7.
Datenrecht und Datenschutzrecht

Datenschutzrechtliche Anforderungen an Confidential Computing nach der DSGVO

Thomas Hoeren

Der Jubilar, zu dessen Festtag ich von Herzen gratulieren möchte, hat sich in den letzten Jahrzehnten vor allem in den Bereichen Medienpolitik und Persönlichkeitsrecht wissenschaftlich verdient gemacht. Seine breit aufgestellten Interessen hat er nicht nur in der gemeinsamen erfolgreich herausgegebenen Schriftenreihe zum Informationsrecht im Dreck verbracht dokumentiert, sondern mit den vielen epochalen Monographien und Aufsätzen.[1] Es ist mir daher eine besondere Ehre und Freude, zu dieser Festschrift beitragen zu dürfen durch einen Beitrag zu einem der großen Probleme des europäischen Datenschutzrechts.

Die DSGVO findet nach Art. 2 I DSGVO nur dann Anwendung, wenn personenbezogene Daten verarbeitet werden und diese Verarbeitung entweder ganz oder zumindest teilweise automatisiert erfolgt.[2] Aus einem Umkehrschluss dieses Anwendungsbereichs der DSGVO ergibt sich, dass sie gerade nicht gilt, wenn anonymisierte Daten verarbeitet werden (so auch ErwGr. 26 ergibt).[3] Ist der Anwendungsbereich der DSGVO erst eröffnet, resultieren daraus viele Pflichten für Verantwortliche einer Datenverarbeitung und Rechte für Betroffene. Als Verantwortlicher im Sinne der DSGVO gilt gem. Art. 4 Nr. 7 DSGVO diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Kontext dieses Festschriftbeitrags würde dies bedeuten, dass der Betreiber durch die wesentliche Entscheidungsbefugnis über Mittel und Zwecke der Verarbeitung als verantwortliche Stelle im Sinne der DSGVO anzusehen wäre. Wird der Dienst als Cloud-Service auf den Servern eines Cloud Service Providers (sog. CSP; bspw. AZURE) angeboten,

1 So etwa Persönlichkeitsschutz und Internet, München 2002; Privacy and the Media - A Comparative Perspective, München 2000.

2 *Kühling*/Buchner/*Raab,* 3. Aufl. München 2020, DS-GVO Art. 2 Nr. 1 Rn. 2; *Gola*/Heckmann, 3. Aufl. München 2022, DS-GVO Art. 2 Rn. 1 – 6.

3 *Kühling*/Buchner/*Klar,* DS-GVO Art. 4 Nr. 1 Rn. 31.

wäre dennoch der eigentliche Betreiber des Dienstes Verantwortlicher im Sinne der DSGVO, während ein CSP in diesem Kontext lediglich im Auftrag eines Verantwortlichen Daten verarbeitet und damit Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) einzuordnen ist, wenn personenbezogene Daten verarbeitet werden.[4]

I. Confidential Computing – was ist das?

Diese Pflichten aus Auftragsverarbeitung können eventuell auch im Falle von Confidential Computing gelten. Bei Confidential Computing handelt es sich um eine vergleichsweise neue Technologie, welche es ermöglicht, die eigentliche Verarbeitung (im technischen, nicht rechtlichen Sinne) von Daten zu verschlüsseln. Die bisher gängigen Verschlüsselungssysteme ermöglichen zwar den Schutz von Datenübertragungen (Data in transit) sowie den Schutz gespeicherter Daten (Data at rest), bei der eigentlichen Verarbeitung von Daten – also der Berechnung im Prozessor und Arbeitsspeicher – war eine Verschlüsselung bisher kaum (praxistauglich) möglich. Um dennoch eine verschlüsselte Datenverarbeitung zu ermöglichen - wodurch die drei grundlegenden Stadien von Daten (Data at rest, in transit, in use) verschlüsselt wären - werden sichere Ausführungsumgebungen geschaffen (allgemein sog. Trusted Execution Enviroments, TEEs), wodurch Daten auch im Prozessor verschlüsselt bleiben. Beim Confidential Computing werden die Daten innerhalb einer sog. sicheren Enklave verarbeitet, wodurch die Daten isoliert von anderen Verarbeitungsvorgängen verarbeitet werden, auch während der Verarbeitung grundsätzlich verschlossen bzw. versiegelt und damit vertraulich sind und auch ein Auslesen eines Speicherüberlaufs von dem Prozessor auf den Arbeitsspeicher durch eine Runtime-In-Memory-Encryption lediglich die Chiffrate offenlegen würde.

