendeter Auftragsverarbeitung

Nach dem Urteil des BGH müssen verantwortliche Unternehmen, die mit externen Dienstleistern zusammenarbeiten, beachten, dass ihre Pflichten nicht mit dem Abschluss eines standardisierten Auftragsverarbeitungsvertrages abgehakt sind. Vielmehr müssen sie auch nach Vertragsende sicherstellen, dass tatsächlich alle personenbezogenen Daten gelöscht oder zurückgegeben werden. Insbesondere müssen sie eine verlässliche Löschbestätigung einholen und dokumentieren. Denn gemäß DSGVO bleiben sie auch nach Auftragsende haftbar für Datenschutzverstöße, die aus unzureichender Löschung resultieren.

Der Datenschutz ist in verschiedenen Gesetzbüchern geregelt, wobei das deutsche Bundesdatenschutzgesetz eine zentrale Rolle spielt und auf eine lange Tradition zurückblickt. Die Entwicklung des deutschen Datenschutzrechts hat maßgeblich zur europäischen Harmonisierung beigetragen. Die Datenschutz-Grundverordnung (DSGVO) wurde in unterschiedlichen Fassungen veröffentlicht und ist im Amtsblatt der Europäischen Union einsehbar. Die Struktur der DSGVO gliedert sich in Kapitel, wobei Kapitel I die Grundsätze und Anwendungsbereiche festlegt. Die DSGVO hat die frühere Datenschutzrichtlinie 95/46/EG abgelöst, um einheitliche Standards zu schaffen. Ergänzend zur DSGVO existieren verschiedene Rechtsakte und Durchführungsrechtsakte, die die Umsetzung und Anwendung regeln. Bei der Umsetzung von Datenschutzmaßnahmen können zudem Kosten oder Gebührensätze (rates) für Unternehmen entstehen, etwa für Beratung oder technische Dienstleistungen.

Sanktionen und Bußgelder bei Datenschutzverstößen

Die Datenschutz-Grundverordnung (DSGVO) sieht bei Verstößen gegen ihre Vorschriften strenge Sanktionen und Bußgelder vor. Unternehmen, die die Vorgaben zur Verarbeitung personenbezogener Daten nicht einhalten, müssen mit empfindlichen finanziellen Konsequenzen rechnen. Die Höhe der Bußgelder kann bis zu 20 Millionen Euro oder bis zu 4 % des weltweit erzielten Jahresumsatzes eines Unternehmens betragen – je nachdem, welcher Betrag höher ist. Diese Regelung gilt für alle Unternehmen, unabhängig von ihrer Größe oder Rechtsform, und betrifft sowohl die Gesellschaft mit beschränkter Haftung (GmbH) als auch andere Kapitalgesellschaften und Organisationen.

Weitere Maßnahmen der Datenschutzaufsichtsbehörden

Neben Geldbußen können die Aufsichtsbehörden weitere Sanktionen verhängen, wie etwa die Einschränkung oder das Verbot der Verarbeitung personenbezogener Daten oder die Anordnung zur Löschung von Daten. Die DSGVO regelt zudem die Haftung für Schäden, die durch eine unrechtmäßige Verarbeitung personenbezogener Daten entstehen. Unternehmen haften für materielle und immaterielle Schäden, die betroffenen Personen durch Verstöße gegen die Datenschutzvorschriften entstehen. Betroffene können ihre Rechte auf Schadensersatz direkt gegenüber dem verantwortlichen Unternehmen geltend machen.

In Deutschland wird die Anwendung der DSGVO durch das Bundesdatenschutzgesetz (BDSG) konkretisiert. Das BDSG enthält zusätzliche Vorschriften für die Verarbeitung personenbezogener Daten und regelt die Zuständigkeit der deutschen Aufsichtsbehörden. Diese Behörden überwachen die Einhaltung der DSGVO und des BDSG, gehen Hinweisen auf Datenschutzverstöße nach und setzen die Sanktionen durch. Unternehmen sind daher gut beraten, die Vorgaben der DSGVO und des BDSG konsequent umzusetzen, um Bußgelder, Haftungsrisiken und Reputationsschäden zu vermeiden.

MTR Legal Rechtsanwälte berät umfassend zu Auftragsverarbeitungsverträgen und weiteren Themen des Datenschutzes.

Nehmen Sie gerne Kontakt zu uns auf!

MTR Legal Rechtsanwälte

Kurfürstendamm 11
10719 Berlin
Deutschland

MichaelRainer

+49 221 9999220

info@mtrlegal.com

www.mtrlegal.com

Portrait

MTR Legal Rechtsanwälte ist eine bundesweit und international tätige Full-Service-Wirtschaftskanzlei mit umfassender Expertise im Wirtschaftsrecht. Die Sozietät berät Unternehmen, institutionelle Investoren und vermögende Privatpersonen in den Bereichen Gesellschafts-, Steuer-, Handels-, Vertrags-, Vertriebs-, Kapitalmarkt- und Bankrecht. Proaktiv. Durchsetzungsstark. Erfolgreich. Diese Prinzipien prägen die Arbeitsweise der Kanzlei – vorausschauend, strategisch und wirtschaftlich fokussiert. MTR Legal arbeitet effizient, schnell, präsent und mit leading technology.

Mit Offices in Berlin, Düsseldorf, Frankfurt, Hamburg, Köln, Leipzig, München und Stuttgart sowie Representative Offices in London, Paris, Amsterdam und Singapore ist die Kanzlei international präsent. MTR Legal ist Mitglied im internationalen Netzwerk IR Global und wird regelmäßig von Handelsblatt und Best Lawyers empfohlen.

News-ID: 1298917 • Views: 405 (Stand: 30.05.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1298917/BGH-verschaerft-Datenschutz-Haftung-bei-Datenlecks.html