KAZEMI & PARTNER  RECHTSANWÄLTE

# Analyse

## der Schlussanträge des Generalanwalt Giovanni Pitruzzella in der Rechtssache C-340/21

**zu den**

**Voraussetzung für die Durchsetzung von Schadenersatzansprüchen von Betroffenen nach einem Cyber-Angriff**

Welche Folgen haben die Schlussanträge des Generalanwaltes beim EuGH vom 27.04.2023 für Verantwortliche und wie reagiert ein Verantwortlicher nach einen Cybervorfall zur Abwendung von Schadenersatzansprüchen bestmöglich?


**Erstellt durch:**

Kazemi & Partner Rechtsanwälte PartG*
Dr. Robert Kazemi (Rechtsanwalt / Partner)
Kennedyallee 2
53175 Bonn
kanzlei [at] medi-ip.de

*PR 2019, AG Essen

Inhalt

# Abstract und Summary

## Führt ein Cyberangriff und der regelmäßig damit verbundene Abfluss personenbezogener Daten ins Darknet automatisch in eine Schadenersatzhaftung des angegriffenen Unternehmens nach Art. 82 DSGVO?

Der Generalanwalt beantwortet diese Frage mit einem Nein!

Jedoch kann die Tatsache, dass der Missbrauch personenbezogener Daten **möglich ist**, bereits ausreichen, um davon auszugehen, dass die betroffene Person einen durch den Verstoß gegen die Verordnung verursachten immateriellen Schaden erlitten haben kann. Es ist nicht erforderlich, dass der Missbrauch bereits eingetreten ist.

Die betroffene Person muss jedoch nachweisen, dass die Befürchtung eines solchen Missbrauchs ihr tatsächlich und konkret einen realen und sicheren emotionalen Schaden zugefügt hat.

Aus Sicht des Verantwortlichen ist es daher entscheidend, den Grad der Möglichkeit eines Missbrauchs möglichst konkret darzulegen und zu bewerten. Hier spielen Aspekte wie die Art der veröffentlichten Daten, ihre Auffindbarkeit im Einzelnen und ihre Struktur eine bedeutende Rolle.

## Muss ein Verantwortlicher einen Cyberangriff mit allen denkbaren technischen und organisatorischen Mitteln verhindern?

Auch der Generalanwalt geht davon aus, dass es keine 100%ige Sicherheit gegen Cyberangriffe geben kann. Es ist nicht anzunehmen, dass es die Absicht des Unionsgesetzgebers war, dem Verantwortlichen die Verpflichtung aufzuerlegen, jede Verletzung personenbezogener Daten zu verhindern, unabhängig von der Sorgfalt, die er bei der Ausarbeitung der Sicherheitsmaßnahmen anwenden muss.

Nicht alles was (theoretisch) möglich ist, muss auch gemacht werden. Vielmehr ist ein angemessener Ausgleich zwischen den Interessen der betroffenen Person, die generell ein

höheres Schutzniveau anstreben, und den wirtschaftlichen Interessen und technischen Möglichkeiten des Verantwortlichen, die zuweilen ein niedrigeres Schutzniveau anstreben, zu schaffen.

## Welche Darlegungslast trägt der Anspruchsteller im Rahmen der Geltendmachung eines Schadenersatzanspruches nach Art. 82 DSGVO?

Der Anspruchsteller muss seine **Aktivlegitimation**, also seine Betroffenheit von den Folgen eines Cyberangriffs, darlegen. Nicht jeder, der anlasslos vermutet, möglicherweise betroffen zu sein, ist für die Geltendmachung von Schadenersatzansprüchen aktiv legitimiert. Unter Beachtung der Grundsätze der sekundären Darlegungs- und Beweislast ist der Anspruchsteller verpflichtet, die Umstände, aus denen sich seine potentielle Betroffenheit ergeben kann, nachvollziehbar und substantiiert darzulegen. Der Verantwortliche kann dem nicht durch ein einfaches Bestreiten entgegentreten, um sich einer Haftung zu entziehen.

Der Anspruchsteller ist nicht verpflichtet, ein **Verschulden des Verantwortlichen** für den Eintritt des Cybervorfalls zu beweisen. Es spricht vielmehr eine widerlegliche Vermutung dafür, dass ein erfolgreicher Cyberangriff auf die unzureichende Umsetzung der Anforderungen in Art. 24, 32 DSGVO durch den Anspruchsgegner (= Verantwortlichen) zurückzuführen ist.

Der Anspruchsteller muss einen **immateriellen Schaden objektivieren**. Die Anforderungen an die nachweisbare Beeinträchtigung der physischen oder psychischen Sphäre oder des Beziehungslebens des Anspruchstellers sind indes gering.

## Welche Informationspflichten treffen den Verantwortlichen nach einem Cybervorfall?

Ein Cyberangriff führt regelmäßig in eine **Meldepflicht nach Art. 33 DSGVO**, nicht jedoch zwingend in eine Benachrichtigungspflicht nach Art. 34 DSGVO. Maßgeblich sind die konkrete Angriffsform und das konkrete Angriffsszenario. Angriffe auf die Vertraulichkeit können eine **Benachrichtigungspflicht nach Art. 34 DSGVO** auslösen. Angriffe auf die Integrität und/oder die Verfügbarkeit von Daten lösen jedenfalls dann eine Benachrichtigungspflicht nach Art. 34 DSGVO aus, wenn Integrität und Verfügbarkeit für

die betroffene Person besondere Bedeutung hat und eine schnelle Systemwiederherstellung, etwa wegen nicht vorhandener oder kompromittierter oder veralteter Backups, nicht möglich ist.

Die **Formulierung einer Art. 34 DSGVO-Benachrichtigung** kann erhebliche Auswirkungen auf den späteren Prozessverlauf eines Schadenersatzprozesses gegen den Verantwortlichen haben. Die präzise und inhaltlich korrekte Information ist daher maßgeblich. Zu breite, unspezifische oder vorsorgliche Benachrichtigungen sind zu vermeiden; dies gilt insbesondere im Rahmen der Information an die Öffentlichkeit nach Art. 34 Abs. 3 lit. c) DSGVO.

Der Verantwortliche schuldet regelmäßig **keine Auskunft nach Art. 15 DSGVO** hinsichtlich der Art der von einem Cyberangriff betroffenen Daten, der Person des Angreifers und/oder der Nutzungshandlungen, die dieser mit erbeuteten Daten vollzieht. Den Verantwortlichen kann jedoch eine sekundäre Darlegungslast dahingehend treffen, zu belegen, dass ein Anspruchsteller nicht aktiv legitimiert ist. Dies kann mit einer **Nachforschungspflicht** des Verantwortlichen in Bezug auf die vorstehenden Gesichtspunkte einhergehen. Die Nachforschung kann sich jedoch für den Verantwortlichen unter zahlreichen Aspekten als sinnvoll erweisen.

