AKTIN Infrastruktur

Datenschutzkonzept

Jonas Bienzeisler, Raphael W. Majeed, Rainer Röhrig, Hauke Heidemeyer, Wiebke Schirrmeister, Ronny Otto, Susanne Drynda, Saskia Ehrentreich

Ansprechpartner

Dr. Jonas Bienzeisler
Institut für Medizinische Informatik
Uniklinik RWTH Aachen
Adresse: Pauwelsstraße 30 • D 52074 Aachen
Telefon.: +49 241 80-88870
Email: jbienzeisler@ukaachen.de

Prof. Dr. Rainer Röhrig
Institut für Medizinische Informatik
Uniklinik RWTH Aachen
Adresse: Pauwelsstraße 30 • D 52074 Aachen
Telefon.: +49 241 80-88790
Email: rroehrig@ukaachen.de

Version 3.0.2 Stand 14.04.2026

Inhaltsverzeichnis

Abkürzungs- und Symbolverzeichnis

Abkürzung	Bedeutung
AKTIN	Aktionsbündnis für Informations- und Kommunikationstechnologie in der Akut- und Notfallmedizin
AKTIN-Broker	Zentrale Softwarekomponente zur Verteilung von Datenabfragen und Sammlung von Ergebnissen innerhalb der AKTIN-Infrastruktur
AKTIN-DWH	AKTIN Data Warehouse
AKTIN-IT	Technische Betriebseinheit der AKTIN-Infrastruktur am Institut für Medizinische Informatik der Uniklinik RWTH Aachen
AKTIN-Office	Geschäftsstelle des AKTIN e. V. am Institut für Public Health in der Akutmedizin in Magdeburg
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BMBF	Bundesministerium für Bildung und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDA	Clinical Document Architecture
DC	Data Collector
DFG	Deutsche Forschungsgemeinschaft
DGINA	Deutsche Gesellschaft Interdisziplinäre Notfall- und Akutmedizin
DIVI	Deutsche Interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin
DLR	Deutsches Zentrum für Luft- und Raumfahrt
DRG	Diagnosis Related Groups
DRKS	Deutsches Register Klinischer Studien
DS	Datenschutzbeauftragte*r / Datenschutz
DSG-EKD	Datenschutzgesetz der Evangelischen Kirche in Deutschland
DSGVO	Datenschutz-Grundverordnung
DUAC	Data Use and Access Committee
DWH	Data Warehouse
e. V.	eingetragener Verein
EDIS	Emergency Department Information System
EU	Europäische Union
FAIR	Findable, Accessible, Interoperable, Reusable
FHIR	Fast Healthcare Interoperability Resources
GDNG	Gesundheitsdatennutzungsgesetz
HL7	Health Level Seven
ID	Identifikator / Kennung
IDAT	Identifizierende Daten
IMI	Institut für Medizinische Informatik

Abkürzung	Bedeutung
IPHAM	Institut für Public Health in der Akutmedizin
IT	Informationstechnologie
i. S. d.	im Sinne des / der
i. V. m.	in Verbindung mit
JAMA	Journal of the American Medical Association
K-Anonymität	Anonymitätskriterium
KDG	Gesetz über den kirchlichen Katholischen Datenschutz
KHEntgG	Krankenhausentgeltgesetz
lit.	littera
MDAT	medizinische Daten
NUM	Netzwerk Universitätsmedizin
OPS	Operationen- und Prozedurenschlüssel
Pat-ID	Patienten-ID
PSN	Pseudonym
RKI	Robert Koch-Institut
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SB	Search Broker
SOP	Standard Operating Procedure
SQL	Structured Query Language
SRE	Secure Research Environment
StGB	Strafgesetzbuch
TDAC	Trusted Data Analytics Center
TempID	temporäre ID
TLS	Transport Layer Security
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung
TOM	Technische und Organisatorische Maßnahmen
WMA	World Medical Association

Glossar

Pseudonym/ Pseudonymisierung: „die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifisch betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können.“ (Art. 4 Nr. 5 DSGVO)

Anonymisierung: Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann (Erwägungsgrund 26, DSGVO).

K-Anonymität: Eigenschaft eines Datensatzes. Die Daten von Individuen sind so weit verallgemeinert, dass für jede Kombination potentiell identifizierender Attribute (Quasi-Identifikatoren) mindestens k-1 weitere Datensätze mit identischen Attributwerten existieren.

AKTIN-Infrastruktur: Technische Gesamtsystemarchitektur zur dezentralen Erhebung, Verarbeitung und standortübergreifenden Analyse von Routinedaten aus Notaufnahmen. Sie besteht aus drei Komponenten: den lokalen AKTIN-DWHs (dezentrale Datenspeicherung und Bereitstellung), dem AKTIN-Broker (föderierte Verteilung und Aggregation von Datenanfragen) und dem SRE (geschützte Analyseumgebung für pseudonymisierte Forschungsdaten).

Infrastrukturbetreibende: Im Rahmen des Netzwerk Universitätsmedizin werden die zentralen AKTIN-Infrastrukturkomponenten durch das Institut für Medizinische Informatik der Uniklinik RWTH Aachen sowie durch das Institut für Public Health in der Akutmedizin der Uniklinik Magdeburg betrieben.

Notaufnahmeregister: die technischen und organisatorischen Strukturen und Verfahren, mit denen über die AKTIN-Infrastruktur Routinedaten aus Notaufnahmen standardisiert, dezentral und datenschutzkonform für wissenschaftliche und statistische Zwecke bereitgestellt werden.

Standort: An der AKTIN-Infrastruktur angeschlossenes Klinikum.

AKTIN Data Warehouse (AKTIN-DWH): Ein DWH ist eine für Analysezwecke optimierte Datenbank, die Daten aus mehreren, in der Regel heterogenen Quellen zusammenführt; wörtlich „Datenlager“. Das AKTIN-DWH ist die lokale DWH-Instanz einer an der AKTIN Infrastruktur teilnehmenden Notaufnahme. Es speichert die über interoperable Schnittstellen aus dem Krankenhausinformationssystem übermittelten Routinedaten, die gemäß dem DIVI-Notaufnahmeprotokoll dokumentiert wurden. Die Daten verbleiben vollständig in der jeweiligen Einrichtung und bilden die Grundlage für die föderierte Datennutzung innerhalb der AKTIN-Infrastruktur. Über das AKTIN-DWH können nach Zustimmung der jeweiligen Klinik standortbezogene Datenauszüge für definierte Zwecke bereitgestellt und im Rahmen der AKTIN-Infrastruktur geteilt werden.

AKTIN-Broker: Anwendung inklusive Web-Frontend für die zentrale Verteilung von Anfragen an die lokalen AKTIN-DWHs und die Zusammenführung der Ergebnisse. Sie wird durch die

Infrastrukturbetreibenden für das Daten- und Studienmanagement genutzt und besteht aus der Query-Broker- und der Data-Aggregator-Komponente.

Data Aggregator: Komponente des AKTIN-Brokers zum Sammeln von Abfrageergebnissen. Die zugehörigen Abfragen werden vom *Query Broker* an alle Standorte übermittelt.

***Query Broker*:** Komponente des AKTIN-Brokers zum Verteilen von Datenabfragen an alle Standorte. Die zugehörigen Ergebnisse werden vom Data *Aggregator* gesammelt.

Datenabfrage*:* Technisch umgesetzte, durch das DUAC geprüfte und durch die Standorte freizugebende Anfrage zur Auswertung standortinterner oder standortübergreifender Datenbestände innerhalb der AKTIN-Infrastruktur. Eine Datenabfrage konkretisiert einen genehmigten Antrag auf Datennutzung in Form standardisierter Abfrageparameter oder Datenbankabfragen.

Antrag auf Datennutzung: Formalisierter Antrag von Forschenden oder teilnehmenden Einrichtungen auf Bereitstellung und Auswertung von Daten des Notaufnahmeregisters im Rahmen eines konkret beschriebenen Vorhabens. Der Antrag enthält u. a. Fragestellung, benötigte Variablen, Auswertungsplan, Rechtsgrundlage sowie Angaben zu Ethikvoten und wird durch das DUAC geprüft und, sofern eine positive Bewertung vorliegt, zur technischen Umsetzung als Datenabfrage an die Standorte und das TDAC weitergegeben.

Search Broker (SB): Rolle innerhalb der AKTIN-IT, die vom DUAC genehmigte Forschungsanfragen in standardisierte Datenbankabfragen und Terminologien überführt und diese im Query Broker für die Verteilung an die Standorte bereitstellt.

Data Collector (DC): Rolle innerhalb der AKTIN-IT, die im Data Aggregator gesammelte, standortübergreifende Abfrageergebnisse authentifiziert abruft und zur weiteren Verarbeitung an das TDAC übermittelt.

Standortkoordinator*in: Benannte, verantwortliche Person eines Standortes für das lokale Datenmanagement im AKTIN-DWH. Prüft, genehmigt oder lehnt Datenabfragen ab, überwacht die Einhaltung rechtlicher und organisatorischer Vorgaben und stellt sicher, dass nur anonymisierte bzw. pseudonymisierte Daten den Standort verlassen.

Auswertestelle: Von externen Partnern oder Forschenden eingerichtete Stelle zur eigenen statistischen oder wissenschaftlichen Auswertung von im Rahmen genehmigter Anfragen übermittelten (pseudonymisierten oder anonymisierten) Daten des Notaufnahmeregisters. Eine Auswertestelle wird nur in begründeten Ausnahmefällen (z. B. Infektionssurveillance, spezialisierte Register) zugelassen, erfordert ein eigenes Datenschutzkonzept, eine geeignete Rechtsgrundlage sowie die vorherige Zustimmung des DUAC und der beteiligten Standorte.

Secure Research Environment (SRE): Das SRE ist eine abgeschottete, kontrollierte Softwareumgebung für die standortübergreifende Analyse pseudonymisierter Forschungsdaten als Teil der AKTIN-Infrastruktur. Es ermöglicht die sichere Verarbeitung und Auswertung der über den Query Broker aggregierten Daten. Innerhalb des SRE können getrennte, voneinander gekapselte Analyseumgebungen eingerichtet werden, um Forschungsprojekte organisatorisch und technisch strikt voneinander zu trennen. Umfassende Schutzmaßnahmen verhindern den unautorisierten Abfluss von Forschungs- oder

Analyseergebnissen; eine Freigabe erfolgt ausschließlich nach formaler Prüfung durch das TDAC.

Trusted Data Analytics Center (TDAC): Unabhängige Stelle zur datenschutzkonformen Pseudonymisierung, Bereitstellung und kontrollierten Weitergabe medizinischer Forschungsdaten. Es nutzt hierfür das SRE der AKTIN-Infrastruktur, in der pseudonymisierte und anonymisierte Daten sicher verarbeitet und analysiert werden können. Das TDAC verantwortet zudem die Prüfung der Analyseergebnisse hinsichtlich Anonymität vor ihrer Ausleitung aus dem SRE.

AKTIN-Office: Ist am Institut für Public Health in der Akutmedizin der Uniklinik Magdeburg angesiedelt und für die organisatorische und administrative Betreuung der AKTIN-Infrastruktur und des Notaufnahmeregisters zuständig.

AKTIN-IT: verantwortet am Institut für Medizinische Informatik der Uniklinik RWTH Aachen den technischen Betrieb des AKTIN-Brokers sowie die Entwicklung und Weiterentwicklung der Softwarekomponenten der AKTIN-Infrastruktur. Sie stellt damit den kontinuierlichen, sicheren und standardkonformen Betrieb der föderierten Daten- und Analyseprozesse sicher.

***Data Use and Access Committee* (DUAC):** W*issenschaftliches Kontrollgremium* für die Prüfung von Datenabfragen an das AKTIN-Notaufnahmeregisters im Rahmen von Forschungsvorhaben. Prüft diese in Hinblick ethischer und datenschutzrechtlicher Gesichtspunkte und gibt entsprechende Datenauszüge frei.

1. AKTIN

Das Aktionsbündnis zur Verbesserung der Kommunikations- und Informationstechnologie in der Intensiv- und Notfallmedizin (AKTIN e.V.) setzt sich für Wissenschaft, Forschung und Qualitätsentwicklung in der Akut-, Notfall- und Intensivmedizin durch die standardisierte und datenschutzkonforme Nutzung digitaler Routinedaten ein. Die aus diesem Bündnis heraus entstandene AKTIN-Infrastruktur und des darauf betriebenen *Notaufnahmeregisters* wurden im Projekt „Verbesserung der Versorgungsforschung in der Akutmedizin in Deutschland durch den Aufbau eines nationalen Notaufnahmeregisters“ entwickelt. Das Projekt wurde mit BMBF-Förderung in Trägerschaft des DLR zwischen 2013 und 2019 durchgeführt. Der Betrieb der AKTIN-Infrastruktur erfolgt seit dem durch das Institut für Medizinische Informatik am Universitätsklinikum RWTH Aachen (IMI) und des Instituts für Public Health in der Akutmedizin der Medizinischen Fakultät der Otto-von-Guericke-Universität Magdeburg (IPHAM) als *Infrastrukturbetreibende* in Kooperation mit den teilnehmenden Notaufnahmen.

Die AKTIN-Infrastruktur bildet die technische und organisatorische Basis für die standortübergreifende, datenschutzkonforme Bereitstellung und Nutzung von Routinedaten aus der Akut- und Notfallversorgung. Technisch umfasst die AKTIN-Infrastruktur insbesondere die lokalen AKTIN-DWHs an den teilnehmenden Notaufnahme Standorten, den AKTIN-Broker sowie das geschützte Secure Research Environment (SRE) für die sicherere Analyse von diesen Gesundheitsdaten.

Im Kontext des Netzwerks Universitätsmedizin (NUM) ist die AKTIN-Infrastruktur seit 2020 eine der Basisinfrastrukturen und fungiert mittlerweile als NUM-Plattform für Routinedaten aus der Akut-, Intensiv- und Notfallmedizin. In dieser Rolle unterstützt sie NUM-Vorhaben, die auf über die AKTIN-Infrastruktur bereitgestellte Routinedaten zugreifen, die Plattform zum Aufbau weiterer Register oder Datenräume nutzen oder zur Weiterentwicklung gemeinsamer NUM-Ziele beitragen. Die AKTIN-Infrastruktur umfasst dabei sowohl Kliniken innerhalb des NUM als auch nicht NUM-geförderte Einrichtungen, die in den Gesamtverbund über Kooperationsvereinbarungen mit den Infrastrukturbetreibenden eingebunden sind.

