AKTUELLES ZU SCHADENSERSATZ-ANSPRÜCHEN NACH CYBER-ANGRIFFEN

DR. PATRICK GROSMANN, DR. CHRISTOPH BAUSEWEIN

Die drei Türme des EuGH (von links nach rechts): Rocca, Montesquieu und Comenius (Foto: Gerichtshof der Europäischen Union)

Beweisanforderungen an immateriellen Schaden im Sinne der DSGVO und die Geeignetheit von technischen und organisatorischen Maßnahmen (TOM)

Cyberangriffe treffen nicht nur eine Vielzahl von Behörden und Unternehmen, sondern beschäftigen auch die Gerichte – bis hin zum Europäischen Gerichtshof (EuGH). Neben dem enormen wirtschaftlichen Schaden, der oftmals aus Cyberangriffen resultiert, sehen sich Verantwortliche immer wieder Haftungsprozessen ausgesetzt. Die Haftungsprozesse können entweder behördliche Bußgelder wegen Datenschutzverstößen oder Schadensersatzprozesse von Betroffenen betreffen. Zur Geltendmachung von Schadensersatzansprüchen hat der EuGH im Dezember 2023 (EuGH, Urt. v. 14.12.2023 – C-340/21) wesentliche Klarstellungen getroffen, die im Folgenden beleuchtet werden sollen.

1. Kernaussagen des EuGH

Unter Anerkennung, dass es nach dem Willen des Unionsgesetzgebers keine absolute Cybersicherheit geben kann, geht der EuGH davon aus, dass es für Verantwortliche nach der DSGVO lediglich die Pflicht gibt Datenschutzverletzungen beziehungsweise Cyberangriffe einzudämmen (EuGH, Urt. v. 14.12.2023 – C-340/21, Rn. 38). Losgelöst davon ist der Verantwortliche schadenersatzpflichtig, wenn infolge eines Cyberangriffs personenbezogene Daten abhandengekommen sind und missbräuchlich genutzt werden. Es sei denn, der Verantwortliche kann nachweisen, dass die von ihm getroffenen TOM angemessen waren. Ein Cyberangriff führt dementsprechend nach der Rechtsprechung des EuGH nicht automatisch zu einem Beweis der Ungeeignetheit der TOM.

2. Sachverhalt

Die Entscheidung des EuGH betrifft einen Cyberangriff auf die bulgarische Finanzbehörde. In dessen Folge wurden durch diverse Betroffene Forderungen auf immateriellen Schadensersatz geltend gemacht. Begründet wurde der Schadensersatzanspruch mit der Befürchtung, dass entwendete Daten in Zukunft möglicherweise missbräuchlich genutzt, im Internet veröffentlicht oder als Druckmittel gegen die Betroffenen verwendet werden könnten.

3. Entscheidung des Gerichts

Kein Beweis ungeeigneter TOM durch einen Cyberangriff

Das Urteil des EuGH beginnt mit der Feststellung, dass alleine durch einen *(erfolgreichen)* Cyberangriff die Ungeeignetheit von TOM nicht bewiesen ist. Aus dem Umstand eines (erfolgreichen)

Cyberangriffs kann also nicht ohne Weiteres geschlossen werden, dass der Verantwortliche keine geeigneten TOM getroffen hatte (Art. 24 Abs. 1 S. 1, 32 DSGVO).

Unter anderem aus der in der DSGVO fest verankerten Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) folgert das Gericht, dass dem Verantwortlichen die Möglichkeit bleiben muss die Geeignetheit seiner TOM beweisen zu können. Zudem ergibt sich für das Gericht aus dem risikobasierten Ansatz[1] der DSGVO ein Argument dafür, dass der Verantwortliche nie einen absoluten Schutz gewährleisten kann – und dies daher dem Verantwortlichen bei einem Cyberangriff auch nicht entgegengehalten werden kann.

Geeignetheit von TOM, abhängig vom Risiko

Weiter bestätigt der EuGH in seinem Urteil, dass sich die Geeignetheit der TOM nach der jeweils konkreten Verarbeitungstätigkeit richtet. Je riskanter eine Verarbeitungstätigkeit und sensibler die verarbeiteten Daten, desto höher sind die Anforderungen an die jeweiligen TOM. Hauptaufgabe des Verantwortlichen ist: Die Risiken für die Betroffenen müssen so weit wie möglich reduziert werden – Stichwort *Risikovermeidung*.