Dadurch, dass Confidential Computing nunmehr – vorbehaltlich ordnungsgemäßer Umsetzung – eine Verschlüsselung aller Stadien von Daten (s.o.) ermöglicht, wird die Frage der Konsequenz dessen für das Datenschutzrecht immanent. Der Anwendungsbereich der DSGVO ist – wie sich aus einem Umkehrschluss zu Art. 2 Abs. 1 DSGVO sowie aus dem ErwGr.

4 Eingehend zu den datenschutzrechtlichen Beziehungen bei der Nutzung von Cloud-Diensten siehe Arnold/Günther/*Hamann/Haußmann,* Arbeitsrecht 4.0, 2. Aufl. München 2022, § 6 Rn. 119; *Jotzo*, Der Schutz personenbezogener Daten in der Cloud, 2. Aufl. Hamburg 2020, Teil 3 Rn. 132 ff.

26 ergibt[5] – nicht für anonymisierte Daten eröffnet, sodass die strengen datenschutzrechtlichen Anforderungen der DSGVO nicht gelten würden, wären Daten, die mittels mit Confidential Computing verarbeitet werden, im Sinne der DSGVO anonymisiert.

Vor diesem Hintergrund wird die Frage virulent, ob Confidential Computing hier Abhilfe schaffen und bereits im ersten Schritt datenschutzrechtlicher Fragen dafür sorgen kann, dass der Anwendungsbereich der DSGVO schon gar nicht eröffnet wird, wenn Daten mittels Confidential Computing beim CSP verarbeitet werden. Davon wäre dann auszugehen, wenn die Daten im Sinne der DSGVO anonymisiert wären.

II. Anonymisierung

Im Folgenden wird daher untersucht, ob mittels Confidential Computing verarbeitete Daten als anonymisiert anzusehen sind, wobei hierzu zunächst in Frage kommenden Perspektiven dargestellt werden, in denen anonymisierte Daten überhaupt sinnvoll erscheinen (1), bevor – auch vor dem Hintergrund eines neuerlichen Urteils des EuG– der Begriff der anonymisierten Daten herausgearbeitet (2) und im Kontext von Confidential Computing subsumiert wird (3).

1. Konstellationen der Anonymisierung

Anonymisierte Daten im Sinne der DSGVO liegen nur dann vor – so viel vorweggenommen – wenn diese sich nicht auf eine identifizierte oder identifizierbare Person beziehen oder einst personenbezogene Daten jeglichen Personenbezug durch die Elimination identifizierender Merkmale verlieren.[6] Im Regelfall wird ein Verantwortlicher einer Datenverarbeitung wenig mit anonymisierten Daten anfangen können, sondern im Zweifelsfalle auch auf den Klartext dieser Daten zugreifen müssen. Dies gilt insoweit auch für verschlüsselte Daten – unabhängig von der Frage, ob diese im Sinne der DSGVO in verschlüsselter Form noch als personenbezogene Daten

5 *Kühling*/Buchner/*Klar,* DSGVO, 3. Aufl. München 2020, DS-GVO Art. 4 Nr. 1 Rn. 31.
6 *Kühling*/Buchner/*Klar,* DS-GVO Art. 4 Nr. 1 Rn. 31.

anzusehen sind. Zur tatsächliche Nutzung müssen die Daten im Regelfall im Klartext und nicht als verschlüsselter ciphertext vorliegen.[7]

Damit stellt die Frage nach der Anonymisierung von Daten durch Confidential Computing allerdings nur in einem Szenario, in dem die Daten nicht allein durch den Verantwortlichen genutzt werden, sondern daneben eine weitere Stelle beispielsweise zur Durchführung von Berechnungen, Speicherung oder zum Hosting eines Softwaresystems, in dem die Daten implementiert werden, Zugriff auf diese erhält.

