Datenschutz-Folgenabschätzung

Notfallregister

im Auftrag des
Bayerischen Staatsministeriums
des Innern, für Sport und Integration

Alexander Roßnagel, Christian L. Geminn, Paul C. Johannes,
Mike Forner, Jürgen Weidner

Version: **1.2**

Datum: **12.03.2021**

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

1 EINLEITUNG

Im Notfallregister (NFR) sollen Daten aus der präklinischen Phase mit Daten aus den Krankenhäusern im Freistaat Bayern und der Kassenärztlichen Vereinigung Bayerns (KVB) zusammengeführt werden, um eine sektorenübergreifende Betrachtung dieser Daten für Qualitätsmanagement im Rettungsdienst und Versorgungsforschung zu ermöglichen. Im Rahmen des Qualitätsmanagements kann durch das NFR erkannt werden, inwieweit medizinische Empfehlungen und Leitlinien beachtet werden. Im Rahmen der Versorgungsforschung ermöglicht das NFR die Erforschung neuer, unbekannter Zusammenhänge. Zielsetzung dieser Forschung ist es, die notfallmedizinische Versorgung und Behandlung zu verbessern.

Der Beurteilungsmaßstab für notfallmedizinische Variablen soll deren Auswirkung auf den Notfallpatienten sein. Dessen professionelle Versorgung beginnt mit dem Absetzen des Notrufs und dem Eintreffen des Rettungsdienstes, endet jedoch nicht mit Einlieferung in die Notaufnahme. Diagnose und Weiterbehandlung erfolgen in der Regel im Krankenhaus. Will man die Wirksamkeit, Effizienz und Sicherheit unterschiedlicher Maßnahmen und Veränderungen entlang der Rettungskette sowie die Auswirkungen der notfallmedizinischen Versorgungsplanung auf den Patienten beurteilen, so erfordert dies eine Betrachtung medizinischer Daten über die präklinische Phase hinaus. Zwar werden derzeit sowohl von den Integrierten Leitstellen (ILS), den Durchführenden des Rettungsdienstes als auch von den Krankenhäusern und der KVB jeweils eigene Dokumentationen zu den einzelnen Fällen erstellt. Diese werden aber nicht zu einer einheitlichen Falldokumentation zusammengeführt. Um wissenschaftlich belastbare statistische Aussagen zu erlangen, muss eine ausreichende Zahl von Fällen betrachtet werden. Dies ist derzeit mangels Verfügbarkeit ausreichender Daten für Qualitätssicherung und notfallmedizinische Forschung nicht möglich. Um die notwendige Datengrundlage gewährleisten zu können, ist ein NFR erforderlich.

Im NFR werden personenbezogene Daten verarbeitet. Eine Anonymisierung erfolgt, sobald dies die Zwecke des NFR, insbesondere die Zusammenführung von Daten aus unterschiedlichen Quellen zur Auswertung, nicht mehr gefährdet. Das NFR soll im Bayerischen Rettungsdienstgesetz (BayRDG) vorgesehen und reguliert werden. Die oberste Rettungsdienstbehörde (oRDB) ist verantwortliche Betreiberin des NFR. Das Bayerische Staatsministerium des Innern, für Sport und Integration (StMI) ist die oRDB. Die folgende Datenschutz-Folgenabschätzung (DSFA) bezieht sich auf den vorliegenden Entwurf eines Änderungsgesetzes der Bayerischen Staatsregierung.

Vor dem Betrieb des NFR muss der Verantwortliche nach Art. 35 Abs. 1 Datenschutz-Grundverordnung (DSGVO) eine Datenschutz-Folgenabschätzung (DSFA) durchführen. Die DSFA ist eine der zentralen Innovationen der DSGVO und soll den Verantwortlichen zwingen, eine Risikoabschätzung seiner Verarbeitungsvorgänge vorzunehmen und dabei die Perspektive der betroffenen Personen einzunehmen. Im Falle eines voraussichtlich hohen Risikos für die Rechte und Freiheiten natürlicher Personen durch die Verarbeitung muss der Verantwortliche in strukturierter Form die möglichen Folgen der Verarbeitung niederlegen und dabei seine Interessen gegen die der betroffenen Personen abwägen (*Roßnagel/Geminn/Johannes*, ZD 2019, 435). Nach Art. 35 Abs. 1 Satz 1 DSGVO ist eine DSFA durch den Verantwortlichen vorab durchzuführen, wenn eine Form der Verarbeitung, insbesondere unter Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Insbesondere ist nach

Art. 35 Abs. 3 lit. b DSGVO eine DSFA erforderlich, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO erfolgen soll. Dies ist bei Notfalldaten, bei denen es sich in der Regel auch um Gesundheitsdaten handelt, der Fall.

Nach der Positivliste der Konferenz der unabhängigen Datenschutzbehörden in Deutschland (DSK) vom 17.10.2018 fällt das NFR unter die Nr. 3 (umfangreiche Verarbeitung von Daten, die einem Berufsgeheimnis unterliegen). Es wird aber auch von Nr. 10 erfasst (Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Verarbeitung der so zusammengeführten Daten).

Art. 14 BayDSG stellt – im Einklang mit Art. 35 Abs. 10 DSGVO – fest, dass eine DSFA durch den Verantwortlichen unterbleiben kann, wenn eine solche bereits vom zuständigen Staatsministerium oder einem Stellvertreter durchgeführt wurde oder wenn die konkrete Verarbeitung in einer Rechtsvorschrift geregelt ist und im Rechtssetzungsverfahren bereits eine DSFA erfolgt ist. Verantwortliche werden damit trotz grundsätzlicher Pflicht zur Durchführung einer DSFA für einen Verarbeitungsvorgang (Projekt-DSFA) von dieser befreit, wenn die Datenverarbeitung a) auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats gemäß Art. 6 Abs. 1 UAbs. 1 lit. c oder e DSGVO, dem der Verantwortliche unterliegt, beruht, wenn b) diese Rechtsvorschriften den konkreten Verarbeitungsvorgang regeln und c) „bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte“ (Gesetzes-DSFA). Eine Rückausnahme besteht lediglich dann, wenn der Gesetzgeber die Durchführung der DSFA durch den Verantwortlichen explizit vorgesehen hat.

Zum NFR und dem dazugehörigen Gesetzgebungsvorhaben wurde diese DSFA im Auftrag des StMI durchgeführt.

Das DSFA-Team bestand aus:

- Prof. Dr. Alexander Roßnagel, Seniorprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel; wissenschaftlicher Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG),
- Dr. Christian Geminn, Geschäftsführer provet,
- Rechtsanwalt Paul C. Johannes, LL.M., stellvertretender Geschäftsführer provet,
- Dr. Jürgen Weidner, Geschäftsführer accellonet consulting und
- Mike Forner, BOrgTec Technologieunternehmung.

Dieser Bericht fasst die Ergebnisse der DSFA zum NFR zusammen.

2 METHODE UND UMFANG DER PRÜFUNG

2.1 Vorrausetzungen für die DSFA durch den Gesetzgeber

Der Bayerische Landtag darf unter den Voraussetzungen des Art. 35 Abs. 10 DSGVO die DSFA an sich ziehen und dadurch die Verantwortlichen entlasten. Art. 14 BayDSG gilt entsprechend und regelt die Möglichkeit einer Gesetzes-DSFA in gleicher Weise.

