Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Universität Bremen | Postfach 33 04 40, 28334 Bremen
IGMR | **FB06**

Fachbereich 06
Rechtswissenschaft

Prof. Dr. jur. Dennis-Kenji Kipker
Wissenschaftlicher Geschäftsführer

GW 1, Raum A 2010
Universitätsallee
28359 Bremen

Tel. 0421 5905 5465
Fax 0421 218-66052
kipker@uni-bremen.de

www.igmr.uni-bremen.de
igmr@uni-bremen.de

Bremen 13. September 2022

Verschlüsselung und Anonymisierung von personenbezogenen Daten mit Confidential Computing:

Rechtliche Besonderheiten und Vorteile einer neuen Technologie

Kurzgutachten

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Executive Summary:

Der Einsatz von Confidential Computing kann aus rechtlicher Sicht mit Blick auf Compliance und Datenschutz am praxisrelevanten Beispiel von Verschlüsselung und Anonymisierung durchaus Vorteile bieten. Soweit man dem Konzept der relativen Anonymisierung folgt, kann durch Einsatz der neuen Technologie rechtlich sogar argumentiert werden, dass die verarbeiteten Daten zumindest für einen gewissen Zeitraum (nach Stand der Forschung liegt dieser Zeitraum zwischen 10-30 Jahren) nicht den datenschutzrechtlichen Anforderungen unterfallen, soweit sie ansonsten personenbezogen wären. Hierzu muss aber technisch-organisatorisch vorausgesetzt werden, dass ein sicheres Verschlüsselungsverfahren verwendet wird und die gesamte Datenverarbeitung von der Erhebung bis hin zur Löschung anonymisiert stattfindet. Mit den Vorteilen, die mit der anonymisierten Datenverarbeitung verbunden sind, sind jedoch ebenso neue Compliance-Pflichten gegeben, indem durch flankierende TOM das Risiko einer De-Anonymisierung möglichst gering zu halten ist. Auch ist regelmäßig zu überprüfen, ob das verwendete Verschlüsselungsverfahren noch den gängigen Standards entspricht bzw. zwischenzeitlich neu entdeckte Schwachstellen aufweist. Damit einher geht die (juristische) Erkenntnis, dass die Anonymität nicht (mehr) als statischer Begriff aufgefasst werden kann.
Selbst wenn man der relativen Theorie zur Anonymisierung nicht zu folgen vermag, bieten sich durch den Einsatz von Confidential Computing erhebliche Vorteile mit Blick auf Datensicherheit und Datenschutz. So können nicht nur die allgemeinen IT-Sicherheitsziele gefördert und unterstützt werden, sondern bei der Verarbeitung von personenbezogenen Daten kann die Technologie bei der Einhaltung der Datenschutzanforderungen gem. Art. 5, 24 und 32 DS-GVO Vorteile bieten sowie als Maßnahme des Datenschutzes durch Technikgestaltung ein praxisnahes Beispiel zur Umsetzung des Art. 25 DS-GVO darstellen.

Gutachten:

Mit dem Confidential Computing als einer Technologie, die sich im praktischen Gebrauch gerade erst zu etablieren beginnt, werden mit Blick auf Datensicherheit und Datenschutz von personenbezogenen Daten hohe Erwartungen verbunden. Das vorliegende Gutachten liefert aus rechtlicher und technischer Perspektive einen Überblick über die Besonderheiten und Vorteile des Confidential Computing, will aber ebenso Grenzen aufzeigen und Denkanstöße für den juristischen Diskurs auf diesem Gebiet mit Blick auf die technische Verschlüsselung und rechtliche Beurteilung der Anonymisierung liefern, der bislang kaum geführt wurde.

Datenverarbeitung als datensicherheitsrechtliche Compliance-Pflicht

Den Verantwortlichen einer jeden Datenverarbeitung treffen aus Compliance-Perspektive zahllose Pflichten, die sich nicht nur aus Verträgen mit Kunden und Auftraggebern, sondern ebenso aus gesetzlichen Vorschriften, gesellschaftsrechtlichen Vorgaben sowie aus unternehmensinternen Anforderungen ergeben können. Wenn überdies personenbezogene Daten verarbeitet werden, treten zusätzlich die allgemeinen und bereichsspezifischen datenschutzrechtlichen Maßgaben hinzu – insbesondere gelten für den Verantwortlichen und den Auftragsverarbeiter die strengen Pflichten aus der DS-GVO, wollen sie eine Datenverarbeitung legitimieren. So ist der Verantwortliche nach Art. 5 Abs. 2 DS-GVO verpflichtet, die Datenverarbeitungsgrundsätze einzuhalten und kann seine Pflichten nicht ohne Weiteres an Auftragsverarbeiter delegieren. Dies sieht auch Art. 28 Abs. 1 DS-GVO vor, der für die Auftragsverarbeitung bestimmt, dass der Verantwortliche nur mit Auftragsverarbeitern kooperiert, die selbst hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen ergriffen werden, damit die Datenverarbeitung im Einklang mit der DS-GVO erfolgt. Hierzu gehört deshalb nach Art. 28 Abs. 3 DS-GVO grds. der Abschluss eines entsprechenden Vertrages zwischen den Parteien, in welchem die Pflichten des Auftragsverarbeiters statuiert sind, wozu insbesondere auch Maßnahmen der Datensicherheit gem. Art. 32 DS-GVO gehören.

