AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

www.austrian-law-journal.at
DOI: 10.25364/01.10:2023.1.1.

Offenlegung von Daten unter Wahrung der Privatsphäre mittels SMPC (Secure Multiparty Computation)

Privacy-preserving disclosure of data via SMPC (Secure Multiparty Computation)

David Bierbauer (Autor) und Lukas Helminger (Co-Autor)

Zusammenfassung: Dieser Beitrag stellt das Konzept „Secure Multiparty Computation" (SMPC) als Möglichkeit zur sicheren Verarbeitung von Datensätzen aus unterschiedlichen Quellen vor, bei der Daten gegenüber anderen Verarbeitungsparteien nicht offengelegt werden müssen.

Nach einem kurzen technischen Aufriss mit Hintergrundinformationen zu den technischen Sicherheitsgarantien wird insbesondere der Frage nachgegangen, wie sich die Verarbeitung personenbezogener Daten in SMPC-Umgebungen in das System des Datenschutzrechts eingliedert. Es wird gezeigt, dass die DS-GVO zwar grundsätzlich auf alle personenbezogenen Daten, die zum Zweck einer Ziel-Berechnung mittels SMPC aufbereitet und verschlüsselt werden, Anwendung findet, jedoch die Daten nicht für alle beteiligten Verarbeitungsparteien als personenbezogen zu qualifizieren sind. Daraus ergeben sich gewichtige Datenschutzgarantien, die bei der Beurteilung der Zweckkompatibilität sowie bei Interessenabwägungen zur Rechtmäßigkeit der Verarbeitung nach Art 6 Abs 1 lit f DS-GVO zu berücksichtigen sind. Weiters werden (rechtliche) Möglichkeiten für grundrechtsschonende Datenverarbeitungen im staatlichen Bereich am Beispiel der österreichischen „Strompreisbremse" aufgezeigt.

Im Ergebnis können mithilfe von SMPC auch Verarbeitungen zwischen Parteien vorgenommen werden, die sich gegenseitig nicht vertrauen oder ihre Datenbestände aus Wettbewerbs- bzw Geheimnisschutzerwägungen nicht miteinander teilen möchten. In diesem Sinne vermag die Technologie die beiden der DS-GVO eingeschriebenen, jedoch scheinbar antagonistisch ausgerichteten Ziele „Datenschutz" sowie „Freier Datenverkehr" jeweils zu fördern und eignet sich so zur datenminimierenden und grundrechtsschonenden Verarbeitung personenbezogener Daten.

Keywords: Personenbezug, Pseudonymisierung, Verschlüsselung, risikobasierter Ansatz, Freier Datenverkehr, Strompreisbremse

Abstract: This paper introduces the concept of „Secure Multiparty Computation" as a way to securely process data sets from different sources without having to disclose data to other processing parties.

After a brief outline with background information on the technical security guarantees, the paper will focus on the question of how the processing of personal data in SMPC environments fits into the system of data protection law. It is shown that the GDPR applies in principle to all personal data that are processed and encrypted for the purpose of a target calculation by means of SMPC, but that the data are not to be qualified as personal for all processing parties involved. These resulting data protection guarantees must be taken into account when assessing the compatibility of purposes and when balancing interests for the lawfulness of processing under Art 6(1)(f) GDPR. Furthermore, (legal) options for data processing in the public sector that safeguard fundamental rights are shown using the example of the Austrian „electricity price brake".

In conclusion, SMPC can be used for data processing between parties who do not trust each other or do not want to share their data for reasons of competition or confidentiality. In this sense, the technology is able to promote the two antagonistic goals of „data protection" and „free movement of data" inscribed in the GDPR and is suitable for processing personal data in a way that minimises data and protects fundamental rights.

Keywords: Personal data, pseudonymisation, encryption, risk-based approach, free movement of data, electricity price brake

Inhaltsverzeichnis

1. Einleitung

Datenschutzrecht wird in der Praxis oft als Gebiet wahrgenommen, das Dinge „kompliziert" macht oder „verhindert".[1] Vor allem dann, wenn Jurist:innen mit erhobenem Finger auf einschlägige Bestimmungen der DS-GVO[2] hinweisen oder vehement vertreten, dass eine bestimmte Projektidee in der jeweiligen Form „rechtlich nicht möglich" sei; der „Schutz natürlicher Personen" bei der Verarbeitung von personenbezogenen Daten darf schließlich nicht unterlaufen werden.

Weniger bekannt ist, dass die DS-GVO neben dem Schutz natürlicher Personen auch den freien Datenverkehr verfolgt, und dieses (zweite) Schutzziel explizit im Verordnungstitel anspricht.[3] Obwohl dieses Normziel historisch vor allem kompetenzrechtliche Gründe bei der Gesetzgebung zur Datenschutzrichtlinie[4] hatte und als klarer Rekurs auf das Binnenmarktprinzip zu verstehen war, hat sich der Unionsgesetzgeber dafür entschieden, den freien Datenverkehr als Schutzziel bei der Fassung von Art 16 Abs 2 AEUV[5] sowie auch der DS-GVO explizit aufzunehmen.[6] Diese beiden Schutzziele der DS-GVO sind insofern als Abwägungshinweis zur Auflösung eines dahinterliegenden multipolaren Grundrechtskonflikts zu verstehen, dem nicht bloß durch die Harmonisierung des Datenschutzes in der Union genügt werden kann.[7]

In Art 1 Abs 3 DS-GVO heißt es explizit: *„Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden"*.[8] Und dennoch gaben 2020 in einer repräsentativen Umfrage etwa 56 %

[1] So etwa *Bitkom,* Jedes 2. Unternehmen verzichtet aus Datenschutzgründen auf Innovationen, 29.09.2020, <bitkom.org/Presse/Presseinformation/Jedes-2-Unternehmen-verzichtet-aus-Datenschutzgruenden-auf-Innovationen> (abgerufen am 22.11.2022); Grundlage für die Veröffentlichung war eine 2020 durchgeführte Umfrage von *Bitkom Research* in Deutschland, bei der 504 für Datenschutz verantwortliche Personen (Betriebliche Datenschutzbeauftragte, Geschäftsführerinnen, IT-Leiter) von Unternehmen aller Branchen ab 20 Mitarbeiter:innen telefonisch befragt wurden.

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1 idF ABl L 2021/74, 35.

[3] „Verordnung […] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten [und] zum freien Datenverkehr"; vgl Volltitel oben.

[4] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31 idF L 2003/284, 1.

[5] Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13. Dezember 2007, ABl C 2007/307, 51.

[6] Vgl etwa *Sydow* in *Sydow/Marsch* (Hrsg), DS-GVO[3] (2022) Art 1 Rz 16.

[7] In diesem Sinne auch Einführung *Kühling/Raab* in *Kühling/Buchner* (Hrsg), DS-GVO[3] (2020) 3; aA jedoch *Sydow* in *Sydow/Marsch*, DS- GVO[3] Art 1 Rz 16.

[8] Vgl zur Entstehungsgeschichte auch *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU (2017) Teil 1 Rz 6.

aller Unternehmen an, dass innovative Projekte in ihrem Unternehmen aufgrund der DS-GVO gescheitert wären.[9]

Die gleichzeitige Verwirklichung der Ziele „Datenschutz" und „freier Datenverkehr" gestaltet sich in der Rechtsanwendung damit diffizil. Dies ist vor dem Hintergrund, dass sich die zugrundeliegenden Interessen zumindest prima facie konträr gegenüberstehen, auch nicht verwunderlich. Zum Interessenausgleich zwischen diesen Schutzzielen und zur Minimierung der Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten, haben sich daher verschiedene Verfahren und Strategien für einen freien Datenverkehr unter möglichst datenschutzfreundlichen Bedingungen entwickelt. Hierbei werden Verfahren zur Anonymisierung[10] oft als „Allheilmittel" angepriesen, obwohl der Personenbezug idR nicht (vollständig) entfernt wird und darüber hinaus durch das Entfernen von identifizierenden Elementen wertvolle Informationen in den Daten verloren gehen. Die Verarbeitung von anonymisierten Daten verringert in der Folge vielfach die Qualität der entwickelten Software[11] und kann deren Fehleranfälligkeit erhöhen.[12] Damit stellt die „klassische" Anonymisierung sowohl für Entwickler als auch für Betroffene ein nicht vollends zufriedenstellendes Verfahren dar.

Tatsächlich gibt es aber neben der Anonymisierung eine Reihe von Möglichkeiten, wie die gegenläufigen Schutzinteressen der DS-GVO unter Einsatz von technischen Werkzeugen beiderseits befriedigt werden können, ohne die Qualität der Daten zu verringern. Hierbei lässt sich rund um sog „Privacy Enhancing Technologies (PETs)"[13] eine hohe Forschungsaktivität beobachten. Wobei vor allem Methoden, die mittels technischer Verfahren die Notwendigkeit verringern, anderen Verarbeitungsparteien gutgläubig vertrauen zu müssen, besondere Aufmerksamkeit erfahren.

Dieser Beitrag stellt das Konzept „Secure Multiparty Computation" als PET mit der Möglichkeit zur sicheren Verarbeitung von Datensätzen aus unterschiedlichen Quellen vor, bei der Daten gegenüber anderen Verarbeitungsparteien nicht

---

[9] *Bitkom Research*, Unternehmen ab 20 Mitarbeiter:innen n=504 (2020); als häufigster Grund für das Scheitern konkreter Projektideen wurden „Unklarheiten im Umgang mit den Vorgaben der DS-GVO" genannt; gefolgt von „Aufgrund konkreter Vorgaben der DS-GVO".

[10] Vgl für eine allgemeine Einführung zu Anonymisierung etwa *Art-29-Datenschutzgruppe*, WP 216, Opinion 05/2014 on Anonymisation Techniques; *Sonntag*, Technische Grenzen der Anonymisierung, jusIT 2018, 137.

[11] Wie etwa bei Training von Modellen zur Entwicklung von KI-Systemen.

[12] Vgl etwa *Bierbauer*, Datenschutzrechtliche Grundsätze bei der Entwicklung Künstlicher Intelligenz, in *Jahnel* (Hrsg), Datenschutzrecht. Jahrbuch 2021 (2022) 194.

[13] *OECD*, Emerging privacy-enhancing technologies: Current regulatory and policy approaches, OECD Digital Economy Papers 2023, 351.

offengelegt werden und kein Informationsverlust in den Daten (wie etwa durch Anonymisierung) hingenommen werden muss.

2. Technische Grundlagen von SMPC

Secure Multiparty Computation (SMPC) ist ein Teilgebiet der Kryptographie, deren Wurzeln auf die 1980er Jahre datieren.[14] Das innovative Potenzial der Technologie liegt darin, dass die verarbeiteten Daten nicht nur während der Speicherung (at rest) und des Versendens (in transit), sondern auch während der Verarbeitung (in use) durch Verschlüsselung geschützt werden.

Anfänglich wegen der hohen Rechen- und Kommunikationsanforderung noch ein rein theoretisches Konzept, hat SMPC im letzten Jahrzehnt stark an Popularität gewonnen. So wurde SMPC mittlerweile in vielen Anwendungen eingesetzt: Von Registerdaten[15]-und medizinischer Forschung[16] über maschinelles Lernen unter Wahrung der Privatsphäre[17] und Bekämpfung von Geldwäsche[18] bis hin zu digitaler Schlüsselverwaltung und Signierung.[19] In diesem Abschnitt soll SMPC als Technologie in ihren Grundzügen dargestellt werden; wobei insbesondere auf jene Eigenschaften eingegangen wird, die für die rechtliche Einordnung der Technologie von Relevanz sind.[20]

2.1. Abgrenzung und Innovationspotenzial

Unter dem Begriff „Berechnung" (alternativ auch „Algorithmus" oder „Analyse") wird eine Prozedur verstanden, die bestimmte Eingabedaten in eine Ausgabe umwandelt.