Wäre dagegen auch der Verantwortliche einer Datenverarbeitung nicht an den Klardaten mit Personenbezug interessiert, bedürfte es schon – aus Sicht des Datenschutzrechts – keines Confidential Computings. Die Daten ließen sich dann bereits beim Verantwortlichen (beispielsweise unmittelbar bei der erstmaligen Erhebung) anonymisieren, sodass – ggf. abgesehen vom Anonymisierungsvorgang selbst – keine weiteren, der DSGVO unterfallenden Datenverarbeitungsvorgänge mehr vorlägen. Confidential Computing würde dann einzig als Aspekt der Datensicherheit (im Sinne eines Geheimnisschutzes) in Betracht kommen

Gegenstand der folgenden Betrachtung ist damit einzig die Perspektive, dass eine Anonymisierung durch Confidential Computing gegenüber einer vom eigentlichen Verantwortlichen verschiedenen datenverarbeitenden Stelle (beispielsweise einem SaaS-Anbieter, Cloud-Hoster etc.) erfolgen könnte. Damit lägen zwar beim Verantwortlichen weiterhin personenbezogene Daten mit den damit Verbundenen datenschutzrechtlichen Verpflichtungen vor, allerdings könnte es – bei der Annahme einer Anonymisierung im Rechtssinne – bei der Verarbeitung durch Dritte unter Einsatz von Confidential Computing zu erheblichen rechtlichen Erleichterungen für den Verantwortlichen und der verarbeitenden Stelle kommen.

2. Anonymisierte Daten im Sinne der DSGVO – absolute oder relative Betrachtung?

Die DSGVO selbst regelt einzig den Umgang mit personenbezogenen Daten und gibt Anhaltspunkte, wann von einem Personenbezug auszugehen ist. Wann anonymisierte Daten vorliegen und wie mit diesen zu verfahren ist, wird von der DSGVO dagegen weitestgehend offengelassen und kann

7 *Erbguth*, Datenschutzkonforme Verwendung,von Hashwerten auf Blockchains, MMR 2019, 654 ff.

einzig mittels Umkehrschluss der Regelungen zum Vorliegen eines Personenbezuges ermittelt werden.[8]

a) Identifizierte oder identifizierbare natürliche Personen

Einigkeit besteht insoweit darin, dass anonyme Daten das Gegenteil von personenbezogenen Daten sind.[9] Der ErwGr. 26 der DSGVO nimmt dann das Vorliegen von anonymisierten Informationen an, wenn sich diese „nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen" oder, wenn „personenbezogene Daten in der Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann". Während anonyme Daten nur am Rande Erwähnung in der DSGVO finden, sind dagegen pseudonyme Daten – als Unterfall der Verarbeitung personenbezogener Daten[10] – umfassend geregelt. Aufgrund ähnlicher Zielrichtungen von Pseudonymisierung und Anonymisierung – dem Entfernen des Personenbezuges – müssen beide Begriffe im Zusammenhang betrachtet werden. Nach Art. 4 Nr. 5 DSGVO handelt es sich bei einer Pseudonymisierung um eine „Verarbeitung personenbezogener Daten in einer Weise, dass die […] Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorische Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.".

Bei der Beurteilung des Vorliegens einer Pseudonymisierung ist damit nach der Legaldefinition der DSGVO ebenfalls die Perspektive entscheidend. Dadurch, dass die DSGVO auf das (Nicht-) Vorliegen von und den Zugang zu „zusätzlichen Informationen" abstellt, wird die Frage virulent, wann solche zusätzlichen für eine Re-Identifizierung genutzt werden können und welche rechtlichen Konsequenzen es hat, wenn eine verarbeitende Stelle einzig auf die pseudonymen Daten zugreifen kann, ihr aber der Zugang zu den zusätzlichen Informationen, ohne die ein Personenbezug nicht hergestellt werden kann, rechtlich und/oder technische verwehrt wird. Aus

8 *Gierschmann*, ZD 2021, 482, (482).

9 *Kühling*/Buchner/*Klar,* Datenschutzgrundverordnung BDSG, Kommentar, 3. Aufl. München 2020,DS-GVO Art. 4 Nr. 1 Rn. 31; *Gierschmann*, ZD 2021, 482, (482).

10 *Schild*, BeckOK DatenschutzR, Art. 4 Rn. 78.

der Perspektive dieser verarbeitenden Stelle lässt sich ein Personenbezug nicht (ohne Weiteres) herstellen, theoretisch bleibt dies jedoch für andere Stellen (bspw. den Verantwortlichen der Datenverarbeitung, bei dem die Informationen zur Re-Identifizierung liegen, weiter möglich). In einer solchen Konstellation wird deutlich, dass Anonymisierung und Pseudonymisierung, je nach der Perspektiv, unter Umständen fließend ineinander übergehen, wenn der Ausschluss des Zugriffs auf die identifizierenden zusätzlichen Informationen für die jeweilige Stelle bedeuten würde, dass es zu einer Anonymisierung im Rechtssinne kommt, auch wenn einer anderen Stelle die Re-Identifizierung ohne weiteres möglich ist.