1.1. Hintergrund

Die Notfallversorgung in Deutschland befindet sich seit einigen Jahren im Umbruch. Außer stichprobenhaften Datenerhebungen im Rahmen von einzelnen Umfragen oder Studien waren lange Zeit keine regelmäßigen und einrichtungsübergreifenden Datensammlungen in der klinischen Notfallmedizin vorhanden. Eine valide und umfassende Datenerhebung zur Anzahl, den Vorstellungsgründen und der Versorgungssituation von Notfallpatient*innen ist zur Bewertung der Maßnahmen allerdings notwendig. Organisatorisch relevante Kennzahlen, die zur Beurteilung der Prozess- und Ergebnisqualität der Notaufnahmen herangezogen werden können, standen im internationalen Vergleich in Deutschland abgesehen von Einzelfällen nur unzureichend zur Verfügung. Ebenfalls fehlte die Datengrundlage für systematische Analysen unterschiedlicher Versorgungsformen mittels organisatorischer und medizinischer Kennzahlen als Grundlage für den notwendigen Prozess der Organisationsentwicklung in der klinischen Notfallversorgung. Mit der AKTIN-Infrastruktur und dem darauf betriebenen Notaufnahmeregister wurde diese Lücke geschlossen. AKTIN hat sich seither als bundesweite, interoperable Dateninfrastruktur für Forschung, Qualitätssicherung und Public-Health-Überwachung in der Notfallmedizin etabliert.

Im Notaufnahmeregister werden unter Nutzung der AKTIN-Infrastruktur die Inhalte der digitalen medizinischen Dokumentation der Versorgung aller Notfallpatienten der teilnehmenden Kliniken (sog. *Standorte*) auf einheitliche und standardisierte Weise zugänglich gemacht. Die Erhebung der Daten aus der klinischen Routine erfolgt ohne zusätzlichen Aufwand für das medizinische Personal und ermöglicht die datenschutzkonforme Sekundärnutzung umfangreicher, tagesaktueller und flächendeckender Datensätze. Die Basis für die Datenerhebung in der AKTIN-Infrastruktur ist der von der Sektion Notfalldokumentation der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin e.V. (DIVI) entwickelte Datensatz Notfalldokumentation bzw. das daraus gebildete Szenario Notaufnahmeregister.

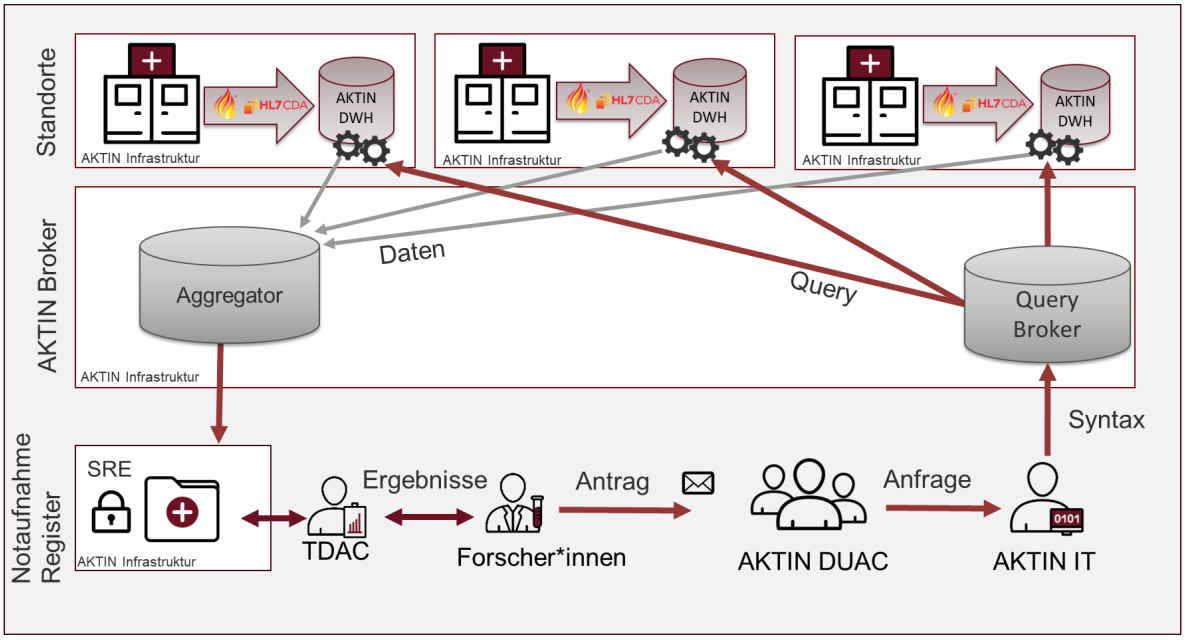

Abbildung 1 Darstellung der AKTIN-Infrastruktur und des AKTIN-Notaufnahmeregisters: Die Grafik zeigt den technischen und organisatorischen Ablauf der dezentralen Datenverarbeitung in der AKTIN-Infrastruktur. An den Standorten werden Routinedaten aus den Notaufnahmen lokal im AKTIN-DWH gehalten. Forschungsanfragen werden über den AKTIN-Broker verteilt und die standortspezifischen Ergebnisse im Aggregator zusammengeführt. Das AKTIN-Notaufnahmeregister nutzt diese Infrastruktur. Das Trusted Data Analytics Center (TDAC) wertet Daten im geschützten SRE-Bereich der AKTIN-Infrastruktur aus und stellt Forschenden nach Prüfung Ergebnisse zur Verfügung.

Die AKTIN-Infrastruktur wurde als dezentrale Architektur (vgl. Abbildung 1) aufgebaut und ermöglicht im Rahmen des Notaufnahmeregisters eine Sekundärnutzung der Routinedaten gemäß den Vorgaben der Datenschutzgrundverordnung (DSGVO) und des Gesundheitsdatennutzungsgesetzes (GDNG). In der klinischen Versorgungsroutine erhobene Daten werden automatisiert in *dezentralen* Data-Warehouses (AKTIN-DWH) der teilnehmenden Standorte gespeichert. Die Daten werden pseudonymisiert und innerhalb des Behandlungskontextes dezentral vorgehalten. Dies geschieht gemäß den Vorschriften des jeweiligen Bundeslandes. Zu Zwecken der Qualitätssicherung und Versorgungsforschung sind diese Daten für die Kliniken über eine Benutzeroberfläche verfügbar. Für wissenschaftliche und statistische Zwecke können die gesammelten Daten über einen *zentralen* AKTIN-Broker zusammengeführt werden – allerdings erst nachdem ein *wissenschaftliches Kontrollgremium* – das *Data Use and Access Committee (DUAC)* – eine entsprechende Anfrage geprüft und

genehmigt hat und der jeweilige Standort zugestimmt hat. Die Datenanalyse erfolgt dann im *Trusted Data Analytics Center* (TDAC) Magdeburg.

1.2. Zweck der Datenverarbeitung

Daten für das Notaufnahmeregister werden zu folgenden wissenschaftlichen und statistischen Zwecken innerhalb der AKTIN-Infrastruktur erhoben:

1. Qualitätssicherung in der medizinischen, pflegerischen und rehabilitativen Akut- und Notfallversorgung, einschließlich einrichtungsinternem und einrichtungsübergreifendem Qualitätsmanagement sowie Benchmarking.
2. Medizinische, rehabilitative und pflegerische Forschung, insbesondere einrichtungsübergreifende Versorgungsforschung in der Akut- und Notfallmedizin
3. Gesundheits- und Infektionssurveillance in Zusammenarbeit mit dem Robert Koch-Institut (RKI) und dem öffentlichen Gesundheitsdienst.
4. Gesundheitsberichterstattung.
5. Datenbereitstellung für externe Partner und spezialisierte Register im Rahmen geregelter Kooperationen.

Ziel ist die Förderung der Qualität und Sicherheit der medizinischen, pflegerischen und rehabilitativen Versorgung durch kontinuierliche Analyse und Verbesserung klinischer Prozesse. Die Daten dienen einer hochwertigen Forschung in der Akut- und Notfallmedizin sowie der Bereitstellung verlässlicher statistischer Grundlagen für Gesundheitsberichterstattung und Infektionssurveillance – stets unter Beachtung der in Deutschland und der Europäischen Union geltenden rechtlichen und ethischen Anforderungen.

1.3. Umfang der Datenverarbeitung

Die **AKTIN-Infrastruktur** dient als technische und organisatorische Plattform, die es am Notaufnahmeregister teilnehmenden Standorten, bzw. deren Notaufnahmen, ermöglicht:

- Routinedaten der Notaufnahme einheitlich und strukturiert pseudonymisiert zu erfassen.
- Routinedaten der Notaufnahme innerhalb der Einrichtung für Qualitätssicherung, Patientensicherheit, eigener Forschung und Forschung im Verbund auszuwerten, einschließlich verteiltem Machine-Learning.
- Routinedaten der Notaufnahme in pseudonymisierter oder anonymisierter Form mit anderen datenverarbeitenden Gesundheitseinrichtungen zu teilen, um gemeinsame Analysen und Verbundforschung zur Verbesserung der Notfall- und Akutversorgung zu ermöglichen.
- Forschungsvorhaben und interventionelle Studien durchzuführen, bei denen aufgrund der Art des Eingriffs, der prospektiven Beteiligung von Patient*innen oder aus ethischen Gründen eine ausdrückliche Einwilligung der Betroffenen erforderlich ist.

Die Datenverarbeitung umfasst insbesondere:

- die lokale Speicherung und Nutzung pseudonymisierter Routinedaten in den teilnehmenden Notaufnahmen zur Qualitätssicherung und Forschung
- die Anonymisierung von gesammelten Routinedaten,
- die Übermittlung pseudonymisierter Daten mehrerer Einrichtungen unter Genehmigung der zuständigen Datenschutzaufsicht nach § 6 Abs. 3 Gesundheitsdatennutzungsgesetz an das **TDAC** für statistische und wissenschaftliche Auswertungen
- sowie die Übermittlung anonymisierter Teildatensätze an das TDAC für statistische und wissenschaftliche Auswertungen.

Auf Grundlage dieser Infrastruktur wird das **Notaufnahmeregister kontinuierlich prospektiv** betrieben. Das Notaufnahmeregister nutzt die AKTIN-Infrastruktur zur datenschutzkonformen Erhebung, Verarbeitung und Auswertung von Routinedaten aus der klinischen Notfallversorgung.

1.3.1. Datenerhebung

Die Datenerhebung erfolgt in den teilnehmenden Kliniken mit Beginn des Anschlusses an die AKTIN-Infrastruktur. In Einzelfällen können Daten auch retrospektiv in die lokalen AKTIN-DWH-Systeme übermittelt werden. Die Daten werden in Notaufnahmen erhoben, die einen einheitlichen Dokumentationsstandard etabliert haben. Die teilnehmenden Krankenhäuser speichern die ausgewählten Daten zu jedem/r Patienten*in der Notaufnahme in einem lokalen AKTIN-DWH. Das AKTIN-DWH ist Teil der AKTIN-Infrastruktur, wird aber von den Standorten eigenverantwortlich administriert. Die Daten und der Server, auf dem diese sich befinden, sind im Besitz bzw. Verantwortungsbereich der Standorte. Die im AKTIN-DWH gespeicherten Daten werden vom jeweiligen Standort eigenständig erhoben. Für wissenschaftliche Fragestellungen können die Daten standortübergreifend über den AKTIN-Broker zentral abgefragt werden. Die übergeordneten Verfahren zur Prüfung, Freigabe und Durchführung solcher Anfragen werden im Rahmen des Notaufnahmeregisters betrieben. Es stellt die organisatorische Struktur und die zuständigen Gremien – einschließlich des unabhängigen wissenschaftlich-ethischen Prüfverfahrens – für die datenschutzkonforme Bearbeitung und Genehmigung standortübergreifender Datennutzungsanfragen bereit.

Eine Übermittlung von (Teil-)Datensätzen oder Analyseergebnissen aus der datenverarbeitenden Gesundheitseinrichtung heraus erfolgt ausschließlich in anonymisierter oder pseudonymisierter Form. Es werden bei den Abfragen an die Standorte die Prinzipien der Datensparsamkeit nach Maßgabe des DUAC angewendet. Die Datenanalyse erfolgt zentral im TDAC, das durch technische und organisatorische Maßnahmen sicherstellt, dass Daten nicht mit anderen Quellen verknüpft oder in identifizierbarer Form weitergegeben werden können. Eine Übermittlung von Ergebnissen an Dritte, die nicht an der Infrastruktur beteiligt sind, erfolgt ausschließlich in aggregierter und/oder anonymisierter Form. Ausnahmen, etwa im Rahmen der Gesundheitsberichterstattung oder auf Grundlage spezifischer Verträge, sind nur nach Prüfung durch das DUAC zulässig.

Für den technischen Betrieb, zum Zwecke der technischen Qualitätssicherung und für den technischen Support werden außerdem Daten von der AKTIN-IT am Institut für Medizinische Informatik am Universitätsklinikum RWTH Aachen verarbeitet. Für die Sicherstellung des technischen Betriebs und zu Zwecken der Qualitätssicherung werden anonyme Importstatistiken jedes aktiven AKTIN-DWH automatisiert an den Broker übermittelt (z. B. Start des AKTIN-DWH, letzter erfolgreicher/fehlgeschlagener Import, die Anzahl importierter, aktualisierte, fehlgeschlagener, fehlerhafte Fälle seit Start, Version der genutzten Softwarekomponenten). Das IT-Team verarbeitet außerdem Daten im Rahmen von Supportanfragen der teilnehmenden Kliniken. Zweck und Umfang der Datenerhebung hängen von der jeweiligen Supportanfrage ab. Es werden – soweit möglich – anonymisierte Daten verarbeitet, die nach Abschluss des technischen Supports gelöscht werden. Sollte im Rahmen des technischen Supports der Zugriff auf personenbezogene Daten erforderlich werden, so ist eine gesonderte Vereinbarung über eine Auftragsverarbeitung zwischen der Uniklinik RWTH Aachen und dem jeweiligen Standort zu schließen.

Jede darüber (und über dieses Datenschutzkonzept) hinausgehende Datenverarbeitung bedarf einer eigenständigen Rechtsgrundlage und eines separaten Datenschutzkonzepts sowie der Zustimmung der teilnehmenden Standorte, dem DUAC, der zuständigen Ethikkommissionen sowie gegebenenfalls der Datenschutzaufsichtsbehörde.