---

[14] *Yao*, Protocols for secure computations, 23rd annual symposium on foundations of computer science, IEEE 1982, 160-164.
[15] *Bogdanov/Kamm/Kubo/Rebane/Sokk/Talviste*, Students and Taxes: A Privacy-Preserving Study Using Secure Computation, Proc. Priv. Enhancing Technol. 2016, 117-135.
[16] *Scheibner/Raisaro/Troncoso-Pastoriza/Ienca/Fellay/Vayena/Hubaux*, Revolutionizing medical data sharing using advanced privacy-enhancing technologies: technical, legal, and ethical synthesis, Vol. 32 Journal of medical Internet research 2021, e25120.
[17] *Mohassel/Zhang*, Secureml: A system for scalable privacy-preserving machine learning, symposium on security and privacy, IEEE 2017, 19-38.
[18] *Maxwell*, Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime' Future of Financial Intelligence Sharing (FFIS) research programme, Version 1.0 (2020).
[19] *Archer/Bogdanov/Lindell/Kamm/Nielsen/Pagter/Wright*, From keys to databases—real-world applications of secure multi-party computation, Vol. 61 The Computer Journal 2018, 1749-1771.
[20] Für eine rigoros technische Einführung siehe *Cramer/Damgård*, Secure multiparty computation, Cambridge University Press 2015, 2 f.

SMPC ist eine spezielle Berechnung, die es mehreren Parteien ermöglicht, Auswertungen an Eingabedaten durchzuführen, ohne die jeweiligen Daten gegenüber den anderen Parteien offenzulegen. Die daraus resultierenden Datenschutzgarantien lassen sich am besten anhand des folgenden Gedankenexperiments verdeutlichen:

Man stelle sich eine ideale Welt vor, in der es eine vollkommen vertrauenswürdige dritte Partei gibt. Wollen zwei oder mehrere Parteien, die sich gegenseitig nicht vertrauen, ihre Daten im Verbund analysieren, so können sie die Daten an die vertrauenswürdige dritte Partei senden. Diese Partei führt dann die gewünschte Analyse auf den zusammengeführten Daten durch und sendet das Ergebnis an die Parteien zurück. Da die vertrauenswürdige Drittpartei nicht korrumpiert werden kann, erfahren die Parteien nur das Ergebnis der Berechnung, erhalten aber keine Information über die Eingabedaten der anderen Parteien.

SMPC bildet die Funktionalität einer solchen fiktiven, vertrauenswürdigen dritten Partei in der realen Welt durch kryptographische Methoden nach.[21] In SMPC-Umgebungen werden alle Eingabedaten umfassend durch Verschlüsselung geschützt und es gibt keine Möglichkeit für Dritte diese Daten einzusehen; auch nicht für Parteien, die selbst an der SMPC-Berechnung partizipieren.

2.2. Beispiel: Schnittmengenberechnung

Angenommen zwei Organisationen (A und B) haben das Ziel, jene Personen zu ermitteln, die in den Datenbeständen ihrer beiden Organisationen gespeichert sind, ohne ihre Daten untereinander oder mit einer sonstigen dritten Partei teilen zu müssen.[22] Im Rahmen einer SMPC-Umgebung können sie diese prima facie und mit traditionellen Mitteln tatsächlich unmögliche Berechnung vornehmen: Hierzu führen sie eine „private Schnittmengenberechnung"[23] ihrer Datenbestände durch und erhalten als Ergebnis, welche Personen sowohl in dem Datenbestand von Organisation A als auch in dem Datenbestand von Organisation B aufscheinen; sie haben jedoch keine Möglichkeit, die Daten der anderen Partei einzusehen.[24]

[21] *Evans/Kolesnikov/Rosulek*, A pragmatic introduction to secure multiparty computation. Foundations and Trends in Privacy and Security (2017) 19-20.
[22] Zum Beispiel für den Zweck eines Abgleichs von Verdächtigen oder das Eruieren gemeinsamer Kunden.
[23] Englisch auch „private set intersection (PSI)".
[24] *De Cristofaro/Tsudik*, Practical private set intersection protocols with linear complexity, Financial Cryptography and Data Security: 14th International Conference, FC 2010, 143-159.

Anstatt die Daten an eine vertrauenswürdige dritte Partei zu senden, verschlüsselt ein SMPC-Protokoll beide Datenbestände und führt anschließend die Berechnung der Schnittmenge auf den verschlüsselten Datenfragmenten durch. Daher ist die Eingabe jedes Datensatzes (Name einer Person) geschützt und kann von der anderen Partei nicht abgerufen werden. Nach Durchführung des SMPC-Protokolls erhalten beide Organisationen eine Liste von Namen, in der ausschließlich jene Personen vorkommen, die in beiden Datenbeständen enthalten sind, sie erfahren jedoch nichts über andere Personen (siehe Abbildung 1).

Der Umstand, dass die Eingabedaten während der gesamten Daten-Übermittlung und Berechnung geschützt sind, gilt für jedes SMPC-Protokoll und ist für die Einordnung der Technologie in das System des Datenschutzrechts wesentlich.

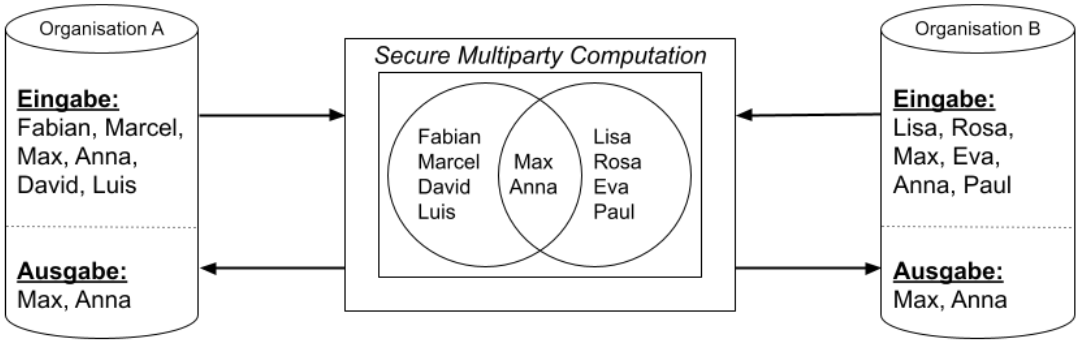

Abbildung 1: Schnittmengenberechnung mithilfe von SMPC

Organisation A und B vergleichen mithilfe von SMPC ihre Datenbestände, bestehend aus jeweils sechs Vornamen (Eingabe). Das Rechteck in der Mitte stellt rein symbolisch die SMPC Berechnung dar. Das Resultat der Berechnung (Ausgabe) ist die Schnittmenge der beiden Datenbestände (Max, Anna).

2.3. Sicherheitsmodelle

Bevor auf die konkrete Datensicherheit von SMPC eingegangen werden kann, sollen die unterschiedlichen Schutzhöhen von SMPC-Modellen kurz vorgestellt werden.
Die im Rahmen eines technischen SMPC-Protokolls[25] erzielte Schutzhöhe gibt an, gegen welche Art von Angreifern die in das Protokoll eingeführten Daten geschützt sind. Sowohl die Fähigkeit eines Angreifers zur Manipulation des Protokolls, als auch die Möglichkeit, dass mehrere Parteien in einer schädlichen Art und Weise zusammenarbeiten (Konspiration) müssen hierbei berücksichtigt werden.

[25] Unter Protokoll werden die im Rahmen von SMPC durchgeführten technischen Abläufe verstanden.

Das Spektrum von Sicherheitsmodellen ist breit und reicht von passiv-sicher (honest-but-curios) bis hin zu aktiv-sicher (malicious). Bei passiv-sicheren Protokollen ist die Sicherheit solange gewährleistet, wie sich jede Partei an das technische Protokoll hält.[26] Hingegen bleiben die Eingabedaten beim aktiv-sicheren Modell auch dann geschützt, wenn Parteien vom Protokoll abweichen.[27] Diese beiden Modelle stellen jedoch bloß das jeweilige Ende des Sicherheitsspektrums dar, das von passiv- bis aktiv-sicher reicht. Innerhalb dieses Spektrums gibt es noch weitere Sicherheits-Abstufungen mit dazugehörigen Modellen.[28]

Zusätzlich zur Art des Angreifers unterscheiden sich SMPC-Protokolle auch in ihrer Robustheit gegen Konspirationen, dh wie viele Parteien (protokollwidrig)[29] Eingabe- und Protokolldaten untereinander austauschen müssten, um Daten anderer Parteien zu erlangen. SMPC-Protokolle können so konzipiert werden, dass die Daten einer ehrlichen Partei auch dann sicher sind, wenn alle anderen Parteien sich gegen die ehrliche Partei zusammenschließen.[30] Erhöhte Sicherheitsgarantien erfordern allerdings stets auch erhöhten Rechen- und Kommunikationsaufwand für alle teilnehmenden Parteien und sind daher nicht in jeder Verarbeitungssituation umsetzbar bzw praktikabel.

Bei der Konzeption von SMPC-Umgebungen stellt sich daher häufig die Frage welche Schutzhöhe im konkreten Fall gefordert ist, bzw welches Sicherheitsmodell angewendet werden sollte. Hierzu kann festgehalten werden, dass SMPC-Protokolle mit sehr hohen Schutzeigenschaften (aktiv-sicher und sicher gegen Konspiration) idR sehr komplex sind und einen erheblichen Ressourcenaufwand erzeugen. Daher muss das Sicherheitsmodell im Einzelfall unter Berücksichtigung der Kosten, dem Verhältnis der teilnehmenden Parteien zueinander sowie der Eintrittswahrscheinlichkeit und Schwere einer möglichen Datenschutzverletzung gewählt werden. Bei dieser Abwägung können auch organisatorische Maßnahmen, wie etwa die (protokollwidrige) Zusammenarbeit von zwei Parteien explizit unter Vertragsstrafe zu stellen, einfließen.

---

[26] *Smart*, Cryptography made simple (2016) 439.
[27] *Smart*, Cryptography 440.
[28] Zum Beispiel „Covert Security", das mit einer gewissen Wahrscheinlichkeit garantiert einen aktiven Angriff abzuwehren. Dieses Sicherheitsmodell eignet sich gut für Anwendungen, die sehr oft durchgeführt werden und gewährleisten somit, einen Angreifer tatsächlich zu entdecken.
[29] Protokollwidrig bedeutet, dass von den technisch vorgegebenen Abläufen abgewichen wird; zB durch Manipulierung der Software.
[30] *Smart*, Cryptography 440.

2.4. Funktionsweise der Ziel-Berechnung

Es gibt zwei weit verbreitete Methoden, um SMPC-Berechnungen zu realisieren: Secret Sharing[31] und Garbled Circuits[32]. Letztere werden bevorzugt für Berechnungen zwischen zwei Parteien angewendet, wobei die Ziel-Berechnung durch einen sog „Boolean-Circuit"[33] angegeben werden muss und oft sehr komplex und schwer skalierbar ist. Die am häufigsten eingesetzte Methode ist daher mittlerweile das sog „Secret Sharing". Diese Methode kann grob in vier Phasen eingeteilt werden und soll hier kurz skizziert werden. Zur besseren Lesbarkeit ist die folgende Beschreibung der Funktionsweise von Secret Sharing für eine Drei-Parteien-Umgebung ausgeführt.[34]

1. Erzeugung: Jede Partei teilt ihre Eingabedaten (zB personenbezogene Daten) in drei Fragmente (Secret Shares) auf. Für sich genommen stellen diese Drittel-Fragmente keine verwertbaren Informationen dar. Erst das Zusammenfügen aller drei Fragmente ermöglicht die Wiederherstellung der ursprünglichen Daten.

2. Verteilung: Jede Partei sendet jeweils ein Drittel-Fragment an die anderen zwei Parteien. Somit hat jede Partei drei Fragmente (ein Fragment jeder teilnehmenden Partei). Indem sich jede Partei ein Fragment ihrer Eingabedaten selbst behält, stellt sie sicher, dass ihre Eingabedaten nicht ohne ihr Mitwirken wiederhergestellt werden können.

3. Ziel-Berechnung: Jede Partei führt die notwendigen mathematischen Operationen für die Ziel-Berechnung auf den ihr bekannten Fragmenten durch. Diese veränderten Fragmente enthalten für sich genommen keine verwertbaren Informationen.