Als konkrete Hilfestellung für Praktiker sieht der EuGH eine Prüfung der Geeignetheit der TOM in zwei Schritten vor:

1. Bestimmung der konkreten Risiken[2] der jeweiligen Verarbeitungstätigkeit für Betroffene.
2. Festlegung angemessener TOM *unter Berücksichtigung des Risikos, des Stands der Technik,[3] der (dem jeweiligen Verantwortlichen gemessen an seiner Grö ße und Leistungsfähigkeit zumutbaren[4]) Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung* (siehe Art. 32 Abs. 1 DSGVO).

Beweislastumkehr bei Schadenersatzforderungen

Der EuGH leitet aus dem Wortlaut des Art. 5 Abs. 2 DSGVO (Rechenschaftspflicht) des Art. 24 Abs. 1 DSGVO (Verantwortung für die Datenverarbeitung) und des Art. 32 Abs. 1 DSGVO (TOM) ab, dass der Verantwortliche die Beweislast für die Geeignetheit der TOM trägt. Bei der Geltendmachung eines immateriellen Schadensersatzes durch Betroffene führt dies zu einer Beweislastumkehr zulasten des Verantwortlichen: Wird ein Verantwortlicher auf (immateriellen) Schadensersatz in Anspruch genommen, muss dieser stets beweisen, dass die TOM geeignet, also für die konkrete Verarbeitung ausreichend waren.

Die Beweislastumkehr stützt der EuGH vor allem auf zwei Argumente: Die Wertungen der DSGVO legen nach Auffassung des Gerichts nahe, dass der Verantwortliche durch seine Schutzmaßnahmen das Risiko für die Betroffenen weitgehend reduzieren muss. Die Möglichkeiten der Betroffenen einen (immateriellen) Schadensersatz gegenüber einem Verantwortlichen geltend zu machen, sähe das Gericht unverhältnismäßig eingeschränkt, wenn Betroffenen beweisen müssten, dass die TOM des Verantwortlichen ungeeignet waren, was sie mangels Einblicks in die Verarbeitungsvorgänge und ein umfassendes technisches Wissen der Betroffenen regelmäßig nicht leisten können.

Haftung des Verantwortlichen auch für eine Offenlegung von Daten durch Dritte

Wenn es bei Cyberangriffen zu einer Offenlegung von Daten kommt (sog. Data-Leaks), erfolgt dies nicht durch den Verantwortlichen selbst, sondern durch Hacker, also durch Dritte. Nach der Auffassung des EuGH führt dieser Umstand (Offenlegung durch Dritte) jedoch nicht dazu, dass der Verantwortliche (durch den nicht unmittelbar das Leaken der Daten erfolgte) von dessen Haftung befreit wird. Es bleibt also dabei, dass dem Verantwortlichen die Datenschutzverletzung nur dann zugerechnet werden kann, wenn dieser die Verletzung, unter Missachtung einer Verpflichtung aus der DSGVO, ermöglicht hat.

Schaden durch Befürchtung einer missbräuchlichen Nutzung

Hinsichtlich der Anforderungen an einen immateriellen Schaden bleibt die Entscheidung vage: Der EuGH geht zwar davon aus, dass bereits aus der bloßen Befürchtung einer (zukünftigen) missbräuchlichen Nutzung der personenbezogenen Daten ein immaterieller Schaden resultieren kann. Welche konkreten Anforderungen an den Beweis eines solchen immateriellen Schadens seitens des Betroffenen zu stellen sind, lässt das Gericht jedoch offen. Ungeklärt bleibt somit, wie ein Betroffener einen immateriellen Schaden (etwa die Befürchtung einer missbräuchlichen Nutzung) konkret beweisen muss. Die Beweislast dafür liegt in jedem Fall beim Betroffenen.

Dass bereits die bloße Befürchtung einer missbräuchlichen Nutzung für einen immateriellen Schaden genügt, schließt der EuGH aus dem Wortlaut des Art. 82 Abs. 1 DSGVO. Eine Unterscheidung zwischen einer bereits erfolgten missbräuchlichen Nutzung und der bloßen Angst davor, erkennt das Gericht darin nicht.

[1] Dieser findet in der DSGVO an unterschiedlichen Stellen seinen Niederschlag. Neben den TOM, wird dieser auch im Zusammenhang der Aufgabenzuschreibung des Datenschutzbeauftragten (Art. 39 Abs. 2 DSGVO) und der Datenschutz-Folgenabschätzung (Art. 35 DSGVO) zugrunde gelegt.

[2] Dies meint ein Risiko iSd ErwG 75 der DSGVO.

[3] Hierbei handelt es sich um einen unbestimmten Rechtsbegriff, der nach den bewährten Methoden auszulegen ist. Hilfestellung kann hierbei etwa die Handreichung zum Stand der Technik des Bundesverband IT-Sicherheit e.V. (TeleTrust) geben, in der englischen Fassung in Kooperation mit der Agentur der Europäischen Union für Cybersicherheit (ENISA), https://www.teletrust.de/publikationen/broschueren/stand-der-technik/.