## Der Verantwortliche trägt die volle Darlegungs- und Beweislast für die Einhaltung der Vorgaben in Art. 32 DSGVO

Der Verantwortliche ist nur dann von der Haftung nach Art. 82 DSGVO nach einem Cyberangriff befreit, wenn er nachweist, dass er für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist, was nur dann der Fall ist, wenn er **angemessene und geeignete technische und organisatorische Maßnahmen zur Verhinderung des Cybervorfalls ergriffen hatte**. Kann der Verantwortliche diesen Nachweis nicht erbringen, soll ein mutmaßliches Verschulden in eine Haftung für die unrechtmäßige Verarbeitung personenbezogener Daten gemäß Art. 82 DSGVO führen.

Der Beweis kann über eine **behördliche Einstellungsmitteilung** nach einer Meldung nach Art. 33 DSGVO oder das Absehen von Maßnahmen nach Art. 83 DSGVO geführt werden. Liegt eine behördliche Einstellungsmitteilung oder eine sonstige „Unbedenklichkeitserklärung“ der zuständigen Aufsichtsbehörde vor, muss dies als Beweis für das Nichtverschulden des Verantwortlichen auch in Schadenersatzprozessen nach Art. 82 DSGVO ausreichen.

Weiterhin kann die **Einführung und nachgewiesene Einhaltung von Verhaltensregeln** den Beweis für ein Nichtverschulden des Verantwortlichen liefern. Gleiches gilt, wenn entsprechende **technische Zertifizierungen** vorliegen bzw. vorgelegen haben.

Insoweit spielt vor allem eine **lückenlose Dokumentation der TOM** des Verantwortlichen in Versionsständen eine bedeutende Rolle. Es ist dabei dringend anzuraten, diese Dokumentationen nicht nur auf den eigenen betrieblichen IT-Systemen, sondern jedenfalls (ausgelagert) an einem weiteren Ort verfügbar zu halten.

# A. Einleitung

**Führt ein Cyberangriff und der regelmäßig damit verbundene Abfluss personenbezogener Daten ins Darknet automatisch in eine Schadenersatzhaftung des angegriffenen Unternehmens nach Art. 82 DSGVO?**

Jedenfalls diese Frage beantwortet Generalanwalt Giovanni Pitruzzella in seinen am 27.04.2023 veröffentlichten Schlussanträgen zur Rechtssache C-340/21 mit einem klaren: Nein!

Ist das Opfer eines Cyberangriffs vielleicht sogar generell von jeder Schadenersatzhaftung nach Art. 82 DSGVO befreit?

Diese Frage beantwortet der Generalanwalt mit einem ebenso deutlichen: Nein!

Mag man sich als betroffenes Unternehmen über das erste NEIN noch freuen, sorgt das zweite NEIN sicherlich schon für einen Dämpfer; Ernüchterung muss jedoch aufkommen, wenn man auch die Antworten des Generalanwaltes auf die weiter gestellten Fragen des vorlegenden Gerichts betrachtet.

# B. DSGVO fordert keine absolute Sicherheit gegen Cyberangriffe

Erfreulich und für jedes durch einen Cyberangriff ohnehin bereits finanziell stark belastetes Unternehmen ist, dass auch der Generalanwalt davon ausgeht, dass es keine 100%ige Sicherheit gegen Cyberangriffe geben kann.

> *„Maßnahmen können zu einem bestimmten Zeitpunkt „geeignet“ sein und trotzdem von*

*Cyberkriminellen umgangen werden, die über sehr ausgeklügelte Instrumente verfügen, mit denen sie selbst modernste Sicherheitsmaßnahmen aushebeln können.“ (Rz. 33)*

Aktuelle Fälle, beispielsweise der diese Woche bekannt gewordene (zweite!) Cyberangriff auf den IT-Dienstleister der gesetzlichen Krankenkassen, BITMARCK, der mehr als 80 Krankenkassen und rund 25 Mio. Versicherte mit Produkten betreut, verdeutlicht dies.

*„Es erscheint unlogisch, anzunehmen, dass es die Absicht des Unionsgesetzgebers war, dem Verantwortlichen die Verpflichtung aufzuerlegen, jede Verletzung personenbezogener Daten zu verhindern, unabhängig von der Sorgfalt, die er bei der Ausarbeitung der Sicherheitsmaßnahmen anwenden muss.“.*

So formuliert es der Generalanwalt in seinen Schlussanträgen. Gleichwohl hebt er auch hervor, welche zentrale Bedeutung ein hohes (technischen) Datenschutzniveau in der DSGVO einnimmt. So erheben Art. 24 und 32 DSGVO die Etablierung technischer und organisatorischer Maßnahmen nach dem Stand der Technik ausdrücklich zu einer an den Verantwortlichen gerichteten Verpflichtung. Jeder Verantwortliche ist daher gehalten, für eine Sicherung der von ihm betriebenen Informationssysteme in technischer (Angemessenheit der Maßnahmen) und in qualitativer Hinsicht (Wirksamkeit des Schutzes) zu sorgen. Daher müsse, so der Generalanwalt, „*auf allen Stufen der Datenverarbeitung stets darauf geachtet werden, dass Sicherheitsrisiken minimiert werden*.“ (Rz. 26). Die hierfür eingesetzten Mittel sind auf der Grundlage einer sorgfältigen Bewertung der spezifischen Situation auszuwählen und zu dokumentieren (Art. 5 Abs. 2 DSGVO). Die DSGVO selbst macht hierzu keine konkreten Vorgaben, der

Generalanwalt hebt jedoch hervor, dass das technologische Niveau der durchzuführenden Maßnahmen auf das, was zum Zeitpunkt des Ergreifens der Maßnahmen vernünftigerweise möglich ist, beschränkt werden darf und die Eignung der Maßnahme zur Gefahrenabwehr in einem angemessenen Verhältnis zu den Lösungen stehen muss, die der aktuelle Stand von Wissenschaft, Technik, Technologie und Forschung bietet. Kurzum: Nicht alles, was (theoretisch) möglich ist, muss auch gemacht werden. Vielmehr ist ein angemessener Ausgleich zwischen den Interessen der betroffenen Person, die generell ein höheres Schutzniveau anstreben, und den wirtschaftlichen Interessen und technischen Möglichkeiten des Verantwortlichen, die zuweilen ein niedrigeres Schutzniveau anstreben, zu schaffen.