4. Rekonstruktion: Die Parteien senden sich gegenseitig die veränderten Fragmente; somit besitzt jede Partei nun wieder alle veränderten Fragmente. Durch das Zusammenfügen der Fragmente erhalten die Parteien das Ergebnis der Ziel-Berechnung.

---

[31] *Shamir*, How to share a secret, Vol. 22 Communications of the ACM 1979, 612-613.
[32] *Yao*, How to generate and exchange secrets. 27th annual symposium on foundations of computer science 1986, IEEE, 162-167.
[33] *Yao*, IEEE, 162-167.
[34] Es besteht jedoch kein konzeptioneller Unterschied der Funktionsweise bei einer anderen Anzahl an Parteien.

Durch die hier beschriebene Vorgehensweise lassen sich etwa Schnittmengen-, Summen- oder Durchschnittsberechnungen durchführen.[35] Aber auch komplexe Berechnungen wie etwa das Trainieren von KI-Modellen sind mittels Secret Sharing möglich. Diese Berechnungen folgen methodisch grundsätzlich demselben Konzept, erfordern allerdings zusätzliche Schritte, weshalb sie hier aus Platzgründen nicht angeführt werden sollen.[36]

2.5. Technische Datensicherheit

Die theoretische Sicherheit des Konzepts SMPC wurde bereits in den 1980er Jahren bewiesen.[37] Die praktische Umsetzung der Protokolle konnte aufgrund der technischen Entwicklungen im Bereich von Verschlüsselungsalgorithmen und Rechenkapazitäten allerdings erst später realisiert werden. Bei der Entwicklung von SMPC-Umgebungen werden in der Regel symmetrische[38], asymmetrische[39] und SMPC spezifische kryptographische Methoden (wie Secret Sharing oder Garbled Circuits) eingesetzt. Nach aktuellem Stand der Technik werden die Sicherheitsparameter von SMPC-Umgebungen üblicherweise so gewählt, dass sie der Sicherheit von TLS 1.3 entsprechen.[40] Es ist gängige Praxis, die Datensicherheit von neu entwickelten SMPC-Protokollen mathematisch zu beweisen und durch ein Peer-Review zu validieren.[41] Für die praktische Umsetzung ist darauf hinzuweisen, dass die sichere Implementierung von SMPC heutzutage noch mehrjährige Erfahrung im Bereich der Kryptographie erfordert. Durch die Bestrebungen SMPC zu standardisieren[42] ist mittelfristig davon auszugehen, dass die korrekte Nutzung dieser Technologie stark erleichtert und in weiterer Folge auch häufiger Anwendung finden wird.

---

[35] Eine anschauliche Erklärung von Secret Sharing ist auf dem Youtube-Kanal des EU-Horizon 2020 Projekts Safe-DEED, https://www.youtube.com/watch?v=90jcXCHsBF0 (abgerufen am 24.3.2022).

[36] Vgl hierzu etwa *Damgård/Pastro/Smart/Zakarias*, Multiparty computation from somewhat homomorphic encryption, CRYPTO, 2012, 643-662.

[37] *Goldreich/Micali/Wigderson,* How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority, Symposium on Theory of Computing 1987.

[38] Das verbreitetste symmetrische Verschlüsselungsverfahren ist AES: *Daemen/Rijmen,* AES proposal: Rijndael (1999).

[39] Die bekanntesten Verfahren sind RSA- und Elliptische Kurven-Verschlüsselung. Beide werden zum Verschlüsseln und Signieren im Internet verwendet.

[40] TLS steht für Transort Layer Security und ist das am häufigsten verwendete Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet (kommt zum Beispiel bei HTTPS zum Einsatz).

[41] *Asharov/Lindell*, A full proof of the BGW protocol for perfectly secure multiparty computation, Vol. 30 Journal of Cryptology 2017, 58-151.

[42] International Organization for Standardization (ISO), Secure multiparty computation, ISO/IEC DIS 4922-1, (under development 2020); sowie Institute of Electrical and Electronics Engineers, IEEE Recommended Practice for Secure Multi-Party Computation, IEEE 2842-2021 (2021).

3. SMPC im System des Datenschutzrechts

Als eines der wesentlichsten Probleme bei der rechtlichen Einordnung von SMPC gestaltet sich die Frage, in welchem Umfang die DS-GVO auf Berechnungen mittels dieser kryptographischen Technologie überhaupt Anwendung findet.[43] Dass diese Frage nicht einfach beantwortet werden kann, ist dem Umstand geschuldet, dass der Anwendungsbereich des Datenschutzrechts seit langem umfehdeter Gegenstand wissenschaftlicher Debatten ist. Diese Situation erscheint unbefriedigend, zumal die Frage, ob ein Gesetz Anwendung findet, aus dem Aspekt der Rechtssicherheit klar beantwortbar sein sollte.

In vielen alltäglichen Verarbeitungssituationen ist der Anwendungsbereich des Datenschutzrechts relativ eindeutig abgrenzbar.[44] Probleme ergeben sich allerdings dann, wenn besondere Verarbeitungssituationen vorliegen oder innovative Technologien Anwendung finden. Die Schwierigkeit bei der Einordnung von SMPC liegt insbesondere darin, dass Daten zuerst von den beteiligten Parteien einzeln verschlüsselt und diese verschlüsselten Daten anschließend von mehreren Parteien gemeinsam für Berechnungen verarbeitet werden:

Ohne an dieser Stelle erneut auf im Einzelfall Anwendung findende Algorithmen[45] einzugehen, folgt SMPC konzeptionell vereinfacht stets den Schritten
(i.) Verschlüsselung der Eingabedaten
(ii.) Zusammenführung der verschlüsselten Daten;
(iii.) Durchführung der jeweiligen Ziel-Berechnung auf den zusammengeführten verschlüsselten Datenfragmenten;
(iv.) Übermittlung des Berechnungsergebnisses an die beteiligten Verarbeitungsparteien, wobei die Ergebnis-Offenlegung auch nur einzelnen Parteien vorbehalten sein kann.

Durch diese Ausgangslage ist prima facie nicht klar, ob bzw gegenüber welchen Parteien die verarbeiteten Daten als personenbezogen zu qualifizieren sind und in welchem Umfang der Anwendungsbereich der DS-GVO auf die Verarbeitung eröffnet

[43] *Schur*, Know-how- und Geheimnisschutz von Daten, in *Leupold/Wiebe/Glossner* (Hrsg), IT-Recht[4] (2021) 6.8. Rz 49.
[44] Man denke etwa an Datenverarbeitung im Rahmen von in Anspruch genommenen Dienstleistungen oder durch Arbeitgeber:innen.
[45] Vgl Garbled Circuits sowie Secret Sharing zuvor in 2.4. „Funktionsweise der Ziel-Berechnung".

wird. Im folgenden Teil wird daher insbesondere der Frage nachgegangen, wie sich die oben skizzierten Verarbeitungsschritte auf die Beurteilung des Personenbezugs auswirken. Hierzu werden in einem ersten Schritt allgemeine Erwägungen zur Beurteilung des Personenbezugs angestrengt, um anschließend die mittels SMPC durchgeführten Verarbeitungen in den Anwendungsbereich der DS-GVO einzuordnen. Darüber hinaus soll kursorisch auf weiterführende Rechtsfolgen und Möglichkeiten wie etwa auf das Prinzip „Data Protection by Design", den Grundsatz der Zweckvereinbarkeit sowie auf allfällige Rechtmäßigkeitstatbestände für die Verarbeitung eingegangen werden.

3.1. Anwendungsbereich der DS-GVO

Wie erwähnt, gewährleistet das Datenschutzrecht den Schutz natürlicher Personen bei der Verarbeitung sie betreffender personenbezogener Daten.[46] Dementsprechend grenzt die DS-GVO in Art 2 Abs 1 ihren Anwendungsbereich auf die *„ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten"* ein.[47] Wobei der in Art 4 Z 2 DS-GVO legaldefinierte Begriff der *„Verarbeitung"* nach hA extensiv interpretiert wird und de facto jeden Vorgang im Zusammenhang mit personenbezogenen Daten erfasst.[48] Damit bleibt als Schlüsselfrage für die Anwendbarkeit der DS-GVO, was unter den Begriff „personenbezogene Daten" fällt und wie diese Informationen von anderen Daten abzuheben sind.

3.2. Personenbezogene Daten

Nicht alle Daten unterliegen dem Regime der DS-GVO, sondern nur sog „personenbezogene Daten". Darunter fallen gem Art 4 Z 1 DS-GVO *„alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen"*. Diese Legaldefinition stellt eine abwägungsfeindliche Formel auf, welche die in casu concretu betreffende Information entweder vollständig oder gar nicht erfasst.[49] Auf den Aussagegehalt oder persönlichkeitsrechtliche Implikationen der Information

[46] So vermittelt das einfachgesetzlich bzw sekundärrechtliche Datenschutzrecht vielfach die grundrechtlich verbürgten Positionen von Art 16 Abs 1 AEUV, Art 8 GRC sowie Art 8 EMRK.
[47] Daneben ist die DS-GVO gem Art 2 Abs 1 HS 2 auch auf die „nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen" anwendbar.
[48] Vgl statt vieler *Herbst* in *Kühling/Buchner* (Hrsg), DS-GVO[3] (2020) Art 4 Z 2 Rz 4.
[49] Vgl „binäre Natur des Personenbezugs" *Karg* in *Simitis/Hornung/Spiecker* (Hrsg), DS-GVO (2019) Art 4 Z 1 Rz 14; dagegen etwa *Haase*, Datenschutzrechtliche Fragen des Personenbezugs (2015) 103.

kommt es nicht an.[50] So hielt auch das dBVerfG in einer - für die Entwicklung des europäischen Datenschutzrechts maßgeblichen - Entscheidung fest, dass es im Kontext der automatisierten Datenverarbeitung *„keine belanglosen Daten"* gebe.[51] „Alle Informationen" ist daher weit zu verstehen und verlangt keine inhaltlichen Anforderungen.[52]

Um festzustellen, ob sich die Informationen auf *„eine identifizierte oder identifizierbare Person beziehen"*, sind nach ErwGr 26 alle Mittel zu berücksichtigen, die vom Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden. Hierbei sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Bei der Beurteilung der Identifizierbarkeit ist damit im Ergebnis eine Risikoanalyse vorzunehmen, in deren Rahmen die Wahrscheinlichkeit einer Identifizierung objektiv evaluiert wird.[53] Ob bzw in welchem Ausmaß auch das Wissen und die Mittel von Dritten in diese Evaluierung einfließen sollen, ist Gegenstand eines langjährig gewachsenen Meinungsstreits (siehe sogleich unten).[54]

Gesichert ist hingegen, dass die DS-GVO auf anonyme Informationen keine Anwendung findet; wobei all jene Informationen als anonym gelten, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Darunter fallen auch Informationen, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Damit bilden anonyme Daten im Ergebnis die „Kehrseite" zu personenbezogenen Daten, auf welche die DS-GVO nach Art 2 Abs 1 e contrario sowie ErwGr 26 nicht anzuwenden ist.

---

[50] *Karg* in *Simitis/Hornung/Spiecker*, DS-GVO Art 4 Z 1 R 25.
[51] DBVerfG 15.12.1983, 1 BvR 209/83 („Volkszählungs-Urteil").
[52] Vgl auch *Bergauer* in *Jahnel* (Hrsg), DS-GVO (2020) Art 4 Rz 9; *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 1 Rz 8.
[53] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 1 Rz 22f.
[54] Vgl hiezu ausführlich *Bergt*, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts - Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365.

3.2.1. Wissen und Mittel anderer Personen

Weiterführend stellt sich die Frage, wie die Grenze zwischen personenbezogenen und anonymen Daten zu ziehen ist. Zu dieser Abgrenzung gibt es unterschiedliche Positionen in Literatur und Rsp. Diese unterscheiden sich im Wesentlichen dadurch, wessen Perspektive bei der Beurteilung des Personenbezugs in Betracht gezogen werden soll.