Die Ausnahmeregelung des Art. 35 Abs. 10 DSGVO greift für den Verantwortlichen nur dann, wenn die Verarbeitung entweder nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO zur Erfüllung einer rechtlichen Pflicht erforderlich ist, der er unterliegt, oder wenn nach Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt, oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Beide Voraussetzungen sind erfüllt. Für die Verpflichteten begründet das Gesetz eine Pflicht zur Datenübermittlung. Der Aufbau und der Betrieb des NFR erfolgen zur Wahrnehmung der hoheitlichen Aufgabe der Notfallversorgung (siehe Gesetzesbegründung).

Die Gesetzes-DSFA muss nach Art. 35 Abs. 10 DSGVO „im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage“ erfolgen. Sie muss zu Beginn des Gesetzgebungsprozesses vorliegen, im Laufe des Gesetzgebungsprozesses eventuell angepasst und am Ende vom Beschluss über den Gesetzentwurf erfasst werden. Art. 14 BayDSG stellt in unionsrechtskonformer Weise klar, dass sie von dem ressortzuständigen Staatsministerium – in diesem Fall durch das StMI – durchgeführt werden kann.

2.2 Umfang der DSFA durch den Gesetzgeber

Weder der Verordnungswortlaut noch die Erwägungsgründe und die Gesetzgebungshistorie geben Hinweise darauf, ob und wie die vom Gesetzgeber vorzunehmende Gesetzes-DSFA von der vom Verantwortlichen durchzuführende Projekt-DSFA inhaltlich und formell abweicht. Die konkreten Anforderungen an die Gesetzes-DSFA lässt die DSGVO offen (*Martini*, in: Paal/Pauly 2018, Art. 35 Rn. 69). Auch das BayDSG enthält dazu keine Hinweise.

Sinn und Zweck der Ausnahme des Art. 35 Abs. 10 DSGVO liegen darin, unnötige Dopplungen zu vermeiden. Führt der Gesetzgeber zu risikospezifischen Regelungen der Datenverarbeitung bereits eine eigene DSFA durch, so soll der Verarbeiter, der ohnehin nur innerhalb des Gesetzes personenbezogene Daten verarbeiten darf, nicht nochmals eine DSFA durchführen müssen (siehe *Wolff*, in: Schantz/Wolff 2018, E Rn. 876; *Jandt*, in: Kühling/Buchner 2018, Art. 35 Rn. 22). Dies soll den Bürokratieaufwand für die Verantwortlichen reduzieren (*Kramer*, in: Gierschmann u.a. 2018, Art. 35 Rn. 120; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 35 Rn. 58).

Für die Ausgestaltung der Gesetzes-DSFA sind grundsätzlich die gleichen Maßstäbe anzulegen wie für eine Projekt-DSFA durch den Verantwortlichen. Nur indem er sich an diesen Vorgaben zur Durchführung einer DSFA orientiert, kann der Durchführende die mit Art. 35 DSGVO verfolgten Schutzziele erreichen.

Allerdings ist der Unterschied zwischen der gesetzlichen Regelung eines Datenverarbeitungsvorgangs und der konkreten Durchführung eines Datenverarbeitungsvorgangs in der Realität zu berücksichtigen. Auch wenn die gesetzlichen Regelungen Anforderungen an die Gestaltung des Datenverarbeitungsvorgangs enthalten und bestimmte Schutzvorkehrungen vorsehen, bleibt eine entscheidende Differenz in der DSFA dieses Gesetzes

zur DSFA einer realen Datenverarbeitung. Eine Gesetzes-DSFA kann daher nur auf einer abstrakten Ebene die prinzipiellen Risiken erfassen und nur grundsätzlich geeignete Schutzvorkehrungen vorsehen. Sie kann nicht alle Risiken umfassend berücksichtigen, die in den konkreten Verarbeitungsvorgängen im Einzelfall auftreten können (*Baumgartner* in: Ehmann/Selmayr 2018, Art. 35 Rn. 75; *Hansen*, DuD 2016, 587 (589).

Da die Regelung des Art. 35 Abs. 10 DSGVO keine Absenkung des Niveaus der DSFA anstrebt, muss sich nachweislich aus dem Gesetzgebungsverfahren ergeben, dass der Gesetzgeber die potentiellen Risiken für die Grundrechte und Freiheiten der betroffenen Personen erkannt und bewertet hat (*Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 35 Rn. 59) sowie Abhilfemaßnahmen bezogen auf die erkannten Risiken veranlasst hat. Dies ist nur möglich, wenn eine methodisch abgesicherte DSFA auf Basis des Gesetzentwurfs erfolgt ist.

2.3 Methode der DSFA durch den Gesetzgeber

Zum Verfahren und zu den methodischen Schritten einer DSFA enthält die DSGVO keine Regelungen. Auch das BayDSG regelt diese Frage nicht. Gewählt werden muss eine geeignete Methode, die gewährleistet, dass die inhaltlichen Vorgaben des Art. 35 Abs. 7 DSGVO eingehalten und die Ziele der DSFA erreicht werden. Zur Methode haben verschiedene Stellen Empfehlungen abgegeben. Zu nennen sind unter anderem die Leitlinien der Art. 29-Datenschutzgruppe (Leitlinien zur Datenschutz-Folgenabschätzung, WP 248 rev.01), die Kurzpapiere der DSK (Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen) sowie einzelner Aufsichtsbehörden, z.B. der französischen Commission Nationale de l'Informatique et des Libertés (CNIL, Impact Assessment, Methodology, Feb. 2018) und der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) (Datenschutz-Folgenabschätzung – Methodik und Fallstudie, Version 2.0, 2019) sowie die Empfehlungen aus der Forschung, z.B. der BMBF-Initiative „Forum Privatheit" (White Paper Datenschutz-Folgenabschätzung, 3. Aufl. 2017). Grundsätzlich sind all diese Methoden zur Durchführung einer Projekt-DSFA nach Art. 35 DSGVO geeignet. Für die Zwecke einer Gesetzes-DSFA sind all diese Methoden allerdings noch anzupassen.

Für diese Gesetzes-DSFA dienten die methodischen Vorschläge des Forums Privatheit und des BayLfD als Orientierungshilfe. Sie sind am Standarddatenschutzmodell der DSK (Standarddatenschutzmodell, v1.1 vom April 2018) orientiert. Dies äußert sich insbesondere in der Verwendung der dort formulierten sieben Gewährleistungsziele (Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, Intervenierbarkeit und Datenminimierung) sowie in einer Fokussierung auf die Betroffenenperspektive. Auch die im Standarddatenschutzmodell angeführten generischen Maßnahmen zur Umsetzung der Gewährleistungsziele spielen eine wichtige Rolle.

3 RECHTSGRUNDLAGEN

Beim Aufbau und Betrieb des NFR sind die gesetzlichen Vorgaben zum Umgang mit personenbezogenen Daten, insbesondere mit medizinischen Daten und mit Forschungsdaten zu beachten. Hinsichtlich des Rechtsrahmens gilt folgendes:

3.1 Datenschutz-Grundverordnung

Sowohl für die Zulässigkeit als auch für die Art und Weise der Datenverarbeitung sind die Vorgaben der DSGVO zu beachten.

3.1.1 Grundsätze für die Verarbeitung personenbezogener Daten

Art. 5 DSGVO enthält allgemeine Grundsätze für die Verarbeitung personenbezogener Daten (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, sowie Rechenschaftspflicht). Trotz ihres unterschiedlichen Abstraktions- und Regelungsniveaus geben die Grundsätze einen Rahmen für die Gestaltung des NFR vor.

