

BMBF-Förderprojekte aus dem Bereich Vernetzung und Sicherheit digitaler Systeme - Bekanntmachung Forschungsnetzwerk Anonymisierung für eine sichere Datennutzung

Akronym	Titel	Inhalt	Verbundkoordinator	Partner	Volumen [Mio. €]	Förderanteil BMBF	Laufzeit	Schwerpunkt	Typ	Link	Bemerkungen
SynthiClick	Synthetische Datenerzeugung anhand von Nutzungsverhalten im World Wide Web	Entwicklung neuer Konzepte zur Anonymisierung und Datensynthese, die Reichweitenmessungen, Nutzungsanalysen und Benchmarking im Online-Marketing datenschutzkonform erlauben	Karlsruher Institut für Technologie (KIT)	- INFOline GmbH, Bonn - Leuphana Universität Lüneburg	1,36	86%	12/2022 - 12/2025	Onlinedienste	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/syntheticclick	
SAM-Smart	Sicherheitsassistentenmanager für das Smart Home	Entwicklung eines sozio-technischen Sicherheitsansatzes für das vernetzte Heim , der auf bestehenden Erkenntnissen zur Human-Centered Security basiert. Mithilfe Künstlicher Intelligenz soll er kostengünstige Sicherheitslösungen mit automatisierten Korrekturmaßnahmen bieten, die für qualitativ niederwertige Produkte des Massenmarktes genutzt werden können.	Fraunhofer FIT, Sankt Augustin	- Universität Siegen - Universität zu Lübeck - open.ING GmbH, Siegen - nuspace GmbH, Rödental - automITe engineering GmbH, Lübeck - Langlauf GmbH, Paderborn	3,23	88%	12/2022 - 12/2025	Smart Home	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/sam-smart	
PrivacyUmbrella	Sichere Privatheit von Daten durch umfassende Bereitstellung von Anonymisierungsverfahren	Gesundheitsbereich - biomedizinischen klinische Daten: Entwicklung hochspezialisierter Anonymisierungslösungen; Kombination mehrerer bisher isolierter Techniken in einem einzigen integrierten Open-Source-Demonstrator und zeigen, dass die Anonymisierungseigenschaften (Privacy-Metriken) der einzelnen Methoden beibehalten werden können und gleichzeitig eine ganzheitliche kombinierte Definition von Privatheit beziehungsweise Anonymisierung abgeleitet werden kann.	Fraunhofer ITEM, Hannover	- Universitätsmedizin der Johannes Gutenberg-Universität Mainz - Johann Wolfgang Goethe-Universität Frankfurt am Main - MCS Data Labs GmbH, Berlin	2,02	87%	12/2022 - 12/2025	Medizin	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/privacyumbrella	
PATH	Plattform für den Austausch von Gesundheits- und Wellness-Daten	Schaffung einer datenschutzkonformen Plattform, um persönliche Gesundheitsdaten aus Patientenakten mit Daten aus häuslichen Gesundheitssystemen zu verknüpfen. Ein Teilaspekt ist der einfache und nutzungsfreundliche Zugang zu Gesundheitsdaten in einer grafischen Übersicht, welche die notwendige Transparenz für eine effektive Kontrolle durch Nutzende schafft.	Technische Universität Dresden	- Ada Health GmbH, Berlin - Universität Leipzig	3,91	93%	12/2022 - 12/2025	Medizin und Pflege	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/path-1	
NEMO	Nicht-Identifizierbarkeit von Daten aus Elektroenzephalografie für Open Science (NEMO)	Entwicklung neuartiger Anonymisierungserfahren, welche die Re-Identifizierungsrisiken bei der Auswertung der EEG-Daten reduzieren. Die EEG-Daten werden bei klinischen Untersuchungen, aber auch über Geräte erhoben, die Patientinnen und Patienten zur Schlafüberwachung auf dem freien Markt kaufen können. Der große Datenpool bietet aufgrund seiner Informationsdichte ein erhebliches Nutzungspotenzial für Forschung und Wirtschaft, birgt aber gleichzeitig ein großes Sicherheitsrisiko.	Fraunhofer IDMT, Oldenburg	- Ascora GmbH, Ganderkesee - Universitätsklinikum Schleswig-Holstein - Campus Kiel	2,03	90%	12/2022 - 12/2025	Medizin	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/nemo	Verbundkoordinator ist Institutsteil des Fraunhofer IDMT, Ilmenau