Nach der absoluten Theorie[55] genügt bereits die hypothetische Möglichkeit eines beliebigen Dritten[56], die in Rede stehenden Informationen auf eine natürliche Person zu beziehen. Ob die (potenziell) verantwortliche Stelle tatsächlich von dieser hypothetischen Möglichkeit der Verknüpfung Gebrauch macht, ist unerheblich.[57] Der Verantwortliche muss sich Wissen und Mittel von Dritten jedenfalls zurechnen lassen. Diese Sicht kann für sich beanspruchen, keine Rechtsschutzlücken offenzulassen, zumal die Schwelle zur Annahme des Personenbezugs äußerst niedrig angelegt und so ein hohes Schutzniveau für Betroffene erzielt wird.[58] Gleichzeitig werden der Theorie allerdings oft ausufernde Tendenzen mit einem überschießenden Anwendungsbereich[59] attestiert sowie auch ein Mangel an Rechtssicherheit, da es vielfach schwierig einzuschätzen ist, welches Wissen und Mittel bei Dritten allenfalls vorhanden sein könnte.[60] Daneben wird auch ins Treffen geführt, dass ein zu weit angelegtes Verständnis nicht dem risikobasierten Ansatz[61] der DS-GVO entspreche und uU sogar zu einer Verminderung des allgemeinen Datenschutzniveaus führen kann: Weil durch einen de facto niemals auszuschließenden Anwendungsbereich Anreize für die Verwendung von datenschutzfreundlichen Technologien wie PETs[62] verloren gehen, wenn ohnedies jede Verarbeitung unabhängig ihrer technischen Schutzgarantien vollumfänglich in den Anwendungsbereich der DS-GVO fällt.[63] ME führt der absolute Ansatz in diesem Sinn zu einer undifferenzierten Gleichschaltung

[55] Auch objektive Theorie genannt.
[56] Teils wird auch die Möglichkeit der betroffenen Person selbst, die Informationen auf sich zu beziehen, als ausreichend angesehen.
[57] *Karg* in *Simitis/Hornung/Spiecker*, DS-GVO Art 4 Z 1 R 58.
[58] *Karg* in *Simitis/Hornung/Spiecker*, DS-GVO Art 4 Z 1 R 58.
[59] *Finck/Pallas* sprechen von einem „Systembruch" und einer de facto Aufgabe der Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten mit einem grundlegend anderen Regulierungsverständnis; *Finck/Pallas,* They who must not be identified – Distinguishing Personal from Non-Personal Data under the GDPR, Max Planck Institute for Innovation and Competition Research Paper No. 19-14, 47.
[60] *Arning/Rothkegel* in *Taeger/Gabel* (Hrsg), DS-GVO[4] (2021) Art 4 Z 1 Rz 34.
[61] Vgl zum risikobasierten Ansatz als Regulierungsstrategie ausführlich *Gellert,* The risk-based approach to data protection, Oxford University Press 2020, 136.
[62] Privacy Enhancing Technologies (PETs).
[63] Vgl etwa *Spindler/Schmechel*, Personal Data and Encryption in the European General Data Protection Regulation, JIPITEC 2016, 163 Rz 26; *Tene/Polonetsky*, Stanford Law Review 2012, 63 (66); *Gellert,* Understanding the notion of risk in the General Data Protection Regulation, Computer Law & Security Review 2018, 279 (280).

von Informationen mit unterschiedlicher Schutzbedürftigkeit, der die Risikowahrnehmung bei Datenverarbeitungen verwischt.

Demgegenüber wird von der relativen Theorie[64] vertreten, dass es bei der Beurteilung des Personenbezugs lediglich auf die Möglichkeiten des Verantwortlichen selbst ankommt. Danach muss (bloß) anhand des Wissens und der Mittel, die dem Verantwortlichen in einer konkreten Verarbeitungssituation tatsächlich zur Verfügung stehen, beurteilt werden, ob sich die Information auf eine Person beziehen lässt. Diese Theorie kann für sich in Anspruch nehmen, besonders nah an der Datenverarbeitung angelegt zu sein, zumal die Perspektive dritter Personen nicht berücksichtigt werden muss und bloß auf die Verhältnisse beim Verantwortlichen selbst abgestellt wird;[65] insofern muss kein (allenfalls) vorhandenes Wissen Dritter zugerechnet werden und es wird ein höheres Maß an Rechtssicherheit für Verantwortliche erzielt.
Eine praktisch über Dritte herstellbare Identifizierung von Betroffenen wäre allerdings demnach bereits dann ausgeschlossen, wenn der Verantwortliche diese nicht herstellen möchte. Damit liegen Kontrolle und Wissen über einen allfälligen Personenbezug der Daten vollständig in den Händen des Verantwortlichen, wodurch Rechtssicherheit und Rechtsschutz für Betroffene erheblich vermindert werden, können diese doch Wissen und Mittel der datenverarbeitenden Stellen vielfach schwer einschätzen. In diesem Sinne sprechen überzeugende Argumente dagegen, die Determinierung der Schutzhöhe für Betroffene in die Kontrolle der Verantwortlichen zu legen. Insofern führen weder die absolute noch die relative Theorie in ihren ursprünglichen Formen zu befriedigenden Ergebnissen.

Neben absoluter und relativer Theorie haben sich in Wissenschaft und Praxis eine Reihe von Mischformen bzw Abschwächungen dieser Positionen entwickelt.[66] Auch das Institut des Personenbezugs nach der DS-GVO lässt sich prima facie nicht zweifelsfrei in eine der beiden Theorien einordnen, da es Elemente aus beiden Theorien enthält. So regt ErwGr 26 zur Beurteilung der Identifizierbarkeit etwa ausdrücklich an, dass „*alle Mittel berücksichtigt werden [sollten], die von dem Verantwortlichen oder einer anderen Person*" genutzt werden; was zunächst für eine absolute Perspektive spricht, zumal die Mittel von „anderen Personen" explizit

[64] Auch subjektive Theorie genannt.
[65] *Karg* in *Simitis/Hornung/Spiecker*, DS-GVO Art 4 Z 1 R 58.
[66] Vgl etwa *Bergt*, der sechs Ansichten zur Evaluierung der „Bestimmbarkeit" nach alter Rechtslage anführt; *Bergt*, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts - Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365.

angesprochen werden. Jedoch schwächt ErwGr 26 diese Nutzung von Mitteln anderer Person noch im selben Satz ein und normiert, dass die Nutzung auch *„nach allgemeinem Ermessen wahrscheinlich"* sein muss. Die Nutzung entsprechender Mittel zur Identifizierung durch eine dritte Person kann aber nur dann wahrscheinlich sein, wenn dieser Dritte mit den in Rede stehenden Daten in Berührung kommt; wodurch eine Beteiligung des Dritten am Verarbeitungsvorgang indiziert ist.[67] Damit ergibt sich der Dreh- und Angelpunkt der Beurteilung wiederum bei der verantwortlichen Stelle und erst davon nachgelagert bei mit diesem in Verbindung stehenden Dritten (was wiederum eher für eine relative Sichtweise spricht). Im Ergebnis sprechen diese normativen Grundlagen damit zumindest teilweise auf beide Theorien an, wodurch sich erklären lässt, warum der Theorienstreit zum Personenbezug noch nicht befriedigend gelöst werden konnte.

3.2.2. Rechtsprechung zum Personenbezug

Während zur Datenschutzrichtlinie[68] noch oft relative oder absolute Positionen in ihrer ursprünglichen Form vertreten wurden (insbesondere von den europäischen Aufsichtsbehörden[69]), haben sich seit der Entscheidung des EuGH in der Rs *Breyer*[70] mehrheitlich vermittelnde Ansätze durchgesetzt. In dieser – zur DSRL ergangenen, aber auf die DS-GVO übertragbaren – Entscheidung stellte der EuGH klar, dass sich nicht *„alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden"* müssen.[71] Vielmehr müsse sich die verantwortliche Stelle das Wissen und Mittel von Dritten zurechnen lassen, sofern mit einem Einsatz dieser Mittel „vernünftigerweise"[72] gerechnet werden könnte.

Bei der Beurteilung, ob die Mittel vernünftigerweise eingesetzt werden könnten, stellte der EuGH neben der tatsächlichen Verfügbarkeit insbesondere auf die rechtliche Zulässigkeit des Zugangs zu Wissen ab. In der Rs *Breyer* wurde der Personenbezug von dynamischen IP-Adressen in der konkret vorliegenden Konstellation unter dem Gesichtspunkt bejaht, dass der Verantwortliche ein

---

[67] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 1 Rz 26.
[68] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31 idF L 2003/284, 1.
[69] Vgl für ein absolutes Verständnis *Art-29-Datenschutzgruppe*, WP 216, Opinion 05/2014 on Anonymisation Techniques, 11, 23; weiters ging auch Vereinigung der obersten Aufsichtsbehörden in Deutschland bereits 2009 vom Vorliegen eines Personenbezug bei IP-Adressen aus; vgl Düsseldorfer Kreis, Beschluss vom 26./29.11.2009 in Stralsund.
[70] EuGH 19.10.2016, C-582/14, *Breyer*, ECLI:EU:C:2016:779, jusIT 2016, 252 (*Jahnel*).
[71] EuGH 19.10.2016, C-582/14, *Breyer*, ECLI:EU:C:2016:779 Rn 43.
[72] Die Formulierung „vernünftigerweise" geht auf ErwGr 26 der DSRL zurück; übertragen auf die DS-GVO muss es „nach allgemeinem Ermessen wahrscheinlich" heißen.

subjektives Recht hatte, sich an eine staatliche Behörde zu wenden, die wiederum über den Internetzugangsanbieter eine Identifikation der betroffenen Person herstellen hätte können. Wobei die bloße Möglichkeit der Identifikation als ausreichend gewertet und keine tatsächlich erfolgte Identifikation der betroffenen Person verlangt wurde.

Unter Berücksichtigung dieser Rsp[73] lassen sich bloß auf einen (strikt) relativen Personenbezug gestützte Positionen kaum mehr halten, zumal der EuGH bei der Beurteilung der Identifizierbarkeit sogar die (potenzielle) Zuhilfenahme staatlicher Stellen durch einen Dritten dem Verantwortlichen zurechnet; wenn auch unter dem deutlichen Korrektiv, dass diese Mittel rechtlich zulässig und vernünftig, dh „nach allgemeinem Ermessen wahrscheinlich" einsetzbar sein müssen. Hierzu sollte nach den Schlussanträgen des Generalanwalts darüber hinaus nur Wissen und Mittel jener Dritten berücksichtigt werden, an die sich der Verantwortliche auch „vernünftigerweise"[74] wenden könnte, weil sich ansonsten *„Niemals [..] mit absoluter Sicherheit ausschließen [lässt], dass es nicht einen Dritten gibt, der im Besitz von Zusatzwissen ist"*. [75] Durch diese Einschränkungen wird deutlich, dass absolute Positionen, die der Beurteilung des Personenbezugs das „Weltwissen" zugrunde legen, mit dieser Rsp ebenso nicht vereinbar sind. Die (fingierte) Annahme einer Identifizierbarkeit über Zurechnung von Wissen und Mittel dritter Personen, die praktisch ausgeschlossen ist, etwa weil keine Verbindung zwischen dem Verantwortlichen und Dritten besteht, ist daher nicht angezeigt. Bei (dauerhaft) im Internet veröffentlichten Daten muss sich der Personenkreis mE allerdings konsequenterweise auf alle „anderen Personen", die Zugang zu den Daten haben, erstrecken; das kann uU auch die Gesamtheit aller Internet-Nutzer:innen sein.

Im Einklang mit der Rs *Breyer* ist auch eine jüngst ergangene Entscheidung des EuG[76] zu sehen, in welcher das Gericht bei der Zurechnung von Wissen und Mitteln ebenso darauf abstellte, ob mit dem Einsatz dieser Mittel auch „vernünftigerweise" gerechnet werden könnte; bzw, ob eine „Rückidentifizierung" auch „praktisch durchführbar" wäre.[77] Eine Pauschal-Zurechnung von Wissen und Mittel im Sinne der absoluten

[73] Vgl der in der Rs *Breyer* entwickelten Linie folgend auch EuGH 20.12.2017, C-434/16, *Nowak*, ECLI:EU:C:2017:994.
[74] GA 12.5.2016, C-582/14, *Breyer*, Rn 68.
[75] Aus den Schlussanträgen des Generalanwalts in der Rs *Breyer*: „Diese weitestmögliche Auslegung würde in der Praxis dazu führen, dass jede Art von Information als personenbezogenes Datum einzuordnen wäre, so unzureichend sie für sich genommen auch wäre, um einen Nutzer bestimmen zu können. Niemals wird sich mit absoluter Sicherheit ausschließen lassen, dass es nicht einen Dritten gibt, der im Besitz von Zusatzwissen ist, das mit der fraglichen Information verbunden werden kann und es damit ermöglicht, die Identität einer Person festzustellen." GA 12.5.2016, C-582/14, *Breyer*, Rn 68.
[76] EuG 26.4.2023, T-557/20, *SRB/EDSB*, ECLI:EU:T:2023:219.
[77] EuG 26.4.2023, T-557/20, *SRB/EDSB*, ECLI:EU:T:2023:219, Rn 104.