3.1.2 Verarbeitung besonderer Kategorien personenbezogener Daten

Die wichtigsten Datenquellen des NFR sind Daten aus Dokumentationen zur Behandlung von Patienten aus der Rettungskette und der krankenhausärztlichen Behandlung. Dabei handelt sich in der Regel um Gesundheitsdaten mit Personenbezug im Sinne von Art. 9 Abs. 1 DSGVO. Das prinzipielle Verarbeitungsverbot für die in Art. 9 Abs. 1 DSGVO genannten besonderen Kategorien personenbezogener Daten durchbrechen die Ausnahmetatbestände in den Art. 9 Abs. 2 und Abs. 3 DSGVO. Für das NFR sind die in den Art. 9 Abs. 2 lit. i (zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung) und lit. j (im öffentlichen Interesse liegende wissenschaftliche Forschungszwecke) DSGVO vorgesehenen Ausnahmeregelungen einschlägig. Werden besondere Kategorien personenbezogener Daten verarbeitet, so muss sich deren gesetzlich festgelegte, besondere Schutzbedürftigkeit in den durch den Verarbeiter zu treffenden technischen und organisatorischen Sicherungsmaßnahmen widerspiegeln. An diese Maßnahmen sind mithin erhöhte Anforderungen zu stellen.

3.1.3 Datenschutz durch Systemgestaltung und Voreinstellungen

Art. 25 DSGVO fordert Datenschutz durch Systemgestaltung als zentrales Prinzip der Verordnung und als allgemeine Pflicht des Verantwortlichen. Die Vorschrift verpflichtet den Verantwortlichen, technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass die Verordnung eingehalten wird und die Rechte der betroffenen Personen geschützt werden. Hinsichtlich des Zeitpunkts legt die Vorschrift fest, dass diese Maßnahmen schon dann getroffen werden müssen, wenn die Zwecke der Verarbeitung festgelegt werden, aber auch zum Zeitpunkt der Verarbeitung selbst. Klassische Beispiele eines „Datenschutzes durch Systemgestaltung“ umfassen Pseudonymisierungs- und Anonymisierungstechniken. Darüber hinaus kommt der Einsatz von sicheren Verschlüsselungsverfahren in Betracht. Der Verantwortliche soll zum Nachweis dafür, dass er die Verordnung einhält, interne Strategien festlegen, die dem Datenschutz durch Systemgestaltung und durch datenschutzfreundliche Voreinstellungen Genüge tun.

Bei der Auswahl der geeigneten technischen und organisatorischen Maßnahmen (TOM) ist stets der Stand der Technik zu berücksichtigen. Der Stand der Technik meint den

effizientesten und fortschrittlichsten Entwicklungsstand der Technik, der am Markt verfügbar und in dem Verarbeitungsgebiet unter wirtschaftlich und technisch vertretbaren Verhältnissen anwendbar ist. Es ist ein Mehr als der jeweils branchenübliche Standard oder allgemein anerkannte Regeln der Technik zu Grunde zu legen, da von den jeweils verfügbaren Techniken immer die effizientesten und fortschrittlichsten ausgewählt werden müssen (*Husemann*, in: Roßnagel 2018, § 5 Rn. 52).

Im engen Zusammenhang mit Datenschutz durch Systemgestaltung steht der Datenschutz durch datenschutzfreundliche Voreinstellungen. Dadurch sollen standardmäßig Voreinstellungen realisiert werden, nach denen nur die für den jeweiligen Zweck erforderlichen Daten verarbeitet werden. Art. 25 Abs. 2 DSGVO fordert, dass der Verantwortliche hierfür geeignete technische und organisatorische Maßnahmen trifft. Damit ist die Pflicht des Verantwortlichen begründet, das Gebot der Datenminimierung bei jeder Datenverarbeitung umzusetzen. Diese Pflicht gilt bedingungslos. So können weder die Implementierungskosten als begrenzender Faktor herangezogen werden noch ist es erforderlich, die Eintrittswahrscheinlichkeit und die Schwere der mit der Verarbeitung verbundenen Risiken abzuwägen (*Husemann*, in: Roßnagel 2018, § 5 Rn. 54).

3.1.4 Sicherheit der Verarbeitung

Werden personenbezogene Daten verarbeitet, hat der Verantwortliche gemäß Art. 32 Abs. 1 DSGVO die Pflicht, geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese TOM müssen stets ein dem Risiko angemessenes Schutzniveau gewährleisten. Der Verarbeiter hat eine Risikobewertung für den Einzelfall durch zuführen und ein darauf abgestimmtes Schutzkonzept zu entwerfen, das er regelmäßig überprüfen muss (*Husemann*, in: Roßnagel 2018, § 5 Rn. 140). Für die Verarbeitung vieler Gesundheitsdaten ist ein sehr hohes Maß an Datenschutz und Datensicherheit zu gewährleisten.

3.1.5 Rechte der betroffenen Person

Die Rechte einer betroffenen Person sind in Art. 12 bis 22 DSGVO festgeschrieben. Aus ihnen ergeben sich spiegelbildlich Pflichten des Verantwortlichen, die dieser zu beachten und in geeigneten Maßnahmen umzusetzen hat.

Art. 12 DSGVO legt allgemein die Anforderungen an eine transparente Information und Kommunikation gegenüber der betroffenen Person sowie die Modalitäten für die Ausübung ihrer Rechte fest.

Gemäß Art. 13 und 14 DSGVO muss der Verantwortliche die betroffenen Personen – auch ohne ihr Verlangen – über Details der Datenverarbeitung informieren. Die Informationen sind aktiv und ohne Aufforderung zu erteilen.

Nach Art. 15 DSGVO hat die betroffene Person das Recht, vom Verantwortlichen Auskunft darüber zu verlangen, ob er personenbezogene Daten über sie verarbeitet.

Gemäß Art. 16 Satz 1 DSGVO hat sie das Recht, von dem Verantwortlichen unverzüglich die Berichtigung ihrer unrichtigen personenbezogenen Daten zu fordern.

Sie hat das Recht, vom Verantwortlichen die Löschung ihrer personenbezogenen Daten zu verlangen, wenn einer der in Art. 17 Abs. 1 lit. a bis f DSGVO genannten Gründe erfüllt ist. Eine Löschung kann jedoch nach Art. 17 Abs. 3 DSGVO nicht verlangt werden, wenn die Daten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit benötigt werden oder wenn die Löschung voraussichtlich die Verwirklichung der Ziele wissenschaftlicher Forschung unmöglich macht oder ernsthaft beeinträchtigt.

Daneben kann die betroffene Person gemäß Art. 18 Abs. 1 DSGVO unter bestimmten Voraussetzungen die Einschränkung der Verarbeitung verlangen.

Das Recht auf Datenübertragung gemäß Art. 20 Abs. 1 DSGVO kommt für das NFR nicht in Betracht, da dieses nur besteht, wenn die automatisierte Datenverarbeitung auf Grundlage einer Einwilligung oder einer Vertragsbeziehung erfolgt.

Der betroffenen Person steht gemäß Art. 21 Abs. 1 Satz 1 HS 1 DSGVO ein allgemeines Widerspruchsrecht gegen eine rechtmäßige Verarbeitung ihrer personenbezogenen Daten zu. Dies gilt nach HS 2 auch für Profiling. Der Verantwortliche kann die Daten nur dann weiterverarbeiten, wenn er zwingende schutzwürdige Gründe hierfür hat, die gegenüber den Interessen, Freiheiten und Rechten der betroffenen Person überwiegen.

Art. 22 Abs. 1 DSGVO verbietet, eine Person einer allein auf automatisierter Verarbeitung beruhenden Entscheidung zu unterwerfen. Da im Betrieb des NFR keine automatisierte personenbezogene Entscheidung erfolgt, ist dieses Recht nicht relevant.