In diesem Zusammenhang kann allerdings nur dann von einer Anonymisierung ausgegangen werden, wenn diese nicht erfordert, dass eine Re-Identifizierung tatsächlich (objektiv) – unabhängig der Perspektive – für Jedermann unmöglich sein muss. Ein solcher objektiver (oder auch absoluter) Ansatz wurde zwar in der Vergangenheit noch diskutiert,[11] ihm wird jedoch in Rechtsprechung und Literatur überwiegend nicht gefolgt.[12] Der EuGH stellt bei der Beurteilung, ob nach dem relativen Ansatz für eine bestimmte Stelle der Personenbezug der Daten besteht darauf ab, ob die verarbeitende Stelle die zur Re-Identifizierung notwendigen Mittel vernünftigerweise zur Wiederherstellung des Personenbezuges einsetzen kann.[13] Von der Möglichkeit der Re-Identifizierung kann nach Ansicht des Gerichts dann vernünftigerweise nicht ausgegangen werden, wenn der betreffenden Stelle die Identifizierung gesetzlich verboten oder diese praktisch nicht durchführbar wäre. Letzteres kann wiederum angenommen werden, wenn die Re-Identifizierung mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften einherginge.[14] Das Gericht nimmt damit eine risikobasierte und vom jeweiligen Bearbeitungskontext abhängige Beurteilung vor.[15]

Auch wenn in der rechtswissenschaftlichen Literatur weitestgehend Einigkeit darüber besteht, dass die zuvor genannten Grundsätze eines relativen Ansatzes sowie einer risikobasierten Betrachtungsweise auch für die

11 so u.a. *Brink*, ZD 2015, 1 (1).
12 Gola/Heckmann/*Pötters*, Datenschutzgrundverordnung, BDSG, Kommentar, DS-GVO Art. 89 Rn. 12; *Gierschmann,* ZD 2021, 482, (483); *Roßnagel,* ZD 2018, 243, (244).
13 EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer, Rn. 43, 46.
14 EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer, Rn. 46.
15 *Gierschmann,* ZD 2021, 482, (483).

Anonymisierung im datenschutzrechtlichen Sinne gelten müssen, haben sich die (europäischen) Gerichte dazu bislang nicht eindeutig positioniert.

b) Zur Abgrenzung pseudonymisierter, anonymisierter und personenbezogener Daten nach dem Urteil des EuG vom 26.4.2023

Erstmalig hat sich ein europäisches Gericht – hier der EuG – mit dem Urteil v. 26.4.2023 – T-557/20 eindeutig zu der Frage nach dem relativen Ansatz der Personenbeziehbarkeit insoweit positioniert, als dass das Gericht festgestellt hat, dass pseudonymisierte Daten dann nicht als personenbezogene Daten gelten, wenn ein Datenempfänger nicht über die Mittel verfügt, die betroffenen Personen zu Re-Identifizieren, auch wenn die übermittelnde Stelle über solche verfügt.[16] Die Entscheidung ist für die Frage, welchen Einfluss Confidential Computing auf datenschutzrechtliche Pflichten von Verantwortlichen und Auftragsverarbeitern haben kann, von entscheidender Bedeutung.

Hintergrund der Entscheidung

Die Verfahrensbeteiligten streiten sich im Wesentlichen um die Frage, ob pseudonymisierte Daten, die an Dritte übermittelt werden, auch dann als personenbezogene Daten anzusehen sind, wenn dem Empfänger die Entschlüsselung der Daten nicht möglich ist. Das Gericht der Europäischen Union (EuG) hatte zu klären, ob im Rahmen des dafür erforderlichen Personenbezugs von Daten auf die Identifizierungsmöglichkeiten der konkreten, datenverarbeitenden Stelle (relativer Ansatz) oder aber einer beliebigen dritten Person (absoluter Ansatz) abzustellen ist.[17] Damit musste zugleich die Frage der Abgrenzbarkeit pseudonymisierte (oder sogar anonymisierter) Daten von personenbezogenen Daten entschieden werden.