Ob dies der Fall ist und (vor einem Cyberangriff) der Fall war, ist - so der Generalanwalt - durch den Verantwortlichen zu beweisen und unterliegt im Streitfall der vollen gerichtlichen Überprüfung(spflicht), die sich nicht auf eine Prüfung technischer Dokumentationen beschränken darf, sondern insbesondere auch die tatsächliche Umsetzung umfassen muss. Diese Feststellungen des Generalanwaltes werden in der Praxis für viele Opfer von Cyberangriffen erhebliche Probleme bereiten. Denn, auch wenn der Generalanwalt den Eintritt eines Cybervorfalls für sich genommen nicht als Beleg eines (haftungsbegründenden) Datenschutzverstoßes werten will, misst er diesem Umstand doch Indizwirkung bei, die schlussendlich zu einer Beweislastumkehr zu Lasten des Verantwortlichen führt.

## C. Anforderungen an die Geltendmachung von Schadenersatz durch die betroffene Person

Der Weg zur Geltendmachung von Schadenersatzforderungen durch Kunden, Mitarbeiter, Lieferanten und sonstige natürlichen Personen, deren Daten bei einem Verantwortlichen im

Zusammenhang eines Cybervorfalls „erbeutet“ werden, ist damit grundsätzlich eröffnet. Mit Blick auf die jüngste Rechtsprechung des BGH (BGH, Urteil vom 28.10.2022 – M 576/22), in der dieser der Betreiberin einer Verbraucherplattform ("VINQO.DE"), die über eine Registrierung gemäß § 10 Abs. 1 Satz 1 Nr. 1 RDG für den Bereich der Inkassodienstleistungen verfügt, die Prüfung und außergerichtliche Geltendmachung und Durchsetzung von Ansprüchen auf Ersatz materiellen und immateriellen Schadenersatzansprüchen ausdrücklich gestattet hat, ist es nur eine Frage der Zeit, bis spezialisierte Rechtsdienstleister sich auch auf diese Ansprüche konzentrieren. Denn setzt sich der Generalanwalt mit seinen Ausführungen durch, reicht bereits die bloße Behauptung,, unzureichende Sicherheitsmaßnahmen hätten den Cyberangriff begünstigt, für eine in diesem Punkt substantiierte Anspruchsberühmung aus.

Die Rechtsprechung, bspw. des OLG Stuttgart (Urteil vom 31.03.2021 – 9 U 34/21), welches eine auf Art. 82 DSGVO begründete Schadenersatzklage noch mit dem Argument „*die Klägerin habe nicht nachgewiesen, dass ein etwaiger Verstoß gegen die gebotenen Sicherungsvorkehrungen für das Abgreifen der Daten durch unbekannte Dritte ursächlich geworden ist*“, hätte dann keinen Bestand mehr.

## I. Nachweis der Aktivlegitimation

Unbeantwortet, weil offenbar im Verfahren unstreitig, ist jedoch, welche Anforderungen an die Darlegung der eigenen Betroffenheit zu stellen sind, denn nur der von einem Datenschutzverstoß konkret Betroffene ist für die Geltendmachung von Schadenersatzansprüchen aktivlegitimiert. Die Aktivlegitimation nachzuweisen ist regelmäßig Aufgabe des Anspruchstellers; die bloße Behauptung ins Blaue hinein reicht hierfür nicht aus. Für den (potentiellen) Anspruchsteller stellt sich hier das Problem, dass er selbst nicht weiß, ob seine personenbezogenen Daten von einem Cybervorfall konkret betroffen sind.

## 1. Bedeutung der Benachrichtigung nach Art. 34 DSGVO

Fraglich ist, welche Bedeutung insoweit einer Betroffeneninformation nach Art. 34 DSGVO zukommt. Hiernach ist der Verantwortliche verpflichtet, die betroffene Person unverzüglich von einer Verletzung des Schutzes seiner personenbezogenen zu benachrichtigen, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person führt. Eine Benachrichtigungspflicht besteht also dem Grunde nach nur dort, wo die Betroffenheit konkret festgestellt wurde. Erhält ein einzelner Betroffener insoweit eine individuelle, an ihn gerichtete Information nach Art. 34 Abs. 2 DSGVO, so wird seine Betroffenheit anzunehmen sein, denn warum sonst wäre er konkret informiert worden. Für den Verantwortlichen heißt das aber auch, dass er mit der Übermittlung von individuellen Benachrichtigungen vorsichtig umgehen muss und alle Strategien, die dahin gehen, vorsorglich einfach mal alle bekannten Kontakte direkt zu informieren, wie man es allzu oft sieht, ein Problem darstellen kann. Wichtig ist auch, im Zusammenhang mit einer individuellen Benachrichtigung sehr genau zwischen den einzelnen „Schutzverletzungen“ konkret zu differenzieren und zu verstehen, dass aktuelle Cyberangriffe regelmäßig einer bestimmten Reihenfolge nach ablaufen. Ausführliche Informationen hierzu hat bspw. das BSI in seinem Leitfaden zur Reaktion auf IT- Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten (dort Abschnitt 3.8) beschrieben. So kommt es regelmäßig zu einer Verschlüsselung der befallenen IT-Systeme, die dort vorhandenen Daten sind dann einem Zugriff des Verantwortlichen entzogen. Zuvor neigen Angreifer jedoch neuerdings dazu, Backup-Pfade und soweit möglich auch die dort abgelegten Backups vollständig zu löschen, häufig werden zudem Daten unbemerkt und lange bevor sich der Hacker durch die Verschlüsselung und das Löschen zu erkennen gibt, exfiltriert, um sie entweder frei abrufbar oder gegen Entgelt, im Darknet zu veräußern. Insbesondere diese Darknet-Veröffentlichungen betreffen selten (schon mit Blick auf die Dauer, die ein versteckter