Die anwendbaren Rechte der betroffenen Person setzen allgemein voraus, dass sowohl die Person als auch ihre Daten identifizierbar sind. Die Regelungen zum NFR zielen jedoch darauf, dass die Meldepflichtigen an das NFR nur pseudonyme Daten übermitteln und dass im NFR nur pseudonyme oder anonyme Daten verarbeitet werden. Sofern das NFR diesen Anforderungen gerecht wird, verfügt es weder über Identitätsdaten noch über Daten, die es ohne weiteres einer natürlichen Person zuordnen kann. In diesem Fall kann es die Rechte der betroffenen Person mangels Identifizierungs- und Zuordnungsmöglichkeit nicht erfüllen.

3.2 Bundesrecht

Das Datenschutzrecht des Bundes wurde als Reaktion auf die DSGVO grundlegend überarbeitet (insbesondere durch das 1. und 2. DSAnpUG-EU).

3.2.1 Telemediengesetz

Datensicherheitsvorschriften finden sich neben Art. 32 DSGVO auch im Telemediengesetz (TMG). So sieht § 13 Abs. 4 TMG vor, dass der Dienstanbieter durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass die in § 13 Abs. 4 Nr. 1 bis 6 TMG genannten Schutzanforderungen verwirklicht werden. Diese Pflichten fallen im öffentlichen Bereich nicht unter Anwendungsvorrang der DSGVO. Hier kommen bezogen auf das NFR allenfalls § 13 Abs. 4 Nr. 2 und 3 TMG in Betracht. Ihre Umsetzung im NFR erfolgt durch Anonymisierung der Falldaten und Verschlüsselung der Übertragungswege.

3.2.2 Strafgesetzbuch

Nach § 203 Abs. 1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer als Arzt unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm anvertraut oder sonst bekannt geworden ist. Die Übermittlung von Notfalldaten über Patienten wäre aufgrund des Arztgeheimnisses unbefugt und damit strafbar, wenn nicht eine gesetzliche Regelung für die Übermittlung der Notfalldaten eine rechtliche Verpflichtung vorsehen würde. Umgekehrt wird mit einer gesetzlichen Verpflichtung die Strafvorschrift des § 203 StGB durch die Übermittlung von Patientendaten an das NFR nicht berührt, da diese nicht unbefugt erfolgt. Damit durch die Übermittlung an das NFR die Geheimnisse nicht gegenüber Unbefugten offenbart werden, sind technische und organisatorische Sicherungsmaßnahmen notwendig.

3.2.3 Sozialdatenschutz

Das NFR erfasst keine Sozialdaten, da keine Leistungsträger Daten für Zwecke der Sozialversicherung verarbeiten. Das System des Sozialdatenschutzes ist daher auf die Datenverarbeitung im Rahmen des NFR nicht anwendbar.

3.3 Landesrecht des Freistaats Bayern

Zwar bestehen in Bayern einige einschlägige Gesetze mit spezifischen Datenschutzregelungen. Diese sind jedoch nicht ausreichend, um den Aufbau und den Betrieb eines NFR rechtlich zu steuern und abzusichern. Soweit das vorliegende Änderungsgesetz spezifische Datenschutzregelungen enthält, gehen diese anderen bayerischen Gesetzen mit Datenschutzregelungen vor. Allerdings gelten die Regelungen des BayDSG ergänzend zu den spezifischen Datenschutzregelungen des Änderungsgesetzes.

3.4 Fazit

Das geplante NFR muss die genannten Regelungen beachten. Die gesetzlich geregelten Schutzvorkehrungen dürfen nicht gegen diese Vorgaben verstoßen und müssen sicherstellen, dass der Schutz personenbezogener Daten ausreichend gewährleistet ist.

4 ZWECKE DER GEPLANTEN VERARBEITUNG

Das NFR ermöglicht, die notfallmedizinische Versorgung in ihren Prozessen, ihrer Qualität und ihrer Wirtschaftlichkeit aus unterschiedlichen Blickwinkeln von Anfang bis zum Ende zu betrachten. Das NFR bindet erstmals alle verfügbaren Quellen in den Gesamtprozess der Notfallversorgung ein und bereitet anonymisierte logistische und medizinische Daten der Notfälle so auf, dass die verfügbaren Informationen die direkte Grundlage für Verbesserungsmaßnahmen bilden können, ohne dabei rechtliche Grenzen, insbesondere des Datenschutzes, zu verletzten.

Die Notfallmedizin hat sich als dritte Säule der Gesundheitsversorgung neben ambulanter und stationärer Versorgung etabliert. Viele der notfallmedizinischen Variablen sind in ihrer Gesamtheit jedoch noch unerforscht. Die Kenntnis dieser Variablen ist unerlässlich, um eine angemessene, zeitgemäße und für die Solidargemeinschaft wirtschaftlich tragbare Versorgung von Notfallpatienten sicherstellen zu können.

Die qualitätsgesicherte Datenbasis des NFR bildet das Fundament für die Versorgungsforschung und das Qualitätsmanagement im bayerischen Rettungsdienst. Die Zusammenführung von Leitstellendaten, Strukturdaten, Einsatzdaten, medizinischen Daten und Falldaten erlaubt Auswertungen gemäß der zu definierenden Qualitätsindikatoren. Aktuelle Leitlinien und Standards können übergreifend auf ihre Umsetzung in der Praxis überprüft werden. Im Rahmen der Versorgungsforschung geht es um die Feststellung neuer, unbekannter Zusammenhänge. Die dabei erzielten Forschungsergebnisse sollen Grundlage für die Verbesserung der Behandlung in der Notfallmedizin sein.

Die Erfassung der Daten soll möglichst so erfolgen, dass bereits etablierte Standards und Verfahren verwendet werden, um den Aufwand für die Erfassung der Daten bei den Datenlieferanten so gering wie möglich zu halten. Für die Daten aus dem klinischen Bereich wird ein neuer, für das NFR spezifischer Variablensatz definiert. Das NFR wird so konzipiert, dass zukünftige Standards für den Austausch medizinischer Daten genutzt und integriert werden können. Das betrifft beispielsweise Formate der elektronischen Fallakte oder der elektronischen Patientenakte.

Daraus entsteht die Herausforderung, dass die Auswertung der Daten mit Fällen umgehen können muss, die unterschiedliche Grade der Vollständigkeit haben.

Nicht benötigte oder nicht gewünschte Daten müssen vor der Übernahme in das NFR aus den Datensätzen entfernt werden. Das betrifft insbesondere Daten mit direktem Personenbezug. Daten, die einen indirekten Personenbezug ermöglichen (z.B. Einsatzdatum und -ort), werden einer Pseudonymisierung unterzogen. Weiterhin müssen Daten aus unterschiedlichen Quellen auf einheitliche Wertebereiche und Codierungsstandards normiert werden. Daher muss das NFR in der Lage sein, eine syntaktische und semantische Prüfung durchzuführen und die Daten seinem internen Modell zuzuordnen. Erst dann können die Daten anonymisiert im NFR gespeichert werden.