Wie bereits dargestellt sind pseudonymisierte Daten personenbezogene Daten, die nur unter Hinzuziehung zusätzlicher Informationen die Zuordnung zu einer bestimmten Person ermöglichen. Pseudonymisierte Daten eröffnen demnach grundsätzlich den Anwendungsbereich des Datenschutzrechts. Anonymisierte Daten lassen hingegen keine Zuordnung zu einer bestimmten oder bestimmbaren Person zu.[18] Auch unter Hinzuziehung zusätzlicher Informationen können danach grundsätzlich keine Rückschlüsse

16 EuG Urt. v. 26.4.2023 – T-557/20, BeckRS 2023, 8240, Rn. 90, 104.
17 Überblick zu den vertretenen Ansichten bei *Breyer,* ZD 2015, 365.
18 Paal/Pauly/*Ernst*, DS-GVO BDSG, Art. 4 Nr. 5 Rn. 48.

auf die Identität des Betroffenen gezogen werden, sodass diese Daten – wie gezeigt – nicht dem Datenschutzrecht unterliegen.

Zugrundeliegender Sachverhalt

Die Single Resolution Board (SRB) ist ein einheitlicher Abwicklungsausschuss, der die ordnungsgemäße Abwicklung insolvenzbedrohter Finanzinstitute in Europa gewährleisten soll. Im Verfahren gegen eine spanische Bank sollten Anteilseigner und Gläubiger mittels elektronischem Formular eine Stellungnahme abgegeben. Die Stellungnahmen wurden zur Auswertung an ein Beratungsunternehmen weitergegeben, wobei die Namen der Befragten zum Zwecke der Anonymisierung durch einen Code ersetzt wurden. Die Zuordnung der Stellungnahmen zu den Anteilseignern und Gläubigern war nur durch den Zugriff auf die Datenbank des SRB möglich, wobei diese Möglichkeit für das datenerhaltende Beratungsunternehmen nicht bestand.

Der Europäische Datenschutzbeauftragte (EDSB) sah darin einen Verstoß gegen Art. 15 Abs. 1 lit. d) Verordnung (EU) 2018/1725 (EU-Datenschutzverordnung; Geltung für Organe der Union, viele wortgleiche Regelungen zur DSGVO). Die Daten der Gläubiger seien nach Ansicht des EDSB lediglich in pseudonymisierte Form übermittelt worden, sodass es sich weiterhin um personenbezogene Daten handele. Die Befragten wurden zudem nicht über die Übermittlung informiert. Der SRB war hingegen der Auffassung, dass die übermittelten Daten keine Wiederherstellung des Personenbezugs ermöglichten, es handele sich vielmehr um anonymisierte Daten auf welche die Vorschriften der Verordnung nicht anwendbar seien.

Die Entscheidung des Gerichts

Das EuG legte in seinem Urteil vom 26.4.2023 bei der in der vorliegenden Rechtssache (T-557/20) maßgeblichen Auslegung des Merkmals der „identifizierbare[n] natürliche[n] Person" im Sinne von Art. 3 Nr. 1 der VO 2018/1725 die gleichen Maßstäbe zugrunde, wie zuvor der EuGH in seinem Urteil vom 19.10.2016 in Bezug auf „personenbezogene Daten" im Sinne von Art. 2 Buchst. a der Richtlinie 95/46/EG[19] (identische Begrifflichkeiten wie inzwischen die DSGVO). Daraus ergeben sich nach Ansicht des Gerichts die folgenden – oben bereits dargestellten – Grundsätze bei der Bestimmung des Personenbezugs: Nach dem absoluten Ansatz seien bei der Frage der Bestimmbarkeit der Person alle dem Verantwortlichen für die Verarbei-

19 EuG Urt. v. 26.4.2023 – T-557/20, BeckRS 2023, 8240, Rn. 88 f.; EuGH Urt. v. 19.10.2016 –C-582/14 –Breyer/Deutschland = NJW 2016, 3579.

tung oder jedem Dritten zur Verfügung stehende Mittel zu berücksichtigen und damit die Identifizierbarkeit rein objektiv zu betrachten.[20] Nach dem relativen Ansatz sei im Sinne einer subjektiven Betrachtungsweise hingegen nur auf die Identifizierungsmöglichkeiten des jeweiligen verantwortlichen abzustellen.[21] Der EuGH hat sich im Grundsatz zwar – wie gezeigt – dem relativen Ansatz angeschlossen, daran jedoch einschränkende Anforderungen geknüpft. So sei grundsätzlich auf die Perspektive der verantwortlichen Stellen und nicht auf die eines Dritten abzustellen. Gleichzeitig muss der Verantwortliche dabei auch das Wisse oder die Mittel Dritter berücksichtigten, soweit diese vernünftigerweise anhand objektiver Kriterien zur Bestimmung der betreffenden Person eingesetzt werden können (siehe oben).