1.4. Organisationsstruktur und Verantwortlichkeiten

Das Notaufnahmeregister wird in Zusammenarbeit vom Institut für Medizinische Informatik am Universitätsklinikum RWTH Aachen (IMI) und dem Institut für Public Health in der Akutmedizin der Otto-von-Guericke-Universität Magdeburg (IPHAM) betrieben (siehe Anlage 2 – Ansprechpartner Datenschutz). Die eigentliche Datenverarbeitung wird in gemeinsamer Verantwortung im Sinne von Artikel 26 DSGVO von dem jeweiligen Standort, der AKTIN-IT und dem TDAC durchgeführt.

Die technischen Komponenten der AKTIN-Infrastruktur werden durch das Institut für Medizinische Informatik der Uniklinik RWTH Aachen sowie durch das Institut für Public Health in der Akutmedizin der Uniklinik Magdeburg entwickelt und betrieben. Die Zusammenarbeit ist in einem Kooperationsvertrag geregelt.

1.4.1. AKTIN Geschäftsstelle

Die AKTIN-Geschäftsstelle (AKTIN-Office) wird am IPHAM in Magdeburg betrieben. Sie ist für die organisatorische und administrative Betreuung der AKTIN-Infrastruktur und des Notaufnahmeregisters verantwortlich. Hierzu zählen insbesondere die Verwaltung und Koordination der beteiligten Einrichtungen, das Management der Verträge für den Anschluss von Kliniken an AKTIN, die Betreuung des Freigabeprozesses für Forschungsanfragen sowie die Kommunikation mit teilnehmenden Standorten, Projektpartnern und Gremien. Darüber hinaus übernimmt die Geschäftsstelle die Abwicklung administrativer und rechtlicher Vorgänge im Zusammenhang mit dem Betrieb und der Weiterentwicklung der Infrastruktur und des Registers und fungiert als zentrale Ansprechstelle für öffentliche und institutionelle Belange.

1.4.2. Studienzentren

An der Datenerfassung im Rahmen des Notaufnahmeregisters beteiligen sich die Notaufnahmen von Kliniken, die ein AKTIN-DWH betreiben – sog. teilnehmende *Standorte* (siehe Anlage 1 – Studienzentren). Ein Standort mit mehreren Notaufnahmen kann mehrere AKTIN-DWH einschließen. Das lokale Datenmanagement wird von Standortkoordinatoren verantwortet. Sie sind für die Umsetzung und Einhaltung aller ethischen, rechtlichen, vertraglichen und organisatorischen Vorgaben zum Datenmanagement verantwortlich (siehe Anlage 1 – Studienzentren). Zusätzlich werden technische Informationen im Rahmen des technischen Supports sowie des Software Monitorings an die AKTIN-IT zu Zwecken der Qualitätssicherung übermittelt.

1.4.3. AKTIN-IT

Die AKTIN-IT am Institut für Medizinische Informatik der Uniklinik RWTH Aachen verantwortet insbesondere den Betrieb und die Weiterentwicklung des AKTIN-Brokers, technischer Integrationskomponenten, das Sicherheits- und Systemmonitoring der durch sie betriebenen Komponenten, den technischen Support der Standorte sowie die technische Umsetzung von Datenabfragen gemäß den Vorgaben des DUAC.

1.4.4. Trusted Data Analytics Center

Das TDAC wird vom Institut für Public Health in der Akutmedizin der Universitätsmedizin Magdeburg (IPHAM) betrieben. Es verarbeitet die von den datenbereitstellenden Projektpartnern übermittelten Datensätze und stellt autorisierten Forschenden eine Secure Research Environment (SRE) in der Universitätsmedizin Magdeburg zur datenschutzkonformen Analyse zur Verfügung, wenn die Analyse der Forschungsdaten nicht durch TDAC-Mitarbeitende selbst durchgeführt wird. Es gewährleistet durch technische und organisatorische Maßnahmen den sicheren Betrieb der Analyseumgebung, die Trennung von Datenquellen sowie den kontrollierten Zugriff auf die bereitgestellten Daten. Es kontrolliert außerdem, dass ausschließlich aggregierte und/oder anonymisierte Analyseergebnisse im Rahmen genehmigter Forschungsanfragen an Dritte weitergegeben oder veröffentlicht werden. Ausnahmen, beispielsweise im Rahmen der Gesundheitsberichterstattung oder auf Grundlage spezifischer Verträge, sind nur nach Prüfung durch das DUAC zulässig.

1.4.5. Data Use and Access Committee

Die Bereitstellung eines Datensatzes des Notaufnahmeregisters kann bei einem unabhängigen wissenschaftlichen Kontrollgremium – dem *Data Use and Access Committee (*DUAC) – von Angehörigen öffentlicher Forschungseinrichtungen, medizinischer Fachgesellschaften oder teilnehmender Kliniken beantragt werden. Eine solche Anfrage basiert auf einer konkreten wissenschaftlichen Fragestellung. Das Gremium prüft den Antrag in Hinblick ethischer, regulatorischer und datenschutzrechtlicher Gesichtspunkte. Bei einer positiven Bewertung wird dann der jeweilige Datenauszug entsprechend der Vorgaben des DUAC erstellt und an das TDAC weitergeleitet, welches die Auswertung hinsichtlich der Fragestellung überwacht. Das genaue Vorgehen ist in einer Geschäftsordnung festgelegt (Siehe Anlage 6). Es stellt zudem zusammen mit dem TDAC sicher, dass unter Wahrung des Datenschutzes und aller gültigen Rechtsvorschriften und ethischen Regularien nur die erforderlichen Daten abgefragt und ausgewertet werden.

1.4.6. Externe Kooperationen

Externe Kooperationen sind im Rahmen der AKTIN-Infrastruktur in begründeten Fällen möglich und ausdrücklich vorgesehen. Für solche Kooperationen kann durch externe Partner eine eigene Auswertestelle oder Datenempfangsstelle eingerichtet werden (Vgl. Abschnitt Auswertestelle), beispielsweise zur Weiterleitung von Daten an ein fachlich spezialisiertes Register, zur Durchführung gemeinsamer Forschungsprojekte oder im Rahmen von Kooperationen zur Gesundheitsberichterstattung und Surveillance. Jede Kooperation dieser Art ist im Voraus vertraglich zu regeln und bedarf einer Rechtsgrundlage sowie der Zustimmung durch das DUAC, das die Einhaltung aller ethischen, datenschutzrechtlichen und regulatorischen Anforderungen prüft. Eine Datenweitergabe an Kooperationspartner erfolgt ausschließlich nach denselben datenschutzrechtlichen und organisatorischen Grundsätzen wie die Datenfreigabe an Forschende innerhalb der AKTIN-Infrastruktur (vgl. Abschnitt 2.2.6).

1.5. Anfallende Daten

Datenstandard für die im Notaufnahmeregister erfassten Routinedaten ist der Datensatz Notfalldokumentation Szenario Notaufnahmeregister der DIVI in der jeweils gültigen Version, aktuell V2025.2 (Stand 12/2024). Die zu erfassenden Daten wurden von der Sektion Notfalldokumentation der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin e. V. (DIVI) erarbeitet [2]. Die DIVI ist eine Dachorganisation der in Deutschland an der Intensiv- und Notfallmedizin beteiligten 18 Fachgesellschaften mit individueller Personenmitgliedschaft. **Es können außerdem *optional* Übergabeprotokolle des Rettungsdienstes an die Notaufnahme** in das lokale AKTIN-DWH integriert werden, basierend auf dem **Datensatz Notfalleinsatzprotokoll in der jeweils gültigen Version der DIVI (derzeit Version V2025.1)**. Beide DIVI-Datensätze werden fortlaufend weiterentwickelt, um den praktischen Anforderungen des medizinischen Personals sowie den aktuellen Entwicklungen in der Notfallversorgung gerecht zu werden. Darüber hinaus können stationäre Behandlungsdaten (einzelne Items aus einem Datensatz gem. § 21 KHEntgG, siehe Anlage 4) ebenfalls *optional* zur Verfügung gestellt werden (Vgl. Tabelle 1). Die Abrechnungsdaten können über eine Benutzerschnittstelle im AKTIN-DWH-Manager in das lokale AKTIN-DWH importiert werden.

Tabelle 1 Im Notaufnahmeregister zu wissenschaftlichen und statistischen Zwecken verarbeitete Daten.

Datensatz	Beschreibung	Beispiele	Verarbeitungsort / Verantwortlichkeit	Schutzbedarf
Protokolle der Notaufnahmebehandlung (Datensatz Notaufnahme)	Dokumentation medizinischer und administrativer Abläufe in der Notaufnahme	Prozesszeiten Vorstellungsgrund, Ersteinschätzungs-kategorie, Vitalparameter, Diagnosen	Lokales DWH am Standort (Krankenhaus)	Sehr hoch
Übergabe Protokolle des Rettungsdienstes (Datensatz Rettungsdienst)	Dokumentation medizinischer und administrativer Abläufe im Rettungsdienst	Einsatzzeitpunkt, Transportmittel, Notarztbeteiligung, Vitalparameter	Lokales DWH am Standort (Krankenhaus)	Sehr hoch

Stationäre Behandlungsdaten (gem. Vorgaben § 21 KHEntgG,)	Erweiterung um stationäre Routinedaten für spezifische Projekte oder DUAC-beschlossene Anlässe	DRG-Informationen, OPS-Codes, Verweildauer	Lokales DWH; ggf. aggregiert an Query Broker / TDAC	Sehr hoch

Die teilnehmenden Kliniken verantworten die im AKTIN-DWH gespeicherten Daten und entscheiden eigenständig, ob einzelne Datensätze oder Items erhoben werden; es bestehen jedoch verbindliche technische Anforderungen an Struktur und Mindestumfang des Datensatzes. Unabhängig vom Umfang oder der Zusammensetzung der erhobenen Variablen werden alle Datensätze in gleicher Weise, wie die anfallenden Daten des Datensatzes Notaufnahme verarbeitet; die technischen Prozesse und Abfragen erfolgen somit standortübergreifend nach einem einheitlichen Verfahren, während die inhaltliche Datenerhebung in der Hoheit der jeweiligen Klinik verbleibt.

1.5.1. Schutzbedarf und Risikoklassifizierung

Bei den im Projekt erhobenen und verarbeiteten Informationen handelt es sich um personenbezogene Daten besonderer Kategorie im Sinne von Artikel 9 Absatz 1 DSGVO. Insbesondere medizinische Daten, wie sie in Notaufnahmen anfallen, besitzen einen sehr hohen Schutzbedarf, da ihre Offenlegung schwerwiegende Folgen für die betroffenen Personen haben könnte (z. B. Diskriminierung, Stigmatisierung oder Nachteile im Versicherungs- bzw. Beschäftigungsverhältnis).

Entsprechend sind Maßnahmen erforderlich, die diesem hohen Schutzbedarf gerecht werden. AKTIN setzt hierzu ein mehrstufiges Sicherheitskonzept um, das auf den Grundsätzen der Datenminimierung, Trennung von Identitäts- und Falldaten, Pseudonymisierung, verschlüsselter Datenübertragung, Zugriffsbeschränkung und Protokollierung beruht. Die Einstufung des Schutzbedarfs erfolgt in Anlehnung an gängige Klassifikationssysteme (z. B. BSI-IT-Grundschutz, TMF-Leitfaden, Empfehlungen der Medizin Informatik Initiative) und berücksichtigt insbesondere die Auswirkungen auf die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit.

Die konkreten technischen und organisatorischen Maßnahmen (TOMs) zur Gewährleistung eines angemessenen Sicherheitsniveaus sind in Kapitel 2 beschrieben.

1.5.2. Re-Identifizierungsmöglichkeiten

Lokal in den teilnehmenden Standorten werden die Daten **pseudonymisiert** im AKTIN-DWH gespeichert i. S. d. Artikel 4 Nr. 5 DSGVO. Die Daten liegen für die Auswertung in anonymisierter oder pseudonymisierter Form vor, abhängig vom Zweck der jeweiligen Datenauswertung.

Die Daten oder die auf den Daten basierenden Analysen werden nur anonymisiert und ausschließlich als aggregierte Ergebnisse veröffentlicht, die insbesondere keine Rückschlüsse zulassen auf einzelne:

- Patienten*innen

- Klinikmitarbeiter*innen

Im Rahmen standortübergreifender Studien oder Forschungsprojekten kann ein Privacy-Preserving Record Linkage durchgeführt werden, beispielsweise unter Einbindung einer Treuhandstelle. Für solche standortübergreifenden Verknüpfungen ist ein separates Datenschutzkonzept zu erstellen, das die Verfahren, Rollen und technischen Schutzmaßnahmen beschreibt und vor Durchführung von den teilnehmenden Standorten, dem DUAC, der zuständigen Ethikkommission sowie gegebenenfalls der Datenschutzaufsichtsbehörde genehmigt wird (Vgl. 1.3 Umfang der Datenverarbeitung).

Zur Erfüllung der Auskunftspflichten nach § 6 Abs. 4 GDNG können Standorte ausschließlich lokal, autorisiert und zugriffsgeschützt prüfen, ob eine betroffene Person in eine bestimmte Datenabfrage einbezogen war, indem das lokale Pseudonym (z. B. Pat-ID) über eine standorteigene Benutzeroberfläche oder eine interne technische Schnittstelle mit den vor Ort vorhandenen Einweg-Hashs abgeglichen wird.

1.5.3. Restrisiko

Trotz der implementierten technischen und organisatorischen Schutzmaßnahmen (Vgl. Abschnitt 2) kann ein Restrisiko bei der Verarbeitung sensibler Gesundheitsdaten nicht vollständig ausgeschlossen werden. Ein mögliches Restrisiko besteht insbesondere in der theoretischen Re-Identifizierung einzelner Patient*innen durch unbefugte Dritte, etwa bei einer Kombination mit externen Datensätzen oder im Falle eines Sicherheitsvorfalls. Darüber hinaus kann bei sehr kleinen Fallzahlen ein geringes Risiko bestehen, dass aus aggregierten Ergebnissen indirekte Rückschlüsse auf Einzelpersonen gezogen werden. Weitere Restrisiken ergeben sich aus allgemeinen Faktoren bei komplexen IT-Systemen, beispielsweise unbeabsichtigten Fehlkonfigurationen, menschlichem Fehlverhalten oder bislang unbekannten Sicherheitslücken in verwendeten Softwarekomponenten.