[4] Martini, in Paal/Pauly/ 3. Aufl. 2021, Art. 32 DSGVO, Rn. 60.

4. Konsequenzen des EuGH-Urteils für die Praxis

Der Auswahl und Implementierung angemessener TOM kommt mehr denn je eine große Bedeutung zu. Die TOM müssen sich stets individuell an den jeweiligen Verarbeitungstätigkeiten orientieren. Für die Praxis bedeutet dies Folgendes: Zur Reduzierung finanzieller Risiken im Zusammenhang mit Cyberangriffen durch individuelle Schadenersatzforderungen von Betroffenen müssen Verantwortliche sich in einem ersten Schritt ernsthaft und sorgfältig mit der Bestimmung der individuellen Risiken befassen. Daran orientiert müssen Verantwortliche im zweiten Schritt passende TOM ergreifen. Hierbei wird es von entscheidender Bedeutung sein, dass sich der Verantwortliche bewusst ist, welche personenbezogenen Daten wie verarbeitet werden. Verantwortliche, die umfassende Verarbeitungsverzeichnisse führen, sind hier klar im Vorteil.

Infolge des EuGH-Urteils kann es für Verantwortliche mehr denn je sinnvoll sein sich nach anerkannten Standards, mit denen gewisse TOM und korrespondierende Kontrollen einhergehen, durch unabhängige Dritte (etwa nach dem ISO-Standard 27001:2022) zertifizieren zu lassen. So lässt sich im Ernstfall einfacher beweisen, dass die TOM geeignet waren. Dasselbe gilt mit Blick auf die Durchführung und Dokumentation von in regelmäßigen Abständen stattfindenden Cyber-Sicherheit-Checks[5] oder Überprüfungen[6] des eigenen Betriebs durch einen qualifizierten und unabhängigen Dritten. Für Verantwortliche empfiehlt sich zudem stets eine sorgfältige Dokumentation des Prozesses – nicht nur zur Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

Ebenso wichtig sind regelmäßige Datenschutz-Audits durch den Datenschutzbeauftragten. Die Entscheidung des EuGH verdeutlicht dabei, wie wichtig ein starker technischer Fokus bei der Durchführung der Audits ist: Sofern der Datenschutzbeauftragte nicht selbst über das erforderliche technische Knowhow verfügt, sollte er sich fachkundige Unterstützung holen (etwa durch den IT-Sicherheitsbeauftragten).

Die konkrete Bestimmung geeigneter TOM fällt in der Praxis oftmals schwer: Neben Regelungen zur IT-Sicherheit (z.B. BSI Grundschutz) kann auch die Handreichung zum Stand der Technik des Bundesverband IT-Sicherheit e.V. (TeleTrust) Hilfestellungen bieten. Der Vorteil dieser Orientierungshilfe liegt darin, dass sie von einer Institution der Europäischen Union (EU), der Agentur der Europäischen Union für Cybersicherheit (ENISA), anerkannt ist und sogar in der englischen Fassung von dieser mitherausgegeben wird.

Ähnlich nützliche Hilfestellung vermag auch ein kürzlich von der schweizerischen Datenschutz-Aufsichtsbehörde, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), veröffentlichter Leitfaden zu TOM liefern.[7] Wenn auch außerhalb des Anwendungsbereichs der DSGVO, enthält dieser einige gute Anhaltspunkte, welche Schutzmaßnahmen gegenwärtig als angemessen angesehen werden können.

Konkrete Anforderungen an die TOM können sich in der Praxis auch aus branchenspezifischen Regelungen, etwa der IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung für kassenärztliche Arztpraxen ergeben.[8] Bei der Bestimmung der geeigneten TOM können solche bereichsspezifischen Regelungen nicht außer Acht gelassen werden. Mit Blick auf die möglichen Kosten einer Massenklage lässt sich infolge des EuGH-Urteils eine Investition in die TOM besser denn je rechtfertigen: In dem Ausgangsverfahren waren laut Medienberichten ca. 6 Mio. Personen von dem Cyberangriff betroffen. Die Klägerin des Ausgangverfahrens machte Schadensersatz in Höhe von ca. 510,- Euro gegen die Verantwortlichen geltend. Wenn nur ein Bruchteil der Betroffenen einen Schadensersatz in dieser Höhe geltend macht, führt dies zu einem enormen finanziellen Risiko.