Einordnung des Urteils

Das EuG führt mit seinem Urteil das durch den EuG geprägte, gemäßigte relative Verständnis der Personenbezogenheit von Daten fort. Dabei hat das EuG nochmal klargestellt, dass nur entscheidend sei, ob der Datenempfänger über die Mittel zur Rückidentifizierung verfüge. Dass der Datenübermittler zur Rückidentifizierung in der Lage ist, sei irrelevant.[22]

Dass sich das EuG dem relativen Ansatz anschließt, ist aus praktischer Sicht zu begrüßen, würde ein absolutes Verständnis des Personenbezuges doch zu einer übermäßigen Ausdehnung des Datenschutzrechts führen. Darüber hinaus wäre der Verantwortliche, mangels rechtssicherer Erkenntnismöglichkeit, ob eine Individualisierung der Daten nicht doch technisch möglich ist, einem erheblichen Maß an Rechtsunsicherheit ausgesetzt.[23]

Praxisfolgen des Urteils allgemein

Sobald das Urteil rechtskräftig geworden ist, hat es aufgrund der Wortlauidentität der streitentscheidenden Normen (Art. 3 Nr. 1 und Art. 15 Abs. 1 lit. d) VO 2018/1725) mit Art. 4 Nr. 1 beziehungsweise Art. 13 Abs. 1 lit. e) DSGVO auch für die Auslegung der DSGVO hohe Relevanz.[24] Es ist davon auszugehen, dass die europäische Rechtsprechung auch in Bezug auf die DSGVO einen relativen Ansatz, wenn auch mit Einschränkungen, vertreten wird. Für die Praxis bedeutet dies, dass grundsätzlich nur die jeweilige datenverarbeitende Stelle prüfen muss, ob ihr die Re-Identifizierung der Daten möglich ist. Nach der neuerlichen EuG-Entscheidung, welche sich

20 *Breyer*, ZD 2014, 400 (400).
21 Ausführlich dazu *Kühling/Klar*, NJW 2013, 3611 (3614 f.).
22 EuG Urt. v. 26.4.2023 – T-557/20, BeckRS 2023, 8240, Rn. 96.
23 Taeger/Gabel/*Arning/Rothkegel,* DSGVO – BDSG – TTDSG, Kommentar,4. Auflage, Frankfurt a.M. 2022, DSGVO Art. 4 Rn. 35.
24 *Desgens-Pasanau*, La Protection des données personnelles, Paris 2016, S. 14.

maßgeblich an den Kriterien des EuGH orientiert, müssen dabei aber auch die einschränkenden Anforderungen berücksichtigt werden, wonach auch das Wissen und die Mittel Dritter zur Identifizierbarkeit beachtlich sind, sofern die Identifizierung nicht gesetzlich verboten oder praktisch undurchführbar ist.

Aus der Rechtsprechung geht aber weiterhin nicht genau hervor, wie mit anderen Personen umzugehen ist, die keine Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO sind. In dem Urteil hat das EuG vor diesem Hintergrund ausdrücklich gerügt, dass der europäische Datenschutzbeauftragte nicht hinreichend geprüft habe, ob eine Person, die nicht Verantwortlicher ist, derer sich der Verantwortliche aber bedient, zur Re-Identifizierung in der Lage ist.[25] Damit dürfte der Frage, wie die Personenbeziehbarkeit von Daten aus Perspektive von anderen Akteuren als den Verantwortlichen zu bewerten ist, eine neue Relevanz zukommen. Aus dem EuG Urteil geht insoweit aber hervor, dass jedenfalls zu prüfen wäre, ob die Dritt-Stelle, welche Daten übermittelt bekommt, das Recht habe, auf die zusätzlichen, identifizierenden Informationen zuzugreifen und so ein Zugriff auch tatsächlich durchführbar wäre. Sofern eine solche Möglichkeit nicht bestünde, sei nicht davon auszugehen, dass sich die übermittelten Daten auf eine „identifizierbare Person" beziehen.[26]