Deshalb werden pseudonyme Daten in der AKTIN-Infrastruktur von datenverarbeitenden Gesundheitseinrichtungen verarbeitet, in denen grundsätzlich hohe gesetzliche, organisatorische und technische Anforderungen an den Umgang mit Gesundheitsdaten gelten. Diese Rahmenbedingungen gewährleisten ein hohes Schutzniveau auch für die im AKTIN-DWH verarbeiteten pseudonymisierten Daten. Das im TDAC betriebene SRE gewährleistet, dass übermittelte Gesundheitsdaten zu keinem Zeitpunkt außerhalb einer geschützten Analyseumgebung verarbeitet werden, sofern Forschenden direkter Zugriff auf die zu analysierenden Daten gegeben wird. Alle Verarbeitungsschritte erfolgen unter enger technischer, organisatorischer und administrativer Kontrolle, einschließlich Protokollierung, Zugriffsbeschränkung und Ergebnisprüfung. Durch die klare Trennung von Verantwortlichkeiten zwischen lokaler Datenhaltung und zentraler Analyse, den kontrollierten Datentransfer sowie die abschließende Anonymisierung der Ergebnisse wird das Risiko einer Re-Identifizierung oder eines unbefugten Datenabflusses auf ein Minimum reduziert.

1.6. Ethische und regulatorische Anforderungen

Die Forschung am Menschen sowie die Verarbeitung der dabei entstehenden Daten sind unerlässlich für die Weiterentwicklung, Sicherheit und Qualität der medizinischen Versorgung und liegen im hohen öffentlichen Interesse. Zugleich sind die Rechte und Interessen der

Patientinnen und Patienten jederzeit zu wahren und in ein angemessenes Verhältnis zum gesellschaftlichen Nutzen der Forschung zu setzen.

Die Arbeiten im Rahmen der AKTIN-Infrastruktur und des Notaufnahmeregisters orientieren sich an den ethischen Leitlinien der medizinischen Forschung. Grundlage bilden die WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects in ihrer jeweils gültigen Fassung (zuletzt revidiert 2024 in Helsinki) [4]. Zudem werden die Richtlinien zur Sicherung der guten wissenschaftlichen Praxis der Deutschen Forschungsgemeinschaft (DFG) [3] eingehalten. Diese stellen sicher, dass wissenschaftliche Integrität, Transparenz und Nachvollziehbarkeit bei der Planung, Durchführung und Publikation der Forschung gewahrt bleiben.

Die AKTIN-Infrastruktur, der Datensatz sowie die Nutzungszwecke des Notaufnahmeregisters wurden durch die Ethikkommission der Medizinischen Fakultät der Universität Magdeburg positiv bewertet (Votum 160/15 und 52/21, siehe Anlage 5). Darüber hinaus ist das Register im Deutschen Register Klinischer Studien (DRKS) registriert (Studien-ID: DRKS00009805).

Die Verarbeitung personenbezogener Daten im Rahmen des Notaufnahmeregisters erfolgt unter strikter Beachtung der geltenden datenschutzrechtlichen Bestimmungen der Europäischen Union, des Bundes und der Länder. Maßgeblich sind insbesondere die EU-Datenschutzgrundverordnung (DSGVO), das Gesundheitsdatennutzungsgesetz (GDNG), das Bundesdatenschutzgesetz (BDSG), sowie die jeweiligen Landesdatenschutz- und Krankenhausgesetze.

An den Stellen, an denen bereichsspezifische Gesetze den Eingriff in das informationelle Selbstbestimmungsrecht spezifischer regeln als allgemeine Datenschutzvorschriften, wird auf die entsprechende Rechtsgrundlage verwiesen. Das Notaufnahmeregister verpflichtet sich, diese Datenschutzvereinbarung regelmäßig zu aktualisieren, wenn technische, organisatorische oder gesetzliche Änderungen dies erforderlich machen.

Bei Störungen des Verarbeitungslaufs, Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten im Sinne von Artikel 4 (12), 33 und 34 DSGVO werden die betroffenen Personen, die Dateneigner sowie die zuständige Aufsichtsbehörde unverzüglich durch die AKTIN-Geschäftsstelle informiert. Personen, die nicht direkt kontaktiert werden können, werden über die offizielle Website des Registers (www.aktin.org) benachrichtigt.

1.7. Rechtsgrundlagen der Datenverarbeitung

1.7.1. Präambel zur rechtlichen Einschätzung der AKTIN-Infrastruktur

Die AKTIN-Infrastruktur stellt eine besondere Form der Registerinfrastruktur dar, die es teilnehmenden datenverarbeitenden Gesundheitseinrichtungen ermöglicht, Routinedaten aus der klinischen Versorgung dezentral, datenschutzkonform und unter Wahrung der informationellen Selbstbestimmung der jeweiligen Einrichtungen zu verarbeiten.

Die Datenverarbeitung erfolgt im Rahmen der gesetzlichen Regelungen des Gesundheitsdatennutzungsgesetzes (GDNG), insbesondere nach § 6 GDNG zur Weiterverarbeitung von Versorgungsdaten durch datenverarbeitende Gesundheitseinrichtungen zur Qualitätssicherung, zur Förderung der Patientensicherheit, zu

Forschungszwecken sowie zu statistischen Zwecken einschließlich der Gesundheitsberichterstattung. Für Einrichtungen in kirchlicher Trägerschaft gelten ergänzend die jeweiligen kirchlichen Datenschutzgesetze, insbesondere erfolgt eine Verarbeitung im öffentlichen Interesse nach § 6, § 13 und § 50 DSG-EKD (evangelische Einrichtungen) sowie § 6, § 11 und § 54 KDG (katholische Einrichtungen) in Verbindung mit Art. 9 Abs. 2 lit. j DSGVO innerhalb des kirchlichen Datenschutzrechts.

Die teilnehmenden Standorte sind datenverarbeitende Gesundheitseinrichtungen im Sinne des GDNG. Die zentralen Funktionen der AKTIN-Infrastruktur werden durch das Institut für Medizinische Informatik der Uniklinik RWTH Aachen und das Institut für Public Health in der Akutmedizin am Uniklinikum Magdeburg wahrgenommen. Die AKTIN-Infrastruktur ist somit ein öffentlich geförderter Zusammenschluss von datenverarbeitenden Gesundheitseinrichtungen nach § 6 GDNG. Jede Einrichtung ist datenschutzrechtlich verantwortlich im Sinne des GDNG und der DSGVO und trägt die Verantwortung für die Durchführung und Freigabe der jeweiligen Datenverarbeitung. Ziel ist eine datenschutzkonforme Nutzung von Routinedaten, die eine evidenzbasierte Qualitätsentwicklung, Forschung und Public-Health-Surveillance in der Notfall- und Akutmedizin unterstützt.

Die Datenverarbeitungen in der AKTIN-Infrastruktur umfassen insbesondere:

- **Lokale Verarbeitung und einwilligungsfreie Nutzung** pseudonymisierter Routinedaten innerhalb der teilnehmenden Notaufnahmen zur Qualitätssicherung, Patientensicherheitsförderung und eigenen Forschung gemäß § 6 Abs. 1 GDNG.
- **Übermittlung pseudonymisierter Daten** mehrerer Einrichtungen an das TDAC zur gemeinsamen wissenschaftlichen Nutzung gemäß § 6 Abs. 3 GDNG. Diese gemeinsame Verarbeitung ist nur zwischen patientenführenden Gesundheitseinrichtungen zulässig und bedarf der Genehmigung der zuständigen Datenschutzaufsichtsbehörde.
- **Anonymisierung von gesammelten Daten** innerhalb der datenverarbeitenden Gesundheitseinrichtungen, sobald dies für den jeweiligen Zweck möglich ist, gemäß § 6 Abs. 2 GDNG.
- **Übermittlung anonymisierter Teildatensätze** an das TDAC für statistische Auswertungen, Gesundheitsberichterstattung oder Public-Health-Analysen
- **Durchführung von Studien** mit informierter Einwilligung der Patient*innen

Durch dieses Modell werden alle Verarbeitungsformen, von der lokalen Eigenverarbeitung bis zur standortübergreifenden Verbundforschung, in Übereinstimmung mit den gesetzlichen Grundlagen des GDNG und den Anforderungen der Datenschutzgrundverordnung (DSGVO) umgesetzt.

Die Daten sind rechtlich der patientenführenden Abteilung, in der Regel der Notaufnahme, zugeordnet und werden dort unter der Verantwortung des jeweiligen Standorts in einem AKTIN-DWH gespeichert. Die Verantwortung für die Prüfung, Freigabe und anschließende Durchführung der Datenabfragen in den AKTIN-DWH-Systemen liegt bei den einzelnen Standorten. Diese erhalten durch die technische Infrastruktur vollständige Einsicht in die

Abfragen sowie in die zu übermittelnden Daten und können prüfen, ob Abfragen und zu übermittelnde Daten den für den Standort gültigen gesetzlichen, internen und externen Regelungen genügen. Erst nach expliziter Freigabe durch den Standort werden die Daten in pseudonymisierter oder aggregierter/ anonymisierter Form zentral zusammengeführt.

1.7.2. Lokale Verarbeitung pseudonymisierter Routinedaten in den Standorten

Die lokale Speicherung und Nutzung pseudonymisierter Routinedaten innerhalb der teilnehmenden Notaufnahmen zur Qualitätssicherung, Patientensicherheitsförderung und eigenen Forschung erfolgt auf Grundlage von § 6 Abs. 1 GDNG in Verbindung mit Art. 9 Abs. 2 lit. h, i und j DSGVO sowie § 22 und 27 Bundesdatenschutzgesetz (BDSG). Gemäß **§ 6 Abs. 1 und 2 GDNG** werden Daten mit **standortspezifischen oder studienspezifischen Pseudonymen** innerhalb der datenverarbeitenden Gesundheitseinrichtung verarbeitet.

Gemäß § 6 Abs. 1 GDNG sind datenverarbeitende Gesundheitseinrichtungen berechtigt, die bei ihnen nach Art. 9 Abs. 2 lit. h und i DSGVO rechtmäßig gespeicherten Gesundheitsdaten ohne Einwilligung der betroffenen Personen weiterzuverarbeiten, soweit dies erforderlich ist:

- zur Qualitätssicherung und Förderung der Patientensicherheit,
- zur medizinischen, rehabilitativen oder pflegerischen Forschung, oder
- zu statistischen Zwecken einschließlich der Gesundheitsberichterstattung.

Eine solche Verarbeitung umfasst sowohl lokale Nutzung als auch verteilte Analyseverfahren, einschließlich föderierter Lernverfahren, sofern diese ausschließlich auf den lokal pseudonymisierten Routinedaten der jeweiligen Einrichtung basieren.

Die im Rahmen der AKTIN-Infrastruktur durchgeführte lokale Weiterverarbeitung dient diesen Zwecken unmittelbar. Eine Einholung individueller Einwilligungen ist im Versorgungskontext der Notaufnahme nicht praktikabel, in der Regel unethisch und würde zu systematischen Verzerrungen führen, da gerade schwer erkrankte oder nicht einwilligungsfähige Personen ausgeschlossen wären. Eine vollständige und repräsentative Datengrundlage ist jedoch Voraussetzung für valide Erkenntnisse in der Qualitätssicherung, Patientensicherheitsanalyse und Versorgungsforschung.

Die Verarbeitung erfolgt daher im öffentlichen Interesse an der Sicherstellung einer hochwertigen und sicheren Notfallversorgung gemäß Art. 6 Abs. 1 lit. e DSGVO, unter Beachtung der besonderen Schutzmaßnahmen nach Art. 9 Abs. 2 lit. i, j DSGVO, § 22 Abs. 2 BDSG und § 6 GDNG.

1.7.3. Übermittlung pseudonymisierter Daten

Die Übermittlung pseudonymisierter Daten mehrerer datenverarbeitender Gesundheitseinrichtungen an das AKTIN-TDAC erfolgt auf Grundlage von § 6 Abs. 3 Gesundheitsdatennutzungsgesetz (GDNG) in Verbindung mit Art. 9 Abs. 2 lit. i und j DSGVO sowie §§ 22 und 27 Bundesdatenschutzgesetz (BDSG). Gemäß § 6 Abs. 3 GDNG ist eine gemeinsame Nutzung und Verarbeitung von Gesundheitsdaten zwischen öffentlich geförderten Zusammenschlüssen datenverarbeitender Gesundheitseinrichtungen – wie im Rahmen der AKTIN-Infrastruktur – zulässig, sofern:

- die Verarbeitung zu Zwecken der Qualitätssicherung, Patientensicherheitsförderung, medizinischen Forschung oder Gesundheitsberichterstattung erforderlich ist,
- die Anforderungen aus § 6 Abs. 1, 2 und 4 GDNG (Pseudonymisierung, Anonymisierung, Transparenz) eingehalten werden,
- die Interessen der betroffenen Personen durch angemessene technische und organisatorische Schutzmaßnahmen gewahrt und die Interessen des Verantwortlichen am öffentlichen Nutzen der Verarbeitung überwiegen, und
- die zuständige Datenschutzaufsichtsbehörde der gemeinsamen Nutzung und Verarbeitung zugestimmt hat.

Alle Anfragen zur standortübergreifenden pseudonymen Datennutzung werden deshalb zunächst einer ethischen und wissenschaftlichen Begutachtung unterzogen und müssen vor Durchführung in einem Studienregister (vgl. Abschnitt 2.2.6) dokumentiert werden. Verhältnismäßigkeit und öffentliches Interesse ist durch ein positives Ethikvotum einer anerkannten Ethikkommission zu belegen. Parallel erfolgt die Bewertung durch das DUAC, dass die wissenschaftliche Notwendigkeit, datenschutzrechtliche Erforderlichkeit und Verhältnismäßigkeit der beantragten Datenverarbeitung prüft. Die Genehmigung der Verarbeitung erfolgt erst nach Zustimmung der zuständigen Datenschutzaufsichtsbehörde, wie in § 6 Abs. 3 Nr. 4 GDNG vorgesehen. Die Datenübermittlung erfolgt nur auf der jeweils einschlägigen Rechtsgrundlage und nach den in § 6 GDNG vorgesehenen Voraussetzungen; die Auswertung erfolgt innerhalb einer geschützten Analyseumgebung am Universitätsklinikum Magdeburg (SRE).