Medinym	KI-basierte Anonymisierung personenbezogener Patientendaten in klinischen Text- und Sprachdatenbeständen	Untersuchung der Möglichkeit der Weiterverwertung sensibler Daten durch das Entfernen der empfindlichen Informationen mittels Anonymisierung; exemplarische Umsetzung von zwei medizinischen Anwendungsfällen; textbasierte Daten aus der elektronischen Patientenakte sowie Sprachdaten aus diagnostischen Arztin-Patient-Gesprächen	Otto-von-Guericke-Universität Magdeburg	- Technische Universität Berlin - Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI), Kaiserslautern - Charité - Universitätsmedizin Berlin - WEVOSYS medical technology GmbH, Bamberg - Averbis GmbH, Freiburg	3,18	92%	12/2022 - 12/2025	Medizin	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/medinym	
KI-AIM	KI-basierte Anonymisierung in der Medizin	Entwicklung einer Anonymisierungsplattform zum Bereitstellen großer Mengen realitätsnaher Daten, die keinen Personenbezug aufweisen; Forschungsschwerpunkte: Verfahren zur flexiblen Kombination von Anonymisierungsmethoden für sensible Patientendaten und von Synthetisierungsmethoden zur Genese von Datensätzen	Westfälische Wilhelms-Universität Münster	- Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI), Kaiserslautern - Berlin Institute of Health in der Charité - Universitätsmedizin Berlin	1,44	97%	12/2022 - 12/2025	Medizin	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/ki-aim	
GANGES	Gewährleistung von Anonymitätsgarantien in Unternehmensanwendungen	Entwicklung praxisorientierter Anonymisierungsverfahren, die sich an realen Bedarfen mit Anonymitätsgarantien orientieren. Anhand konkreter Anwendungsfälle aus der Energie- und Gebäudewirtschaft sowie von existierenden Basisverfahren neue Verfahren zur Stream-Anonymisierung entwickelt. Dabei werden besonders in der Praxis genutzte, komplexe Datenarten berücksichtigt, die eine besondere Anonymisierungsherausforderung darstellen.	Technische Universität Berlin	- Ampeers Energy GmbH, München	2,37	85%	12/2022 - 12/2025	Energie- und Gebäudewirtschaft	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/ganges	Ampeers Energy ist eine Ausgründung aus dem Fraunhofer IOSB AST Ilmenau und hat Betriebsstätte in Erfurt
EAsyAnon	Empfehlungs- und Auditsystem zur Anonymisierung	Konzipierung eines Empfehlungssystems, welches Datenverantwortlichen basierend auf einer standardisierten Metabeschreibung des spezifischen Datensatzes konkrete Empfehlungen zur Anonymisierung gibt. Berücksichtigung sowohl rechtlicher als auch ethischer Aspekte; Aufbau eines Auditsystems zur kontextbezogenen Bewertung der Zweckmäßigkeit der Anonymität von Datensätzen	THD - Technische Hochschule Deggendorf	- Universität Augsburg - Smart In Media AG, Köln - Passion4IT GmbH, Viechtach - IT-Sicherheitscluster e.V., Regensburg	2,13	90%	12/2022 - 12/2025	allgemein	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/easyanon	
DARIA	Identitätsbetrug und Ausfallrisiko durch datenschutzkonforme Verwertung von Daten minimieren	Erforschung und Erprobung von Verfahren und Werkzeugen, die es ermöglichen aus anonymisierten Kunden- und Nutzerdaten gewonnene Informationen datenschutzkonform zur Betrugsprävention zusammenzuführen. Dazu Auswertung der Datensätze von verschiedenen Onlinediensten und Nutzenden. Die daraus gewonnenen Erkenntnisse sollen unmittelbar genutzt werden, um die Risiken eines Zahlungsausfalls oder Identitätsbetrugs zu erkennen und anschließend zur Prävention des Ereignisfalles verwendet werden.	Rheinische Friedrich-Wilhelms-Universität Bonn	- FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur GmbH, Eggenstein-Leopoldshafen - Universität Duisburg-Essen	1,46	100%	12/2022 - 12/2025	Onlinedienste	Forschungsprojekt	https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/daria	