Cloud Computing als bislang ungelöste Herausforderung der Datensicherheit

Mehr denn je wird die unternehmerische IT-Compliance mit Blick auf Datensicherheit und Datenschutz durch die vernetzten IT-Strukturen und Outsourcing-Prozesse erschwert – bestes Beispiel sind in dem Zusammenhang Cloud Computing Provider, deren Unternehmens- und ggf. auch Serverstandort im außereuropäischen Ausland belegen ist. Mit Blick auf umfassende (sicherheits)behördliche Zugriffsbefugnisse auf Serverdaten US-amerikanischer Unternehmen (u.a. „Cloud Act“) ist diese Problematik vor allem seit dem Jahr 2020 dadurch bekannt geworden, dass der Europäische Gerichtshof (EuGH) das EU-US-Datenschutzabkommen „Privacy Shield“ für ungültig erklärt hat. Mangels entsprechender Nachfolgeregelung versuchen sich Unternehmen derweil für die transatlantische Übermittlung personenbezogener Daten mit den neuen sog. „Standardvertragsklauseln“ zu behelfen, die im Juni 2021 durch die Europäische Kommission veröffentlicht wurden. Allein durch solche vertraglichen Regelwerke, die die datenschutzrechtlichen Pflichten aus der DS-GVO in das Verhältnis zwischen Daten

übermittelnder und empfangender Stelle übertragen, lassen sich die umfassenden Zugriffsbefugnisse auf Cloud Provider nach US-amerikanischem Recht jedoch nicht unterbinden. Zu Recht wird deshalb von verschiedenen Stellen und auch den Datenschutzaufsichtsbehörden in der aktuellen Debatte gefordert, dass mit Blick auf die Datensicherheit zusätzliche technisch-organisatorische Maßnahmen getroffen werden müssen, wozu Anonymisierung, Pseudonymisierung und Transport- sowie Inhaltsverschlüsselung gehören können.

Sicheres Cloud Computing – (k)eine Frage der digitalen Souveränität?

Daran wird deutlich, dass mit Blick auf Datensicherheit und Datenschutz im transnationalen Übermittlungskontext (personenbezogener) Daten nicht nur immer mehr rechtliche Anforderungen existieren, sondern dass diese allein durch die abstrakt gefassten rechtlichen Maßgaben selbst kaum erfüllbar sein dürften. Gleichzeitig können die meisten Unternehmen im Kontext der digitalen Souveränität immer noch nicht bzw. vielleicht sogar immer weniger auf ausländische Diensteanbieter verzichten – eine rechts- und damit compliancekonforme Gestaltung unternehmerischer Datenverarbeitungsvorgänge kommt mithin nicht mehr ohne zusätzliche technisch-organisatorische Gestaltungsmaßnahmen aus. In anderen Worten: Recht geht nicht ohne die entsprechende Technik.

Confidential Computing als rechtlicher Impulsgeber

Für diesen vorgenannten prominenten Anwendungsfall und weitere Szenarien, in denen es auf sichere und datenschutzkonforme Datenverarbeitung in unsicheren Betriebsumgebungen ankommt, könnte das Confidential Computing neue Impulse liefern, um Rechtspflichten in den Bereichen Datensicherheit und Datenschutz angemessen zu erfüllen. Die technische Besonderheit des Confidential Computing liegt darin, dass die Daten auch während der Verarbeitung („date in use“) geschützt werden, indem die Speicher- und Netzwerkverschlüsselung einer exklusiven Kontrolle unterliegt und die Daten während des Verarbeitungsprozesses in einer verschlüsselten Ausführungsumgebung, der sog. „Enklave“, isoliert sind. Die Besonderheit ist somit, dass während einer Datenverarbeitung nicht einmal der (Cloud) Service Provider den Zugang zu den Daten in einer Enklave hat, sondern einzig die CPU zur Laufzeit den Prozess entschlüsselt, ausführt, und wieder verschlüsselt im Speicher ablegt. Zahlreiche Anbieter haben schon entsprechende technische Lösungen auf den Weg gebracht, so auch die Hyperscaler Microsoft, AWS und Google.