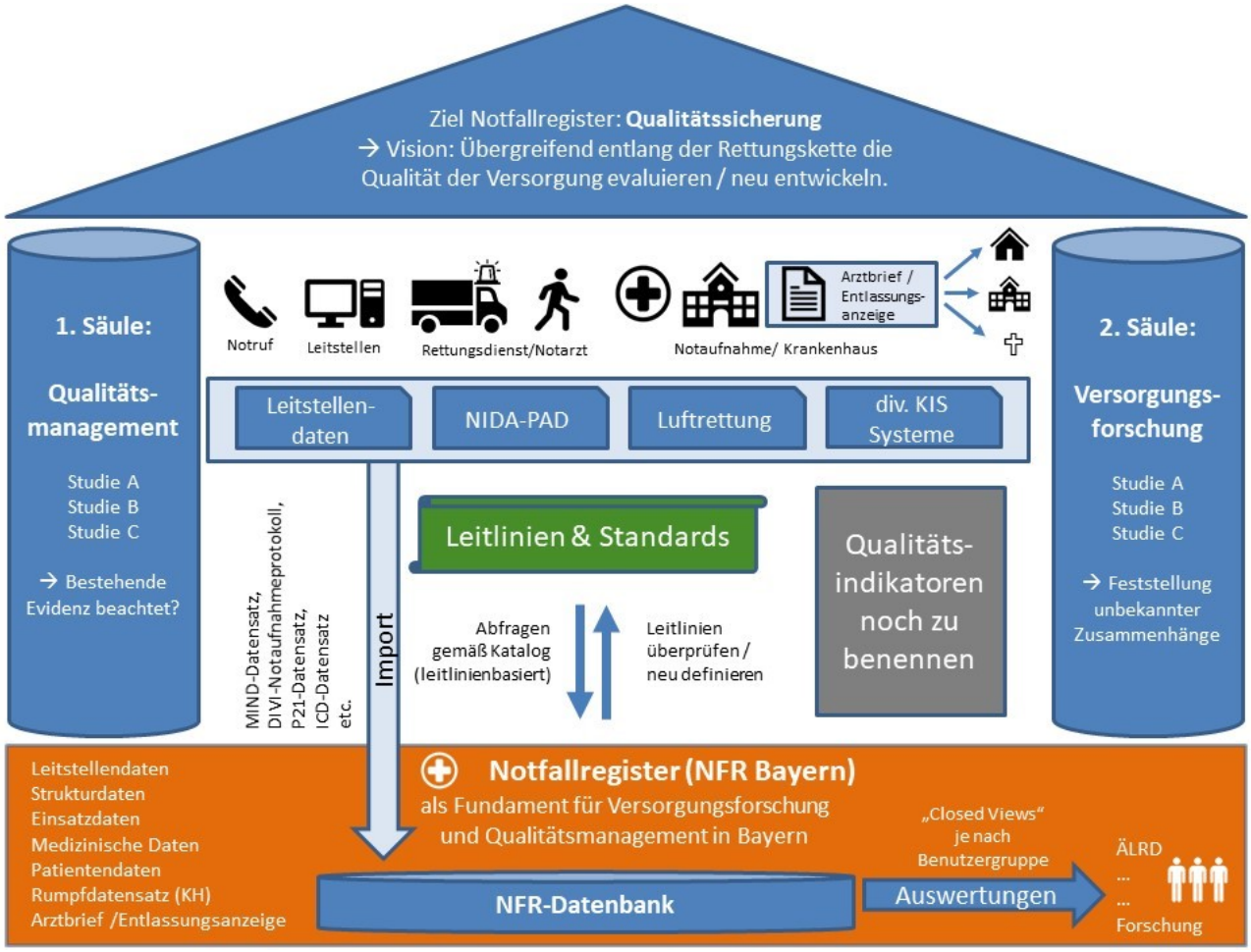

Abbildung 1: Säulenschaubild Notfallregister (NFR)

4.1 Plan zur Zweckerreichung

Kernstück des NFR ist ein qualitätsgesicherter Datenpool, der aus logistischen und medizinischen Daten entlang der Rettungskette besteht, die von Datenlieferanten aus deren Systemen extrahiert, aufbereitet und in einem vereinbarten Format zur Datenannahme im Eingangsbereich des NFR übertragen werden. Dieser Grunddatenbestand wird im NFR nur für die geplante Zeit der Qualitätssicherung vorgehalten. Eine Aggregation erfolgt in dieser Phase noch nicht.

Für die Zusammenführung von Daten aus unterschiedlichen Quellen (Matching bzw. fallweise Konsolidierung) wurde ein Konzept entwickelt, das dafür sorgt, dass die Daten vor der Aufnahme in das NFR pseudonymisiert werden und dass nach Abschluss eines Falls eine vollständige Anonymisierung erfolgt.

Die anonymisierten Basis-Falldaten werden im NFR als Journal in der zeitlichen Abfolge des Entstehens gespeichert. Jedes Ereignis erzeugt einen Datensatz, der Ereignisdetails (logistische Daten wie Zeitstempel, Einsatzmittel etc.) sowie medizinische Daten, die den bekannten Zustand eines Patienten zum Zeitpunkt des Ereignisses abbilden, enthält. Der Patient ist aufgrund der Anonymisierung nicht mehr individualisierbar.

Die dem NFR zugrundeliegenden Basis-Falldaten bilden die Grundlage für statistische Auswertungen. Das betrifft insbesondere die Generierung periodisch erscheinender Reports mit Statistiken, Metriken und Trends.

Im Rahmen der Versorgungsforschung sollen durch die Auswertung des Datenmaterials bisher unbekannte Zusammenhänge festgestellt werden. Die Ergebnisse sind als Handlungsempfehlungen zur Verbesserung der Versorgungsqualität zu formulieren. Daraus können geänderte Vorgaben für die Qualitätssicherung entstehen, die wiederum Einfluss auf die Standardreports haben und deren Wirksamkeit anhand der folgenden Auswertungen überprüft werden sollen.

4.2 Anwendungsszenarien

Für das NFR sind derzeit folgende Anwendungsszenarien absehbar:

Das NFR soll ermöglichen, innerhalb eines Falls Verkettungen, z.B. die Weiterbehandlung in einer anderen Klinik und den Transport dorthin, abzubilden. Dadurch lassen sich Schlüsse auf die Effektivität der notfallmedizinischen Versorgung ziehen.

Dies erfordert eine Gesamtprozessbetrachtung. Das NFR soll eine Datenbasis über die gesamte Rettungskette schaffen, die eine übergreifende Evaluierung der Versorgungsqualität erlaubt und nicht mit dem Ende des Rettungsdiensteinsatzes abbricht.

Mit Hilfe des NFR und der darin vorgenommenen Datenverarbeitung soll sich konkret eine Vielzahl von Fragen zur Qualität der notfallmedizinischen Versorgung beantworten lassen. Dazu zählen zum Beispiel:

- Welche Maßnahmen werden im Krankenhaus nach Einlieferung des Patienten über den Rettungsdienst ergriffen?
- Werden Diagnosen der Präklinik in den Kliniken bestätigt?
- In welche Aufnahme- und Entlassungsdiagnosen münden die Einsatzstichworte und Verdachtsdiagnosen?
- Wurde die Tracerdiagnose in der Klinik bestätigt?
- Wie oft wurde nach Behandlung in der Notaufnahme die Diagnose „Sepsis“ gestellt, obwohl sie präklinisch nicht als solche erkannt wurde?
- Welche Prozesszeiten ergeben sich bei der innerklinischen Versorgung des Herzinfarkts (Aufnahme/Beginn Herzkatheter Untersuchung)?
- Welcher Anteil der vom Rettungsdienst eingelieferten Patienten wurde ambulant oder stationär behandelt?
- Welcher NACA-Score (Einschätzungssystem für die Schwere von Verletzungen, Erkrankungen oder Vergiftungen in der Notfallmedizin) wurde bei ambulant behandelten Patienten vom Rettungsdienst erhoben?
- Wie hoch ist der Anteil der vom Rettungsdienst eingelieferten Patienten, die während des Aufenthalts verstorben sind?