Download benötigt) alle auf den betroffenen IT-Systemen gespeicherten Daten, auch werden Datenpakete oft nur „häppchenweise“, ggf. sogar nur unvollständig im Darknet unstrukturiert veröffentlicht, bei Terabyte-großen Veröffentlichungspaketen, die sich nur schwer und sehr langsam sichten lassen, kann selbst eine frei zugängliche Veröffentlichung kaum auf einzelne Betroffene heruntergebrochen werden; jedenfalls nicht ohne versierte technische und juristische Unterstützung. Welche Daten abgeflossen sind, ist den Verantwortlichen daher regelmäßig unbekannt. Verhält sich eine Art. 34 DSGVO-Mitteilung, wie man sie in den letzten Wochen und Monaten vermehrt findet, schlicht dazu, dass ein Verantwortlicher Opfer einer Cyber-Attacke geworden ist und in diesem Zusammenhang Daten abhandengekommen und im Darknet veröffentlicht worden sind, ohne darauf hinzuweisen, dass man hieraus nicht auf die individuelle Betroffenheit schließen kann, eröffnet dies bereits eine Umkehr der Darlegungs- und Beweislast zum Nachteil des Verantwortlichen. Dies ganz ohne Not, denn wenn der Verantwortliche nicht weiß, wer konkret von einer Exfiltration betroffen ist, dann kann er weder den Einzelnen noch die Allgemeinheit aller natürlichen Personen, über die er Daten verarbeitet, darüber informieren, dass „ihre“ Daten im Darknet veröffentlicht worden sind. Die Information muss also korrekt lauten: „Es sind Daten exfiltriert worden. Hierunter können sich auch personenbezogene Daten von Kunden, Mitarbeitern oder Vertragspartnern befinden, dies ist aber aktuell weder positiv bekannt, noch für einzelne Betroffene ermittelt.“. Fällt eine Art. 34 DSGVO-Information im Zusammenhang mit dem Darknet so aus, kann sie jedenfalls nicht als Begründung einer Aktivlegitimation jeder Person, die behauptet, mit dem Verantwortlichen in geschäftlichen Beziehungen gestanden zu haben oder zu stehen, herangezogen werden. Warum ist es darüber hinaus wichtig zu unterscheiden? Auch die Verschlüsselung von Dateisystemen durch Hackerangriffe, kann für sich genommen unter dem Aspekt des „Verlustes der Verfügbarkeit“ personenbezogener Daten meldepflichtig sein. Sicher besteht regelmäßig eine Meldepflicht gegenüber den Datenschutzaufsichtsbehörden nach Art. 33

DSGVO, jedoch nicht zwingend auch gegenüber allen betroffenen Personen, von denen Daten auf den verschlüsselten Systemen gespeichert waren. Dies kommt nur dann in Betracht, wenn die Verschlüsselung (für einen dauerhaften oder wesentlichen) Zeitraum die Verfügbarkeit über die Daten (voraussichtlich) verhindert. Sind Backups nicht betroffen und tagesaktuell vorhanden, und können die Systeme hierüber schnell wiederhergestellt werden, dürfte - ist es nicht zu einer Exfiltration gekommen oder sind diese noch nicht bekannt - keine Meldepflicht nach Art. 34 DSGVO bestehen. Sind Backups ebenfalls betroffen, und die Daten damit dauerhaft nicht mehr verfügbar und wiederherstellbar, kann eine Meldung ggf. - je nach Qualität der hiervon betroffenen Daten - im Sinne des Art. 34 DSGVO erforderlich werden. Wichtig ist jedoch auch hier, die „Schutzverletzung“ so konkret wie möglich zu beschreiben, um nicht unnötig ein Einfallstor für die Darlegung der Aktivlegitimation zu Gunsten (potentiell betroffener) Personen zu schaffen. Dies gilt vor allem bei Mitteilungen nach Art. 34 Abs. 3 lit. c) DSGVO an die Öffentlichkeit. Diese sollten nicht allein der Kommunikationsabteilung überlassen, sondern in jedem Fall juristisch wie technisch kritisch geprüft und sorgsam formuliert werden. Auch hier zeigen sich in der Praxis immer wieder erhebliche, mit Blick auf die jüngsten Schlussanträge des Generalanwaltes bei EuGH u.U. äußerst haftungsträchtige, Nachlässigkeiten und Fehler.

## 2. Bedeutung des datenschutzrechtlichen Auskunftsanspruches (Art. 15 DSGVO) nach einem Cyberangriff

Ist die Art. 34 DSGVO-Information für sich genommen ungeeignet, die individuelle Betroffenheit zu begründen, so werden (potentiell) betroffene Personen ggf. versuchen, über einen Auskunftsanspruch nach Art. 15 DSGVO ihre eigene Betroffenheit in Erfahrung zu bringen. Für die Schutzrechtsverletzungen, die mit der Verschlüsselung einhergehen, mag dies ggf. noch zielführend

sein; eine Information zur Darknet-Veröffentlichung wird man hierüber indes nicht erhalten (können).

### *a. Alle Daten verschlüsselt - Kein Backup vorhanden*

Sind die IT-Systeme verschlüsselt worden und hält der Verantwortliche kein Backup vor bzw. ist dieses gelöscht oder ebenfalls verschlüsselt worden, wird sich die Frage stellen, ob er die Frage danach, ob der Auskunftsbegehrende überhaupt eine betroffene Person ist, nicht beantworten können. Die verschlüsselten Daten auf seinen Systemen sind für den Verantwortlichen nicht einsehbar, faktisch also anonym und damit nicht personenbezogen. Mangels Backup kann auch nicht nachvollzogen werden, ob die Person zu einem früheren Zeitpunkt auf den Systemen verarbeitet wurde und diese Dateien der Verschlüsselung zu Opfer gefallen sind. Der Verantwortliche kann insoweit lediglich und bezogen auf den Cyberangriff eine sog. Negativauskunft erteilen, denn er verarbeitet aktuell keine personenbezogenen Daten. Eine auf die Betroffenheit im Zusammenhang mit einem Cyber-Vorfall gerichtetes Auskunftsersuchen nach Art. 15 DSGVO ginge damit ins Leere.

### *b. Alle Daten verschlüsselt - Wiederherstellung möglich / erfolgt*

Ist die Wiederherstellung der verschlüsselten Systeme möglich, so wird der Verantwortliche die Wiederherstellung betreiben können und müssen, um festzustellen, ob die anfragende Person auch von der Verschlüsselung betroffen ist. Hier ist auf die Monatsfrist zu achten und wird regelmäßig die Verlängerungsoption zu ziehen sein. In den hier behandelten, weitreichenden Fällen, in denen die Wiederherstellung länger gedauert hat, ist dies regelmäßig auch behördlicherseits entschuldigt worden. Dies ist verständlich, weil ein Cyberangriff regelmäßig einen Gesamt-Shutdown aller, auch der nicht betroffenen Systeme zur Folge hat und die Wiederherstellung und Prüfung all dieser Systeme oft nicht innerhalb der verlängerten 2-Monats-Frist erledigt werden kann. Ein Auskunftsanspruch kann hier jedoch regelmäßig Sicherheit

über die Einzelbetroffenheit hinsichtlich der Schutzverletzung „Verfügbarkeit“ der personenbezogenen Daten für den Betroffenen mit sich bringen. Für den Verantwortlichen bedeutet das jedoch, dass er sich gerade nach einem Cybervorfall auf Auskunftsansprüche einrichten und Systeme etablieren muss, um diese – möglichst innerhalb der 2-Monats-Frist – bedienen zu können.