Verschlüsselung = Anonymisierung?

Soweit in einer Cloud-Umgebung personenbezogene Daten verarbeitet werden sollen, könnten sich für das Confidential Computing bereits dergestalt rechtliche Besonderheiten ergeben, dass die dort verarbeiteten Daten infolge einer Anonymisierung nicht mehr als personenbezogene Daten gelten und damit nicht mehr dem Anwendungsbereich des europäischen Datenschutzrechts unterfallen. Mit Blick auf das vorangehend skizzierte Szenario der gegenwärtig rechtlich unsicheren Übermittlung personenbezogener Daten in die USA hätte ein solches Ergebnis erhebliche rechtliche Vorteile für Datenverarbeiter.

Dies wäre dann anzunehmen, falls der technische Vorgang der Datenverarbeitung in einer verschlüsselten Enklave mit einer Anonymisierung im Rechtssinne gleichzusetzen wäre. Die damit verbundenen datenschutzrechtlichen Erleichterungen können sich letztlich aber nur dann ergeben, wenn für sämtliche Verarbeitungsschritte inklusive schon der Erhebung der personenbezogenen Daten direkt beim Nutzer/Kunden bis hin zur letztendlichen Löschung/Vernichtung der Daten eine hinreichende technische Verschlüsselung anzunehmen wäre, die einer Anonymisierung im Rechtssinne gleichkommt – was zunächst juristisch umstritten und vom jeweiligen technischen Einzelfall abhängig ist.

Absolute versus relative Theorie

Dabei sollte sich die entsprechende rechtliche Debatte zunächst weniger davon lenken lassen, ob dem absoluten Ansatz (die Zuordnung einer Einzelangabe zu einer konkreten Person ist unmöglich) oder dem mittlerweile vorzugswürdigen relativen Ansatz (die Zuordnung einer Einzelangabe zu einer konkreten Person ist zwar nicht tatsächlich unmöglich, aber nur mit einem unverhältnismäßig großen Aufwand erreichbar: „faktische Anonymität“) zur Beurteilung der Anonymität gefolgt wird. Denn ergab sich bislang bei der Verwendung von Cloud Service Providern an dieser Stelle noch das Problem, dass die eigentliche Datenverarbeitung in der Cloud-Infrastruktur außerhalb der Transportverschlüsselung in unverschlüsselter Form erfolgte, so wird für das Confidential Computing wie beschrieben hingegen ein anderer technischer Ansatz verfolgt, der die Datenverarbeitung in einer gesicherten Umgebung ermöglicht, sodass es von der technischen Architektur her betrachtet für Dritte inklusive des Cloud Services Providers nicht möglich ist, über eine Entschlüsselung der Daten den Personenbezug wiederherzustellen. Dass im Zweifelsfall die durch die Datenverarbeitung betroffene Person in bestimmten technischen Konstellationen selbst die Daten entschlüsseln und damit den Personenbezug herstellen kann, dürfte für die Frage der Anonymität der Daten für den Cloud Service Provider oder weitere Dritte (sowie gegebenenfalls selbst für den Verantwortlichen) hingegen unschädlich sein (vgl. *Spies*, MMR-Aktuell 2011, 313727).

Verschlüsselungsstandard als Gretchenfrage

Der eigentlich entscheidende Aspekt zur Beantwortung der Frage, ob – und falls ja: für wie lange – durch die Verschlüsselung im Rahmen des Confidential Computing eine Anonymisierung im Rechtssinne hergestellt werden kann, betrifft die Stärke des eingesetzten Verschlüsselungsverfahrens und damit verbunden auch den Zeitraum, für welchen die Daten verarbeitet werden sollen und damit die Aufrechterhaltung der Verschlüsselung und eine im faktischen rechtlichen Sinne verstandene Anonymisierung gewährleistet werden kann. Erkenntnis dabei: So, wie generell keine absolute Datensicherheit existiert, ist ebenso wenig von einer hundertprozentig sicheren Verschlüsselungsmethode auszugehen.

