Rechtsprechung

ITRB0063498

>>>> Immaterieller Schaden durch Hackerangriff

Ein Cyberangriff führt für sich genommen nicht automatisch zum Beweis der Ungeeignetheit der getroffenen Schutzmaßnahmen. Der Verantwortliche trägt die Beweislast für die Geeignetheit der getroffenen Schutzmaßnahmen.

Für die Offenlegung personenbezogener Daten durch Cyberkriminelle trägt der Verantwortliche die Verantwortung, es sei denn, er kann nachweisen, in keinerlei Hinsicht für den Schaden verantwortlich zu sein.

Die bloße Befürchtung einer missbräuchlichen Nutzung personenbezogener Daten kann einen immateriellen Schaden begründen. Erfoderlich ist jedoch ein entsprechender Nachweis.

DSGVO Art. 4 Nr. 12, 5 Abs. 1, 2, Art. 24 Abs. 1, 2, Art. 32 Abs. 1, 2, Art. 82 Abs. 1, 2, 3
EuGH Urt. v. 14.12.2023 – C-340/21

Das Problem Die Daten einer natürlichen Person wurden bei einem Cyberangriff auf eine bulgarische Finanzbehörde (NAP) im Jahr 2019 Cyberkriminellen zugänglich. In der Folge des Angriffs kam es zu einer Veröffentlichung entwendeter Daten. Einige hundert Personen, darunter auch die Betroffene, erhoben Klage gegen die NAP auf Zahlung des Ersatzes eines immateriellen Schadens. Den Schaden begründete die Betroffene mit der Befürchtung einer möglichen künftigen missbräuchlichen Nutzung der veröffentlichten Daten.

Die Entscheidung des Gerichts Der EuGH hatte über **fünf Vorlagefragen** zu entscheiden, die insb. Beweisfragen im Zusammenhang der Geeignetheit getroffener Schutzmaßnahmen und der bloßen Befürchtung eines künftigen Datenmissbrauchs als Haftungsgrund eines immateriellen Schadensersatzanspruchs betrafen.

Kein Beweis der Ungeeignetheit von ergriffenen technischen und organisatorischen Maßnahmen (TOM): Ein Cyberangriff genüge für sich genommen nicht für die Annahme ungeeigneter Maßnahmen des Verantwortlichen zum Schutz vor Vernichtung, Verlust, Veränderung, oder unbefugter Offenlegung von bzw. unbefugtem Zugang zu personenbezogenen Daten i.S.d. Art. 24 Abs. 1 Satz 1, 32 DSGVO. Dem Verantwortlichen müsse die Möglichkeit bleiben, Beweis dafür zu erbringen, dass die von ihm getroffenen Schutzmaßnahmen i.S.v. Art. 32 DSGVO geeignet gewesen seien. Die Rechenschaftspflicht des Verantwortlichen aus Art. 5 Abs. 2 DSGVO laufe ansonsten ins Leere. Nach dem risikobasierten Ansatz habe der Verantwortliche zwar jede Verletzung des Schutzes personenbezogener Daten so weit wie möglich zu verhindern. Gleichwohl sei jedoch anzuerkennen, dass ein absoluter Schutz in der Praxis weder gewährt werden könne, noch durch den Verordnungsgeber als Voraussetzung formuliert worden sei.

Verarbeitungsrisiko: Die Geeignetheit der TOM beurteile sich stets konkret mit Blick auf den jeweiligen Verarbeitungsvorgang. Durch die Anknüpfung an die jeweilige Verarbeitungstätigkeit sei weder die Wirksamkeit der durch den Verantwortlichen zu treffenden Maßnahmen noch die Wirksamkeit der gerichtlichen Rechtsbehelfe gegen den Verantwortlichen eingeschränkt. Für die Geeignetheitsprüfung sei eine Zweischritt-Prüfung vorzunehmen: Zunächst seien die konkreten Risiken der jeweiligen Verarbeitungstätigkeit zu bestimmen. danach sei über die Angemessenheit der getroffenen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung (Art. 32 Abs. 1 DSGVO) zu befinden. Dieser einer vollen gerichtlichen Überprüfbarkeit unterliegende Prüfungsmaßstab korrespondiere mit der Systematik und dem durch Art. 35 Abs. 1 Satz 1 DSGVO vorgesehenen Ablauf einer Datenschutz-Folgenabschätzung.