BMBF-Förderprojekte aus dem Bereich Vernetzung und Sicherheit digitaler Systeme - Bekanntmachung Forschungsnetzwerk Anonymisierung für eine sichere Datennutzung

Akronym	Titel	Inhalt	Verbundkoordinator	Partner	Volumen [Mio. €]	Förderanteil BMBF	Laufzeit	Schwerpunkt	Typ	Link	Bemerkungen
ATLAS	Datentreuhänder für anonymisierte Analysen in kommunalen Datenräumen Hand vor Bildschirmwand	Entwicklung eines Open-Source-Systems, das verschiedene Werkzeuge zur sicheren und datenschutzfreundlichen Speicherung sowie Analyse personenbezogener Daten vereint. Praxistaugliche Lösung durch Verfolgung eines Use-Case-getriebenen Ansatzes; Bestimmung möglicher rechtlicher Risiken bei der Zusammenführung der Daten anhand eigens entwickelter Metriken.	Polyteia GmbH, Berlin	- Hasso-Plattner-Institut für Digital Engineering gGmbH, Potsdam - Technische Universität Berlin - SINE e.V., Berlin - KIProtect GmbH, Berlin - Verband Region Rhein-Neckar, Mannheim	2,41	88%	12/2022 - 12/2025	Öffentliche Verwaltung	Forschungsprojekt	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/atlas	
ANONY-MED	Rechtskonforme Nutzung von Gesundheitsdaten durch Anonymisierung	Entwicklung eines einheitlichen Werkzeugkastens mit Methoden für die Anonymisierung von unterschiedlichen medizinischen Daten zu entwickeln. Die darin enthaltenen Privacy-Metriken sollen es ermöglichen, Daten rechtskonform an Dritte weitergeben und in der Folge für innovative Produkte und Serviceangebote nutzen zu können.	Fraunhofer AISEC, Berlin	- Charité Lab for AI in Medicine (CLAIM) - Charité Universitätsmedizin Berlin - Smart Reporting GmbH, München	1,52	93%	12/2022 - 12/2025	Medizin	Forschungsprojekt	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/anony-med	
AnoMoB	Anonymisierte Erfassung und Nutzung von Mobilitäts- und Bewegungsdaten	Entwicklung von Anonymisierungsverfahren zu entwickeln, die den Anbietenden von Mobilitätsdiensten eine verbesserte Erhebung und Verarbeitung von Mobilitätsdaten ermöglichen und gleichzeitig den Schutzbedürfnissen der Bürgerinnen und Bürger gerecht werden.	Hochschule Esslingen, University of Applied Sciences	- Fraunhofer IAO, Stuttgart - cantamen GmbH, Hannover - MotionTag GmbH, Potsdam	2,76	91%	12/2022 - 12/2025	Mobilität	Forschungsprojekt	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/anomob	
PriSyn	Repräsentative, synthetische Gesundheitsdaten mit starken Privatsphärengarantien	Synthetisierung von Gesundheitsdaten , so dass diese für die Forschung an Behandlungsmethoden und Medikamenten nutzbar sind. Synthetische Daten verfügen über die gleichen Eigenschaften wie reale, geben aber keine privaten Informationen preis. Darüber hinaus werden im Rahmen des Projekts Metriken und Prüfmethode ausgearbeitet, um die Qualität und Anwendbarkeit der synthetischen Daten in verschiedenen Anwendungsfällen, wie der medizinischen Diagnostik und pharmazeutischen Forschung zu bewerten und sicherzustellen.	CISPA - Helmholtz-Zentrum für Informationssicherheit gGmbH, Saarbrücken	- Deutsches Zentrum für Neurodegenerative Erkrankungen e.V. (DZNE), Bonn - QuantPI GmbH, Saarbrücken - Hewlett-Packard GmbH, Böblingen	2,54	88%	12/2022 - 12/2025	Medizin	Forschungsprojekt	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/prisyn	