Wenn man will, kann man hierin mit Blick auf die rechtliche Frage der Anonymisierung einerseits auch die Schwachstelle des Confidential Computing sehen, das jeweils nur so stark wie das ihm zugrunde gelegte Verschlüsselungsverfahren sein kann. Gemessen an den aktuellen Entwicklungen im Bereich des Quantencomputings dürfte dabei von immer kürzeren Halbwertszeiten mancher noch gängiger Verschlüsselungsverfahren auszugehen sein. Bekannt ist überdies mit Blick auf das Beispiel der transatlantischen Datenübermittlung, dass sich US-

amerikanische Sicherheitsbehörden auch den Zugriff auf zunächst nur verschlüsselt vorliegende Datensätze verschaffen können, um diese sodann zu kopieren und zu einem späteren Zeitpunkt zu entschlüsseln, sollte die technische Machbarkeit gegeben sein. Diese Möglichkeit, von der das Cloud Computing technisch nicht ausgenommen ist, stellt sich neben den Sicherheitsbehörden denknotwendigerweise auch für den Cloud Service Provider.
Andererseits jedoch erkennt heutzutage auch die Rechtswissenschaft mehr und mehr an, dass es im Zeitalter allgegenwärtiger Vernetzung, steigender Leistungsfähigkeit und Computerisierung immer weniger die Garantie für absolute Anonymität gibt (so auch *Hackenberg*, in Handbuch Multimedia-Recht, Teil 15.2 Big Data und Datenschutz, Rn. 53: „Soweit das BDSG von der Vorstellung ausgeht, dass es eine ‚absolute' Anonymisierung gäbe, bleibt diese Vorstellung wohl hinter der technischen Wirklichkeit zurück."; ähnlich auch *Roßnagel*, ZD 2021, 188, 189: „Ein absoluter Ausschluss der Zuordnung ist weder möglich noch erforderlich.") Vielmehr ist, dem relativen Konzept der Anonymität folgend, anhand einer Risikoprognose zu bestimmen, ob die nach der Anonymisierung verbleibenden Daten noch personenbeziehbar sind. Dabei spielt auch das Interesse des Datenverarbeiters mitsamt der von ihm nutzbaren Mittel zur Zuordnung von Einzelpersonen eine Rolle. Maßgeblich wird dabei auf das Verhältnis von Re-Identifizierung und dem dazu erforderlichen Aufwand abgestellt: Dieser muss so unverhältnismäßig sein, dass eine Identifizierung nach allgemeiner Lebenserfahrung oder dem Stand der Wissenschaft und Technik nicht zu erwarten ist. In diese Betrachtung einzubeziehen sind „das vorhandene oder erwerbbare Zusatzwissen des Verantwortlichen, aktuelle und künftige technische Möglichkeiten der Verarbeitung sowie der mögliche Aufwand und die verfügbare Zeit" (*Roßnagel/Geminn*, ZD 2021, 487, 488). Eine weitere rechtliche Besonderheit nach dem relativen Ansatz: Die Anonymisierung gilt bereits dann als ausreichend, „wenn zum Zeitpunkt der Anonymisierung vernünftigerweise ausgeschlossen ist, dass der Verantwortliche mit dem ihm verfügbaren oder absehbar erwerbbaren Zusatzwissen eine Zuordnung der Daten zur betroffenen Person vornehmen kann" (*Roßnagel,* ZD 2021, 188, 191).

Abschied von zeitlich unbegrenzter Anonymisierung
Das relative Konzept zur Beurteilung der Anonymisierung bezieht folglich die zukünftigen technischen Entwicklungen mit ein, um die Frage der Anonymität eines Datums entsprechend rechtlich einzuordnen. Wenn zuvor im Hinblick auf das Confidential Computing folglich festgestellt wurde, dass einerseits eine Schwachstelle des Verfahrens darin zu sehen sein könnte, dass ein bestimmter, hierfür genutzter Verschlüsselungsstandard nach Zeitablauf technisch obsolet wird, könnte andererseits genauso festgestellt werden, dass ein in der Enklave verarbeitetes und verschlüsseltes Datum grundsätzlich rechtlich anonym ist, solange ebenjener Zeitpunkt noch nicht eingetreten ist bzw. sein Eintritt auch nicht absehbar ist. Die Erkenntnis ist somit, dass man sich vom (rechtlichen) Konzept einer absoluten und zeitlich unbegrenzten Anonymität verabschieden muss und in der Praxis auch durchaus kann (wohl für die Anonymität in diesem Sinne auch *Schröder*, ZD 2021, 302, 305).
Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) schlägt argumentativ einen ähnlichen Weg ein, wenn er in seinem „Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche" aus Juni 2020 feststellt, dass für eine Anonymisierung nicht gefordert wird, dass der Personenbezug von

niemandem mehr hergestellt werden kann. Ausreichend sei in der Regel, dass eine Re-Identifizierung praktisch nicht durchführbar ist. Bei anonymen Daten sei die Wiederherstellung des Personenbezugs für jedermann zumindest praktisch unmöglich. Es bleibt nach Auffassung des BfDI aber die Aufgabe des Verantwortlichen, die Überprüfung der Anonymisierung auf ihre Validität fortwährend durchzuführen. Dies wird entsprechend durch die Datenschutzaufsicht überwacht.