### *c. Abfluss von Daten erfolgt*

Was jedoch, wenn Daten nicht „nur“ verschlüsselt oder gelöscht wurden, sondern zusätzlich eine Exfiltration stattgefunden hat. Wie schon beschrieben, wird der Verantwortliche regelmäßig schon selbst nicht beurteilen können, welche Daten ein Angreifer exfiltriert hat, bevor er sich als solcher zu erkennen gibt. Auch wenn Daten im Anschluss – wie häufig – im Darknet veröffentlicht werden, bleibt eine erhebliche Unsicherheit, ob eine Veröffentlichung vollständig ist oder nicht. Die Datenveröffentlichungen im Darknet ziehen sich oft über Wochen hin; die meisten Verantwortlichen werden nicht einmal wissen, wie sie diese Veröffentlichungen im Darknet finden und aufrufen können; selbst der Verantwortliche, der diese Hürde noch nehmen kann, wird mit unstrukturierten Veröffentlichungen konfrontiert, die sich nicht einfach durchsuchen lassen und deren Herunterladen – ohne Fachkenntnisse – erhebliche Zeiten beansprucht. Ebenso besteht natürlich stets die Gefahr, dass auch die Darknet-Daten selbst kompromittiert sind. Muss der Verantwortliche insoweit gleichwohl über Art. 15 DSGVO Auskunft erteilen? Ich meine nicht. Insoweit könnte argumentiert werden, der Verantwortliche habe über den Empfänger personenbezogener Daten „Auskunft“ zu erteilen und die Angreifer seien ja auch irgendwie Empfänger. Schon dies greift jedoch zu kurz und verkennt die Legaldefinition in Art. 4 Nr. 9 DSGVO. Hiernach ist ein Empfänger „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht“. Das Offenlegen beschreibt nach meinem Verständnis indes eine

„aktive“ Handlung, kein unwissentliches und strafbares sich Verschaffen. Ob ein Angreifer insoweit ein „Empfänger“ ist, mag bezweifelt werden. Des Weiteren sind die konkreten Personen, die für einen Angriff verantwortlich sind, gar nicht auszumachen. Oft hinterlassen die Angreifer nur unspezifische E-Mail-Adressen, über die man Kontakt aufnehmen kann. Oft sind „Hackerkonglomerate“ am Werk, die sich schneller auflösen und neu formieren, als man denkt. Eine Anschrift oder sonstige Kontaktinformationen sind zudem regelmäßig unbekannt. Selbst wenn ein Hacker insoweit ein „Empfänger“ wäre, so könnte er als solcher kaum so spezifisch bezeichnet werden, wie es die DSGVO fordert. Schließlich hilft ein Auskunftsverlagen nach Art. 15 DSGVO hier auch deshalb nicht weiter, weil allenfalls über die Person des (vermeintlichen) Hackers informiert werden könnte, nicht jedoch über die genauen Daten, die er erhalten hat. Zudem wäre die „Verarbeitung“ durch den Hacker als seine eigene Verantwortlichkeit zu sehen, für die der Hacker, nicht jedoch das angegriffene Unternehmen auskunftspflichtig wäre. Was der Hacker nach Übermittlung im Darknet oder sonst wo mit den erbeuteten Daten macht, wie er sich also im datenschutzrechtlichen Sinne „verarbeitet“, steht nicht in der Verantwortung des angegriffenen Unternehmens, sondern in der des Angreifers. Eine Auskunft nach Art. 15 DSGVO läuft insoweit ins Leere.

### 3. Sekundäre Darlegungslast des Verantwortlichen

So schön es auf den ersten Blick klingt, grundsätzlich nicht mit Auskunftsansprüchen konfrontiert zu sein; es kann nicht das Ergebnis sein, dass Schadenersatzansprüche des Betroffenen an der Unmöglichkeit der Darlegung der eigenen Betroffenheit scheitern. Schließlich ist das Risiko für den ggf. eingetretenen Datenschutzverstoß beim Verantwortlichen gesetzt worden und daher in einer von ihm allein kontrollierten Sphäre entstanden.

Nach der deutschen Rechtsprechung kommt insoweit ausnahmsweise eine sekundäre Darlegungslast bei der Partei in

Betracht, die nicht die primäre Darlegungs- und Beweislast trägt. Dies ist nach ständiger Rechtsprechung des BGH dann der Fall, wenn die Partei, die primär die Darlegungslast trägt, dieser nachgekommen ist und ihr weiterer Vortrag nicht möglich und nicht zumutbar ist, da sie außerhalb des von ihr vorzutragenden Geschehensablaufes steht. Der Gegenseite hingegen muss der entsprechende Tatsachenvortrag unschwer möglich und zumutbar sein (BGH, NJW-RR 2019, 467, 468). Erfüllt aber die primär belastete Partei die Darlegungslast nicht, darf der Gegenseite keine sekundäre Darlegungslast auferlegt werden (BGH NJW 2015, 468, 469), da andernfalls die sekundäre Darlegungslast zu einer Ausforschung führen würde. Eine solche Ausforschung wäre unzulässig. Insoweit stellt sich die Frage, was der (potentiell) Betroffene tun muss, um seine eigene Betroffenheit hinreichend darzulegen und eine sekundäre Beweislast beim Verantwortlichen auszulösen? Grundsätzlich dürfte es nicht reichen, einfach zu behaupten, es könne ja irgendwie sein, dass auch die eigenen Daten betroffen seien. Es muss zumindest dargelegt werden, dass und in welchem Zusammenhang ein Anspruchsteller überhaupt von Verarbeitungen durch den Verantwortlichen betroffen sein kann. Bspw., weil es einen Vertrag gegeben hat, dessen Daten noch eine aktuelle Verarbeitung oder einer Dokumentations- oder Aufbewahrungspflicht unterfallen. Andere Einschränkungen sind möglich. Der Verantwortliche tut gut dran, diese durch entsprechende Maßnahmen, die am besten mit der zuständigen Aufsichtsbehörde abgestimmt werden, zu orchestrieren. Kann der Anspruchsteller die potentielle Betroffenheit glaubhaft machen, stellt sich die Frage, ob die sekundäre Beweislast greift. Insoweit fragt sich, ob es dem Verantwortlichen unschwer möglich und zumutbar ist, diese Behauptung zu verifizieren oder ob sich der Verantwortliche hier darauf zurückziehen kann, dass er selbst keine weiteren Informationen habe. Nicht ausgeschlossen werden kann, dass den Verantwortlichen hier eine Nachforschungspflicht trifft, was der BGH insbesondere in Filesharing-Fällen in der Vergangenheit schon angenommen hat. Hierfür spricht jedenfalls der Umstand, dass sich der Verantwortliche – ohne entsprechende

Nachforschungen – durch ein einfaches Bestreiten einer Haftung entziehen könnte. Die Anforderungen an die Reichweite einer Nachforschungspflicht haben sich, zieht man die Ausführungen des Generalanwaltes zur Frage der Beweislast für die Wirksamkeit der ergriffenen technischen und organisatorischen Maßnahmen (Rz. 45 ff.) entsprechend heran, daran zu orientieren, dass die DSGVO die Rechte der betroffenen Personen und die Pflichten der Verantwortlichen im Vergleich zur Richtlinie 95/46, die sie ersetzt, stärken wollte. Insoweit verbietet sich zwar für den Umfang der Nachforschungspflichten des Verantwortlichen eine verallgemeinernde Aussage, die Anforderungen an den Nachweis der Unzumutbarkeit dürften jedoch relativ hoch anzusetzen sein.