1.7.4. Anonymisierung von gesammelten Daten

Die Anonymisierung der über die AKTIN-Infrastruktur für das Notaufnahmeregister erhobenen Routinedaten erfolgt auf der gesetzlichen Grundlage des § 6 Abs. 2 und Abs. 3 Gesundheitsdatennutzungsgesetz (GDNG) in Verbindung mit Art. 9 Abs. 2 lit. i und j DSGVO sowie den §§ 22 und 27 Bundesdatenschutzgesetz (BDSG). Sie stellt eine ausdrücklich im GDNG vorgesehene Pflicht- und zugleich Rechtsgrundlage für die Weiterverarbeitung dar, sobald der jeweilige Verarbeitungszweck ohne Personenbezug erreicht werden kann. Damit wird dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO Rechnung getragen und der Personenbezug vollständig aufgehoben. Die Anonymisierung erfolgt dezentral in den teilnehmenden datenverarbeitenden Gesundheitseinrichtungen durch Aggregierung oder Datenminimierung. Im TDAC werden zusätzlich technische Verfahren zur Datenminimierung, Unterdrückung, Aggregation oder Generalisierung identifizierender Merkmale durchgeführt, um eine Re-Identifizierbarkeit mit vertretbarem Aufwand auszuschließen.

1.7.5. Übermittlung anonymisierter Daten

Die Übermittlung anonymisierter Daten im Rahmen der AKTIN-Infrastruktur erfolgt auf Grundlage von § 6 Abs. 3 Satz 3 GDNG in Verbindung mit Art. 9 Abs. 2 lit. i und j DSGVO sowie §§ 22 und 27 BDSG. Sie ist zulässig, soweit die Daten zuvor so verarbeitet wurden, dass eine Re-Identifizierung mit vertretbarem Aufwand ausgeschlossen werden kann und die Übermittlung den in § 6 Abs. 1 GDNG genannten Zwecken – insbesondere Qualitätssicherung, Patientensicherheit, medizinische Forschung und Gesundheitsberichterstattung – dient.

Um verbleibende Restrisiken auszuschließen, unterliegt jede Übermittlung einem mehrstufigen Prüf- und Freigabeverfahren. Alle Datenübermittlungen werden durch das DUAC auf wissenschaftliche Notwendigkeit, datenschutzrechtliche Erforderlichkeit und Verhältnismäßigkeit geprüft. Nur Daten, die für die jeweilige Fragestellung erforderlich sind, dürfen übermittelt werden. Die Daten werden zunächst dezentral in den teilnehmenden Einrichtungen geprüft und nur in pseudonymisierter oder bereits teilanonymisierter Form an das TDAC übermittelt. Dort erfolgt eine Verarbeitung ausschließlich innerhalb einer geschützten Analyseumgebung (SRE), in der zusätzliche technische und statistische Verfahren angewendet werden (z. B. zur Erhöhung der k-Anonymität), um die Anonymität und die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen. Nach Abschluss der Analysen werden Ergebnisse erst nach formaler Prüfung einer hinreichenden Anonymität freigegeben.

Durch dieses Verfahren wird gewährleistet, dass jede Übermittlung anonymisierter Daten innerhalb des AKTIN-Systems rechtmäßig erfolgt, den Anforderungen des GDNG entspricht und die Interessen der betroffenen Personen gemäß § 22 Abs. 2 Satz 2 BDSG sowie Art. 9 Abs. 2 lit. i DSGVO gewahrt bleiben.

1.7.6. Forschungsvorhaben mit Einwilligungserfordernis

Forschungsvorhaben und interventionelle Studien, bei denen aufgrund der Art des Eingriffs, der prospektiven Beteiligung von Patient*innen oder aus ethischen Gründen eine ausdrückliche Einwilligung erforderlich ist, können innerhalb der AKTIN-Infrastruktur durchgeführt werden. Hierzu zählen insbesondere klinische Studien oder registerbasierte klinische Studien (registry-based clinical trials), bei denen zusätzlich zur routinemäßigen Datenerhebung spezifische Forschungsdaten oder Einwilligungen verarbeitet werden. Hierzu können im AKTIN-DWH studienspezifische Pseudonyme und Einwilligungsmarker hinterlegt werden, ohne den Behandlungskontext zu verlassen (vgl. Abschnitt 1.7.6).

Die rechtliche Grundlage für diese Datenverarbeitung ergibt sich aus Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit Art. 9 Abs. 2 lit. a DSGVO, wonach die Verarbeitung personenbezogener und besonderer Kategorien personenbezogener Daten rechtmäßig ist, wenn die betroffene Person freiwillig, informiert und ausdrücklich in die Verarbeitung zu einem bestimmten Zweck eingewilligt hat. Für diese Forschungsvorhaben kann innerhalb der AKTIN-Infrastruktur ein Einwilligungsmarker oder Einwilligungsnachweis hinterlegt werden, der die Zuordnung der entsprechenden Datensätze ermöglicht, ohne den Behandlungskontext zu verlassen. Die konkrete Ausgestaltung der Einwilligung, einschließlich Erhebung, Dokumentation, Widerruf und Nachvollziehbarkeit, wird in einem gesonderten, studienspezifischen Datenschutzkonzept geregelt. Dieses Datenschutzkonzept muss durch die zuständige Ethikkommission geprüft und genehmigt werden.

Tabelle 2 Anforderungen und Umsetzung des Gesundheitsdatennutzungsgesetzes (GDNG)

GDNG-Pflicht	Beschreibung	Umsetzung
Transparenzpflicht (§6 Abs. 4 GDNG)	Öffentliche Information über Zwecke der Datenweiterverarbeitung, laufende	• Bereitstellung von Informationen über Zwecke der Daten-verarbeitung an teilnehmende Standorte.

	und abgeschlossene Forschungsvorhaben; Registrierung in WHO-Primärregister	• Öffentliche Informationen über Zwecken der Datenverarbeitung auf www.aktin.org. • Öffentliche Informationen zu Zwecken der Datenverarbeitung durch Standort.
Auskunftspflicht (§6 Abs. 4 GDNG)	Betroffene Patient*innen müssen auf Verlangen über Art, Umfang und konkreten Zweck der Datenverarbeitung informiert werden	• Standardisierter lokaler AKTIN-DWH Export zu Art, Umfang und Zweck der Datenverarbeitung in Form von Studienlisten. • Lokale Kontaktmöglichkeit am Standort.
Sichere Datenverarbeitung (§6 GDNG)	Rechte- und Rollenkonzept, Protokollierung der Weiterverarbeitung, Ahndung unbefugter Verarbeitungen	• Rollen- und Rechtekonzept • TDAC mit SRE, betrieben auf Grundlage verbindlicher SOPs, Dienstanweisungen und regelmäßiger Schulungen. • Automatische Protokollierung aller Anfragen • Verschlüsselung nach Stand der Technik
Registrierungspflicht (§8 GDNG)	Eintragung in WHO-Primärregister; Beratungspflicht durch Ethik-Kommission	• Registrierung im DRKS (Studien-ID: DRKS00009805) • Registrierungspflicht in WHO-Primärregister
Veröffentlichungspflicht (§6 Abs. 4 GDNG & §8 GDNG)	Ergebnisse spätestens 24 Monate nach Abschluss veröffentlichen	• Publikationsordnung Notaufnahmeregister • Listung von Veröffentlichungen auf www.aktin.org
Geheimhaltungspflicht und Strafbewehrung (§9 GDNG)	Keine unzulässige Weitergabe an Dritte; keine Nutzung für andere Zwecke	• Zweistufige Datenübermittlung nach Datensparsamkeit • Datenverarbeitung nur durch datenverarbeitende Gesundheitseinrichtungen • Vertraulichkeits- und Verschwiegenheitspflicht für alle Personen mit Datenzugriff gemäß § 203 StGB, festgelegt durch Dienstanweisungen.
Genehmigungspflicht (§6 Abs. 3 GDNG)	Bei Verbundforschung: Zustimmung der Datenschutzaufsichtsbehörde innerhalb eines Monats	• Forschungsanfragen werden durch das DUAC geprüft. • Zustimmung von Forschungsanfragen durch zuständige Datenschutzaufsichtsbehörde gemäß § 6 Abs. 3 GDNG. • Zustimmung von Forschungsanfragen durch Standorte.
Pseudonymisierung & Anonymisierung (§6 Abs. 1, 2 GDNG)	Datenverarbeitung ohne Einwilligung nur mit pseudonymisierten Daten, Anonymisierung sobald möglich	• Lokale, standortspezifische pseudonymisierte Speicherung der Routinedaten mittels kryptographischem Einwegverfahren (Hash). • Schrittweise Anonymisierung der Daten vor jeder zentralen Übermittlung oder Veröffentlichung.
Datenminimierung (§6 Abs. 1,2 GDNG)	Nur die für den jeweiligen Zweck erforderlichen Daten verarbeiten	• Nur für Zwecke benötigte Daten werden abgefragt. • DUAC prüft Erforderlichkeit der einzelnen Variablen bei jeder Anfrage. • Standorte prüfen Notwendigkeit der Datenabfragen.

Positive Nutzen-Risiko-Abwägung (§6 Abs. 3 Nr. 3 GDNG)	Interessen des Verantwortlichen müssen Interessen der betroffenen Person erheblich überwiegen	• Verhältnismäßigkeit und öffentliches Interesse der Forschungsanfragen werden durch ein Ethikvotum einer anerkannten Ethikkommission belegt. • Das DUAC bewertet die Angaben im Hinblick auf Wissenschaftlichkeit, Erforderlichkeit und Verhältnismäßigkeit. • Technische und organisatorische Maßnahmen zur Datensicherheit minimieren verbleibende Risiken für Betroffene.

2. Technische und Organisatorische Maßnahmen

Für die verarbeiteten Daten gilt ein sehr hoher Schutzbedarf und entsprechende technische und organisatorische Maßnahmen. Sämtliche Daten werden Einweg-pseudonymisiert unter der Datenhoheit der behandelnden Einrichtung, d.h. der Notaufnahme des jeweiligen Standortes, gesammelt. Für Datenabfragen zu Forschungszwecken gelten die Anweisungen des DUAC, welches datenschutzrechtliche und ethische Standards garantiert.

Die technisch-organisatorischen Maßnahmen bei den teilnehmenden Standorten sind nicht Bestandteil dieses Datenschutzkonzepts, da der Schutzbedarf dort unabhängig vom Projekt besteht und bereits entsprechend umgesetzt ist (siehe Anlage 1 - Studienzentren). Insbesondere handelt es sich dabei primär um Datenverarbeitungen mit anderen Zwecken und Rechtsgrundlagen außerhalb der Regelungskompetenz der AKTIN-Infrastruktur und des Notaufnahmeregisters. Die teilnehmenden Kliniken tragen die Betriebsverantwortung für den Betrieb der lokalen Infrastrukturkomponenten (AKTIN-DWH und etwaige Schnittstellen).

2.1. Rollen und Rechte

Für alle Daten, die im Rahmen des Notaufnahmeregisters erhoben werden, gelten Maßnahmen entsprechend einem sehr hohen Schutzbedarf. Die Daten werden deshalb lokal gespeichert und nur nach einem standardisierten Freigabeprozess durch das DUAC an Dritte übermittelt. Es gilt ein striktes Rollenkonzept mit den Rechten limitiert auf das notwendigste. Alle vergebenen Rollen und die damit verbundenen Rechte werden regelmäßig überprüft. Das Notaufnahmeregister implementiert ein Rechte- und Rollenkonzept nach § 6 Abs. 1 S. 3 GDNG i. V. m. Art. 32 DSGVO.

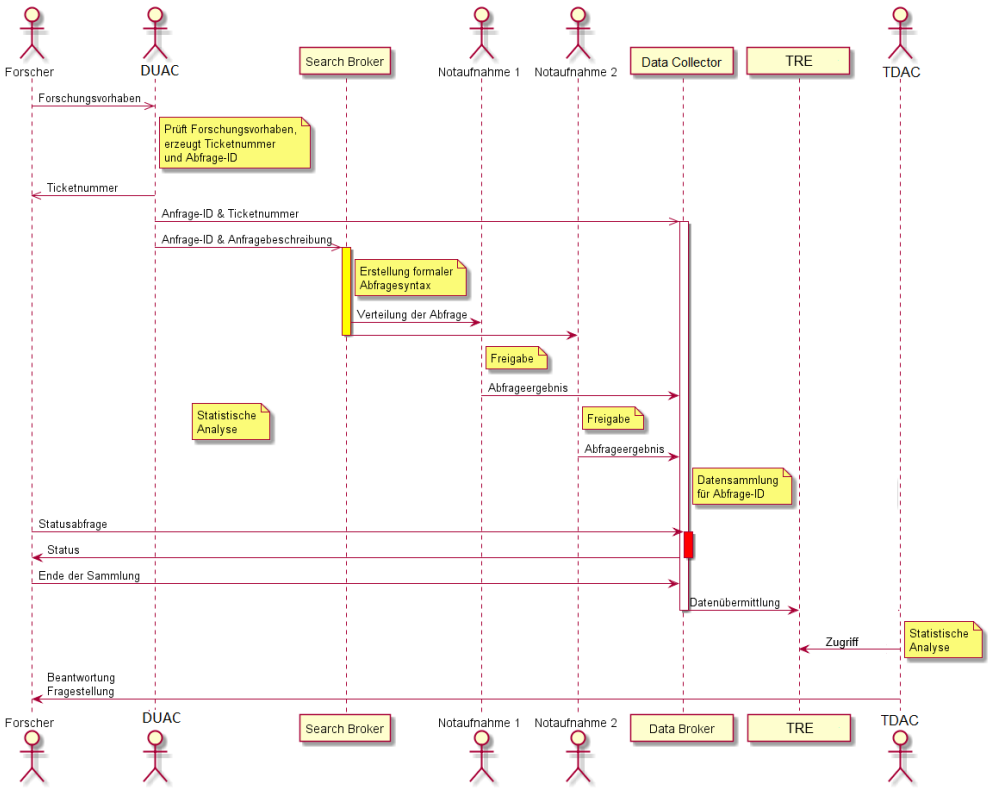

Abbildung 2 Prozessübersicht gemäß dem Rollen- und Rechtekonzept

2.1.1. Data Use and Access Committee (DUAC)

Das DUAC prüft und bewertet alle Anträge auf Datenauswertung, bevor diese an die teilnehmenden Standorte übermittelt oder zur Verarbeitung im TDAC freigegeben werden. Die Aufgaben des DUAC gehen dabei über eine rein wissenschaftliche Kontrolle hinaus. Es gewährleistet, dass jede Anfrage den rechtlichen und ethischen Anforderungen entspricht. Hierzu gehören insbesondere:

- die Bewertung der Datensparsamkeit, also die Prüfung, ob nur die für die jeweilige Fragestellung erforderlichen Variablen und Zeiträume angefragt werden,
- die Beurteilung der Anonymität und Angemessenheit der beantragten Verarbeitung im Hinblick auf § 6 Abs. 1–3 GDNG, einschließlich der technischen Angemessenheit der Anonymisierung und der Einhaltung der Grundsätze der Datenminimierung und Zweckbindung,
- die Nutzen-Risiko-Abwägung bei Anfragen, die eine Verarbeitung pseudonymisierter Daten erfordern, sowie die Prüfung der Erforderlichkeit und Verhältnismäßigkeit im Sinne des öffentlichen Interesses bei pseudonymisierten Anfragen gemäß § 6 GDNG.