Die angeführten Fragestellungen sind nur einen kleinen Auszug der möglichen Auswertungen, zeigen jedoch die Möglichkeiten, die eine solche Datenbasis für die Verbesserung der klinischen Versorgung und die Verbesserung der Abläufe und Prozesse hat.

5 SYSTEMATISCHE BESCHREIBUNG DER GEPLANTEN VERARBEITUNGSVORGÄNGE

5.1 Verpflichtete

Im NFR sollen Daten aus einer Vielzahl von Quellen zusammengeführt werden, die im Zusammenhang mit der notfallmedizinischen und medizinischen Versorgung stehen und von den Verpflichteten ohnehin erhoben werden. Insbesondere Falldaten inkl. medizinischer Daten sollen dem NFR zur Verfügung gestellt werden durch

- ILS in Bayern,
- Durchführende des Rettungsdienstes in Bayern,
- durch Rechtsverordnung nach Art. 60 Nr. 17 bestimmte Krankenhäuser in Bayern,
- die KVB, soweit sie Aufgaben nach dem BayRDG wahrnimmt, und
- Betreiber der Telenotarztstandorte in Bayern.

Die oRDB setzt die Pflicht zur Bereitstellung der Daten gegenüber den Verpflichteten durch.

5.2 Berechtigte

Zur Auswertung des NFR sind nach Art. 56 Abs. 1 des vorliegenden Änderungsgesetzes berechtigt

- die oRDB zu Zwecken der Steuerung und der Fortentwicklung des Rettungsdienstes,
- die Ärztlichen Leiter Rettungsdienst (ÄLRD) und Ärztlichen Bezirksbeauftragten Rettungsdienst (ÄBRD) sowie der Ärztliche Landesbeauftragte Rettungsdienst (ÄLBRD) zum Zweck des Qualitätsmanagements des Rettungsdienstes,
- die meldepflichtigen Krankenhäuser zum Zweck des eigenen Qualitätsmanagements,
- das Bayerische Landesamt für Statistik zur Erstellung amtlicher Statistiken,
- dritte öffentliche und nicht-öffentliche Stellen auf Antrag zu Zwecken der wissenschaftlichen Forschung in Notfallmedizin und notfallmedizinischer Versorgung.

Über den Antrag entscheidet der Freistaat Bayern durch die oRDB. Es ist Aufsichtsbehörde für das NFR. Die Anforderungen an den Antrag beschreibt der Gesetzentwurf in Art. 56 Abs. 2 Satz 2.

5.3 Verantwortliche und sonstige Beteiligte

Das NFR wird vom Freistaat Bayern geführt und von der oRDB betrieben (Verantwortlicher).

Das IT-Dienstleistungszentrum des Freistaates Bayern (IT-DLZ) soll die technische Bereitstellung (Hosting) des NFR übernehmen.

Den operativen technischen Betrieb des NFR (als Verwaltungshelfer) soll ein wissenschaftlicher Dienst leisten.

Die Aufgaben des wissenschaftlichen Dienstes sind in Art. 54 Abs. 2 beschrieben. Sie beinhalten insbesondere

- den Aufbau, die Weiterentwicklung und die Qualitätssicherung des NFR,
- den Betrieb des NFR, die Beratung und die Unterstützung der Auswertungsberechtigten,
- die Umsetzung der wissenschaftlichen Auswertung des NFR für die Auswertungsberechtigten,
- die Unterstützung in der Umsetzung der Datenschutzmaßnahmen,
- die Unterstützung der Genehmigungsverfahren nach Art. 56 Abs. 2,

Mitumfasst ist der technische Betrieb des Fachverfahrens, einschließlich First- und Second-Level Support für die Anwender.

Der wissenschaftliche Dienst wird mit den hier festgehaltenen Anforderungen ausgeschrieben.

Weitere Beteiligte werden der Lieferant oder die Lieferanten des Systems sein, die Test- und Supportdienstleitungen erfüllen werden.

5.4 Prozessabläufe im NFR

Die verpflichteten ILS, Durchführenden des Rettungsdienstes und Krankenhäuser in Bayern erheben bereits heute die später zu übermittelnden Daten.

Die Durchführenden des Rettungsdienstes verwenden hierfür die NIDApad-Geräte. Die darin eingegebenen Daten werden bisher bereits an das BRK weitergeleitet und dort für die Abrechnung und Auswertung aufbereitet.

Die Notärzte verwenden zukünftig ebenfalls die NIDApad-Geräte zur Erfassung der medizinischen Daten. Die darin eingegebenen Daten werden bisher bereits an die KVB übermittelt. Bei der KVB werden nur die per NIDApad erhobenen Daten aus dem Notarztdienst entgegengenommen, gesammelt und aufbereitet.

Die Verpflichteten speisen die Datensätze über vordefinierte Schnittstellen in das NFR ein. Eine von allen Verpflichteten über alle Stufen der Rettungskette hinweg gemeinsam genutzte Fallnummer als Notfall-Identifikationsdatum (Fall-ID) ermöglicht im NFR die Zusammenführung von zum gleichen Fall gehörenden Daten, die von verschiedenen Verpflichteten übermittelt werden. Vor der Übermittlung pseudonymisieren sie die Daten, indem sie soweit wie möglich Merkmale entfernen, die eine Rückführung auf den jeweiligen Patienten ermöglichen. Sie schützen die Daten auf dem Transportweg durch Verschlüsselung und digitale Signaturen und weitere wirksame Maßnahmen (gegenseitige Authentisierung der Kommunikationsendpunkte, Kanalverschlüsselung mittels TLS, Inhaltsdatenverschlüsselung der Pakete und digitale Signaturen für Integrität und Zurechenbarkeit; ggfs. Zeitstempel zur Beweisbarkeit des Meldezeitpunkts) vor unbefugtem Zugriff oder Datenverlust.

Der wissenschaftliche Dienst als technischer Verwaltungshelfer beim Betrieb des NFR entfernt im Eingangsbereich des NFR in den einzelnen Datensätzen doppelt vorhandene oder nicht benötigte Variablen. Er ersetzt nach Abschluss der Qualitätssicherung die Fall-ID, die die Zusammenführung von zusammengehörigen Daten aus unterschiedlichen Quellen ermöglicht, durch eine neue, zufallsgenerierte Fallnummer (Register-ID), sobald er davon ausgehen kann, dass keine neuen Daten zu diesem Fall mehr eintreffen werden. Eine Ersetzung der Fallnummer soll spätestens dann erfolgen, wenn im Laufe von drei

Monaten keine neuen Daten zum Fall mehr im NFR eintreffen.

Zur Auswertung der im NFR gesammelten Daten berechtigt sind die in Art. 56 Abs. 1 aufgeführten Stellen. Die Bereitstellung von Daten aus dem NFR an dritte öffentliche und nicht-öffentliche Stellen erfolgt auf Antrag durch die oRDB. Hierbei wird es durch den wissenschaftlichen Dienst als seinen Verwaltungshelfer unterstützt. Dieser hat selbst keine Auswertungsberechtigung bezogen auf die im NFR vorgehaltenen Daten. Sollte er in seiner eigenständigen Rolle als wissenschaftliche Einrichtung selbst Daten aus dem NFR für wissenschaftliche Zwecke nutzen wollen, muss er wie jede andere dritte Stelle ihre Auswertung beantragen. Genehmigt die oRDB die Nutzung, generiert der wissenschaftliche Dienst die beantragten Daten. Die oRDB gibt die Auswertungsdaten an den Auswertungsberechtigten frei.