Unsere Erfahrung im Umgang mit der Beratung von Verantwortlichen im Zusammenhang mit Cyber-Angriffen zeigen, dass ein – hier zusammen mit versierten IT-Spezialisten – entwickeltes Verfahren, über welches die Betroffenheit im Einzelfall auf Nachfrage tatsächlich festgestellt werden kann, auch tatsächlich erhebliche Vorteile bietet; auch und vor allem im Umgang mit den Aufsichtsbehörden und mit Meldepflichten nach Art. 34 DSGVO. Ein solches Vorgehen vermeidet im Ergebnis auch eine Vielzahl von Klagen nach Art. 82 DSGVO bzw. erleichtert deren Verteidigung erheblich, weil auf diese Weise schon auf der Aktivlegitimationsebene vielen Ansprüchen entgegengetreten und auch sichere Aussagen zu den mit einem Vorfall für die betroffene Person verbundenen Risiken getroffen werden können, die wiederum, hierzu sogleich, auch erhebliche positive Auswirkungen auf die Reduzierung des Schadenersatzrisikos haben.

## II. Schadenskausalität – Beweislastumkehr zu Lasten des Verantwortlichen

Sieht sich der Verantwortliche einem Anspruch eines aktivlegitimierten, weil tatsächlich betroffenen, Anspruchstellers gegenüber, stellt sich die Frage, wie der Verantwortliche sich gleichwohl von einer erfolgreichen Inanspruchnahme auf

Schadenersatz exkulpieren kann. Eingangs ist bereits festgehalten worden, dass allein das Vorliegen eines Cyber-Angriffs für sich genommen, keinen Beweis für ein „Verschulden“ des Verantwortlichen mit Blick auf einen Verstoß gegen Art. 32 DGSVO indiziert. Mit Blick auf die zutreffende Feststellung des Generalanwaltes dahingehend, dass Cyberangriffe nicht zu 100% durch technische oder organisatorische Maßnahmen ausgeschlossen werden können und die DSGVO einen solchen 100%igen Schutz von Daten vom Verantwortlichen auch nicht einfordert, stellt sich die Frage, wann von einem gleichwohl haftungsbegründenden Verschulden des Verantwortlichen ausgegangen werden muss.

Auch hierzu verhält sich der Schlussantrag des Generalanwaltes und trifft auch hier für den Verantwortlichen „ungünstige“ Feststellungen.

### 1. Nachweis der Etablierung geeigneter TOM zur Verhinderung des Cyberangriffs

So hebt der Generalanwalt hervor, dass der Verantwortliche nur dann von der Haftung befreit werden kann, wenn er **nachweist**, dass er für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist, was nur dann der Fall sein könne, wenn er angemessene und geeignete technische und organisatorische Maßnahmen zu der Verhinderung des Cybervorfalls ergriffen hatte. Kann der Verantwortliche diesen Nachweis nicht erbringen, soll ein mutmaßliches Verschulden in eine Haftung für die unrechtmäßige Verarbeitung personenbezogener Daten gemäß Art. 82 DSGVO führen (Rz. 62). Daraus folgert der Generalanwalt, dass der Verantwortliche nachweisen muss, dass er alles Mögliche getan hat, um die Verfügbarkeit und den Zugang zu den Daten rasch wiederherzustellen und den unberechtigten Zugriff zu vermeiden, um einer Haftung dem Grunde nach zu entgehen.

Da, so der Generalanwalt, allgemein bekannt sei, dass externe Angriffe auf die Systeme öffentlicher oder privater Einrichtungen,

die über eine große Menge personenbezogener Daten verfügen, weitaus häufiger sind als interne Angriffe, **müsse der Verantwortliche insbesondere geeignete Maßnahmen ergreifen, um Angriffen von außen begegnen zu können**.

*a. Zwingende Maßnahmen*

Zu diesen **technischen und organisatorischen Maßnahmen** zählen, auch wenn der Generalanwalt sie nicht explizit erwähnt, jedenfalls

- ein professioneller Virenschutz
- ein vollständiges Patch- und Updatemanagement auf allen Systemen
- eine Spam- und Virenfilterung auf Netzwerkebene über Firewalls
- ein ordnungsgemäßes und wirksames Backup- und Recovery-Konzept
- die regelmäßige Sensibilisierung und Schulung personeller Ressourcen
- Überprüfung von Soft- und Hardware auf Aktualität (veraltete Soft- und Hardware kann u.U. nicht mehr dem Stand der Technik entsprechen und eine Schwachstelle für Angriffe darstellen)
- Ordnungsgemäße und restriktive Konfiguration der beim Verantwortlichen eingesetzten Software-Produkte, insbesondere in Bezug auf die Aktivierung von Sicherheitsfunktionen und die Vergabe von Zugriffsrechten und Rollen.
- Weitere Maßnahmen werden bspw. durch das BSI im Maßnahmenkatalog Ransomware (abrufbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.pdf?__blob=publicationFile&v=2) beschrieben.

### *b. Beweismittel*

Wie aber kann der Nachweis geführt werden, dass die ergriffenen Maßnahmen dem Stand der Technik entsprochen und den Cyberangriff nicht begünstigt haben? Hierfür ist der Verantwortliche mit Blick auf die ihm zugeschriebene Beweislast zunächst verpflichtet, die konkrete Angriffsform und das Angriffsszenario zu ermitteln, welches (vermutlich) zu dem Datenschutzvorfall geführt hat, denn nur wenn dargelegt werden kann, wie sich ein Angriff vollzogen hat, können die relevanten technischen und organisatorischen Maßnahmen ermittelt werden, die für die Betrachtung eines Verschuldensvorwurfs im Rahmen der Inanspruchnahme aus Art. 82 DSGVO überhaupt relevant sind. Die so ermittelten technischen und organisatorischen Maßnahmen sind dann darauf hin zu überprüfen, ob sie dem Stand der Technik und den sonst in Art. 32 DSGVO beschriebenen Voraussetzungen entsprechen bzw. entsprochen haben und grundsätzlich geeignet waren den Cyberangriff zu verhindern.