Damit fungiert das DUAC als unabhängiges Gremium zur Sicherstellung von Datenschutz, wissenschaftlicher Qualität und Rechtskonformität in allen datenschutzrelevanten Prozessen im Notaufnahmeregister. Ihm gehört mindestens ein Mitglied des TDAC an, um eine enge Abstimmung zwischen wissenschaftlicher Bewertung, technischer Umsetzung und datenschutzrechtlicher Prüfung sicherzustellen.

2.1.2. Search Broker (SB)

Die Search Broker setzen die vom DUAC genehmigten Anfragen in Datenbankabfragen und standardisierte Terminologie um und stellt diese im Query Broker ein. Sie übermitteln die Abfragen anschließend an die Standortkoordinatoren mittels AKTIN-B. Ein Search Broker ist Teil des AKTIN-IT-Teams am Institut für Medizinische Informatik am Universitätsklinikum RWTH Aachen.

2.1.3. Standortkoordinator*in

Die Standortkoordinatoren*innen haben die Befugnis das lokale Datenmanagement in einem Standort zu verantworten. Standortkoordinatoren*innen werden vom jeweiligen Standort bestimmt. Bei Bedarf kann die Rolle von einem oder mehreren Personen gemeinsam ausgefüllt werden. Sie sind für die Umsetzung und Einhaltung aller ethischen, rechtlichen, vertraglichen und organisatorischen Vorgaben zum Datenmanagement verantwortlich. Sie verantworten somit eine lokale Prüfung jeder Abfrage, sowie die Festsetzung und Prüfung der Einhaltung der geltenden Kriterien der Anonymität durch die eigene Institution und institutionsspezifische Anforderungen. Der/die Standortkoordinatoren*innen müssen einer Datenabfrage zustimmen, bevor sie auf den Daten des entsprechenden Standorts durchgeführt wird. Sie können die Zwecke, die Beschreibung der Query, die eigentliche Query sowie die geplanten Ergebnistabellen einsehen und dabei insbesondere bewerten, ob die geplante Datennutzung den Prinzipien der ‚Five Safes' entspricht (Safe Projects, Safe People, Safe Settings, Safe Data, Safe Outputs).

2.1.4. Data Collector (DC)

Nur ein Data Collector hat die Berechtigung, im Data Aggregator gesammelte Abfrageergebnisse über den AKTIN-Broker authentifiziert abzurufen. Der Data Collector ist

zuständig für die Weiterleitung der Abfrageergebnisse der Standorte, die im Data Aggregator gesammelt werden, an das TDAC. Der/die Antragsteller*in kann beim Data Collector den Stand der Rückmeldungen erfragen und das Ende der Datenerhebung bzw. -sammlung festlegen. Außerdem können die Ergebnisse von technischen Anfragen an das AKTIN-IT weitergeleitet werden.

2.1.5. Trusted Data Analytics Center (TDAC)

Die Aufgabe der Mitarbeiterinnen und Mitarbeiter des TDAC umfasst die Prüfung, Aufbereitung, Aggregation und Auswertung der im Rahmen genehmigter Datenabfragen gesammelten Ergebnisse. Hierzu verarbeitet das TDAC die übermittelten anonymisierten oder pseudonymisierten Rohdaten innerhalb einer strikt kontrollierten und abgesicherten Secure Research Environment (SRE). Gemäß den Anforderungen des GDNG stellt das TDAC sicher, dass sämtliche Verarbeitungsschritte ausschließlich zu den genehmigten Zwecken erfolgen und dass die Anonymität und informationelle Selbstbestimmung der betroffenen Personen zu jedem Zeitpunkt gewahrt bleibt. Die Verarbeitung erfolgt unter strenger Einhaltung der Grundsätze der Datenminimierung, Zweckbindung und Transparenz nach § 6 Abs. 1–4 GDNG. Bei der Erstellung von Analyseergebnissen oder der Bereitstellung aggregierter Datensätze für Externe gewährleistet das TDAC, dass keine Rückschlüsse auf Einzelpersonen möglich sind. Dabei werden Verfahren wie k-Anonymität, l-Diversität und vergleichbare statistische Schutzmechanismen angewendet, um Re-Identifikationsrisiken auszuschließen. Das TDAC ermöglicht darüber hinaus, dass Angehörige anderer datenverarbeitender Gesundheitseinrichtungen, die einem genehmigten Forschungsvorhaben zugeordnet sind, innerhalb der SRE auf die entsprechenden Daten zugreifen und dort eigenständig Analysen durchführen können. Ein solcher Zugriff ist jedoch ausschließlich nach vorheriger Zustimmung des DUAC zulässig und muss im jeweiligen Forschungsantrag auf Datenabfrage explizit ausgewiesen und genehmigt werden. Alle Aktivitäten innerhalb des SRE erfolgen unter nachweisbarer Protokollierung, Zugriffsbeschränkung und ggf. Autorisierung durch Aufsichtsbehörden.

2.1.6. Forscher*in

Der/die Forscher*in (Angehörige öffentlicher Forschungseinrichtungen, medizinischer Fachgesellschaften und teilnehmender Standorte) kann über das AKTIN-Office Forschungsanträge über Daten aus dem Notaufnahmeregister stellen. Alle Anfragen werden protokolliert.

2.1.7. Auswertestelle

In begründeten Ausnahmefällen (z. B. bei periodischen Abfragen im Rahmen von Infektionssurveillance an Partner wie das Robert Koch-Institut) kann auch eine Übermittlung von Rohdaten an Forscher*innen eingerichtet werden, wenn dies zuvor vom DUAC genehmigt wurde und entweder die hinreichende Anonymisierung grundsätzlich bereits anhand der Abfrage gegeben ist (z. B. Struktur der Daten, automatisierte Anonymisierung) oder eine andere Rechtsgrundlage (beispielsweise aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren im Falle einer Pandemie nach § 22 Abs. 1 Nr. 1 lit. c BDSG in Verbindung mit Art. 9 Abs. 2 lit. g DSGVO) für die Datenübertragung vorliegt. Von den Forscher*innen wird dann eine *Auswertestelle* eingerichtet. Dies ist entsprechend in der

Anfrage an das DUAC zu beschreiben; ggf. muss ein zusätzliches Datenschutzkonzept erstellt werden.

2.1.8. Rollenkonflikte

Alle Rollen können in einigen Fällen geteilt werden. Die Rolle des Datenschützers darf an einem teilnehmenden Standort ausgeübt werden, nicht jedoch in Kombination mit anderen datenverarbeitenden Stellen, da diese überwacht werden sollen. Der Datenschutzbeauftragte muss unabhängig sein - er kann einem Standort zugehörig sein, darf aber keinen operativen Auftrag in der Datenverarbeitung haben.

Tabelle 3 Rollen, die geteilt werden können: Standortkoordinator (Standort) Datenschutz Standorte, Data Use and Access Committee (DUAC), Search Broker, Data Collector, Trusted Data Analytics Center (TDAC).

	Standort	Datenschutz	DUAC	Search Broker	Data Collector
Standort					
Datenschutz	Ja				
DUAC	Ja	Nein			
Search Broker	Ja	Nein	Ja		
Data Collector	Nein	Nein	Ja	Nein	
TDAC	Nein	Nein	Ja	Nein	Ja

2.2. Datenflüsse und IT-Infrastruktur

Die AKTIN-Infrastruktur für das Notaufnahmeregister besteht aus einer dezentralen Datenerhebung in den Notaufnahmen, die über eine zentrale IT-Komponente – dem AKTIN-Broker – verfügbar gemacht werden kann.

2.2.1. Dezentrale Datenerhebung in der Notaufnahme

Die Notaufnahmen der teilnehmenden Standorte verwenden elektronische Systeme zur Erfassung der medizinischen Routinedokumentation gemäß Datensatz Notaufnahme. Zusätzlich betreibt jedes Krankenhaus eine einheitliche AKTIN-DWH-Software auf einem eigenen dedizierten Server. Die AKTIN-DWH-Software wird von der AKTIN-IT bereitgestellt. Mittels einer Exportschnittstelle werden die entsprechenden Daten aus dem Informationssystem der Notaufnahme digital exportiert und als standardisierte HL7-CDA-Dokumente oder alternativ als HL7-FHIR-Ressourcen-Bundles des Datensatzes Notfalldokumentation (Szenario Notaufnahmeregister) an das AKTIN-DWH übermittelt. Über denselben HL7-FHIR-REST-Endpunkt können zudem optional Bundles des Szenario Notfalleinsatzprotokoll übermittelt werden. Nach dem Empfang erfolgt eine automatisierte syntaktische und inhaltliche Validierung der übermittelten Daten (CDA oder FHIR-Bundle) anhand umfangreicher Schematron-Regeln, um Struktur, Vollständigkeit und Konsistenz der Inhalte sicherzustellen.

Zusätzlich zu Notaufnahmedaten haben teilnehmende Standorte die Möglichkeit, weitere Daten aus dem stationären Aufenthalt (z. B. Entlassungsgrund, Entlassungszeit, Hauptdiagnose, Nebendiagnosen, Prozeduren, Operationstag, Beatmungsstunden) oder präklinischer bzw. rettungsdienstlicher Versorgung zu ihren Notaufnahmepatienten*innen in

das lokale AKTIN-DWH zu integrieren. Die Zuordnung zu den vorhandenen Daten erfolgt über das kryptographische Einwegverfahren wie oben beschrieben. Derartige Daten können anschließend auch für Berichte, Benchmarks und zentrale Abfragen verwendet werden.

Das lokale AKTIN-DWH kann von den lokalen Mitarbeitern für eigene Fragestellungen genutzt werden. Der Zugriff erfolgt authentifiziert personenbezogen über die Benutzeroberfläche des AKTIN-DWH. Das AKTIN-DWH selbst enthält keine unmittelbaren Patienten*innen-identifizierenden Merkmale (z. B. Pat-ID, Name, Vorname), jedoch eine Nummer, die mit einem kryptographischen Einwegverfahren (Hash) standortspezifisch erzeugt wird. Dieses Pseudonym kann nicht dazu verwendet werden, um auf die unmittelbare Identität des/der Patienten*in zu schließen, erlaubt es jedoch, Folgedaten den passenden Datensätzen zuzuordnen. Die lokalen Mitarbeiter haben keinen direkten Zugriff auf diesen Einweg-Hash. Nur der Datenbank Administrator kann dieses Pseudonym technisch bedingt einsehen. Der standortspezifische Einweg-Hash dient ausschließlich der internen technischen Zuordnung von Folgedaten und wird nicht für wissenschaftliche oder statistische Zwecke verwendet.

Für Forschungsprojekte kann zusätzlich ein studienspezifisches Pseudonym oder ein entsprechender Einwilligungsmarker im AKTIN-DWH automatisiert oder von authentifizierten lokalen Mitarbeitern hinterlegt werden, um die Zuordnung zu Studienkohorten, den Nachweis einer Einwilligung oder die Vorbereitung eines standortübergreifenden Privacy-Preserving Record Linkage zu ermöglichen. Die Nutzung solcher studienspezifischer Pseudonyme erfolgt ausschließlich im Rahmen genehmigter Forschungsvorhaben und unterliegt einem gesonderten Datenschutzkonzept, das die technischen Verfahren, Rollen und Schutzmaßnahmen beschreibt und – sofern erforderlich – von den teilnehmenden Standorten, dem DUAC, der zuständigen Ethikkommission sowie der Datenschutzaufsichtsbehörde freigegeben wird (Vgl. 1.3 Umfang der Datenverarbeitung).