FIIPS-at-Home	Frühwarn-, Informations- und Angriffserkennungssystem für Smart Home	Entwicklung einer niedrigschwelligen und kostenlosen mobilen Anwendung (FIIPS-App) für Smart-Home-Anwenderinnen und Anwender zu entwickeln, die einen Überblick über die Geräte im Heimnetz ermöglicht, einfache Schwachstellen-Scans durchführt und so ein Problembewusstsein für IT-Sicherheitsrisiken im Heimnetz schafft. Zweite Ausbaustufe: Entwicklung einer aktiven Sensorkomponente (FIIPS-Stick) , die sich auf USB-Sticks installieren lässt, die ständig präsent im Heimnetz Geräte-Fingerprints ermitteln sowie fortlaufend Angriffe auf das Heimnetz erkennen. Dritte Ausbaustufe: Bereitstellung einer aktiven sogenannten Middlebox für den bestmöglichen Schutz, die Verbindungen trennen und Teilnetze abschotten kann, wenn ein Angriff droht.	Universität Hamburg	- Johann Wolfgang Goethe-Universität Frankfurt am Main - Tenzir GmbH, Hamburg	2,28	96%	12/2022 - 12/2025	Smart Home	Forschungsprojekt	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/fiips-at-home	
explanym	Erklärbare Anonymisierung intermodaler Mobilitätsdaten	Pro Anwendungsumgebung werden konkrete Mobilitätsdaten erhoben und verschiedene Varianten von Erklärungen erarbeitet, um das Verständnis von Betroffenen für die Wirkungsweise von Anonymisierungs- und De-Personalisierungstechniken mittels interaktiver Austauschformate, wie zum Beispiel Lernspielen, und verschiedener Informationsmedien zu fördern.	Otto-Friedrich-Universität Bamberg	- Dashfactory GmbH, Jena - HTK Hygiene Technologie Kompetenzzentrum GmbH, Bamberg - Psoido GmbH, Erfurt - safactory GmbH, Bamberg - Stadtwerke Bamberg Verkehrs- und Park GmbH	3,44	84%	12/2022 - 12/2025	Mobilität	Forschungsprojekt	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/explanym	Psoido ist eine Ausgründung aus dem Fraunhofer IDM Dashfactory hat ihren Sitz in Jena
AnGer	Anonymisierung von Gerichtsentscheidungen für die digitale Justiz	Erforschung der Möglichkeiten automatischer Verfahren zur datenschutzkonformen Nutzung von Gerichtsurteilen; Innovationen insbesondere mithilfe von Verfahren der Computerlinguistik und der KI arbeiten; Mit Unterstützung des Bayerischen Staatsministeriums der Justiz werden rechtsgebietspezifische Demonstratoren zur automatischen Anonymisierung von Gerichtsurteilen entwickelt. Um die maschinellen Lernverfahren zu trainieren und zu evaluieren, erstellt das Forschungsteam sogenannte Goldstandards (Datensätze, in denen zu anonymisierende Textstellen aufwändig manuell identifiziert und pseudonymisiert wurden).	Friedrich-Alexander-Universität Erlangen-Nürnberg	- keine-	1,46	100%	12/2022 - 12/2025	Justiz	Forschungsprojekt	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/anger	
IIP	Intelligente Nutzung verschiedener Verkehrsmittel	Erforschung von Technologien, Verfahren und Methoden zur Anonymisierung bzw. Depersonalisierung personenbezogener Mobilitätsdaten . Dazu werden Daten im heftlichen Kontext einer Kommune erfasst und dynamisch, das heißt für konkrete Anwendungen und externe Lösungsanbieter, anonymisiert. Auf einer Plattform werden die vorhandenen behördlichen und öffentlich verfügbaren Daten zusammengeführt und durch neue Datenquellen aus Crowdsourcing und Bürgerbeteiligung ergänzt.	SWO Netz GmbH, Osnabrück	- Hochschule Osnabrück - Westfälische Wilhelms-Universität Münster - Stadt Osnabrück - items GmbH & Co. KG, Münster - iotec GmbH, Osnabrück - Lambus GmbH, Osnabrück - cybob communication GmbH, Osnabrück	5,50	79%	11/2022 - 11/2025	Mobilität	Kompetenzcluster	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/iip	