#### aa. Sachverständigenbeweis

Dieser Beweis kann auf unterschiedliche Arten geführt werden. Nicht immer ist hierfür, dies hebt der Generalanwalt hervor, ein umfangreiches Sachverständigengutachten erforderlich oder auch ausreichend (Rz. 56 und 57).

#### bb. Behördliche Einstellungsmitteilung der Datenschutzaufsichtsbehörde

Ein wichtiges Verteidigungs- und Beweismittel kann insoweit aber bspw. eine behördliche Einstellungsmitteilung nach einer Meldung nach Art. 33 DSGVO oder entsprechenden Ermittlungen nach Art. 83 DSGVO sein. Denn hat die (unabhängige) Datenschutzaufsicht ihrerseits die Ursachen und auch den Verschuldensbeitrag des Verantwortlichen geprüft und ist zu dem Ergebnis gelangt, dass keine weiteren Maßnahmen erforderlich sind, ist ein Verschulden des Verantwortlichen nicht gegeben.

Insoweit muss nämlich beachtet werden, dass der EUGH die Verpflichtung der Aufsichtsbehörde hervorgehoben hat, jede Beschwerde mit aller gebotenen Sorgfalt zu bearbeiten, um die Einhaltung der Bestimmungen der DSGVO sicherzustellen (EuGH, Urteil vom 16. Juli 2020, Facebook Ireland und Schrems C-311/18, EU:C:2020:559, Rn. 109). In den aktuellen Schlussanträgen des Generalanwaltes Pikamäe vom 16.03.2023 in den verbundenen Rechtssachen C-26/22 und C-64/22 hebt dieser zudem hervor (Rz. 38 f.):

> *„Ferner ist festzustellen, dass im 141. Erwägungsgrund der DSGVO klargestellt wird, dass „[d]ie auf eine Beschwerde folgende Untersuchung … so weit gehen [sollte], wie dies im Einzelfall angemessen ist“ (Hervorhebung nur hier). All dies führt mich zu der Annahme, dass die Aufsichtsbehörde* ***zwingend verpflichtet ist****, Beschwerden einer betroffenen Person mit der im Einzelfall gebotenen Sorgfalt zu bearbeiten. Da jeder Verstoß gegen die DSGVO grundsätzlich eine Beeinträchtigung der Grundrechte darstellen kann, halte ich es für unvereinbar mit dem durch diese Verordnung geschaffenen System, der Aufsichtsbehörde ein Ermessen bei der Entscheidung einzuräumen, ob sie sich mit Beschwerden befasst oder nicht. Ein solcher Ansatz würde die ihr durch die DSGVO übertragene entscheidende Rolle in Frage stellen, die darin besteht, für die Einhaltung der Vorschriften über den Schutz personenbezogener Daten zu sorgen, und liefe folglich den vom Unionsgesetzgeber verfolgten Zielen zuwider. Letztlich darf nicht vergessen werden, dass die Beschwerden eine wertvolle Informationsquelle für die Aufsichtsbehörde darstellen, die es ihr ermöglicht, Verstöße aufzudecken.“.*

Liegt also eine behördliche Einstellungsmitteilung oder eine sonstige „Unbedenklichkeitserklärung“ der zuständigen Aufsichtsbehörde vor, kann und muss dies als Beweis für das Nichtverschulden des Verantwortlichen auch in Schadenersatzprozessen nach Art. 82 DSGVO ausreichen. Ähnliches dürfte auch für Stellungnahmen der oft eingeschalteten polizeilichen Stellen (LKA, BKA) gelten, die jedoch nur äußerst selten vorliegen dürften. Die Kommunikation mit der Aufsichtsbehörde stellt sich damit, nicht nur zur Abwendung möglicher Bußgelder nach Art. 83 DSGVO, sondern auch im Zusammenhang mit Schadenersatzprozessen, als besonders wichtig dar.

### cc. Verhaltensregeln und Zertifizierungen

Weiterhin kann – so der Generalanwalt – „*die Einführung von Verhaltensregeln oder Zertifizierungssystemen ein nützliches Element der Bewertung zum Zweck der Erfüllung der Beweispflicht und der damit verbundenen gerichtlichen Überprüfung darstellen*.“ (Rz. 42), wobei der Generalanwalt ausdrücklich hervorhebt, dass „*es nicht ausreicht, dass der Verantwortliche Verhaltensregeln eingehalten hat, sondern dass er gemäß dem Grundsatz der Rechenschaftspflicht nachweisen muss, dass er die darin vorgesehenen Maßnahmen tatsächlich ergriffen hat. Die Zertifizierung hingegen stellt „als solche den Beweis für die Übereinstimmung der durchgeführten Verarbeitungen mit der Verordnung dar, auch wenn sie in der Praxis widerlegt werden kann*“ (Rz. 42). Es ist daher jedem Verantwortlichen dringend anzuraten, entsprechende Zertifizierungen in Betracht zu ziehen; jedenfalls aber vorhandene Verhaltensregeln seiner Unternehmensbranche unbedingt zu beachten. Beispiele hierfür wären für den ärztlichen und zahnärztlichen Bereich bspw. die IT-Sicherheitsrichtlinie für Arzt- und Zahnarztpraxen oder für Notare die vom Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) nach Art. 40 DSGVO genehmigten datenschutzrechtlichen Verhaltensregeln zu technischen und organisatorischen

Maßnahmen der Notarinnen und Notare im Hinblick auf elektronische Aufzeichnungen und Hilfsmittel (abrufbar: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Verhaltensregeln/VerhaltensregelnNotarinnen-Notare.pdf?__blob=publicationFile&v=6).

### dd. Bedeutung von Nachweisdokumenten

Schließlich – so der Generalanwalt (Rz. 43) „*ist darauf hinzuweisen, dass diese Maßnahmen gemäß Art. 24 Abs. 1 erforderlichenfalls überprüft und aktualisiert werden müssen. Auch dies wird Gegenstand der vom nationalen Gericht anzustellenden Prüfung sein. Art. 32 Abs. 1 der Verordnung verpflichtet den Verantwortlichen nämlich zu einer ständigen Kontrolle und Überwachung vor und nach der Verarbeitung und zur Erhaltung und eventuellen Aktualisierung der getroffenen Maßnahmen, um Verstöße zu verhindern und gegebenenfalls ihre Auswirkungen zu begrenzen*.“.