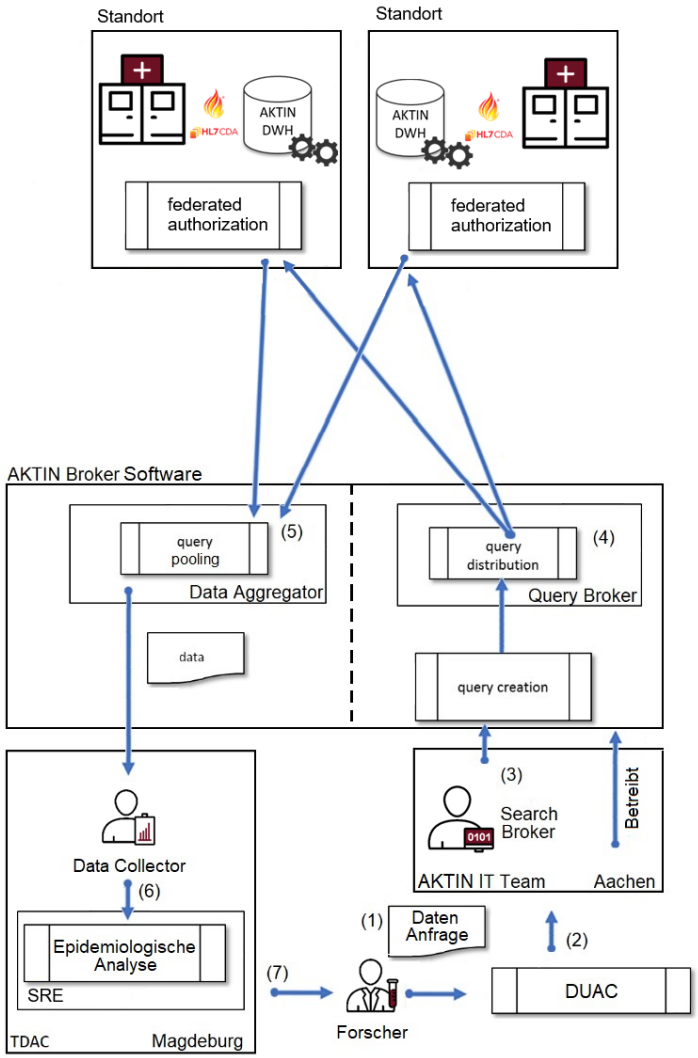

*Abbildung 3 Architekturübersicht und Datenflüsse. (1) Antrag auf Datenauswertung, (2) Prüfung durch DUAC und Weitergabe an Search Broker, (3) Erstellung der digitalen Abfrage durch den Search Broker, (4) Verteilung der Abfrage an teilnehmende Notaufnahmen über den Query Broker, (5) Sammlung Datenexporte, (6) Übermittlung gesammelter Rückmeldungen an die auswertenden Mitarbeiter*innen im TDAC für Analysen im Secure Research Environment (SRE), (7) Übermittlung der Auswertungsergebnisse an Forscher*innen.*

2.2.2. Zentrale Datenerhebung

Alle Anträge auf Datenauswertung für wissenschaftliche oder statistische Zwecke werden durch ein Review-Verfahren durch das DUAC geprüft und anschließend an die Standorte weitergeleitet. Die im Rahmen einer Abfrage angefragten Datensätze können je nach Vorhaben anonym oder pseudonym sein; dies wird durch das DUAC im Prüfprozess festgestellt, und die jeweils zutreffende Rechtsgrundlage (vgl. Kapitel 1.7) wird in der Datenanfrage ausgewiesen. Der *Query Broker* ist die Kommunikationsschnittstelle und verteilt die Anfragen für Datenauszüge als SQL-Query an alle Standorte. In jedem Standort muss der SQL-Query von den Standortkoordinatoren*innen explizit zugestimmt werden, bevor eine Abfrage durchgeführt und Daten exportiert werden. Es werden unmittelbar identifizierende Merkmale automatisch entfernt, sodass die Daten auf Fallebene bzw. Patientenebene ohne direkten Personenbezug vorliegen. Sollten studienspezifische Pseudonyme oder Einwilligungsmarker verarbeitet werden, erfolgt die Nutzung im TDAC ausschließlich

projektbezogen und auf Grundlage eines gesonderten, freigegebenen Datenschutzkonzepts (Vgl. 1.3 Umfang der Datenverarbeitung).

Die Exporte der Standorte werden an einer zentralen, unabhängigen Stelle (dem *Data Aggregator*) gesammelt und können dann vom TDAC abgerufen werden. Dort erfolgen Aufbereitung und Auswertung sowie Übermittlung der aggregierten Ergebnisse bzw. vergröberten Datensätze nach Prüfung einer vorab festgelegten ausreichenden Anonymität an den Forscher*in. Zusätzlich zu herkömmlichen verteilten Abfragen können periodisch wiederkehrende SQL-Queries erstellt werden. Die Anwender haben die Möglichkeit, wiederkehrende Abfragen über eine einmalige Zustimmung für weitere Ausführungen vollautomatisch freizugeben, wobei ein Widerspruch der Zustimmung möglich ist. Die Aufgaben des Data Aggregator und Query Broker werden über eine Webanwendung, den AKTIN-Broker, umgesetzt. Über diesen können Abfragen eingestellt und die Ergebnisse gesammelt werden. Der AKTIN-Broker wird auf einem dedizierten Server im Rechenzentrum des Uniklinikum RWTH Aachen betrieben.

2.2.3. Anträge auf Datenauswertung

Der Freigabeprozess für Anträge auf Datenauswertung für Forschungsanfragen und weitere Fragestellungen wird von der AKTIN-Geschäftsstelle organisiert. Datenauswertungen können in einem vorgegebenen Antragsformular an das DUAC, z. Hd. der AKTIN-Geschäftsstelle, gerichtet werden. Bei der Formulierung werden die Forscher*innen durch einen Katalog mit den für die Auswertung verfügbaren Daten und durch Beratungsleistungen des TDAC unterstützt. Mit dem Einreichen des Antrags erhält der/die Forscher*in eine Projekt-ID, die in der weiteren Kommunikation genutzt werden kann. Der Antrag wird vom DUAC inhaltlich und gemäß den rechtlichen Anforderungen geprüft und ggf. in Abstimmung mit dem/der Forscher*in angepasst. Der Antrag wird dann (mit Projekt-ID) an die AKTIN-IT zur Erstellung der Datenabfrage an die Standorte weitergegeben.

2.2.4. Verteilung von Datenabfragen

Nach Erhalt eines Antrags auf Datenauswertung und Erstellung der Datenabfrage wird diese durch die AKTIN-IT in eine SQL-Abfrage übertragen. Die SQL-Abfrage wird dann zusammen mit der Datenabfragebeschreibung und der Abfrage-ID an alle teilnehmenden Standorte per Query-Broker des AKTIN-Brokers verteilt. Alle teilnehmenden Standorte erhalten bezogen auf die Abfrage-ID das identische Abfragepaket. Sämtliche Datenabfragen (nur die Anfrage selbst – nicht die klinischen Datensätze) werden vom AKTIN-Broker archiviert und für einen Zeitraum von 10 Jahren nach Studienveröffentlichung aufbewahrt.

2.2.5. Beantwortung der Datenabfrage an jedem Standort

Im Zielsystem kann die Datenabfrage vom Standortkoordinator über die AKTIN-DWH-Manager Benutzeroberfläche geöffnet, geprüft, beantwortet (Freigabe/Ablehnung) und die Abfrageergebnisse (nach Freigabe) angezeigt werden. Die Abfrageergebnisse enthalten keine Patienten*innen-identifizierenden Merkmale. Nach Kontrolle durch den Standortkoordinator*in können diese/r die Ergebnisse der Datenabfrage prüfen und diese erneut ablehnen oder ihr zustimmen. Durch die Zustimmung wird eine Übermittlung der Abfrageergebnisse an den Data Aggregator ausgelöst. Zusätzlich zu den Abfrageergebnissen und der Abfrage-ID wird eine Standortidentifikation übermittelt. Abfragedurchführung und Ergebnisübermittlung können mehrfach als Serie (zukünftig) wiederholt werden; Serienfreigaben werden ausdrücklich in der jeweiligen Datenanfrage ausgewiesen.

2.2.6. Verarbeitung von Datenabfrageergebnissen

Die Ergebnisse von Datenabfragen können jederzeit nach Übermittlung vom TDAC über den AKTIN-Broker vom Data Collector abgerufen werden. Die Daten werden im TDAC in einem geschützten, zugriffsbeschränkten und überwachten Bereich, dem SRE, verarbeitet. Die Verarbeitung findet durch Mitarbeiter*innen des TDAC statt. Die Mitarbeiter*innen des TDAC erstellen zunächst eine deskriptive Übersichtsauswertung der eingegangenen Daten und erstellen dann die Auswertungen gemäß Analyseplan des Antrags auf Datenauswertung der Forscher*innen. Zu diesem Zweck können Mitarbeiter des TDAC und Forscher*in in Dialog treten.

Nach Abschluss der Auswertung erhalten Forscher*innen die aggregierten Ergebnisse. Falls Forscher*innen Datensätze benötigen, so wird vom TDAC ein hinreichender Grad an Anonymisierung sichergestellt.

In begründeten Fällen kann Forscher*innen durch das DUAC ein zeitlicher und zweckgebundener Zugriff auf Rohdaten innerhalb der SRE des TDAC gewährt werden. Eine solche Zugriffsgewährung erfolgt ausschließlich nach Prüfung der Erforderlichkeit und Verhältnismäßigkeit durch das DUAC und wird in der jeweiligen Datenabfrage für die Standorte transparent dokumentiert. Sollte ein Zugriff auf pseudonymisierte Daten erforderlich sein, kann dieser ausschließlich durch Angehörige datenverarbeitender Gesundheitseinrichtungen erfolgen. Die technische Infrastruktur des SRE stellt sicher, dass die Daten ausschließlich innerhalb der geschützten Umgebung verarbeitet werden können. Jegliche Form des Exports, Kopierens oder unautorisierter Weitergabe ist technisch unterbunden. Alle Verarbeitungsschritte werden protokolliert und bei Export von aggregierten Ergebnissen durch Mitarbeiter*innen des TDAC auditiert. Das TDAC schließt mit den Forscher*innen eine Vereinbarung zur Datenüberlassung, welche die Rechte und Pflichten regelt.

2.3. Verschlüsselung

Die Übertragung der Daten zwischen den Beteiligten geschieht grundsätzlich mit Transport-Verschlüsselung (TLS 1.3) nach Stand der Technik. Es werden niemals Pseudonyme, (temporäre) IDs oder sonstige personenbeziehbare Daten über eine unverschlüsselte Internetverbindung übertragen.

2.4. Gewährleistung der Vertraulichkeit

Die Vertraulichkeit des Search Broker wird technisch gewährleistet, indem der Webserver und die Datenbank im entsprechend gesicherten und zertifizierten Rechenzentrum des UK RWTH Aachen betrieben werden. Dort gibt es insbesondere Schließ- und Alarmanlagen nach gängigen Standards, restriktiv konfigurierte Firewalls und Überwachungssoftware.

2.5. Gewährleistung der Integrität

Bei der Übertragung der Daten wird anhand von Checksummen geprüft, ob die Daten korrekt übermittelt wurden. Dazu wird über die gesamte Datenmenge (Nutzdaten und IDs) ein Message Digest-Verfahren angewendet, das jede Form von Übertragungsfehlern (Anzahl der Zeilen, fehlerhafte Übertragung der Inhalte etc.) detektiert. Bei Fehlern werden die

empfangenen Daten gelöscht und der Versand wird erneut durchgeführt. Diese Checksummen werden automatisch durch das Übertragungsverfahren erzeugt und überprüft.

Die Daten eines Falls (HL7 CDA bzw. HL7 FHIR) werden beim Import in das lokale AKTIN-DWH auf Lesbarkeit, Übereinstimmung mit der konsentierten Datensatzbeschreibung, Vollständigkeit und Plausibilität getestet, soweit diese Prüfalgorithmen a-priori festgelegt werden können. Sind die Daten in einem Umfang fehlerhaft, dass eine Nutzung für die Zwecke der Evaluation nicht möglich ist (nur basierend auf den Vorgaben der Prüfalgorithmen, darüber hinaus können sie trotzdem nicht plausibel bzw. falsch sein), wird der Import des Falls abgelehnt. Mitarbeitende des TDAC führen beim Anschluss einer Klinik eine inhaltliche Validierung der Datenübertragung durch (Abgleich zwischen EDIS und AKTIN-DWH). Nach erfolgtem Anschluss werden die Daten regelmäßig im Rahmen automatisierter und manueller Prüfungen auf Vollständigkeit sowie auf Veränderungen in den Datenstrukturen und Wertverteilungen kontrolliert.

2.6. Gewährleistung der Verfügbarkeit

Am Standort des UK RWTH Aachen ist die Verfügbarkeit der Daten durch den Betrieb im jeweiligen Rechenzentrum gesichert. Es gibt bzgl. der Notstromversorgung, redundanter Klimatisierung, Netzanbindung etc. gängige Vorkehrungen. In den lokalen AKTIN-DWHs gelten jeweils lokale Bestimmungen.

2.7. Gewährleistung der Belastbarkeit der Systeme

Die Belastbarkeit der Hardware bzw. des Rechenzentrums des Uniklinikums der RWTH Aachen genügt den gängigen (höchsten) Anforderungen. Eine hohe Belastung der Systeme ist nicht zu erwarten, und auch kurzzeitige Ausfälle würden die Projektziele nicht gefährden. In den lokalen AKTIN-DWHs gelten jeweils lokale Bestimmungen.

2.8. Verfahren zur Wiederherstellung der Verfügbarkeit der Daten nach einem physischen oder technischen Zwischenfall

Die Daten des AKTIN-Brokers werden in täglichen Backups gesichert. Im Bedarfsfall können die vorliegenden Daten aus einem Backup wiederhergestellt werden. Die Backups werden für einen Monat gespeichert und anschließend automatisch gelöscht. In den lokalen DWHs gelten jeweils die lokalen Bestimmungen des jeweiligen Standorts.

2.9. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Eine jährliche Überprüfung (zu Beginn eines Kalenderjahrs, dokumentiert durch das AKTIN-IT-Team) der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen ist Bestandteil des Betriebskonzepts. Dabei werden die von AKTIN betriebenen Komponenten hinsichtlich der technischen und organisatorischen Maßnahmen jährlich intern überprüft. Die Standorte werden über die Überprüfung und das Ergebnis der Überprüfung informiert. Dabei werden die folgenden Aspekte geprüft und ggf. Maßnahmen ergriffen:

- Release-Stände der verwendeten Betriebssysteme und Anwendungssoftware inkl. Prüfung, ob Patches regelmäßig installiert wurden

- Einsatz von Updateverfahren von Firewall und Virenschutz
- Evaluation von Sicherheitsvorfällen und Störungen
- Entsprechen die Maßnahmen noch dem Stand der Technik (insbesondere Entwicklungen bzgl. der Verschlüsselungstechnologien u. ä.)
- Wirksamkeit der Backup-Verfahren (ggf. Recovery-Test)
- Schulung der mit der Datenverarbeitung betrauten Personen

In den lokalen DWHs gelten jeweils lokale Bestimmungen.

2.10. Schriftliche Dokumentation von sonstigen Maßnahmen

Für das Rechenzentrum des Uniklinikums RWTH Aachen existieren diverse technische und prozessorientierte Dokumentationen, die auf der Ebene der technischen Infrastruktur einen Betrieb nach dem Stand der Technik gewährleisten.

In den lokalen AKTIN-DWHs gelten jeweils lokale Bestimmungen und obliegen der Verantwortlichkeit des einzelnen Standorts.

2.11. Verfahren bei Sicherheitsvorfällen, Protokollierung und Ahndung

In der AKTIN-Infrastruktur und dem Notaufnahmeregister ist festgelegt, wie bei technischen Störungen, Datenschutzverletzungen oder sicherheitsrelevanten Vorfällen vorzugehen ist. Auftretende Vorfälle werden unverzüglich von der betroffenen Einrichtung an das AKTIN-Office gemeldet, die als zentrale Koordinationsstelle fungiert. Sofern eine Meldepflicht nach DSGVO besteht, informiert dieses die zuständige Datenschutzaufsichtsbehörde.