3. Fazit zur (Nicht-) Identifizierbarkeit von Personen

Aus dem Vorgenannten ergibt sich eine Gemengelage verschiedenster abstrakter Anforderungen, die an das (Nicht-) Vorliegen der Personenidentifizierbarkeit zu stellen sind. Trotz einzelner Urteile zu dieser Thematik fehlt bislang jedoch eine eindeutige Positionierung des obersten europäischen Gerichts (EuGH). Zwar bietet das neue EuG Urteil erstmalig konkrete Anhaltspunkte zur Eröffnung des Anwendungsbereichs des Datenschutzrecht im Falle übermittelter, pseudonymisierter Daten, nichts destotrotz verbleiben weiterhin Rechtsunsicherheiten hinsichtlich der Beurteilung der Re-Identifizierbarkeit und den Pflichten, die Verantwortliche bezüglich des Zugangs zu identifizierenden, zusätzlichen Informationen treffen.

Dennoch lassen sich konkrete Anforderungen an anonyme Daten stellen: sowohl der EuGH als auch das sich auf die EuGH Entscheidung berufende

25 EuG Urt. v. 26.4.2023 – T-557/20, BeckRS 2023, 8240, Rn. 103.
26 EuG Urt. v. 26.4.2023 – T-557/20, BeckRS 2023, 8240, Rn. 103.

EuG gehen davon aus, dass eine Re-Identifizierbarkeit nicht vollständig ausgeschlossen sein muss. Vielmehr wird ein risikobasierter Ansatz vertreten. Das Risiko, dass es zu einer Re-Identifizierung kommen kann, muss gering – nicht aber völlig ausgeschlossen – sein. Zur Beurteilung der Wahrscheinlichkeit des Risikoeintritts sind dabei gerade auch die Risiken der Identifizierung durch Dritte bzw. das Zusatzwissen Dritter zu berücksichtigen, soweit ein Zugriff auf dieses Zusatzwissen aus Perspektive der jeweils beurteilten datenverarbeitenden Stelle vernünftigerweise zu erwarten ist.[27] ErwGr. 26 DSGVO gibt ferner vor, dass bei der Risikoabwägung auch die zum Zeitpunkt der Verarbeitung verfügbaren Technologien und technologischen Entwicklungen zu berücksichtigen sind – bei der dauerhaften Nutzung von Daten beispielsweise im Rahmen eines SaaS-Dienstes muss damit die Risikobewertung laufend durchgeführt und aktualisiert werden. Die Maßstäbe der Risikobeurteilung ergeben sich aus einer Zusammenschau der besprochenen Urteile und variieren je nach Art der Daten, des Verarbeitungskontextes und der jeweiligen verarbeitenden Stelle, insbesondere in deren Beziehung zum datenschutzrechtlich verantwortlichen.

Eine umfassende Risikobeurteilung und die dazu erforderliche technisch-rechtliche Bewertung von Confidential Computing führt – vorbehaltlich einer eingehenden IT-Sicherheitstechnischen Überprüfung der getroffenen Annahme – in bestimmten Konstellationen zu der Erkenntnis, dass nach dem relativen, risikobasierten Ansatz von einer Anonymität der so verarbeiteten Daten ausgegangen werden kann. Das Ergebnis der Risikobeurteilung zeigt insoweit auf, dass der für eine Re-Identifizierung erforderliche Aufwand bei einer datenverarbeitenden Stelle, die keinen Zugriff auf den Schlüssel hat, so unverhältnismäßig ist, dass damit nach dem Stand der Wissenschaft und Technik sowie der allgemeinen Lebenserfahrung nicht zu rechnen ist. Aufgrund möglicher technischer Entwicklungen kann jedoch nicht von einer zeitlich unbegrenzten Anonymisierung ausgegangen werden – vielmehr machen es dauerhafte Neuentwicklungen erforderlich, dass die Risikoeinschätzung im Zuge eines dauerhaften Monitorings während der gesamten Verarbeitungstätigkeit laufend erfolgt. Eine technische Umsetzung der sogenannten Kryptoagilität bietet hier die Möglichkeit, die genutzten Verschlüsselungen laufend an den aktuellen Stand der technischen Forschung anzupassen.

27 So auch *Gierschmann,* ZD 2021, 482, (483).