Die ÄLRD, die ÄBRD sowie der ÄLBRD und die oRDB können direkt auf die vom wissenschaftlichen Dienst vorgenommenen Aufbereitungen des Registerbestands zugreifen. Die Bereitstellung der Daten aus dem NFR setzt voraus, dass stets eine Grundgesamtheit von mindestens vier Datensätzen vorliegt. Dies verhindert, dass durch die Eingrenzung von Suchkriterien eine Rückführung der Daten auf einen spezifischen Patienten möglich wird. Auswertungen über eine Datenmenge von weniger als vier Datensätzen werden abgewiesen. Dies ist die Untergrenze für die Anzahl der Datensätze mit der gleichen Wertekombination von Quasi-Identifikatoren zur möglichen Identifizierung von betroffenen Personen. Je höher diese Untergrenze, desto größer sind die Gruppen der gemeinsam betrachteten Personen und umso stärker ist die Anonymisierung. Die meisten Gruppierungsverfahren zur statistischen Anonymisierung gehen von Gruppengrößen von mindestens drei Werten aus (vgl. z.B. *Rothe*, Bayern in Zahlen 2015, 294 (299); *Ronning/Sturm/Höhne u.a.* 2005). Bei nur zwei Merkmalsträgern können die Werte des einen Merkmalsträgers bei Kenntnis der Werte des anderen Merkmalsträgers in jedem Fall enthüllt werden. Bei drei gleichen Datensätzen wird das Risiko der Re-Identifizierung minimiert. Durch die im NFR vorgesehene Untergrenze von vier Datensätzen wird das Identifizierungsrisiko noch effektiver minimiert und die Anonymisierung verbessert.

5.5 Verarbeitungsvorgänge

Es können folgende Verarbeitungsvorgänge unterschieden werden:

Tabelle 1: Verarbeitungsvorgänge

Bezeichnung	Beschreibung	TOM
1. Übermittlungen an das NFR	Von den Meldepflichtigen nach Art. 55 werden Notfalldatensätze im Sinne von Art. 2 Abs. 18 an das NFR übermittelt. Die Daten müssen nach Art. 57 vor der Übermittlung normalisiert und bereinigt werden. Die Übermittlung muss durch eine geeignete Verschlüsselung gesichert werden.	
2. Datenannahme im NFR	Im Eingangsbereich des NFR wird überprüft, ob die übermittelnden Daten von den Meldepflichtigen nach Art. 55 stammen. Das NFR stellt Methoden bereit, um die meldende Stelle sicher zu identifizieren und zu authentifizieren.	
3. Datenbereini-	Der wissenschaftliche Dienst prüft nach Art. 58 Abs. 1 die gemeldeten Notfalldatensätze auf Lesbarkeit, Qualität und Konsistenz	✓

gung bei Eingang in das NFR	und bereinigt und normalisiert sie soweit erforderlich. Es findet eine Inhaltsüberprüfung der Daten statt.	
4. Prüfung der Pseudonymisierung bei Eingang in das NFR und Entfernung potentiell identifizierbarer Merkmale	Der wissenschaftliche Dienst überprüft nach Art. 58 Abs. 1 die Eignung der Pseudonymisierung der gemeldeten Notfalldatensätze mit dem Ziel der Datenminimierung. Er extrahiert aus den übermittelten Daten die relevanten Daten nach definierten Regeln. Nicht relevante Daten werden gelöscht. Er entfernt vor und nach Zusammenführung der Datensätze potentiell identifizierende Merkmale.	✓
5. Zusammenführung der gemeldeten Notfalldatensätze	Der wissenschaftliche Dienst führt nach Art. 58 Abs. 1 Daten zum gleichen Notfall, die unterschiedliche Meldepflichtige übermitteln, im NFR unter der gemeinsamen Fall-ID zusammen. Dabei entfernt er Dopplungen. Er weist die aufzubewahrenden Inhalte Fallakten zu.	
6. Ersetzung der Fall-ID durch eine Register-ID	Nach Abschluss der Zusammenführung ersetzt der wissenschaftliche Dienst nach Art. 58 Abs. 2 Satz 2f. zur Anonymisierung die Fall-ID durch ein neu erzeugtes, nicht rückführbares eindeutiges Datum (Register-ID). Die Fallakten werden damit abgeschlossen. Die Fall-ID wird aus den abgeschlossenen Fallakten gelöscht.	✓
7. Übernahme abgeschlossener Fallakten in den Registerbestand	Die abgeschlossenen und anonymisierten Fallakten werden in den Registerbestand übernommen. Sie stehen im Eingangsbereich des NFR nicht mehr zur Bearbeitung zur Verfügung und werden dort gelöscht.	
8. Auswertung der anonymisierten Daten durch die oRDB	Nach Art. 56 Abs. 1 Nr. 1 ist die oRDB berechtigt, anonymisierte Daten (Art. 56 Abs. 3) zu Zwecken der Steuerung und der Fortentwicklung des Rettungsdienstes auszuwerten. Hierfür kann es über den wissenschaftlichen Dienst auf den anonymisierten Datenbestand zugreifen. Die Auswertung erfolgt über die vom wissenschaftlichen Dienst regelmäßig vorgenommenen Aufbereitungen des Registerbestands. Ein Zugriff auf noch nicht abgeschlossene Fallakten, also noch pseudonym im Eingangsbereich des NFR vorliegende Daten, ist nicht vorgesehen. Auswertungen können sein: • Zur statischen Auswertung logistischer Daten die Selektion einer Anzahl von anonymisierten Fallakten nach z.B. Zeitraum, geografischem Bereich, Einsatzmittel und Auswertung von Alarmierungszeiten, Eintreffzeiten als Mittelwerte oder Trends. • Zur Auswertung bezogen auf medizinische Fragestellungen die Selektion einer Anzahl von anonymisierten Fallakten nach z.B. Zeitraum, geografischem Bereich, Einsatzmittel und Auswertung von Einsatzstichwörtern und folgenden Diagnosen als Behandlungspfad und statistische Auswertung von Abweichungen.	