Zur Sicherstellung einheitlicher Abläufe bestehen definierte Wiederherstellungszeiten (RTO/RPO) sowie abgestimmte Kommunikationswege und Vorlagen. Auf Infrastrukturebene greift ein Incident-Response-Plan, der Meldekette, Rollen, Verantwortlichkeiten und Eskalationsstufen verbindlich regelt. Die Umsetzung ist in der SOP „Incident Response“ dokumentiert und wird regelmäßig überprüft.

Die konsortiale Datenschutz-Folgenabschätzung (Art. 35 DSGVO) umfasst Risikoanalyse, Verhältnismäßigkeitsprüfung und Maßnahmenplan und wird fortlaufend aktualisiert.

3. Betroffenenrechte

Die Wahrung der Rechte der betroffenen Personen bildet einen zentralen Bestandteil der datenschutzkonformen Umsetzung der AKTIN-Infrastruktur. Da im Notaufnahmeregister pseudonymisierte oder anonymisierte Daten verarbeitet werden, können Betroffenenrechte, insbesondere Auskunft, Berichtigung, Löschung oder Widerspruch, grundsätzlich nur über die datenführenden Standorte ausgeübt werden. Nur dort liegt der Personenbezug vor.

Das AKTIN-Office selbst verfügt zu keinem Zeitpunkt über identifizierende Informationen und kann daher keine individuelle Zuordnung oder Auskunft vornehmen. Betroffene, die sich direkt an das AKTIN-Office wenden, erhalten allgemeine Informationen gemäß Art. 13 / 14 DSGVO und werden an den jeweils verantwortlichen Standort verwiesen.

Die nachfolgenden Abschnitte beschreiben die konkreten Verfahren zur Wahrung der Informations-, Auskunfts-, Widerspruchs- und Löschrechte sowie die Verantwortlichkeiten der beteiligten Einrichtungen.

3.1. Erfüllung der Informationspflicht nach Art. 13/14 DSGVO bzw. § 6 Abs. 4 GDNG

Für die Erhebung und Weiterverarbeitung personenbezogener Daten gelten die Informationspflichten nach Art. 13 und 14 DSGVO. Ergänzend verpflichtet § 6 Abs. 4 GDNG datenverarbeitende Gesundheitseinrichtungen dazu, die Öffentlichkeit in präziser, transparenter und leicht verständlicher Form über die Zwecke der Datenverarbeitung, laufende Forschungsvorhaben und veröffentlichte Ergebnisse zu informieren.

Diese Anforderungen werden im Rahmen der AKTIN-Infrastruktur wie folgt umgesetzt:

- Eigenverantwortliche Bereitstellung von Informationen zu Zwecken der Datenverarbeitung durch teilnehmende Standorte,
- ergänzende öffentliche Information durch die teilnehmenden Standorte über deren lokale Kommunikationskanäle (z. B. Krankenhauswebseiten oder Patienteninformationen),
- Veröffentlichung der Informationen über Zwecke, laufende Forschungsvorhaben und Ergebnisse auf der Website www.aktin.org.

Damit wird sichergestellt, dass sowohl betroffene Patient*innen als auch die Öffentlichkeit jederzeit nachvollziehen können, zu welchen Zwecken und unter welchen Bedingungen Routinedaten in der AKTIN-Infrastruktur verarbeitet werden.

3.2. Erfüllung der Auskunftspflicht nach Art. 15 DSGVO bzw. § 6 Abs. 4 GDNG

Betroffene Personen haben das Recht, Auskunft darüber zu verlangen, ob und in welchem Umfang sie betreffende personenbezogene Daten im Rahmen der AKTIN-Infrastruktur verarbeitet werden. Da die Daten in der Regel ohne Personenbezug außerhalb der teilnehmenden Gesundheitseinrichtung verarbeitet werden, kann eine Zuordnung zu einzelnen Personen nur an den jeweiligen patientenführenden Standorten erfolgen.

Anfragen auf Auskunft sind daher grundsätzlich an den jeweiligen Standort zu richten. Nur dort besteht die Möglichkeit einer Zuordnung zwischen Patient*in und pseudonymisierten Datensätzen. Das AKTIN-Office kann bei Anfragen allgemeine Informationen zu den Verarbeitungszwecken, Rechtsgrundlagen und Verantwortlichkeiten bereitstellen (Art. 13 bzw. 14 DSGVO), verweist jedoch im Falle einer individuellen Auskunft auf das jeweils verantwortliche Krankenhaus und unterstützt Betroffene. Sollte eine Auskunftsanfrage irrtümlich an eine andere an der AKTIN-Infrastruktur teilnehmende Einrichtung gelangen, wird sie an das AKTIN-Office oder die jeweils zuständige datenführende Gesundheitseinrichtung weitergeleitet. Sofern Daten im SRE bzw. AKTIN-TDAC nicht faktisch anonym, sondern im Rahmen eines Forschungsvorhabens studienspezifisch pseudonymisiert verarbeitet werden, gelten die Auskunftspflichten fort; ihre Umsetzung erfolgt dann nach dem jeweils

projektspezifischen Datenschutzkonzept und in Abstimmung mit den verantwortlichen Standorten.

Zur Umsetzung der Auskunftspflicht können die Standorte die grafische Benutzeroberfläche oder eine technische Schnittstelle des AKTIN-DWH nutzen. Diese ermöglicht den Export eines standardisierten Auszugs über Art, Umfang und konkreten Zweck der Datenverarbeitung (d.h. Studienliste mit Übersicht der Studien und Datenabfragen, in denen die betroffene Person berücksichtigt wurde). So können Transparenz- und Auskunftspflichten gemäß § 6 Abs. 4 GDNG lokal umgesetzt werden. Negativauskünfte – also Bestätigungen, dass keine Verarbeitung stattgefunden hat – werden direkt durch den Standort an die betroffene Person übermittelt. Eine weitere Kommunikation zwischen Projektpartnern ist bei Auskünften nicht erforderlich.

3.3. Verfahren bei Widerspruch nach Art. 21 bzw. Löschanfragen nach Art. 17 DSGVO

Die Betroffenen können eine Löschung der sie betreffenden personenbezogenen Daten verlangen. Da der wissenschaftliche Forschungszweck bei der zu erwartenden geringen Fallzahl an Löschungen bzw. Widersprüchen nicht „unmöglich oder ernsthaft beeinträchtigt“ werden würde (Art. 17 Abs. 3 lit. d DSGVO), bleibt bei den Betroffenen das Widerspruchsrecht nach Art. 17 bzw. Art 21 DSGVO bestehen.

Die Anfrage zur Löschung bzw. Widerspruch sollte über den jeweiligen Standort erfolgen, da nur das jeweilige Krankenhaus Zugriff auf identifizierende Daten hat. Sollten sich Betroffene direkt an die AKTIN-Geschäftsstelle wenden, wird der Patient über diesen Umstand aufgeklärt und an die Datenschutzbeauftragten des Standortes vermittelt, vorausgesetzt dem/der Patient*in liegt diese Information vor. Der Ausschluss von Patienten wird vom Standort im AKTIN-Consent-Manager dokumentiert.

Negativ-Auskünfte (wenn die Person nicht betroffen oder die Zuordnung nicht mehr möglich ist) werden direkt an den Betroffenen zurückgegeben. Eine weitere Kommunikation unter den Projektpartnern ist dann nicht erforderlich. Für Datenauszüge, die bereits erstellt worden, ist es nicht möglich betroffene Personen zu identifizieren, hier finden die Art. 15 bis 20 DSGVO keine Anwendung.

3.3.1. Widerspruchsfolgen bzw. Folgen von Löschanfragen

Ein Widerspruch führt zu einer Löschung[1] bzw. Sperrung (für externe Datenverarbeitung) der im lokalen AKTIN-DWH gespeicherten medizinischen Daten des/der Patienten*in nach Maßgabe und durch die jeweilige Klinik. Eine Sperrung (für externe Datenverarbeitung) durch die jeweilige Klinik ist dann notwendig, wenn der Widerspruch eine Datenverarbeitung zu Zwecken und Rechtsgrundlagen außerhalb der Regelungskompetenz der AKTIN-Infrastruktur und des Notaufnahmeregisters berührt (bspw. allgemeine Dokumentations- und Aufbewahrungspflichten, Qualitätssicherungszwecke).

[1] Die dafür notwendige SQL-Syntax kann vom AKTIN-IT-Team angefragt werden.

3.4. Verantwortung für die Umsetzung der Betroffenenrechte

Für die Erfüllung der Betroffenenrechte übernimmt der Standort die Verantwortung im Sinne von Art. 26 DSGVO. Die beteiligten Projektpartner werden vertraglich verpflichtet, entsprechend des hier definierten Prozesses, an der Erteilung der Auskunft mitzuwirken. Die Dateneigner verpflichten sich ebenfalls zur Mitwirkung.

3.5. Datenlöschung

Datenübermittlungen bzw. -erhebungen finden seit 2015 statt. Es gelten die Lösch- und Aufbewahrungsfristen gemäß den rechtlichen Vorgaben am jeweiligen Standort.

Für Abfragen zusammengeführte Daten werden gelöscht, (1) sobald die gesammelten Daten abschließend hinsichtlich der Fragestellung analysiert wurden; oder (2), wenn innerhalb von 90 Tagen keine Interaktion zwischen Forscher*in und TDAC erfolgt ist. Die Löschung kann durch den Forscher*in nicht aufgeschoben oder verhindert werden. Bei der Löschung wird die Abfrage-ID und Ticketnummer weiterhin aufbewahrt und als gelöscht gekennzeichnet. Alle anderen zugehörigen Daten werden gelöscht. Sollten nach der Löschung weitere Abfrageergebnisse von Standorten geliefert werden, so werden diese sofort gelöscht. Für die Auswertungsdauer von (ggf. vollständig anonymen) Daten durch die Forscher*innen gelten Löschfristen gemäß den Vorgaben des DUAC und SOPs des TDAC (Anlage 8).

Support- und Kommunikationsdaten, die im Rahmen des technischen Betriebs oder der Fehlerbehebung anfallen (z. B. E-Mail-Verkehr mit dem AKTIN-Support), werden beim Institut für Medizinische Informatik der RWTH Aachen für einen Zeitraum von bis zu 10 Jahren aufbewahrt, um die Nachvollziehbarkeit und Qualitätssicherung des technischen Supports zu gewährleisten. Personenbezogene Supportdaten, die im Rahmen eines konkreten Supportfalls verarbeitet werden müssen (z. B. temporärer Zugriff auf Benutzerkonten oder Konfigurationsdaten), werden unmittelbar nach Abschluss des jeweiligen Vorgangs gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

4. Vereinbarung zur gemeinsamen Verantwortlichkeit und Inkrafttreten

Das vorliegende Datenschutzkonzept wurde von allen genehmigt, die in den Prozess der Datenverarbeitung einbezogen sind. Dieses Datenschutzkonzept regelt die Zusammenarbeit und die Verantwortungsabgrenzung zwischen den datenverarbeitenden Stellen im Sinne einer gemeinsamen Datenverarbeitung nach Art. 26 DSGVO. Das Datenschutzkonzept und die impliziten Pflichten werden durch die Teilnahme an der AKTIN-Infrastruktur bzw. dem Notaufnahmeregister anerkannt. Es kann außerdem ein expliziter Vertrag zwischen den Parteien geschlossen werden, der dann stattdessen als eine solche Vereinbarung gilt.

5. Datenerhebung gemäß Leitfaden zum Datenschutz der TMF

Die Datenerhebung bzw. die organisatorische Trennung von identifizierenden und medizinischen Daten folgt den Empfehlungen der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF). Es erfolgt eine Datenerhebung im Sinne des Basismodells (mit dezentralen Patientenlisten) des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten – generische Lösungen der TMF 2.0 [1]. Eine Abweichung vom TMF-Datenschutzleitfaden liegt im Verzicht auf eine explizite Einwilligung der Betroffenen und die Nutzung des GDNG als Rechtsgrundlage. Der vollständige Einschluss aller in der Notaufnahme behandelten Patient*innen ist erforderlich, um eine verzerrungsfreie Datengrundlage für die Infektionssurveillance, Qualitätsmessung und Versorgungsforschung sicherzustellen. Eine Einholung individueller Einwilligungen würde zu systematischen Ausfällen ganzer Patientengruppen durch das Fehlen der Einwilligungsfähigkeit in der Notaufnahme führen und damit die Aussagekraft und Repräsentativität der Analysen erheblich beeinträchtigen. Die Datenverarbeitung erfolgt daher auf einer gesetzlichen Grundlage im öffentlichen Interesse an der Gesundheitsforschung und Gesundheitsberichterstattung unter Einhaltung aller datenschutzrechtlichen Schutzmechanismen.

6. Anlagen

Anlage 1 – Studienzentren

Anlage 2 – Ansprechpartner Datenschutz

Anlage 3 – Datensatzbeschreibung Datensatz Notaufnahmeregister V2025.3.tr

Anlage 4 – Datensatz stationäre Behandlungsdaten

Anlage 5 – Ethikvotum 160/15 – 52/21

Anlage 6 – Geschäftsordnung DUAC in der aktuell gültigen Fassung

Anlage 7 – Publikationsordnung AKTIN-Notaufnahmeregister in der aktuell gültigen Fassung

Anlage 8 – SOP Löschfristen TDAC

7. Literatur

[1] K. Pommerening, J. Drepper, K. Helbing, T. Ganslandt, *Leitfaden zum Datenschutz in medizinischen Forschungsprojekten: Generische Lösungen der TMF 2.0,* MWV Med. Wiss. Verl.-Ges, Berlin, 2014.

[2] M. Kulla, M. Baacke, T. Schöpke, F. Walcher, A. Ballaschk, R. Röhrig, J. Ahlbrandt, M. Helm, L. Lampl, M. Bernhard, and D. Brammen, Kerndatensatz „Notaufnahme“ der DIVI. Notfall Rettungsmed **17** (2014), 671–681.

[3] Deutsche Forschungsgemeinschaft, Guidelines for Safeguarding Good Research Practice. Code of Conduct (2019).

[4] World Medical Association Declaration of Helsinki: ethical principles for medical research involving human subjects. JAMA **310** (2013), 2191–2194.