Theorie ließ das Gericht nicht zu, sondern stellte unter Verweis auf Rn 45 der Rs *Breyer* auf die Sicht der datenverarbeitenden Stelle ab.[78]

Im Ergebnis lassen sowohl EuGH als auch EuG die Zurechnung von Wissen und Mitteln Dritter zwar prinzipiell zu, schränken diesen Zurechnungsweg jedoch gleichzeitig auf Fälle ein, in welchen mit dem Einsatz von Wissen und Mittel auch nach allgemeinem Ermessen wahrscheinlich gerechnet werden könnte. In der Rs *Breyer* rechnete der EuGH dem Verantwortlichen die rechtlichen Möglichkeiten eines Dritten zu. Ob er damit bei der Beurteilung des Personenbezugs allerdings auch tatsächliche alle rechtswidrigen Mittel ausschließen wollte[79], wird in der Literatur insbesondere für jene Fälle bezweifelt, in denen eine faktische Nähe zu den beim Dritten befindlichen Daten vorliegt (wie insbesondere Auftragsverarbeitungsverhältnissen) sowie bei besonders sensiblen Daten (wie etwa klinischen Studien); allerdings unter der Prämisse, dass die rechtswidrige Herstellung des Personenbezugs zumindest „nicht unwahrscheinlich" erscheint.[80]

Zusammengefasst muss sich der Verantwortliche etwaiges Wissen und Mittel von Dritten, über das diese uU noch nicht verfügen, dann zurechnen lassen, wenn den Dritten rechtlich zulässige Mittel zustehen, um sich dieses Zusatzwissen zu verschaffen und es darüber hinaus auch nach allgemeinem Ermessen wahrscheinlich ist, dass diese Mittel genutzt werden könnten, um eine natürliche Person zu identifizieren.

3.2.3. Personenbezug von „Verschlüsselten Daten"

Verschlüsselung bezeichnet ein kryptographisches Verfahren, mit welchem „Klartext"[81], durch einen geheimen Schlüssel, in eine unverständliche Zeichenfolge umgewandelt wird (sog „Geheimtext"). Verschlüsselte Daten können nur durch den geheimen Schlüssel wieder entschlüsselt und lesbar gemacht werden. Die zu verschlüsselnden Daten müssen nicht zwingend Textnachrichten sein. Alle denkbaren digitalen Inhalte, inklusive Bilder, Videos oder Musik, können verschlüsselt werden.[82]

[78] EuG 26.4.2023, T-557/20, *SRB/EDSB*, ECLI:EU:T:2023:219, Rn 103-105.
[79] So wie in den Schlussanträgen vorgeschlagen; vgl GA 12.5.2016, C-582/14, *Breyer*, Rn 73; in diese Richtung nunmehr auch EuG 26.4.2023, T-557/20, *SRB/EDSB*, ECLI:EU:T:2023:219, Rn 105.
[80] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 1 Rz 29.
[81] „Klartext" bedeutet, dass die Informationen offen lesbar sind.
[82] *Bierbauer* „Verschlüsselung" in *Piska* (Hrsg), Fachwörterbuch Rechtswissenschaften[2] (in Druck); vgl auch *Ferguson/Schneier/Kohno,* Cryptography Engineering (2010).

Der Prozess der Verschlüsselung stellt eine Verarbeitung von personenbezogenen Daten dar, wenn die Klartext-Eingabedaten sich auf eine natürliche Person beziehen lassen.[83] Das Ergebnis der Verschlüsselung, nämlich die verschlüsselten Daten per se, sind jedoch nur dann als personenbezogen zu qualifizieren, wenn es nach allgemeinem Ermessen wahrscheinlich ist, dass mit den Daten eine natürliche Person identifiziert werden könnte.

Damit sind verschlüsselte Daten jedenfalls für jene datenverarbeitenden Stellen als personenbezogen zu qualifizieren, die über den geheimen Schlüssel verfügen, um die Daten zu entschlüsseln.[84] Werden darüber hinaus auch die Zwecke und Mittel der Verschlüsselung durch die datenverarbeitende Stelle festgelegt, so sind diese als Verantwortliche iSd DS-GVO einzuordnen. Verschlüsselte Daten erfüllen für Verarbeiter die über die Mittel zur Entschlüsselung und damit zur Herstellung eines Personenbezugs verfügen idR auch die Anforderungen der „Pseudonymisierung"[85] nach Art 4 Z 5 DS-GVO.[86] Auf Voraussetzungen[87] und Rechtsfolgen[88] bzw Privilegierungen[89] dieser besonderen Verarbeitungsform personenbezogener Daten soll hier aber aus didaktischen Gründen nicht näher eingegangen werden, zumal in dieser Untersuchung nur der Anwendungsbereich nach Art 2 DS-GVO interessiert, welcher expressis verbis bloß auf die „*Verarbeitung personenbezogener Daten*"[90] abstellt und grundsätzlich keinen Bezug zur „Pseudonymisierung" aufweist. An dieser Stelle sei nur festgehalten, dass die Verarbeitung (ordnungsgemäß) pseudonymisierter Daten durch Stellen die nicht über die Mittel zur Aufhebung der Pseudonymisierung verfügen grundsätzlich auch eine anonymisierende Wirkung entfalten kann.[91]

---

[83] *Hansen* in *Simitis/Hornung/Spiecker* (Hrsg), DS-GVO (2019) Art 4 Z 5 Rz 33.
[84] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 1 Rz 80; *Hansen* in *Simitis/Hornung/Spiecker*, DS-GVO Art 32 Rz 33.
[85] "Pseudonymisierung" wird in Art 4 Z 5 definiert als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden".
[86] Vgl etwa *Bergauer/Gosch*, Die Pseudonymisierung personenbezogener Daten gemäß der DSGVO - zugleich eine Replik auf *Geuer/Wollmann*, Verarbeitung von pseudonymen Daten mit besonderem Fokus auf Art 26 und 28 DS-GVO, jusIT 2020, 63; *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 5 Rz 8; *Gosch*, Pseudonymisierung und Verschlüsselung sensibler Daten, jusIT 2019, 107.
[87] Vgl zu den kumulativen Voraussetzungen der Pseudonymsierung anschaulich *Bergauer/Gosch*, Pseudonymisierung, jusIT 2020, 67; *Hansen* in *Simitis/Hornung/Spiecker*, DS-GVO Art 4 Z 5 Rz 30; *Paal/Pauly*, DS-GVO[3] (2021) Art 4 Z 5 Rz 40.
[88] Vgl etwa *Arning/Rothkegel* in *Taeger/Gabel* (Hrsg), DS-GVO[4] (2021) Art 4 Z 5 Rz 128.
[89] Vgl etwa *Arning/Rothkegel* in *Taeger/Gabel*, DS-GVO[4] Art 4 Z 5 Rz 131.
[90] Vgl Art 2 DS-GVO: *"Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten".*
[91] *Ziebarth* in *Sydow/Marsch* (Hrsg), DS-GVO[3] (2022) Art 4 Z 5 Rz 97; *Arning/Rothkegel* in *Taeger/Gabel*, DS-GVO[4] Art 4 Z 5 Rz 128;
Klar/Kühling in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 5 Rz 12; *Hansen* in *Simitis/Hornung/Spiecker*, DS-GVO Art 32 Rz 33.

Für andere Stellen (die nicht über den geheimen Schlüssel verfügen) muss stets erwogen werden, ob sie sich die Mittel zur Entschlüsselung der Daten von einem Verantwortlichen allenfalls zurechnen lassen müssen oder ob sie die Verschlüsselung durch Brute-Force oder ähnliche Methoden aufzuheben im Stande wären. Um dies zu beurteilen, sollten alle objektiven Faktoren, wie die Kosten und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Diese objektiven Faktoren müssen laufend beurteilt werden, wodurch der Personenbezug in der Zukunft jederzeit aufleben kann. Bei der Beurteilung dieser Faktoren ist allerdings stets auf den Verarbeitungszeitpunkt abzustellen. Das bedeutet, dass eine Verschlüsselung nicht schon allein deshalb als unsicher einzustufen ist, weil sie allenfalls in der Zukunft mithilfe von neuen Technologien aufgehoben werden könnte. Bei einer dem Stand der Technik entsprechenden Verschlüsselung darf daher angenommen werden, dass Dritte nicht in der Lage sind, die Entschlüsselung zu brechen.

Die Verarbeitung von verschlüsselten Daten durch Stellen, die sich die Mittel des Verantwortlichen nicht zurechnen lassen müssen und darüber hinaus auch nach allgemeinem Ermessen nicht imstande sind, die Verschlüsselung aufzuheben, unterliegt damit – mangels Vorliegens eines Personenbezugs – nicht der DS-GVO.[92] Dieses Ergebnis steht systematisch auch in Einklang mit Art 34 Abs 3 lit a DS-GVO der für verschlüsselte Daten eine Ausnahme für Benachrichtigungen bei Datenschutzverletzungen vorsieht.

3.3. Zwischenfazit zum Personenbezug in SMPC-Umgebungen

In Gesamtschau sind bei der Feststellung, ob eine natürliche Person identifizierbar ist, sowohl relative als auch absolute Elemente des Personenbezugs zu berücksichtigen. In der Literatur wird daher oft vermittelnd von einem „absoluten

[92] So auch *Fuchs*, Anonymisierende Wirkung der Verschlüsselung, Dako 2019, 34; *Hofer*, Überlegungen zur anonymisierenden Wirkung der Pseudonymisierung im Außenverhältnis am Beispiel Cloud-Computing, jusIT 2022, 173; *Ziebarth* in *Sydow/Marsch*, DS- GVO[3] Art 4 Z 5 Rz 97; *Arning/Rothkegel* in *Taeger/Gabel*, DS-GVO[4] Art 4 Z 5 Rz 128; *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 5 Rz 12; *Hansen* in *Simitis/Hornung/Spiecker*, DS-GVO, Art 32 Rz 33.

Ansatz mit relativen Elementen" oder von einem „relativen Ansatz mit Einschränkungen/objektivierenden Elementen" gesprochen.[93] Hierbei wird im Wesentlichen auf das Kriterium der Wahrscheinlichkeit einer Identifizierung abgestellt und damit dem risikobasierten Ansatz der DS-GVO entsprochen. Eine bloß fingierte Annahme des Personenbezugs über die Zurechnung von Wissen Dritter, mit der praktisch nicht zu rechnen ist, muss daher nicht angenommen werden.

Diese vermittelnde Position ist nach der hier vertretenen Meinung zutreffend, zumal - wie bereits ausgeführt wurde - weder ein absolutes noch ein relatives Verständnis des Personenbezugs zu unproblematischen Ergebnissen führt, wenn auch beide Positionen (teilweise überzeugende) Argumente für sich beanspruchen können. Im Übrigen ist noch anzumerken, dass der Status des Personenbezugs nie endgültig ist und sich aufgrund technologischer Entwicklungen oder Änderungen im organisatorischen Rahmen der Verarbeitung jederzeit ändern kann.

Umgelegt auf die Verarbeitungssituation bei SMPC bedeutet dies, dass die Verarbeitung von (vollständig) verschlüsselten Daten nicht dem Anwendungsbereich der DS-GVO unterliegt, wenn nach allgemeinem Ermessen nicht wahrscheinlich ist, dass eine natürliche Person identifiziert werden könnte.[94]

Hierbei kommt es stets auf die Sicht der datenverarbeitenden Stelle an: Für den Verantwortlichen, der die Daten verschlüsselt hat, sind diese personenbezogen;[95] für andere beteiligte Verarbeitungsparteien jedoch nicht, weil diese die Daten technisch nicht entschlüsseln können und sich die Mittel des Verantwortlichen nicht zurechnen lassen müssen, wenn nach allgemeinem Ermessen nicht wahrscheinlich ist, dass der Verantwortliche die Mittel zur Entschlüsselung mit ihnen teilt.[96] Vorausgesetzt wird dabei, dass die Verschlüsselung dem Stand der Technik entspricht und eine Aufhebung der Verschlüsselung unwahrscheinlich ist.

Da die DS-GVO konzeptuell den risikobasierten Ansatz verfolgt, kommt der Abschätzung des Risikos der Verarbeitung personenbezogener Daten mittels SMPC besondere Bedeutung zu. Nimmt man nun eine Risikoabwägung vor, so ist nach

---

[93] Vgl *Arning/Rothkegel* in *Taeger/Gabel*, DS-GVO[4] Art 4 Z 1 Rz 34; ähnlich auch *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 4 Z 1 Rz 31.

[94] In diesem Sinne auch *EDSA*, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, 10.11.2020, 44.

[95] Zumal der Verantwortliche mit dem Geheimschlüssel über Mittel verfügt, die Verschlüsselung wieder aufzuheben.

[96] Vgl hierzu jüngst EuG 26.4.2023, T-557/20, *SRB/EDSB*, ECLI:EU:T:2023:219.

allgemeinem Ermessen nicht damit zu rechnen, dass der Verantwortliche die Mittel zur Verschlüsselung mit den anderen Verarbeitungsparteien teilt, zumal er das SMPC-Verfahren ja gerade dazu einsetzt, um seine Eingabedaten gegenüber den anderen Parteien nicht offenzulegen. Bei der Beurteilung dieses Risikos sind auch die jeweilige Sicherheitsarchitektur sowie eingesetzte TOMs des Verantwortlichen zu berücksichtigen: Wenn auch das Risiko einer Weitergabe durch illoyale Mitarbeiter:innen nie gänzlich auszuschließen ist, so können Zugriffs-Hierarchien, Zugriffs-Kontrollen und andere Maßnahmen derartige Risiken auf ein Niveau reduzieren, bei dem nicht mehr damit gerechnet werden muss, dass eine (rechtswidrige) Weitergabe geschieht. Der Verantwortliche muss den eigenen Mitarbeiter:innen bei der Risikoabwägung somit kein rechtswidriges Verhalten unterstellen, wenn diese sorgfältig ausgewählt wurden und eine hinreichende Sicherheitsarchitektur vorliegt.
Wollte der Verantwortliche die Daten hingegen tatsächlich mit anderen Verarbeitungsparteien teilen, so müsste er im Übrigen dafür nicht das rechenintensive und organisatorisch aufwendige Verfahren SMPC implementieren. Sollten die Mittel zur Entschlüsselung – aus welchen Gründen auch immer – tatsächlich offengelegt werden, so würde der Personenbezug aufleben und die Verarbeitung vollständig der DS-GVO unterliegen.

Die nachfolgende Tabelle qualifiziert das Vorliegen des Personenbezugs während der einzelnen Verarbeitungsschritte von SMPC:

Verarbeitungsschritt	Qualifikation des Personenbezugs
(i.) Präparation und Verschlüsselung der Eingabedaten durch die einzelnen Verarbeitungsparteien	Die Eingabedaten liegen im Klartext vor, die einbringenden Verarbeitungsparteien können die jeweils betroffenen Personen identifizieren; die Eingabedaten sind personenbezogen.
(ii.) Zusammenführung der verschlüsselten Daten	Verschlüsselte Daten können nur durch die dateneinbringende Partei entschlüsselt werden. Eine Identifizierung durch die anderen Verarbeitungsparteien ist technisch nicht möglich und daher nach allgemeinem Ermessen auch nicht wahrscheinlich; die Daten weisen für die anderen Verarbeitungsparteien keinen Personenbezug auf.
(iii.) Durchführung der jeweiligen Ziel-Berechnung auf den zusammengeführten verschlüsselten Datenfragmenten	Für die Durchführung der Berechnung müssen die Daten nicht entschlüsselt werden, die Daten weisen für andere Verarbeitungsparteien keinen Personenbezug auf.
(iv.) Übermittlung des Berechnungsergebnisses an die beteiligten Verarbeitungsparteien, wobei die Ergebnis-Offenlegung auch nur einzelnen Parteien vorbehalten sein kann.	Die Partei erhält das Ergebnis der Berechnung. Je nach Art der Ziel-Berechnung sind die Ausgabedaten personenbezogen oder nicht: Erhält die Partei nur statistische Informationen, muss nicht zwingend ein Personenbezug vorliegen. Reichert die Partei ihre Eingabedaten hingegen mit den Ergebnissen an, so kann sie die betroffenen Personen identifizieren; die Berechnungsergebnisse wären daher personenbezogen.

Im Ergebnis entfaltet die DS-GVO ihre Schutzwirkung auf alle personenbezogenen Daten, die in eine SMPC-Verarbeitung miteinbezogen werden, da durch die

Aufbereitung und Verschlüsselung der Daten jeweils eine Verarbeitung personenbezogener Daten durch die einzelnen Parteien vorliegt. Die weiterführende Verarbeitung von verschlüsselten Daten unterliegt allerdings nicht (mehr) dem Regelungsregime der DS-GVO, weil die anderen Parteien nicht in der Lage sind die Daten zu entschlüsseln und sich die Mittel zur Entschlüsselung auch nicht zurechnen lassen müssen. Obwohl die DS-GVO auf die Verarbeitung dieser verschlüsselten Daten keine Anwendung findet, ergeben sich hierdurch jedoch keine Rechtsschutzdefizite, da jede Verarbeitungspartei bereits durch die Aufbereitung und Verschlüsselung der eigenen Datenbestände zum Zweck einer Berechnung mittels SMPC rechenschaftspflichtig wird und den Bestimmungen der DS-GVO entsprechen muss (zum allfälligen Vorliegen einer gemeinsamen Verantwortlichkeit der Verarbeitungsparteien später).

3.4. Datenminimierung und Data Protection by Design

Unter dem Titel der „Datenminimierung" verlangt Art 5 Abs 1 lit c DS-GVO eine Verarbeitung, die *„dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt"* ist. Diese Anforderungen ergeben zusammengenommen die Bedingung, dass die Verarbeitung zur Erreichung des festgelegten Zwecks erforderlich sein muss; über das erforderliche Maß hinausgehende Verarbeitungen sind nicht zulässig.[97]

Ein Verstoß gegen den Grundsatz der Datenminimierung kann demnach etwa auch dann vorliegen, wenn der Verarbeitungszweck ebenso mit anonymisierten oder verschlüsselten Daten erreicht werden hätte können; zumal die Verarbeitung nicht-anonymisierter Daten dann vermeidbar und somit nicht erforderlich gewesen wäre. Weitere Konkretisierung erfährt der Grundsatz der Datenminimierung auch in Art 25 Abs 1 DS-GVO, der vielfach unter dem Titel „Data Protection by Design"[98] geführt wird und explizit geeignete Garantien bzw technische und organisatorische Maßnahmen (TOMs) zur Umsetzung des Grundsatzes einfordert:[99] Demnach soll Datenschutz möglichst früh und damit bereits bei der Auswahl, Festlegung und dem Einsatz von IT-Systemen zur Verarbeitung von personenbezogenen Daten berücksichtigt

[97] Vgl zur Datenminimierung bei datenintensivem Training von KI-Modellen schon *Bierbauer*, Datenschutzrechtliche Grundsätze 191.
[98] Vgl hiezu ausführlich *EDPB*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20.10.2020.
[99] *Herbst* in *Kühling/Buchner* (Hrsg), DS-GVO[3] (2020) Art 5 Rz 58.

werden.[100] Im besten Fall wird die Einhaltung datenschutzrechtlicher Vorgaben bereits systemimmanent durch technische Restriktionen sichergestellt und nicht auf datenverarbeitende Stellen oder Systemanwender, denen vertraut werden müsste, ausgelagert: Was nicht erlaubt ist, soll technisch schlicht unmöglich gemacht werden.[101]

Ähnlich wie auch in den Bestimmungen zur Datensicherheit wird jedoch bei der Umsetzung nicht (immer) das höchstmögliche Schutzniveau verlangt, sondern bloß ein angemessenes Niveau unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie aller sonstigen Umstände der konkreten Verarbeitung. Diese Erwägungen sind insbesondere auch bei der Entscheidung, mit welcher Schutzhöhe die jeweilige SMPC-Umgebung konzipiert werden soll, zu berücksichtigen.[102]

In Zusammenschau der angeführten Bestimmungen eignet sich die Verarbeitung personenbezogener Daten in SMPC-Umgebungen hervorragend dazu, dem Grundsatz der Datenminimierung sowie Art 25 DS-GVO zu entsprechen, weil die gesamte Ziel-Berechnung auf verschlüsselten Datenfragmenten durchgeführt wird und keine personenbezogenen Daten gegenüber anderen Parteien offengelegt werden müssen: In diesem Sinne werden alle personenbezogenen Datenbestände nur dezentral verarbeitet, ohne die Angriffsfläche durch Spiegelung der Datenbestände zu vergrößern oder potenziell rechtswidrige Verarbeitungen zu ermöglichen. Ferner besteht insbesondere keine Gefahr, dass Daten an Dritte weitergegeben werden, da innerhalb des Protokolls nur die konkret angestrebte Verarbeitung durchgeführt werden kann.

Wollte man dieselbe Ziel-Berechnung ohne SMPC durchführen, so müssten die jeweiligen Datenbestände kopiert und zusammengeführt werden, was einer Offenlegung der Daten und anschließender Verarbeitung des gesamten Datenbestands an einer Stelle entsprechen würde. Zweifellos wäre diese Alternative datenschutzrechtlich weitaus invasiver als SMPC.

---

[100] *Hartung* in *Kühling/Buchner* (Hrsg), DS-GVO[3] (2020) Art 25 Rz 11.
[101] *Bergauer* in *Jahnel* (Hrsg), DS-GVO (2020) Art 25 Rz 1.
[102] Vgl aktiv bzw passiv-sichere Modelle in 2.2. „Funktionsweise der Ziel-Berechnung".

3.5. Ausblick auf weiterführende Rechtsfragen

Die Untersuchung zum Personenbezug hat gezeigt, dass die DS-GVO auf alle personenbezogenen Daten, die zum Zweck einer Ziel-Berechnung mittels SMPC aufbereitet und verschlüsselt werden, Anwendung findet. Die daraus resultierenden Rechtsfragen sollen an dieser Stelle kursorisch thematisiert werden.

Hinsichtlich der weiterführenden Zusammenführung und Berechnung auf den verschlüsselten Datenfragmenten liegt gegenüber anderen beteiligten Verfahrensparteien kein Personenbezug (mehr) vor, wodurch die Verarbeitung der Datenfragmente grundsätzlich nicht dem Regelungsregime der DS-GVO unterliegt.[103] Durch den Umstand, dass die Daten während der gesamten Verarbeitung verschlüsselt bleiben, ergeben sich für Betroffene starke Datenschutzgarantien.

Die abschließende Übermittlung der Berechnungsergebnisse an die beteiligten Verfahrensparteien ist, abhängig von der durchgeführten Ziel-Berechnung und den vorliegenden Datenbeständen, wieder eine Verarbeitung von personenbezogenen Daten; allerdings können die (übermittelten) Berechnungsergebnisse sich nur auf Personen beziehen, die in den von der jeweiligen Partei eingebrachten Datensätzen enthalten waren; es werden also keine Informationen über Betroffene übermittelt, die der einzelnen Partei unbekannt waren.

3.5.1. (Gemeinsame?) Verantwortlichkeit

Anknüpfend an die Beurteilung, ob eine Verarbeitung personenbezogener Daten vorliegt, stellt sich die Frage, wer für diese Verarbeitung verantwortlich ist. Die Beurteilung dieser Rolle richtet sich nach Art 4 Z 7 DS-GVO, der bei der Zuweisung der Verantwortung darauf abstellt, wer *„über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet"*.
Relativ unproblematisch lässt sich die Verantwortung in einem ersten Schritt derjenigen datenverarbeitenden Stelle zuweisen, welche die Daten zum Zweck einer Ziel-Berechnung mittels SMPC aufbereitet und verschlüsselt.

[103] Allerdings bleiben die verschlüsselten Daten jeweils für die Partei personenbezogen, welche sie verschlüsselt und in die SMPC-Umgebung eingebracht hat, zumal sie über die Mittel verfügt, die Daten auf eine natürliche Person zu beziehen.

Art 4 Z 7 leg cit DS-GVO normiert jedoch weiter, dass die Entscheidung über Zwecke und Mittel *„allein oder gemeinsam mit anderen"* getroffen werden kann. Für Fälle der gemeinsamen Verantwortlichkeit[104] sieht die DS-GVO in Art 26 als Spezialbestimmung zu Art 4 Z 7 weitere Verpflichtungen vor:[105] Demnach ist etwa eine Vereinbarung[106] zwischen den gemeinsamen Verantwortlichen zu treffen, in der festgelegt wird, wer welche Bestimmungen der DS-GVO erfüllen muss; zu denken ist hier insbesondere an Transparenzpflichten und Betroffenenrechte.[107]

Nach den Leitlinien des EDSA kommt es bei der Zuweisung von gemeinsamen Verantwortlichkeiten va darauf an, „dass die Verarbeitung ohne die Beteiligung beider Parteien nicht möglich wäre, und zwar in dem Sinne, dass die Verarbeitungen jeder der Parteien untrennbar, dh unauflösbar miteinander verbunden sind".[108]

Für SMPC liegt es geradezu im Archetyp der Verarbeitungsform, dass sich mehrere Parteien zusammenschließen, um gemeinsam eine Berechnung vorzunehmen (dies deutet bereits der Name der Technologie an: „Secure *Multiparty* Computation" bzw „Mehr-Parteien-Berechnung"). Insbesondere müssen sich die beteiligten Parteien darüber verständigen, welche Ziel-Berechnung auf welchen Datenkategorien durchgeführt werden soll (zB Schnittmengenberechnung von Personenlisten zwischen den beteiligten Parteien). Insofern nehmen alle beteiligten Parteien Einfluss auf die Zwecke und Mittel der Verarbeitung und haben idR ein Eigeninteresse daran teilzunehmen. Diese funktionalen Gesichtspunkte sprechen für das Vorliegen einer gemeinsamen Verantwortlichkeit nach Art 26 DS-GVO.

Praktisch sprechen aufgrund der hohen Datenschutzgarantien allerdings auch Argumente gegen eine allfällige gemeinsame Verantwortlichkeit: Es stellt sich etwa die Frage, ob sich die anderen Verfahrensparteien an der Verarbeitung durch die dateneinbringende Partei beteiligen können, obwohl die eingebrachten Daten ihnen gegenüber keinen Personenbezug aufweisen. Die beteiligten Parteien können Anfragen von Betroffenen in SMPC-Umgebungen – die nicht aus ihren eigenen Datenbeständen stammen – gar nicht selbständig beantworten und müssen die

[104] Vgl ausführlich *Art-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169; *EDSA*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 07.07.2021; sowie auch *Bergauer*, Die Rollenverteilung nach der DS-GVO - zugleich Überlegungen zu einem Übermittlungsprivileg im Konzern innerhalb enger Grenzen, jusIT 2018, 61.
[105] Vgl weiterführend auch *Lang* in *Taeger/Gabel* (Hrsg), DS-GVO[4] (2021) Art 26 Rz 13 ff.
[106] Oft auch als Joint-Controller-Vereinbarung bezeichnet.
[107] Vgl auch *Jahnel*, DS-GVO Art 26.
[108] *EDSA*, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DS-GVO, 7.7.2021, 22.

Anfrage an alle anderen Verarbeitungsparteien weiterleiten. Nur diejenige Partei, welche die Datensätze des Betroffenen in die Verarbeitung eingebracht hat, kann die Betroffenen-Anfrage tatsächlich beantworten. Diese Partei wäre jedoch ohnedies bereits individuell für die Verarbeitung verantwortlich. Insofern könnte ins Treffen geführt werden, dass die anderen Verarbeitungsparteien weniger geeignete Adressaten für eine Verantwortlichkeit sind, als die Parteien, welche die Daten in die SMPC-Umgebung einbringen; wenn auch der Haftungsfonds und die Anzahl der Ansprechpartner:innen durch die gemeinsame Verantwortlichkeit zugunsten der Betroffenen vergrößert wird.

Das Institut der gemeinsamen Verantwortlichkeit wurde vom EuGH in der Vergangenheit extensiv interpretiert und setzt nicht voraus, dass alle beteiligten Akteure tatsächlich Zugang zu den betreffenden personenbezogenen Daten haben.[109] Im konkreten Fall ist daher prima facie nicht von der Hand zu weisen, dass hinsichtlich der Datenaufbereitung, Verschlüsselung und anschließenden Ziel-Berechnung mittels SMPC eine gemeinsame Verantwortlichkeit vorliegt, obwohl durch die Verarbeitung der verschlüsselten Daten mangels Personenbezugs keine risikoerhöhenden Umstände für Betroffene hinzutreten. Insofern unterscheidet sich die Verarbeitung personenbezogener Daten im Rahmen von SMPC-Umgebungen hinsichtlich der Rollenverteilung grundsätzlich nicht von gewöhnlichen Verarbeitungen zu denselben Zwecken; wenn auch die erhöhten Datenschutzgarantien die Verantwortlichkeit der anderen Verarbeitungsparteien „graduell" verringern mögen.[110]

3.5.2. Grundsatz der Zweckbindung

Nach dem Zweckbindungsgrundsatz gem Art 5 Abs 1 lit b DS-GVO müssen personenbezogene Daten *„für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden".* Demnach dürfen personenbezogene Daten nicht zu Zwecken weiterverarbeitet werden, die mit den (originären) Erhebungszwecken nicht vereinbar sind. Dieser Grundsatz ist allerdings nicht so restriktiv zu verstehen, dass eine Verarbeitung zu anderen als den Erhebungszwecken explizit verboten ist.

[109] EuGH 5.6.2018, C-210/16, *Wirtschaftsakademie*, ECLI:EU:C:2018:388; EuGH 29.7.2019, C-40/17, *Fashion ID*, ECLI:EU:C:2019:629.
[110] Vgl zum „Grad von Verantwortlichkeiten" *EDSA*, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DS-GVO, 7.7.2021, 23.

Auszuschließen sind vielmehr nur solche Verarbeitungen, die mit dem ursprünglichen Zweck nicht zu vereinbaren, also *„unvereinbar"* sind. Dh anders ausgedrückt: es kommt darauf an, ob der neue Zweck mit dem ursprünglichen Zweck kompatibel ist.[111] Für die Unterscheidung zwischen kompatiblen und inkompatiblen Zweckänderungen werden in Art 6 Abs 4 DS-GVO demonstrativ eine Reihe von Beurteilungskriterien statuiert (sog „Kompatibilitätstest").[112] Ausschlaggebend ist demnach:

a. *„jede Verbindung"* zwischen dem ursprünglichen und dem neuen Zweck;[113]

b. der *„Zusammenhang"* in dem die Daten erhoben wurden;

c. die *„Art"* der personenbezogenen Daten;

d. die *„möglichen Folgen"* der beabsichtigten Weiterverarbeitung; sowie

e. das Vorliegen von *„geeigneten Garantien"*.

Der Grundsatz der Zweckbindung spielt für die Verarbeitung mittels SMPC praktisch insofern eine große Rolle, als dieses Verfahren häufig in Situationen angewendet wird, in welchen die betreffenden Datenbestände ursprünglich zu einem anderen Zweck erhoben wurden. Denn die gemeinsame Verarbeitung von Datenbeständen mehrerer Verarbeitungsparteien ermöglicht Berechnungen, welche die einzelne Partei nicht vornehmen könnte, zumal sie sich erst durch den Zusammenschluss mehrerer Parteien ergeben; insofern sind die Berechnungen mittels SMPC zum Zeitpunkt der Datenerhebung häufig noch nicht absehbar, weswegen durch die Verarbeitung in SMPC-Umgebungen regelmäßig Zweckänderungen vorliegen.

Ohne einer Kompatibilitätsbewertung im Einzelfall der konkreten Verarbeitung vorzugreifen, sprechen insbesondere die hohen Datenschutzgarantien für Betroffene während der Verarbeitung für die Kompatibilität: Mangels Personenbezugs gegenüber den anderen Verarbeitungsparteien sind die *„möglichen Folgen"* der beabsichtigten Weiterverarbeitung aus Gesichtspunkten der Datensicherheit als gering einzustufen und das Vorliegen von *„geeigneten Garantien"* iSv Art 6 Abs 4 lit e DS-GVO zu bejahen; insbesondere in Fällen wo die Daten von der

[111] Vgl auch die englische Sprachfassung: *„incompatible"*.
[112] Vgl hiezu schon *Art-29-Datenschutzgruppe,* WP 203, Purpose Limitation, 2.3.2013; sowie auch *Bergauer*, Zur Rechtmäßigkeit der (Weiter-)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 2018, 233.
[113] Vgl ausführlich *Roßnagel* in *Simitis/Hornung/Spiecker*, DS-GVO Art 5 Rz 32.

Verarbeitungspartei ursprünglich selbst erhoben wurden und das Vertrauensverhältnis zur betroffenen Person aufrecht ist.[114]

3.5.3. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten sind nach Art 5 Abs 1 lit a DS-GVO „auf rechtmäßige Weise" zu verarbeiten.[115] Demnach muss für jede Verarbeitung eine Rechtsgrundlage nach Art 6 bzw Art 6 iVm Art 9 DS-GVO vorliegen.[116]

Bei staatlich indizierten Verarbeitungen in SMPC-Umgebungen kann als Rechtsgrundlage für nicht-sensible Daten Art 6 Abs 1 lit e bzw lit c DS-GVO herangezogen werden, für deren Rechtmäßigkeit allerdings zusätzlich eine entsprechende gesetzliche Grundlage notwendig ist (Art 6 Abs 3 DS-GVO). Diese gesetzliche Grundlage muss wiederum verhältnismäßig sein und insbesondere den materiellen Eingriffsvorbehalten des Grundrechts auf Datenschutz (§ 1 Abs 2 DSG, Art 8 GRC) und des Grundrechts auf Achtung des Privat- und Familienlebens (Art 8 Abs 2 EMRK, Art 7 GRC) entsprechen. Bei staatlichen Verarbeitungen, die mit SMPC oder einer anderen datenminimierenden Technologie durchgeführt werden sollen, bietet sich zur Wahrung der Verhältnismäßigkeit daher an, materielle Kriterien[117] als Anforderung an die Verarbeitung zu normieren, um sicherzustellen, dass weder die staatliche Eingriffsnorm noch die tatsächliche Verarbeitung überschießend in die grundrechtlichen Schutzbereiche eingreifen.

Bei der Verarbeitung personenbezogener Daten in SMPC-Umgebungen durch Private kommt insbesondere die Einwilligung sowie auch die Verarbeitung im Rahmen von berechtigten Interessen nach Art 6 Abs 1 lit f DS-GVO in Betracht; auf letztere soll hier kurz eingegangen werden:

Die Verarbeitung auf Grundlage von „berechtigten Interessen" ist die zentrale Interessenabwägungsklausel der DS-GVO. Als kumulative Voraussetzung zur Erfüllung dieses Erlaubnistatbestands muss (i.) ein berechtigtes Interesse an der Verarbeitung vorliegen, (ii.) diese Verarbeitung zur Verwirklichung des berechtigten

---

[114] Vgl auch *Scholz* in *Simitis/Hornung/Spiecker*, DS-GVO (2019) Art 6 Abs 4 Rz 61.
[115] Vgl zu Verständnis und Tragweite des Grundsatzes auch *Herbst* in *Kühling/Buchner*, DS-GVO[3] Art 5 Rz 8.
[116] *Buchner/Petri* in *Kühling/Buchner* (Hrsg), DS-GVO[3] (2020) Art 6 Rz 1; *Jahnel*, Kommentar zur DS-GVO Art 6 Rz 4.
[117] Als Vorbild könnten die gesetzlichen Ausformulierungen im Zusammenhang mit dem bereichsspezifischen Personenkennzeichen dienen, die freilich im Sinne der hier in Rede stehenden datenminimierenden Technologie angepasst werden müssten; vgl § 9 E-Government-Gesetz (E-GovG), BGBl I 10/2004 idF BGBl I 119/2022; sowie E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV), BGBl II 289/2004 idF BGBl II 213/2013.

Interesses auch erforderlich sein und dürfen (iii.) die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.[118]

Die möglichen berechtigten Interessen[119] zur Durchführung einer Ziel-Berechnung mittels SMPC sind vielfältig und können etwa die Auswertung von (Kunden-)Daten innerhalb einer Unternehmensgruppe aus wirtschaftlichen Gründen umfassen oder die Berechnung eines KI-Modells innerhalb eines Verbunds von Forschungsinstitutionen. Werden der dateneinbringenden Stelle durch die Berechnung keine Ergebnisse offengelegt, so ist dies nicht schädlich, zumal Verarbeitungen grundsätzlich auch zugunsten der Interessen von Dritten auf Art 6 Abs 1 lit f DS-GVO gestützt werden dürfen.[120]

Jedenfalls müssen die angestrengten Verarbeitungen aber zur Wahrung dieser Interessen auch tatsächlich erforderlich sein, dh es dürfen keine milderen, gleich effektiven Mittel zur Verfügung stehen. Sofern die Berechnung nicht alleine durchgeführt werden kann, weil die Ziel-Berechnung nur im Verbund mit den Datenbeständen anderer Parteien möglich ist, darf die Verarbeitung mittels SMPC für Betroffene als besonders schonend qualifiziert werden, weshalb auf Ebene der Erforderlichkeit keine besonderen Probleme, die gegen eine Verarbeitung sprechen würden, auftreten sollten.

Darüber hinaus ergeben sich durch die zwingend datenminimierende Ausgestaltung von SMPC-Umgebungen besonders hohe Datenschutzgarantien für Betroffene, die eine Verarbeitung außerhalb des angestrebten Verarbeitungszweckes verunmöglichen und keine Spiegelung oder Weitergabe der Daten ermöglichen. Diese Umstände sind bei der Beurteilung, ob die Interessen oder Grundrechte und Grundfreiheiten von Betroffenen einer Verarbeitung entgegenstehen, zugunsten des Vorliegens berechtigter Interessen zu berücksichtigen. Wenn auch nicht verkannt werden darf, dass bei der Durchführung dieser Interessenabwägung stets auf den Einzelfall abgestellt werden muss; daher ist etwa in Fällen wo Datenverarbeitungen der Erstellung von Persönlichkeitsprofilen dienen mE von einem Überwiegen schutzwürdiger Interessen von Betroffenen auszugehen.

---

[118] EuGH 11.12.2019, C-708/18, *Asociatia de Proprietari bloc M5A-ScaraA*, ECLI:EU:C:2019:1064, Rn 40.
[119] Vgl etwa *Jahnel*, Kommentar zur DS-GVO Art 6 Rz 66.
[120] *Klar/Kühling* in *Kühling/Buchner*, DS-GVO[3] Art 6 Abs 1 lit f Rz 146a.

4. Anwendungsfall Strompreisbremse

Medienberichten zufolge scheitert die Umsetzung zielgerichteter staatlicher Maßnahmen häufig an Datenschutzbedenken.[121] So wurden auch jüngst bei der sog „Strompreisbremse"[122] datenschutzrechtliche Bestimmungen als Verhinderungsgrund für eine zielgerichtete Förderung ins Treffen geführt und schließlich eine Pauschal-Lösung umgesetzt.[123] Im Folgenden soll am Beispiel der „Strompreisbremse" daher kurz vorgestellt werden, wie zielgerichtete staatliche Maßnahmen in einer datenschutzschonenden Weise mittels SMPC umsetzbar wären.

Als Sachverhalt wird angenommen, dass für jeden Haushalt eine zielgerichtete Förderhöhe[124] auf Basis des Haushaltseinkommens, des letztjährigen Stromverbrauches sowie der Art des Wohnsitzes berechnet werden soll. Für diese Berechnung müssen Informationen von drei unterschiedlichen Datenquellen (Parteien) herangezogen werden: Einkommen (Finanzministerium), Energieverbrauch (Energieversorger) sowie Meldedaten (Innenministerium).

SMPC ermöglicht es den drei Parteien, die Förderhöhe jedes einzelnen Haushalts zu berechnen, ohne dass dabei Informationen außer der Förderhöhe miteinander geteilt werden müssen:[125] Alle verarbeiteten Informationen (Einkommen, Energieverbrauch und Meldedaten) bleiben während der gesamten Berechnung der Förderhöhe verschlüsselt und sind für die beteiligten Parteien nicht einsehbar. Auch die Förderhöhe selbst muss nur an jene Parteien ausgegeben werden, die sie zwingend für die weitere Abwicklung benötigen.

Wie bei den Ausführungen zur Rechtmäßigkeit der Verarbeitung erwähnt, ist bei staatlich indizierten Verarbeitungen eine (explizite) gesetzliche Grundlage notwendig.[126] Diese Rechtsgrundlage müsste mangels bestehender einschlägiger Bestimmungen eigens positiviert werden und darf als staatliche Eingriffsnorm nicht überschießend in grundrechtlich verbürgte Schutzbereiche eingreifen. Um die Verhältnismäßigkeit dieser (neuen) Eingriffsnorm zu wahren und den einschlägigen

[121] Vgl etwa *Oberhofer,* Regierung auf der Datenbremse, DerStandard, 11.9.2022, <https://www.derstandard.at/story/2000138979110/regierung-auf-der-datenbremse-und-taeglich-gruesst-das-murmeltier>.
[122] Unter dem Titel „Strompreisbremse" wurden unterschiedliche staatliche Maßnahmen zur Senkung des Strompreises für Konsument:innen diskutiert.
[123] Vgl Bundesgesetz über die befristete Einführung eines Stromkostenzuschusses für Haushaltskundinnen und Haushaltskunden (Stromkostenzuschussgesetz – SKZG), BGBl I 156/2022.
[124] Zielgerichtet bedeutet in diesem Fall, allen Haushalten eine verhältnismäßig gleiche Kompensation zukommen zu lassen.
[125] Vgl für den Technischen Hintergrund auch 2.2. „Beispiel Schnittmengenberechnung".
[126] Vgl oben 3.5. „Rechtmäßigkeit der Verarbeitung".

grundrechtlichen Anforderungen[127] zu entsprechen, könnten die oben ausgeführten datenminimierenden Garantien als materielle Kriterien[128] in die neue Bestimmung mitaufgenommen werden: Denkbar wäre etwa, die Berechnung der Förderhöhe an ein striktes „Need-to-know-Prinzip" sowie an ein „Informations-Duplizierungsverbot" zu binden. Auf diese Weise wäre gesetzlich sichergestellt, dass keine zentralisierte Datenbank[129] angelegt werden darf und die Verarbeitung auf das technisch erforderliche Ausmaß beschränkt ist, ohne dabei Informationen an beteiligte Parteien offenzulegen, die für die Abwicklung der Förderung nicht absolut erforderlich sind. Im Ergebnis könnte damit eine zielgerichtete Förderung verwirklicht werden, ohne auf datenschutzrechtlich gebotene Vorkehrungen zu verzichten.

5. Conclusio

Das Innovationspotenzial von SMPC liegt in der Möglichkeit Auswertungen an umfangreichen Datenbeständen mehrerer Parteien in einer Weise vornehmen zu können, als wären sämtliche Daten an einer Stelle gebündelt zusammengeführt, ohne dass diese Datenbestände – im datenschutzrechtlichen Sinne – gegenüber den anderen Parteien offengelegt werden müssen: Die teilnehmenden Verarbeitungsparteien haben weder technisch noch organisatorisch die Möglichkeit, auf Daten, die von anderen Parteien in die SMPC-Umgebung eingebracht werden, zuzugreifen.

Damit können im Ergebnis mithilfe von SMPC auch Verarbeitungen zwischen Parteien vorgenommen werden, die sich gegenseitig nicht vertrauen oder ihre Datenbestände aus Wettbewerbs- bzw Geheimnisschutzerwägungen nicht miteinander teilen möchten. Die Technologie vermag in diesem Sinne die beiden antagonistisch ausgerichteten Ziele „Datenschutz" sowie „Freier Datenverkehr" ohne (größere) Abstriche beiderseits zu fördern; und zwar auch in Konstellationen und Bereichen in denen im Wege der klassischen Klartext-Verarbeitung kein Datenverkehr zustande kommen würde.

---

[127] Insbesondere Grundrecht auf Datenschutz (§ 1 Abs 2 DSG, Art 8 GRC) und Grundrecht auf Achtung des Privat- und Familienlebens (Art 8 Abs 2 EMRK, Art 7 GRC).

[128] Vgl auch die Kriterien im Zusammenhang mit dem bereichsspezifischen Personenkennzeichen in § 9 E-Government-Gesetz (E-GovG), BGBl I 10/2004 idF BGBl I 119/2022.

[129] Vgl die Bedenken rund um das untechnisch oft als „Super-Datenbank" bezeichnete Register im Zusammenhang mit dem „Grünen Pass", das letztlich nie umgesetzt wurde; *Bierbauer/Piska*, COVID-19: Grundrechtsdogmatik in der Krise?, ZTR 2021, 69; Ministerialentwurf 122/ME XXVII GP, <https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00122/index.shtml>

Die Untersuchungen zum Personenbezug haben gezeigt, dass die DS-GVO auf alle personenbezogenen Daten, die zum Zweck einer Ziel-Berechnung mittels SMPC aufbereitet und verschlüsselt werden, Anwendung findet. Hierdurch ist grundsätzlich nicht mit dem Auftreten von Rechtsschutzlücken zu rechnen.

Der Umstand, dass die von einer Partei eingebrachten Datenbestände nach deren Verschlüsselung gegenüber den anderen beteiligten Parteien als nicht personenbezogen einzustufen sind, ist eine gewichtige Datenschutzgarantie, die bei der Beurteilung der Zweckkompatibilität sowie bei Interessenabwägungen zur Rechtmäßigkeit der Verarbeitung nach Art 6 Abs 1 lit f DS-GVO Berücksichtigung finden muss.

Durch die hohen Datenschutzgarantien und der Möglichkeit zur gemeinsamen Datenverarbeitung ohne Offenlegung eignet sich SMPC als PET für eine besonders datenminimierende und grundrechtsschonende Verarbeitung personenbezogener Daten. Dennoch findet die Technologie bis dato nur zaghaft Anwendung und Verantwortliche greifen vielfach eher auf organisatorische oder konservative technische Maßnahmen zurück. Dies mag neben Rechtsunsicherheit beim Einsatz neuer Methoden auch insbesondere dem aktuell noch höheren Ressourcenaufwand beim Einsatz von PETs geschuldet sein. Durch die erfolgversprechenden Ergebnisse der Forschung[130] und der zunehmenden Skalierbarkeit[131] dieser Technologien ist jedoch mittelfristig mit einer Etablierung im Methodenkanon des Stands der Technik zu rechnen; weswegen die Kenntnis dieser Technologie auch für Jurist:innen zweckmäßig ist.

[130] *Archer/Bogdanov/Lindell/Kamm/Nielsen/Pagter/Wright*, From keys to databases. real-world applications of secure multi-party computation, The Computer Journal, 2018, 1749-1771.

[131] *Kales/Rechberger/Schneider/Senker/Weinert*, Mobile Private Contact Discovery at Scale. USENIX Security Symposium, 2019, 1447-1464.
Bogdanov/Kamm/Kubo/Rebane/Sokk/Talviste, Students and Taxes: a Privacy-Preserving Study Using Secure Computation, Vol. 3 Proc. Priv. Enhancing Technol. 2016, 117-135.