5. Auswirkungen für die deutsche Rechtsprechung

Neben diesen für die Praxis äußerst relevanten Klärungen verbleiben auch nach der Entscheidung des EuGH Unklarheiten bezüglich der Anforderungen für die Geltendmachung eines immateriellen Schadensersatzanspruchs vor nationalen Gerichten. Insbesondere bleibt unklar, wie ein immaterieller Schaden aufgrund der bloßen Befürchtung einer missbräuchlichen Nutzung personenbezogener Daten zu begründen und schlussendlich zu beweisen ist. Dies muss durch die nationalen Gerichte noch definiert werden. Aktuell zeichnet sich im Lichte der in jüngerer Vergangenheit ergangener Gerichtsentscheidungen in Deutschland folgendes Bild: Erforderlich bleiben konkrete Angaben zu den individuellen Auswirkungen auf die jeweilige betroffene Person.[9]

[5] Dazu wurde vom ISACA Germany Chapter e. V. ein gleichnamiger Leitfaden zuletzt im Jahre 2020 veröffentlicht, der Anleitung zur Vorgehensweise gibt: https://www.isaca.de/images/Publikationen/Leitfaden/Leitfaden_Cyber-Sicherheits-Check_V2.pdf.

[6] Folgende Überprüfungen kommen dabei in Frage: Response Readiness Exercise, Soc Assessment, Cybersecurity Maturity Assessment, Cybersecurity Program Semi-Annual Review, Security Program In-Depth Assessment, Ransomware Defense Assessment, Cybersecurity Technical Tabletop Exercise, Executive Briefings, Compromise Assessment. Technical Risk Assessment, Cyber Threat Risk Evaluation, Cloud Security Assessment, Cloud Compromise Assessment, Identity Security Assessment.

[7] Siehe unter: https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/km2024/23012024_leitfaden_tom.html.

[8] Siehe dazu: https://www.kbv.de/html/it-sicherheit.php.

[9] Das OLG Stuttgart stellte in diesem Zusammenhang fest: „im Einzelfall ist es deshalb ausreichend, aber auch erforderlich, dass der Betroffene Umstände darlegt, in denen sich seine erlebten Empfindungen widerspiegeln, und dass nach der Lebenserfahrung der Datenschutzverstoß mit seinen Folgen Einfluss auf das subjektive Empfinden hat“, OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, in GRUR-RS 2023, 32883, Rn. 295.

"Massenklagen" sind daher in der Praxis zunächst nur eingeschränkt umsetzbar.

So hat unter anderem das OLG Hamm im Dezember 2023 entschieden, dass bei dem sog. Scraping[10] von Daten von einem Facebook-Account im Einzelfall zu beweisen ist, worin der immaterielle Schaden der betroffenen Person liegt (OLG Hamm, Beschl. v. 21.12.2023 – 7 U 137/23).

In einer anderen Entscheidung zu Saturn hat der EuGH im Januar 2024 entschieden, dass die bloße versehentliche Veröffentlichung personenbezogener Daten, ohne dass diese von einem Dritten zur Kenntnis genommen wurden, keinen immateriellen Schaden begründet (EuGH, Urt. v. 25.01.2024 – C-687/21).

FAZIT

Jeder Verantwortliche (und jeder Datenschutzbeauftragte) sollte sich regelmäßig und intensiv damit beschäftigen, ob die TOM geeignet sind und dem Stand der Technik entsprechen. Wurde der Verantwortliche erst einmal zum Opfer eines Cyberangriffs, ist es dafür bereits zu spät. Regelmäßige Datenschutz-Audits durch den Datenschutzbeauftragten und unabhängige Dritte können aufzeigen, an welchen Stellen die TOM lückenhaft sind. Gleichzeitig ist eine gute Dokumentation der TOM sinnvoll, da sich Verantwortliche damit gegen Schadensersatzforderungen von Betroffenen verteidigen können.

[10] Scraping ist das meist automatisierte Abgreifen fremder Inhalte im Internet.

Über die Autoren

Dr. Patrick Grosmann, M.A.
Rechtsanwalt der Kanzlei FPS PartG mbB in Frankfurt. Zert. Datenschutzbeauftragter (TÜV®) und Datenschutz-Auditor (DGI®), Promotion zu Interessenkonflikten der Datenschutzbeauftragten, Dozent für Datenschutzbeauftragte. Er berät im IT- & Datenschutzrecht.

Dr. Christoph Bausewein
CIPP/E | CIPT
BvD Vorstand, Assistant General Counsel, Data Protection & Policy bei der US-Cybersicherheitsfirma CrowdStrike, Mitglied des Expertenrats des Europäischen Datenschutzausschuss (EDSA) für neue Technologien.