Zurück von der Kür zur Pflicht: flankierende technische und organisatorische Maßnahmen (TOM)

Was bedeutet das nun konkret für die Umsetzung von Anonymisierung im Rechtssinne für das Confidential Computing? Zunächst liegen die rechtlichen Vorteile der Anonymisierung personenbezogener Daten auf der Hand: Daten, die auf diese Weise nicht mehr dem Datenschutzrecht unterliegen, können frei(er) verarbeitet und auch in das außereuropäische Ausland übermittelt werden. Dadurch können nicht nur Kosten für aufwändige unternehmerische Compliance-Prozesse gesenkt, sondern im Zweifelsfall auch neue, datengetriebene Geschäftsmodelle entwickelt werden, so auch mit Blick auf den Einsatz künstlicher Intelligenz oder Data Warehousing als im datenschutzrechtlichen Sinne besonders risikoträchtige Verarbeitungstechnologien.

Trotz der zunächst einmal rechtlich feststellbaren Anonymität der Daten ist das Unternehmen jedoch nicht von allen Pflichten befreit: So schützt das Datenschutzrecht auch vor der De-Anonymisierung, die vorliegend durch Zeitablauf wie festgestellt durchaus eintreten kann. Aus dieser Tatsache erwächst die Pflicht des Unternehmens, zum einen vor der Verwendung eines bestimmten Verschlüsselungsverfahrens im Confidential Computing zu prüfen, ob dieses zum Zeitpunkt seines Einsatzes hinreichend sicher ist und zum anderen regelmäßig festzustellen, ob sich außerordentliche Umstände ergeben haben, die eine andere technische Wertung rechtfertigen. Denkbar ist außerdem, anhand von technischen Empfehlungen oder Richtlinien automatisiert festzulegen, ab welchem Zeitpunkt ein faktisch anonymisiertes Datum durch Zeitablauf nicht mehr als rechtlich anonym anzusehen ist und dann beispielsweise automatisch gelöscht wird. Für das Risiko einer De-Anonymisierung ist überdies allgemein einzubeziehen, dass ein Datum durch zunehmende Verwendung, d.h. durch seine Verbreitung/Übermittlung an Dritte und in Kombination mit zahlreichen weiteren Daten wieder zu einem personenbezogenen Datum werden kann. Somit muss sich ein Unternehmen auch im Rahmen der Verwendung von Confidential Computing im beschriebenen Sinne die Risiken und Rechtsfolgen einer De-Anonymisierung stets vor Augen führen und das tatsächliche Vorliegen der Anonymität ist mit Blick auf neue technische Mittel fortwährend zu überprüfen.

Vorzuschlagen ist außerdem, dass technisch-organisatorische Vorsorgeregelungen zum unternehmerischen Umgang mit anonymisierten Daten zu treffen sind. Diskutiert werden u.a. folgende Maßnahmen (so in Teilen *Roßnagel/Geminn*, ZD 2021, 487, 489 f.):

- Klare Regelungen zu Verfahren und Anforderungen der Anonymisierung
- Beschränkung der Weitergabe und Weiterverarbeitung
- Beschränkung der Zwecke einer Datenverwendung (Zweckbindung)
- Formulierung von Transparenzvorschriften zum Umgang mit anonymisierten Daten
- (Automatische) Löschung von anonymisierten Daten, wenn sie nicht mehr benötigt werden, um den künftigen Möglichkeiten der De-Anonymisierung vorzubeugen

Literatur:

- *Spies, Axel*: Cloud Computing: Keine personenbezogenen Daten bei Verschlüsselung, MMR-Aktuell 2011, 313727
- *Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd* (Hrsg.): Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, 57. EL September 2021
- *Roßnagel, Alexander*: Datenlöschung und Anonymisierung – Verhältnis der beiden Datenschutzinstrumente nach DS-GVO, ZD 2021, 188
- *Roßnagel, Alexander/Geminn, Christian L.*: Vertrauen in Anonymisierung – Regulierung der Anonymisierung zur Förderung Künstlicher Intelligenz, ZD 2021, 487
- *Schröder, Meinhard*: Datenschutz beim Kameraeinsatz im Automobil – Personenbezug bei Daten von Dashcams & Co., ZD 2021, 302
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI): Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche (Stand: 29. Juni 2020), abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf