Beschluss
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder vom 17. Juni 2026

Datenschutz im Kontext von Integrated Sensing and Communication (ISAC)

Positionspapier zum Standardisierungsvorhaben im Bereich WiFi und Mobilfunk der sechsten Generation (6G)

1. Einführung

Mit **Integrated Sensing and Communication**, kurz ISAC, soll Radar-Sensorik zukünftig mit verbreiteten Funk-Technologien gekoppelt werden. Die Idee hierbei ist, die bestehende Funk-Kommunikation (elektromagnetische Wellen) so anzupassen, dass sie gleichzeitig als Funk-Sensorik (Radarfunktionalität) genutzt werden kann. So lassen sich Kommunikation und Sensorik (Sensing) in einem System und Frequenzspektrum betreiben. Derzeit bedarf Sensing noch einer proaktiven Nutzung von dedizierten Sensorik-Geräten. Zukünftig wird potentiell jedes Gerät, welches Funk-Kommunikation betreiben kann, auch in der Lage sein, als Radarsensor zu fungieren, was einen flächendeckenden Einsatz zur Folge hat.

Sensing beschreibt die Fähigkeit, physikalische, chemische oder biologische Signale aus der Umwelt automatisiert zu erfassen und zu interpretieren, um so ein vertieftes Verständnis über die Umgebung zu erlangen. Mit der Etablierung des Internets der Dinge (IoT) werden dazu geeignete Sensoren immer häufiger in Alltagsgegenständen integriert. Neben bekannten optischen (bspw. Video, Lidar oder Wärmebild) oder akustischen Sensoren (bspw. Mikrofone), kommen hierbei u. a. auch Radar-Sensoren zum Einsatz.

Radar, die Abkürzung für "radio detection and ranging", beschreibt verschiedene Erkennungs- und Ortungsverfahren auf Basis elektromagnetischer Wellen, welche von Objekten innerhalb des Strahlungsbereiches reflektiert werden. Auf Basis der reflektierten Signale können Informationen über die entsprechenden Objekte gewonnen werden. Genutzt wird dies insbesondere für die Erkennung, Entfernungsmessung und Ortung von Objekten.

ISAC kann dabei in Verbindung mit unterschiedlichen Arten von Kommunikationssystemen bzw. -technologien verwendet werden. So soll zum einen das **WiFi-Sensing**[1] mit der Entwicklung des **IEEE 802.11bf Standards** etabliert werden. Zum anderen soll mit der Entwicklung des neuen **Mobilfunkstandards der 6. Generation (6G)**, welcher voraussichtlich

[1] https://xplorestaging.ieee.org/document/10547188 , https://www.ieee802.org/11/Reports/tgbf_update.htm

um das Jahr 2030 eingeführt wird[2], ISAC auch im Mobilfunk etabliert werden und somit eine "integrierte mehrdimensionale Erfassung zur Verbesserung der unterstützten Navigation und hochpräzisen Positionierung, einschließlich Objekt- und Anwesenheitserkennung, Lokalisierung, Bildgebung und Kartierung" ermöglichen[3]. Im Mobilfunk-basierten ISAC können dabei nicht nur Basisstationen, sondern ebenso alle angebundenen Endgeräte, bspw. Smartphones, als Sensoren fungieren. Zudem gibt es Bestrebungen, auch WiFi-Sensing im 6G Standard zu integrieren[4].

Diese sensorischen Fähigkeiten, integriert als Basisdienst in zukünftigen Funknetzen, bieten eine Vielzahl potentieller Anwendungsbereiche. Gleichzeitig ermöglicht ISAC aber auch eine übergreifende und weitreichende Überwachung des öffentlichen wie auch des privaten Raumes und erzeugt damit **regulative Herausforderungen** im Hinblick auf den Schutz personenbezogener Daten. In diesem Positionspapier sollen deshalb in einem ersten Schritt die grundlegenden beteiligten Entitäten sowie die Vereinbarkeit aktueller datenschutzrechtlicher Regulation mit der Einführung von ISAC und damit einhergehende regulative Herausforderungen beleuchtet werden. Grundlegend lassen sich entsprechende Herausforderungen auch auf andere Sensing-Bereiche übertragen.

2. Zukünftige Anwendungsfelder für ISAC

Die Anwendungsbereiche[5] von Radar-Sensorik sind vielfältig und reichen vom Flug- und Schiffsverkehr, über die Raumfahrt, die Geologie, die Archäologie, bis hin zum Automobilbereich, bspw. für automatische Abstandshalter oder Einparkhilfen.

Die Integration von Radar-Sensorik in zukünftige Funkstandards mittels ISAC ermöglicht dabei potentiell eine flächendeckende Erfassung von Bewegungen, Positionen, Objektdichte und auch Materialstrukturen direkt über die Kommunikationsinfrastruktur und vereinfacht und erweitert damit mögliche Anwendungsfelder, ohne dedizierte Sensorik-Hardware verteilen zu müssen.

Im **Bereich Verkehr** hilft die dadurch ermöglichte präzise Ortung (Geolokalisation) von Objekten und genaue Situationserkennung insbesondere im Bereich des autonomen Fahrens, der Verkehrsüberwachung, der mobilen Robotik oder Drohnensteuerung – ggf. auch in Ergänzung zu optischer Sensorik, welche Einschränkungen beim Erfassen großer Umgebungen und bei schlechten Wetterbedingungen aufweist[6]. Auch die Überwachung von Bahnübergängen bis hin zur einfachen Unterstützung bei der Parkplatzsuche gehören hier zu den potentiellen Anwendungsgebieten.

Auch für den Bereich der **Meteorologie** ergeben sich neue Möglichkeiten, bspw. durch verbesserte und weitreichende **Niederschlagsüberwachung** für Katastrophenschutz, Landwirtschaft, Forschung, oder Wetterdienste[7].

---

[2] https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx

[3] https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I%21%21PDF-E.pdf

[4] 3GPP TR 22.870 V1.0.0 *Study on 6G Use Cases and Service Requirements.* Kapitel 7.17. 2025 - https://ir.interdigital.com/news-events/press-releases/news-details/2026/InterDigital-and-Trk-Telekom-Achieve-Worlds-First-Collaborative-Cellular-and-Wi-Fi-Sensing-Using-Preliminary-6G-Architecture/default.aspx

[5] ETSI GT ISC 001 v1.1.1 Integrated Sensing And Communications (ISAC); Use Cases and Deployment Scenarios. 2025

[6] https://www.vde.com/resource/blob/2103246/e9ead7b7c95eacb5cb7f2eb88103eaa9/position-paper-jc-s--engl---data.pdf

[7] Open6GHub. *JCAS and Privacy*. https://web.archive.org/web/20241107153521/https://www.open6ghub.de/app/uploads/2024/07/JCAS-and-Privacy.pdf

Ein weiteres mögliches Anwendungsfeld ist die Überwachung und Steuerung von **Großveranstaltungen**, etwa von Festivals oder Sportereignissen. So kann das Besucheraufkommen in Echtzeit getrackt werden, bspw. um die Besucherdichte zur Vermeidung kritischer Menschenmengen zu messen oder um die Besucherströme gezielt zu lenken. Weiterhin sind Lenkungsmöglichkeiten bei Evakuierungen sowie eine Unterstützung der Einsatzleitung bei Sicherheitsvorfällen oder Notfalleinsätzen denkbar. Notwendigerweise müsste der Mobilfunkanbieter bzw. Provider die erfassten Bewegungsdaten, die aus der Netztechnik stammen, zur Veranstaltungssteuerung weitergeben. Adressaten wären zum Beispiel die Veranstalter und Betreiber der Veranstaltungsstätte und ggf. Betreiber digitaler Dienste für Veranstaltungsmanagement sowie Polizei und Rettungsdienste als staatliche Akteure. Im Vergleich zu bspw. mobilem Crowd-Sensing[8], was auch durch ISAC in verschiedenen Aspekten komplementiert werden könnte, verstärken sich hier allerdings auch die Aspekte der fehlenden Transparenz, Kontrolle bzw. potentieller Überwachungsmöglichkeiten sowie der Umfang der Datenerhebung und die Risiken der Profilbildung, ohne dass eine konkrete Interaktion mit Geräten erfolgt.

ISAC bietet auch im Zusammenspiel mit **Augmented-Reality**(=AR)-Anwendungen neue Möglichkeiten, die damit standort- und kontextbezogene Informationen in Echtzeit bereitstellen können. AR wird damit nahtloser und immersiver[9]. Ultra-niedrige Latenz ermöglicht flüssige Interaktionen sowie präzise Positionsdaten, sodass virtuelle Inhalte exakt in die reale Umgebung integriert werden können. Mit dieser Nutzung entsteht jedoch auch ein komplexes Beziehungsgeflecht zwischen den beteiligten Akteuren: Privatpersonen werden einerseits zu Empfängern personalisierter Dienste, andererseits aber auch zu Datenquellen. Gerätehersteller bzw. Plattformbetreiber sichern sich hier eine Schlüsselrolle, da sie nicht nur die Hardware, sondern auch die dafür erforderlichen Daten- und Sensortechnologien kontrollieren. AR macht Privaträume, Personen und Verhaltensweisen digital erfassbar, in der Regel ohne dass es den Nutzenden bewusst ist. Zudem wird AR oft von Kindern spielerisch genutzt, hier stellt sich die Frage nach entsprechenden technischen und organisatorischen Schutzmechanismen. Weitere kritische Aspekte kommen hinzu, wenn zusätzlich der Einsatz von KI integriert wird[10].

Einen Anwendungsbereich für WLAN- oder WiFi-Sensing[11] stellt u. a. der Bereich der **Medizin** und dort beispielsweise die Beobachtung von Vitalparametern wie Atmung oder Herzschlag, aber auch die Detektion von Anwesenheit, Stürzen oder Bewegungslosigkeit von Personen dar[12]. Mittels ISAC genügen hierfür (künftige) WiFi-fähige Geräte. Denkbar wäre etwa ein Einsatz in einem Krankenhaus oder bei der ambulanten Pflege. Akteure sind in diesem Anwendungsbeispiel die Personen, deren Aktivitäten mit Hilfe des WiFi-Sensing registriert und ausgewertet werden („Betroffene“), sowie die Personen, die diese Ergebnisse weiterverarbeiten. Beteiligt auf Hardwareseite sind die in das Monitoring involvierten Geräte sowie diejenigen Geräte, die für die Auswertung der Rohdaten und die Darstellung der Ergebnisse genutzt werden. Je nach Ausgestaltung der Verarbeitung erfolgt die Auswertung der Rohdaten auf der vorhandenen Hardware lokal im Heimnetzwerk oder außerhalb der eigenen Räumlichkeiten, ggf. unter Einbindung weiterer Parteien, bspw. des Zugangsproviders. Bestehende Zugriffsmöglichkeiten auf die Daten hängen zudem davon ab, wo die Ergebnisse dargestellt werden – ein Zugriff kann z. B. von innerhalb des Heimnetzes

---

[8] Schierbaum, Vesna. *Mobile Crowdsensing: Interaktionsmodelle des mobilen Sensing und die infrastrukturelle Allgegenwart der ›mobile sensor networks‹*. Un/Reale Interaktionsräume: Formen sozialer Ordnung im Spektrum medienspezifischer Interaktion. 2024

[9] https://www.rohde-schwarz.com/de/unternehmen/magazine/6g-vision-or-reality/6g-vision-oder-wirklichkeit_255445.html, Stand: 13.03.2026.

[10] Méndez, Julián and Satkowski, Marc. *ARbiter: Generating Dialogue Options and Communication Support in Augmented Reality*. arXiv. 2025. https://arxiv.org/abs/2503.05220

[11] Du, Rui, et al. *An overview on IEEE 802.11 bf: WLAN sensing.* IEEE Communications Surveys & Tutorials. 2024

[12] https://web.archive.org/web/20250316193547/https://www.telekom.com/de/konzern/details/wi-fi-sensing-einfach-erklaert-1087176

erfolgen (bspw. in einem Krankenhaus) oder von außerhalb (z. B. im Szenario der ambulanten Pflege). Wird die Methodik bestimmungsgemäß angewendet, sind der Erfassungsbereich, die Beteiligten sowie die Datenströme schnell erfasst und die Verarbeitung kann z.B. auf der Grundlage einer Einwilligung erfolgen. Die Gefahr einer missbräuchlichen Nutzung hingegen ist groß: WiFi-fähige Geräte (z.B. Smartphones, Laptops oder WLAN-Access-Points) sind omnipräsent und werden – im Gegensatz zu Videokameras – nicht mit Überwachung assoziiert.

3. Rechtliche und technische Überlegungen

Die im vorangegangenen Abschnitt erläuterten Anwendungsfälle verdeutlichen exemplarisch die umfassende Überwachung, die durch den geplanten omnipräsenten Einsatz von ISAC möglich wird. Die künftige Etablierung von ISAC als Teil der Telekommunikationsinfrastruktur (WiFi und Mobilfunk) birgt deshalb erhebliche Herausforderungen für den Datenschutz, wie bspw. das European Telecommunications Standards Institute (ETSI) in einem aktuellen Bericht zu 6G aufzeigt[13].

Forschungsarbeiten beschäftigen sich seit längerem mit der Frage der Personenbeziehbarkeit radargestützter Objekterfassung. Die Ergebnisse zeigen, dass erfasste Radardaten in Kombination mit maschinellem Lernen das Inferieren von Objekteigenschaften ermöglichen, die weit über eine simple Objekterkennung hinausgehen. Dies reicht von der Unterscheidung und Erkennung von Personen[14] durch die Extraktion biometrischer Indikatoren wie bspw. der Gangart, des Geschlechts, von Gesichtsmerkmalen oder Gesten, bis hin zu Atmungs- und Herzschlag-Analysen[15]. Dies umfasst also auch besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO.

Die Möglichkeiten der Extraktion sind dabei u. a. abhängig von der Art und physischen Eigenschaften der genutzten elektromagnetischen Wellen. Neben der Objekterkennung ist derzeit noch nicht abschließend abzuschätzen, welche Möglichkeiten mit dem neuen 6G Standard via ISAC flächendeckend erreicht werden können.

Grundlegend ist bzgl. ISAC eine Personenbeziehbarkeit, sei es durch unmittelbare Erkennung oder Wiedererkennung individueller Personen oder durch eine Identifizierung unter Hinzunahme weiterer Informationen, gegeben, so dass in aller Regel der Geltungsbereich der datenschutzrechtlichen Vorschriften eröffnet ist. Mit der Fähigkeit der zugrundeliegenden Radartechnik, auch Hindernisse wie bspw. Wände zu durchdringen, könnte zudem u. a. auch das Recht auf die Unverletzlichkeit der Wohnung gemäß Art. 13 GG tangiert werden. Dies würde zusätzlich einen besonders schwerwiegenden Grundrechtseingriff darstellen. Auf die sich aufdrängende Parallele zum „visuellem Sensing“, bei welchem Eingriffe in § 201a StGB sogar strafrechtlich sanktioniert sind, sei gesondert hingewiesen.

---

[13] ETSI GR ISC 004 V1.1.1 *Integrated Sensing And Communications (ISAC); Security, Privacy, Trustworthiness and Sustainability*. 2026

[14] J. Todt, F. Morsbach and T. Strufe, *BFId: Identity Inference Attacks Utilizing Beamforming Feedback*. 2025 Information, ACM CCS, 2025, https://publikationen.bibliothek.kit.edu/1000185756/168100988

[15] https://github.com/NTUMARS/Awesome-WiFi-CSI-Sensing Stand: 13.03.2026
- Martins, Óscar G., et al. *Delving Into Security and Privacy of Joint Communication and Sensing: A Survey.* IEEE Open Journal of the Communications Society. 2025.
- Liu, Jian, et al. *Wireless sensing for human activity: A survey*. IEEE Communications Surveys & Tutorials. 2019.

3.1 Betrachtung der beteiligten Entitäten

Die konkrete Verantwortlichkeit bei der Datenerfassung und Verarbeitung von Sensing-Daten wird allein durch die Vielzahl beteiligter Akteure unübersichtlich. Dies reicht von Zugriffsmöglichkeiten auf Sensordaten durch Betriebssysteme, lokale Anwendungen, bis hin zu Gerätebesitzern selbst. Bei der Integration von ISAC in WLAN und Mobilfunknetze müssen zusätzlich die Infrastrukturbetreiber sowie Anwendungsanbieter mit Zugriff auf die Sensing-Daten der Telekommunikationsanbieter berücksichtigt werden.

Als potentiell **verantwortliche Akteure** explizit zu berücksichtigen wären also:

- Hersteller von Infrastrukturkomponenten,
- Infrastrukturanbieter (Telekommunikationsprovider, WiFi Provider etc.),
- Anwendungsanbieter mit Zugriff auf globale Sensing-Daten (Zugriff auf Telekommunikationsanbieter-Daten),
- Anwendungsanbieter mit Zugriff auf lokale Sensing-Daten (bspw. App-Anbieter für Endgeräte),
- Betriebssystemhersteller von Sensing-fähigen Geräten mit Zugriff auf lokale Sensing-Daten,
- Endnutzer mit Zugriff auf lokale Sensing-Daten.

Privatpersonen würden einen direkten Beitrag zur Erhebung und Weitergabe von Sensing-Daten leisten, schon allein durch die Nutzung entsprechender Endgeräte. Den Herstellern kommt hierbei eine besondere Rolle zu, da ihre Produkte die Grundlage für die Verarbeitung personenbezogener Daten und den Rahmen für deren datenschutzrechtskonforme Ausgestaltung liefern. Bei der Konzeption der eingesetzten Komponenten und Produkte sollte daher ein besonderes Augenmerk daraufgelegt werden, dass diese die Anforderungen des Datenschutzes durch Technikgestaltung bestmöglich unterstützen.

Die Verarbeitungsobjekte von ISAC sind insbesondere natürliche Personen. Ähnlich dem Einsatz audiovisueller Sensoren sind dabei nicht nur aktive Nutzer solcher Systeme betroffen, sondern potentiell alle Personen, die in den Bereich der Sensorik-Erfassung geraten, hier bezeichnet als Bystander. Diese müssen dabei nicht zwingend mobile Endgeräte mit sich führen, was insbesondere die Herstellung von Transparenz und die Einholung von Einwilligungen erschweren dürfte.

Als potentiell **betroffene Akteure** zu berücksichtigen wären also:

- Bystander mit/ohne mobilem Endgerät und
- Endnutzer mit aktiver Beteiligung am Sensing.

3.2 Betrachtung der Rechtsgrundlagen

Hinsichtlich der Rechtsgrundlagen ergeben sich besondere Herausforderungen. Die Verarbeitungen und Anwendungen im ISAC-Umfeld stehen vor dem Problem, dass sich möglicherweise nicht die gesamte Bandbreite potentieller Verarbeitungen personenbezogener Daten auf die die von der DSGVO eröffneten Rechtsgrundlagen für die stützen lässt. Die DSGVO benennt in Art. 6 Abs. 1 die folgenden Rechtsgrundlagen: Einwilligung, Vertragserfüllung, rechtliche Verpflichtungen, lebenswichtige Interessen, öffentliche Interessen und berechtigtes Interesse des Verarbeiters.

Eine *Einwilligung* gemäß Art. 6 Abs. 1 Buchst. a DSGVO als Rechtsgrundlage erweist sich im Bereich der flächendeckenden Sensorik als ungeeignet, um die Nutzung einer Technologie zu rechtfertigen, von der eine Vielzahl von Personen betroffen sind, inkl. der Bystander ohne mobile Endgeräte. Allein die Erreichbarkeit aller von der Datenverarbeitung betroffenen Personen im Vorfeld ist mit erheblichen praktischen Schwierigkeiten verbunden. Dies lässt die Möglichkeit zur Einholung wirksamer Einwilligungen fraglich erscheinen, insbesondere vor dem Hintergrund der Anforderungen an eine solche gemäß Art. 7 DSGVO und ErwGr. 32 DSGVO. Ferner stellt sich die Frage, welche Folgen es hat, wenn eine eventuelle Zustimmung nicht erteilt oder widerrufen wird. Lediglich in zeitlich und räumlich begrenzten Anwendungsszenarien ist es daher überhaupt vorstellbar, mit einer Einwilligung eine Rechtsgrundlage für eine Verarbeitung zu schaffen.

Aufgrund noch unbekannter möglicher Einsatzszenarien bzw. fehlender rechtlicher Regelungen ist derzeit noch nicht abzusehen, inwiefern die Rechtsgrundlagen der *Vertragserfüllung* oder der Erfüllung *rechtlicher Verpflichtungen* geeignet sein können, um den Einsatz von ISAC zu legitimieren.

Denkbar sind Einsatzmöglichkeiten aufgrund *lebenswichtiger Interessen* von Betroffenen. Hier sind Möglichkeiten im medizinischen Bereich (z. B. Erkennung von gefährlichen Situationen und Alarmierung im Pflegesektor) oder im Bereich der Überwachung lebensbedrohlicher Gefahrenstellen (z. B. Erkennung von Personen auf Gleisen im Bahnverkehr) vorstellbar. Soweit der Anwendungsbereich des Art. 9 DSGVO durch das Sensing eröffnet ist, wäre allerdings auch für die Einsatzmöglichkeiten aufgrund lebenswichtiger Interessen nach Art. 9 Abs. 2 Buchst. c DSGVO zusätzlich erforderlich, dass die betroffene Person „aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben“.

Ein breitflächiger Einsatz von ISAC ist daher derzeit vor allem auf Basis der Rechtsgrundlagen des *öffentlichen Interesses* oder des *berechtigten Interesses* des Verarbeiters vorstellbar. Sollte ISAC im öffentlichen Interesse (z. B. zur Unterstützung der Sicherheitsbehörden) eingesetzt werden, erfordert dies ggf. die Schaffung einfachgesetzlicher Grundlagen. Die Rechtfertigung über ein berechtigtes Interesse von verarbeitenden privaten Stellen erfordert wiederum eine Abwägung mit den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen; die Eingriffstiefe ist dabei – wie oben dargestellt – erheblich. Ist Art. 9 DSGVO anwendbar, kann allein ein überwiegendes Interesse privater Stellen im Sinne des Art. 6 Abs. 1 Buchst. f DSGVO oder ein öffentliches Interesse im Sinne des Art. 6 Abs. 1 Buchst. e DSGVO zudem nicht genügen, sondern bedarf zusätzlich einer Verarbeitungsbefugnis im Sinne des Art. 9 Abs. 2 DSGVO.

Grundsätzlich lässt sich ISAC hinsichtlich der möglichen Eingriffstiefe mit einer nicht wahrnehmbaren Videoüberwachung vergleichen, die zusätzlich zur optischen Erfassung auch das Potenzial hat, nicht-sichtbare Bereiche zu erfassen. Potenziell ist damit ein sehr hohes Risiko eines tiefgreifenden Eingriffs in Persönlichkeitsrechte gegeben. Dies ist insbesondere zu beachten, wenn private Akteure Anwendungen und Szenarien auf Basis eines berechtigten Interesses planen und umsetzen wollen. Die datenschutzrechtliche Praxis hat in vielen Fällen gezeigt, dass insbesondere das berechtigte Interesse von Seiten der Verantwortlichen nicht selten überdehnt und einseitig zu Lasten der betroffenen Person ausgelegt wird bzw. eine Feststellung der mit der Verarbeitung verbundenen Risiken nur punktuell erfolgt.

3.3 Datenschutz durch Technikgestaltung

Ziel des Datenschutzes durch Technikgestaltung ist es, durch technische und organisatorische Gestaltung die Eingriffe in Persönlichkeitsrechte auf ein erforderliches und angemessenes Maß zu reduzieren.

Dies kann zum einen durch Transparenz erreicht werden. Die Schaffung von angemessener Transparenz im Hinblick auf die Verarbeitung personenbezogener Daten und von Einwirkungsmöglichkeiten betroffener Personen im Bereich flächendeckender Radar-Sensorik scheint jedoch fragwürdig. Während bei fest installierten optischen Sensoren (bspw. Überwachungskameras) eine analoge Transparenz (bspw. Schilder) noch geeignet erscheint, ist dies im dynamischen und mobilen IoT Bereich (Smartphones, Drohnen, AR Brillen, Fahrzeuge etc.) und bzgl. ISAC allgemein (Infrastruktur) nicht praktikabel. Transparenz ist hier allenfalls durch digitale Informationen erreichbar. Allerdings bleiben betroffene Bystander ohne mobiles Endgerät von solchen Maßnahmen ausgeschlossen.

Zum anderen ist es notwendig, Technik durch Gestaltung vom Möglichen hin zum Erforderlichen zu bewegen. Dies entspricht dem in der DSGVO festgelegten Grundsatz der Datenminimierung. Die Privacy-Forschung bietet hierfür verschiedene Lösungsansätze – von spezifischen ISAC-Architekturvorschlägen[16], welche konkrete Datenschutz-Herausforderungen adressieren, bis hin zu generellen Anonymisierungs- und Pseudonymisierungstechniken. Unter letzteres fallen Methoden wie Datenaggregation, Randomisierung oder Maskierung, mit deren Hilfe identifizierende Informationen schon während des Sensings entfernt werden könnten. Methoden der differential privacy o. Ä. bewahren statistische Eigenschaften, während sie Rauschen in die Daten einfügen, um konkrete Identifikationen zu verhindern[17]. Allerdings bleiben diese Lösungen Use-Case-gebunden, je nachdem welche Sensing-Daten benötigt werden. Da jedoch die Bereitstellung der Sensing-Daten über den Telekommunikationsanbieter für unterschiedliche Use-Cases konzipiert ist, gestaltet sich eine generalisierte Strategie potentiell schwierig, insbesondere gegenüber dem Telekommunikationsanbieter. Derzeit hält keine dieser Methoden Einzug in die Etablierung des WiFi- oder 6G-Standards.

Die Aufsichtsbehörden bieten zahlreiche Praxishilfen, die bei einer Gestaltung einer datenschutzgerechten Umsetzung von Standards hilfreich sind, dies sind insbesondere die vom EDSA verabschiedeten Leitlinien zur Pseudonymisierung[18] bzw. die in Abstimmung befindlichen Leitlinien zur Anonymisierung[19] sowie das für eine Modellierung von Maßnahmen und Managementprozessen zu nutzende Standard-Datenschutzmodell (SDM)[20].

4. Forderungen und Folgerungen

Im Ergebnis lässt sich festhalten, dass es erforderlich sein wird, dass der **Gesetzgeber** sowohl für öffentliche als auch private Akteure die **Schaffung eines Regelwerks für ISAC** anstrengt.

Für eine flächendeckende Einführung von ISAC ist eine **grundlegende Regulierung** unverzichtbar, die die Interessen aller Beteiligten und Betroffenen berücksichtigt. Eine solche

---

[16] Dass et al. *Addressing Privacy Concerns in Joint Communication and Sensing for 6G Networks: Challenges and Prospects. 2024*

[17] Carvalho et al. *Survey on Privacy-Preserving Techniques for Data Publishing*. 2022

[18] https://www.edpb.europa.eu/news/news/2025/edpb-adopts-pseudonymisation-guidelines-and-paves-way-improve-cooperation_de, Stand: 03.03.2026

[19] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/informationen/Europaeischer_Datenschutztag_2026_Daldrop_Operationalisier-ungspapier.pdf, Stand: 03.03.2026

[20] https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/, Stand: 03.03.2026

Regulierung muss datenschutzrechtliche Instrumente bereitstellen, um die möglichen Vorteile der ISAC-Nutzung und die Eingriffe in die Grundrechte der betroffenen Personen in einen angemessenen Ausgleich zu bringen. Weitere Herausforderungen ergeben sich insbesondere aus der potenziellen **Allgegenwärtigkeit der Technologie** und den eingeschränkten Möglichkeiten, Grundrechte auf technischer Ebene zu gewährleisten.

Angesichts der absehbaren Eingriffstiefe von ISAC ist es notwendig, den aktuellen Standardisierungsprozess von 6G im Sinne des „**Data Protection by Design**“ zu gestalten. Dies gilt in besonderem Maße, da durch diesen Prozess nicht zuletzt das Fundament für die später omnipräsente Infrastruktur sowie die damit verbundenen Rollen und Verantwortlichkeiten gelegt wird. Überzeugende technische und regulatorische Lösungen bilden die Grundlage, um ein System wie ISAC erfolgreich etablieren zu können.