Beweislastumkehr: Aus dem Wortlaut der Art. 5 Abs. 2, 24 Abs. 1, 32 Abs. 1 DSGVO gehe hervor, dass der Verantwortliche die Beweislast für die Gewährleistung eines

angemessenen Schutzniveaus durch die getroffenen TOM trage. Mangels gegenteiliger Anhaltspunkte in der DSGVO sei diese Beweislastumkehr auch auf Schadensersatzansprüche anwendbar (vgl. gegen eine Beweislastumkehr LG München I v. 9.12.2021 – 31 O 16606/20, RDV 2022, 107 m.w.N. = ITRB 2022, 227 [*Rössel*]). Der Verantwortliche solle mittels der ihm obliegenden Beweislast für die Geeignetheit dieser Maßnahmen dazu angehalten werden, alles zu unternehmen, um Verarbeitungsvorgänge zu verhindern, die nicht im Einklang mit der DSGVO stünden. Ohne Beweislastumkehr ergebe sich in der Praxis eine starke Einschränkung der Wirksamkeit des Schadensersatzanspruchs. Für die Beurteilung der Geeignetheit der TOM bilde ein gerichtliches Sachverständigengutachten kein generell notwendiges und ausreichendes Beweismittel.

Keine Haftungsbefreiung wegen Offenlegung durch Dritte: Der Verantwortliche sei nicht allein aufgrund einer unbefugten Offenlegung der Daten durch Dritte von der Haftung befreit. Auf Basis des Art. 82 Abs. 3 DSGVO könne sich der Verantwortliche nur dann von einer Haftung freizeichnen, wenn ihm der Nachweis gelinge, dass es keinen Kausalzusammenhang zwischen der etwaigen Verletzung der Verpflichtung zum Datenschutz durch ihn und dem der natürlichen Person entstandenen Schaden gebe.

Möglichkeit eines immateriellen Schadens: Ein immaterieller Schaden könne bereits aus der bloßen Befürchtung einer (zukünftigen) missbräuchlichen Nutzung der personenbezogenen Daten resultieren. Aus dem Wortlaut des Art. 82 Abs. 1 DSGVO sei zu schließen, dass für einen immateriellen Schaden nicht zwischen einer bereits erfolgten missbräuchlichen Nutzung und der Angst vor einer solchen zu unterscheiden sei. Dafür spreche auch die intendierte Gewährleistung eines hohen Schutzniveaus für natürliche Personen. Auch der bloße Kontrollverlust könne zu einem Schaden führen.

Beweislast: Die Beweislast für einen kausalen, immateriellen Schaden obliege dem Betroffenen. Das entscheidende Gericht des Mitgliedstaats müsse konkret feststellen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden könne.

Auswirkungen in der Praxis Haftung des Verantwortlichen: Der Verantwortliche muss im Fall einer Inanspruchnahme auf Schadensersatz nach einem Cyberangriff für die Geeignetheit der ergriffenen TOM Beweis erbringen. Der EuGH geht hinsichtlich die Erfüllung der Pflichten aus den Art. 24 Abs. 1 Satz 1, 32 DSGVO von einer Beweislastumkehr zu Lasten des Verantwortlichen aus, wenngleich der Verantwortliche keine absolute Sicherheit vor einer Datenschutzverletzung bieten kann. Daher lässt sich alleine aus einem Cyberangriff nicht ableiten, dass der Verantwortliche ungeeignete Schutzmaßnahmen getroffen hat. Ohne eine trennscharfe Abgrenzung zu einer möglichen eigenen Verantwortlichkeit der Cyberkriminellen i.S.d. Art. 4 Abs. 7 DSGVO vorzunehmen, wird durch den EuGH eine Haftung des (gehackten) Verantwortlichen für die Offenlegung von Daten durch Dritte bestätigt.

Anspruch auf Ersatz des immateriellen Schadens: Weiterhin ungeklärt sind die konkreten Darlegungs- und Beweisanforderungen zur Begründung eines immateriellen Schadens aufgrund der bloßen Befürchtung einer missbräuchlichen Nutzung personenbezogene Daten. Es obliegt somit weiterhin den nationalen Gerichten, sie zu definieren. Nötig bleibt dabei jedoch ein konkreter Vortrag zu den individuellen Auswirkungen auf die betroffene Person, so dass Massenklagen in der Praxis weiterhin nur eingeschränkt umsetzbar sind. Weiterhin fraglich erscheint es, ob eine einheitliche Schadensersatzpraxis der Gerichte zu erreichen sein wird.

Beraterhinweis Es obliegt in der Zukunft dem Verantwortlichen (oder dem Auftragsverarbeiter), die Geeignetheit der getroffenen Schutzmaßnahmen zu beweisen – angenommen wurde eine Beweislastumkehr lediglich hinsichtlich des Verschuldens (vgl. *Golland*/*Kriegesmann*, MMR 2023, 733, 736 m.w.N.). Dies verlangt jedem Verantwortlichen und Datenschutzbeauftragten eine strenge Prüfung (unter Berücksichtigung des konkreten Verarbeitungskontextes) und Dokumentation der TOM ab. Gleichzeitig wird die Bedeutung von IT-Sicherheitszertifizierungen (wie die ISO 27001) an Bedeutung gewinnen, da diese zu Beweiserleichterungen führen können.

Schutzmaßnahmen: Verantwortliche sollten bereits vor einem Cyberangriff in der Lage sein aufzuzeigen, welche Risiken für personenbezogene Daten sowohl zum Zeitpunkt der Festlegung der Schutzmaßnahmen als auch zum Zeitpunkt der eigentlichen Verarbeitung identifiziert wurden. Ferner muss der Verantwortliche darlegen können, dass die von ihm ergriffenen Schutzmaßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit dem festgestellten Risiko angemessen waren. Hierbei kann es für den Verantwortlichen im Zug der allgemeinen Prävention und Sorgfaltspflichterfüllung dienlich sein, einen **Cybersicherheits-Check** oder andere Maßnahmen durchzuführen und deren Ergebnisse dokumentiert. Ein zusätzliches Maß an Absicherung kann der Verantwortliche durch die **Auditierung** des eigenen Betriebs durch qualifizierte und unabhängige Dritte wie z.B. ein darauf spezialisierte Cybersicherheit-Beratungsunternehmen erreichen. Das Urteil des EuGH zeigt, dass erhebliche finanzielle Risiken dadurch gemindert werden können. Eine absolute Sicherheit gegen Cyberangriffe kann es jedoch nicht geben. Die Methoden der Angreifer sind heutzutage derart ausgefeilt, dass immer wieder Schwachstellen bestehen (vgl. CrowdStrikes jährlich erscheinenden Global Threat Report). Gleichwohl kann die Absicherung verbessert werden, indem auf den Einsatz **fortschrittlicher Technologien** nach dem Stand der Technik (vgl. dazu etwa die gleichnamige Handrei-

ITRB 2024, 34

chung des Bundesverband IT-Sicherheit e.V. [TeleTrust], der in der englischen Fassung in Kooperation mit der Agentur der Europäischen Union für Cybersicherheit [ENISA] herausgegeben wird) gesetzt wird, die sich beim Schutz gegen bekannte Angriffsmethoden bewährt haben (vgl. dazu etwa MITRE Engenuity ATT&CK Evaluations).

Abwehr von Ansprüchen: Bei der Verteidigung gegen Schadensersatzansprüche kann weiterhin die hinreichende Substantiierung der individuellen Auswirkungen auf den jeweiligen Betroffenen entgegengehalten werden. Zudem kann angeführt werden, dass durch die Beeinträchtigung die Schwelle der bloßen Unannehmlichkeit nicht überschritten wurde (vgl. LG Bielefeld v. 10.3.2023 – 19 O 147/22, GRUR-RS 2023, 3855 Rz. 46; OLG Dresden v. 14.12.2021 – 4 U 1278/21, ZD 2022, 235 Rz. 35.). Ein gewichtiges Argument für eine bloße Unannehmlichkeit dürfte dabei stets ein **geringes praktisches Missbrauchsrisiko** der erbeuteten Daten bilden.

RA Dr. Patrick Grosmann, M.A., zert. Datenschutzbeauftragter (TÜV), FPS PartGmbB, Frankfurt/M. / Dr. Christoph Bausewein, Assistant General Counsel, Data Protection & Policy, CrowdStrike, Frankfurt/M.