Insoweit spielt vor allem eine lückenlose Dokumentation der TOM des Verantwortlichen in Versionsständen eine bedeutende Rolle. Es ist dabei dringend anzuraten, diese Dokumentationen nicht nur auf den eigenen betrieblichen IT-Systemen, sondern jedenfalls (ausgelagert) an einem weiteren Ort verfügbar zu halten, damit – insbesondere bei einem Verschlüsselungs- und/oder Löschungsangriff – nicht auch die für die Nachweiszwecke so bedeutende Dokumentation „verloren“ geht. Ob man hier auf digitale Auslagerungen in anderen Umgebungen oder den klassischen regelmäßigen Ausdruck auf Papier setzt, spielt keine Rolle.

## III. Anforderungen an die Darlegung eines immateriellen Schadens

Führt ein Verstoß gegen Art. 32 DSGVO durch einen Verantwortlichen, der einen unbefugten Zugang zu personenbezogenen Daten und/oder eine unbefugte Offenlegung dieser Daten durch Cyberkriminelle begünstigt oder ermöglicht hat, und die damit verbundene Befürchtung eines möglichen künftigen Missbrauchs der personenbezogenen Daten zwingend zur einem (immateriellen) Schaden, der die betroffene Person zum Schadenersatz berechtigt?

### 1. Anschluss an die Schlussanträge in der Rechtssache C-300/21

In Übereinstimmung mit den Schlussanträgen in der Rechtssache C-300/21 (UI gegen Österreichische Post AG, abrufbar: https://curia.europa.eu/juris/document/document.jsf;jsessionid=B4D457AC534EB26252ADE1D01EB7CF5E?text=&docid=266842&pageIndex=0&doclang=de&mode=req&dir=&occ=first&part=1&cid=7848782, hierzu auch *Kazemi*, https://de.linkedin.com/pulse/generalanwalt-kein-ersatz-immaterieller-sch%C3%A4den-bei-ohne-kazemi?trk=public_post) verneint auch Generalanwalt Giovanni Pitruzzella einen solchen Automatismus (Rz. 71 ff.).

> *„Dem Verstoß gegen die Verordnung folgt nicht automatisch der Schaden, der durch den Verstoß „verursacht" wird" (Rz. 71).*

Vielmehr – so der Generalanwalt – müsse der Betroffene auch im Rahmen der Geltendmachung von Schadenersatzansprüchen wegen eines Verstoßes gegen Art. 32 DSGVO einen konkreten Schaden nachweisen. Ein zwingender Kausalzusammenhang zwischen dem festgestellten Verstoß und dem Schadenersatzanspruch allein aufgrund der von der betroffenen Person erlittenen Sorgen, Befürchtungen und Ängste vor einem

möglichen künftigen Missbrauch personenbezogener Daten besteht nicht.

Eine Entschädigung, die für das bloße Gefühl des Unwohlseins über die Nichteinhaltung des Gesetzes durch einen Dritten reicht grundsätzlich nicht aus, um einen immateriellen Schadenersatzanspruch zu begründen.

## 2. Besonderheit Cyberangriff – Möglicher Missbrauch ggfs. ausreichend

Gleichwohl soll – so der Generalanwalt – „*die Tatsache, dass unter Umständen wie denen des Ausgangsverfahrens der Missbrauch personenbezogener Daten* ***nur möglich und nicht bereits eingetreten ist***," bereits ausreichen, „*um davon auszugehen, dass die betroffene Person einen durch den Verstoß gegen die Verordnung verursachten immateriellen Schaden erlitten haben kann, sofern die betroffene Person nachweist, dass die Befürchtung eines solchen Missbrauchs ihr tatsächlich und konkret einen realen und sicheren emotionalen Schaden zugefügt hat*.".

Entscheidend, so heißt es weiter, „*ist, dass es sich nicht um eine bloße subjektive Wahrnehmung handelt, die veränderlich ist und auch vom Charakter und von persönlichen Faktoren abhängt, sondern um die Objektivierung einer, wenn auch geringfügigen, aber nachweisbaren Beeinträchtigung der physischen oder psychischen Sphäre oder des Beziehungslebens einer Person; die Art der betroffenen personenbezogenen Daten und die Bedeutung, die sie im Leben der betroffenen Person haben, und vielleicht auch die Wahrnehmung, die die Gesellschaft zu diesem Zeitpunkt von dieser spezifischen, mit der Datenverletzung verbundenen Beeinträchtigung hat*." (Rz. 83).

Wie dies vom Betroffenen dargelegt werden muss, bspw. über entsprechende medizinische Gutachten, wird die zukünftige Rechtsprechungspraxis zeigen. Aus Sicht des Verantwortlichen ist

es daher entscheidend, den Grad der Möglichkeit eines Missbrauchs möglichst konkret darzulegen und zu bewerten. Auch hier hat sich in unserer Beratungspraxis insbesondere eine Analyse entsprechender Darknet-Veröffentlichungen als wirksam erwiesen. So können die Art der dort veröffentlichten Daten, ihre Auffindbarkeit im Einzelnen und ihre Struktur und sonstige, mit hier eingesetzten Mitteln und Analysen nachzuweisende Faktoren, die Missbrauchsgefahr relativieren und die „Möglichkeit“ eines Missbrauchs so weit verringern, dass ein Schadenersatzanspruch ausgeschlossen werden kann.

## C. Hilfestellungen durch die Kanzlei / Urheber- und Haftungshinweis

Es ist daher nicht nur dringend anzuraten, die unternehmensinterne IT-Infrastruktur stetig auf den Prüfstand zu stellen und dem Thema IT-Sicherheit eine gesteigerte Bedeutung beizumessen, sondern auch nach einem eingetretenen Vorfall besonnen und professionell zu reagieren. Die Kanzlei Kazemi & Partner unterhält eine eigene Taskforce zum Thema Cyberangriffe und unterstützt Unternehmen im Ernstfall nicht nur juristisch, sondern auch über angeschlossene IT-Experten, die über umfangreiche Erfahrung verfügen und mit uns Hand in Hand zusammenarbeiten.

Die Inhalte dieser Analyse sind mit größtmöglicher Sorgfalt recherchiert und erstellt worden. Fehler sind dennoch nicht auszuschließen. Eine Haftung für die Richtigkeit, Vollständigkeit und Aktualität kann trotz sorgfältiger Prüfung nicht übernommen werden. Die Darstellung spiegelt vielmehr die persönliche Einschätzung des Erstellers dar.

Bonn, den 01.05.2023

Dr. Robert Kazemi
(Rechtsanwalt)

# D. Anhang Schlussanträge in der Rechtssache C-340/21