Quelle:

<https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/synthetic>

BMBF-Förderprojekte aus dem Bereich Vernetzung und Sicherheit digitaler Systeme - Bekanntmachung Forschungsnetzwerk Anonymisierung für eine sichere Datennutzung

Akronym	Titel	Inhalt	Verbundkoordinator	Partner	Volumen [Mio. €]	Förderanteil BMBF	Laufzeit	Schwerpunkt	Typ	Link	Bemerkungen
ANYMOS	Anonymisierung für vernetzte Mobilitätssysteme	Erforschung, wie Techniken zur Anonymisierung in hochgradig vernetzten Mobilitätssystemen effektiv eingesetzt werden können. Langfristig verfolgen die Verbundpartner das Ziel, die Anonymisierung als Basistechnologie zu etablieren, um Unsicherheiten im Hinblick auf Erfordernisse des Datenschutzes beim Teilen und Nutzen von Daten abzubauen.	FZI Forschungszentrum Informatik	- Fraunhofer IOSB, Karlsruhe - Fraunhofer ISI, Karlsruhe - AVL Deutschland GmbH, Karlsruhe - Karlsruher Verkehrsverbund (KVV) - INIT GmbH, Karlsruhe - DResearch Fahrzeugelektronik GmbH, Berlin - Karlsruher Institut für Technologie (KIT)	9,09	85%	11/2022 - 11/2025	Mobilität	Kompetenzcluster	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/anymos	
AnoMed	Anonymisierung für medizinische Anwendungen	Bündelung von Forschung an Technologien, Verfahren und Methoden zur Anonymisierung, in dem ein kontinuierlicher Anonymisierungswettbewerb für medizinische Anwendungen auf einer Plattform vorbereitet wird. AnoMed wird für die Plattform eine Reihe medizinischer Referenzaufgaben für Referenzdatensätze aufbereiten. Gleichzeitig sollen Angriffsverfahren zur Deanonymisierung entwickelt werden und neue, sogenannte Differentially-Private-Anonymisierungsverfahren als erste Pilotlösungen für die Aufgaben des Wettbewerbs erforscht werden.	Universität zu Lübeck	- Unabhängiges Landeszentrum für Datenschutz, Kiel - Eppdata GmbH, Hamburg - Ingrano Solutions GmbH, Berlin - Perfood GmbH, Lübeck - UniTransferKlinik Lübeck GmbH - DFKI, Kaiserslautern - Universität Hamburg - Universitätsklinikum Schleswig-Holstein, Lübeck - Fraunhofer IMTE, Lübeck	10,07	95%	11/2022 - 11/2025	Medizin	Kompetenzcluster	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/anomed	
AnigED	Rechtskonforme Anonymisierung bei der Kombination von Datensätzen mit Georeferenzierung	Vernetzung wissenschaftlicher und anwendungsorientierter Akteure zur Erforschung von Anonymisierungstechniken für georeferenzierte und verknüpfte Daten . Drei Schwerpunkte: Erstens: Untersuchung des Potenzials des vielversprechenden Ansatzes der Anonymisierung durch künstlich erzeugte, sogenannte synthetische Daten, die von Natur aus keiner Einzelperson zuzuordnen sind, aber trotzdem den untersuchten Sachverhalt korrekt abbilden. Zweitens: Erforschung bestehender Verfahren der Anonymisierung vor allem für die Kombination unstrukturierter Mobilfunkdaten mit strukturierten Umfragedaten. Drittens Entwicklung eines rechtlichen Rahmenwerk zur Anonymisierung sowie Werkzeuge zur effizienten Bereitstellung von anonymen, georeferenzierten Daten entwickelt.	Statistisches Bundesamt, Wiesbaden	- Deutsche Universität für Verwaltungswissenschaften, Speyer - Technische Hochschule Köln - Institut für Arbeitsmarkt- und Berufsforschung, Nürnberg - Freie Universität Berlin	4,37	100%	11/2022 - 11/2025	Statistik	Kompetenzcluster	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/aniged	
AVATAR	Anonymisierung persönlicher Gesundheitsdaten durch Erzeugung digitaler Avatare in Medizin und Pflege	Neuer Anonymisierungsansatz: Dabei werden alle erhobenen Daten in einen dezentralen Datenpool eingespeist. Auf Anfrage werden daraus Daten mit den erforderlichen Merkmalen entnommen und digitale Avatare erzeugt (Anonymisierungsprozess), die als künstliche Personen zu verstehen sind, aber auf realen Daten basieren. So lassen sich keine Rückschlüsse mehr auf die realen Datenspende ziehen und es gibt erstmals eine praxistaugliche Nutzungsperspektive für die Vielzahl vorhandener Daten. Das AVATAR-Konzept ermöglicht darüber hinaus, Einwilligungen zur Datenspende für konkret vorliegende Nutzungsanfragen einzuholen und dies nicht – wie bisher üblich – vor der Erhebung der Daten, sondern eben anlassbezogen.	medways e.V., Jena	- InfectoGnostics Forschungscampus Jena e.V. - ITnet Thüringen e.V., Erfurt - ISMA AG, Sonneberg - Ernst-Abbe-Hochschule Jena - Navimatix GmbH, Jena - Friedrich-Schiller-Universität Jena - SRH Wald-Klinikum Gera - room AG, Jena - JEN-OPHTHALMO, Jena - DLR e.V., Köln - Fraunhofer IOSB, Ilmenau - Königsee Implantate GmbH, Allendorf - Technische Universität Ilmenau - Universitätsklinikum Jena - Fraunhofer IDMT, Ilmenau - Data In Motion Consulting GmbH, Jena - LIEBENSTEIN LAW - Kanzlei für Wirtschaftsrecht, Frankfurt am Main	9,95	90%	11/2022 - 11/2025	Medizin und Pflege	Kompetenzcluster	https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/avatar	

Quelle:

<https://www.forschung-itsicherheit-kommunikationssysteme.de/projekte/synthetic>