	• Zur Überwachung von Schwellwerten die automatisierte Überwachung einer Selektion von anonymisierten Fallakten auf Überschreitung eines Schwellwertes, z.B. Überschreitung der Alarmierungszeit in einem Rettungsdienstbereich bei mehr als 10% der Einsätze innerhalb eines Jahres.	
9. Auswertung der anonymisierten Daten durch ÄLRD und ÄBRD und ÄLBRD sowie meldepflichtige Krankenhäuser	Nach Art. 56 Abs. 1 Nr. 2 sind die ÄLRD, die ÄBRD sowie der ÄLBRD berechtigt, anonymisierte Daten (Art. 56 Abs. 3) zum Zweck des Qualitätsmanagements des Rettungsdienstes auszuwerten. Hierfür verfügen sie über einen unmittelbaren Zugang zu den vom wissenschaftlichen Dienst vorgenommenen Aufbereitungen des Registerbestands. Nach Art. 56 Abs. 1 Nr. 3 sind Krankenhäuser, die nach Maßgabe der Verordnung nach Art. 60 Nr. 17 Notfalldaten an das NFR übermitteln, berechtigt, Auswertungen zum Zweck des Qualitätsmanagements vorzunehmen. Auch sie erhalten unmittelbaren Zugang zu den vom wissenschaftlichen Dienst vorgenommenen Aufbereitungen des Registerbestands. Die Auswertungsmöglichkeiten entsprechen denen bei Vorgang 8 genannten.	
10. Auswertung der anonymisierten Daten durch das Bayerische Landesamt für Statistik	Nach Art. 56 Abs. 1 Nr. 4 ist das Bayerische Landesamt für Statistik berechtigt, anonymisierte Daten (Art. 56 Abs. 3) zur Erstellung amtlicher Statistiken vom wissenschaftlichen Dienst auswerten zu lassen, beispielsweise die Erzeugung von KPI nach Metriken gemäß statistischer Vorgaben über den Aktenbestand. Zur statistischen Auswertung logistischer Daten kann die Selektion einer Anzahl von anonymisierten Fallakten nach z.B. Zeitraum, geografischem Bereich, Einsatzmittel und Auswertung von Alarmierungszeiten, Eintreffzeiten als Mittelwerte oder Trends erfolgen.	
11. Auswertung der anonymisierten Daten durch öffentliche und nicht-öffentliche Stellen	Nach Art. 56 Abs. 1 Nr. 5 sind öffentliche und nicht-öffentliche Stellen nach einer Genehmigung (Art. 56 Abs. 2) durch die oRDB berechtigt, anonymisierte Daten (Art. 56 Abs. 3) zur wissenschaftlichen Forschung in Notfallmedizin und notfallmedizinischer Versorgung vom wissenschaftlichen Dienst auswerten zu lassen, beispielsweise die Erzeugung von Auszügen aus Teilmengen des Aktenbestands zur Darstellung in Menschmodellen (Arbeitshypothesen). Die Auswertungsmöglichkeiten entsprechen denen bei Vorgang 8 genannten.	
12. Operativer Betrieb des NFR durch den wissenschaftlichen Dienst	Die Aufgaben des wissenschaftlichen Dienstes sind in Art. 54 Abs. 2 festgelegt. Er führt den operativen Betrieb des NFR und die Verarbeitungsvorgänge 2 bis 11 durch. Zusätzlich übernimmt er technische Kontroll- und Monitoringaufgaben sowie die Auditierung und Fortentwicklung des Gesamtsystems NFR und seiner Teile.	

6 BEWERTUNG DER NOTWENDIGKEIT UND VERHÄLTNISMÄßIGKEIT DER VERARBEITUNGSVORGÄNGE IN BEZUG AUF DEN ZWECK

Das NFR kann auf Grundlage eines Landesgesetzes errichtet und betrieben werden. Die Zulässigkeit der datenschutzrechtlichen Bestimmungen eines solchen Gesetzes bestimmt sich nach Art. 6 Abs. 2 und 3 DSGVO sowie nach Art. 9 Abs. 2 lit. i und j DSGVO in Bezug auf die Verarbeitung von Gesundheitsdaten und anderen Daten besonderer Kategorien.

Der vorliegende Gesetzentwurf genügt hinsichtlich der Bestimmungen zum NFR den Anforderungen nach Art. 6 Abs. 2 und 3 DSGVO. Insbesondere sind sie hinsichtlich der unionsrechtlichen Vorgaben zur Rechtssetzung in den Mitgliedstaaten bestimmt genug.

Auch dient das NFR einem öffentlichen Interesse im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO. Durch das NFR soll die Qualität der notfallmedizinischen Versorgung gesichert und verbessert werden. Nur durch die Erkenntnisse, die das NFR ermöglicht, kann sie auf eine der Aufgabe angemessene, den Herausforderungen zeitgemäße und für die Solidargemeinschaft wirtschaftlich tragbare Grundlage gestellt werden. Da die notfallmedizinische Versorgung als Teil der Daseins- und Grundvorsorge zur Erfüllung staatlicher Pflichten gewährleistet werden muss (vgl. nur Art. 1 BayRDG), ist auch die Forschung zu deren Verbesserung und Anstrengungen zur deren Qualitätssicherung im öffentlichen Interesse. Im NFR werden Daten aus der präklinischen Phase mit Daten aus Krankenhäusern und der KVB zusammengeführt, um die erforderlichen wissenschaftlichen Untersuchungen in Notfallmedizin und notfallmedizinischer Versorgung zu ermöglichen.

Die im Gesetz geregelten Verarbeitungsvorgänge sind bezogen auf den Zweck notwendig. Will man die Wirksamkeit, Effizienz und Sicherheit unterschiedlicher Maßnahmen und Veränderungen entlang der Rettungskette sowie die Auswirkungen der notfallmedizinischen Versorgungsplanung auf den Patienten beurteilen, so erfordert dies eine gesamthafte Betrachtung medizinischer Daten über alle Phasen der Rettungskette hinweg. Zwar erstellen derzeit sowohl die ILS, die Durchführenden des Rettungsdienstes als auch die Krankenhäuser und die KVB jeweils für ihre Zwecke Dokumentationen zu den einzelnen Fällen. Diese Informationen werden aber bisher nicht zusammengeführt und ausgewertet.

Auch die Verarbeitung von Gesundheitsdaten, also von Daten besonderer Kategorien, im NFR ist zulässig, da dies entweder zur Gewährleistung hoher Qualitätsstandards im Sinne von Art. 9 Abs. 2 lit. i DSGVO oder der wissenschaftlichen Forschung im Sinne von Art. 9 Abs. 2 lit. j DSGVO dient.

Die Verarbeitungsvorgänge sind gemessen an den Zwecken auch verhältnismäßig:

Tabelle 2: Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf

den Zweck

Verarbeitungs-vorgang	Verhältnismäßigkeitsprüfung in Bezug auf den Zweck
1. Übermittlungen an das NFR	Die Übermittlung dient der Zusammenführung von Daten zur Auswertung. Sie ist Grundvoraussetzung für die Zielerreichung des NFR. Die Übermittlung greift in die Rechte der betroffenen Personen auf Datenschutz und informationelle Selbstbestimmung ein. Der Eingriff in die Rechte der Einzelnen ist von geringer Intensität. Es werden keine neuen Daten erhoben, sondern lediglich bereits im Kontext der notfallmedizinischen Behandlung und deren Abrechnung anfallende Daten weiterverarbeitet. Es erfolgt zwar eine Zweckänderung. Diese ist jedoch gesetzlich zulässig und zielt auf eine Minimierung der Daten und letztlich auf einen Ausschluss des Personenbezugs im NFR. Der Eingriff wird durch die Pseudonymisierung vor der Übermittlung und die weiteren Verarbeitungsschritte zur Pseudonymisierung und Anonymisierung im NFR abgemildert. Ein Personenbezug ist nach der Übermittlung allenfalls noch für die übermittelnde Institution möglich, die ohnehin bereits über diese Daten verfügt. Für alle anderen Beteiligten fehlt es an einer Zugriffsmöglichkeit. Für das NFR ist ein Personenbezug nach der Übermittlung nicht möglich. Technische und organisatorische Maßnahmen sichern die Übermittlung selbst vor unberechtigtem Zugriff ab. Die Übermittlung ist nur ein notwendiger Zwischenschrift, dessen Eingriffsintensität durch zusätzliche Verarbeitungsvorgänge hin zur wissenschaftlichen und statistischen Auswertbarkeit der aggregierten Daten minimiert wird. Der Verarbeitungsvorgang ist für die Zielsetzung, eine statistisch auswertbare und erforschbare Datenlage zu schaffen, auch geeignet. Er ist auch erforderlich, weil kein eingriffsschwächeres Mittel denkbar ist. Der Verarbeitungsvorgang ist angemessen, weil die Verbesserung und Qualitätskontrolle, der über die Solidargemeinschaft finanzierten und öffentlich organisierten Notfallversorgung auf die Datenzusammenführung angewiesen ist und der Eingriff von geringer Intensität ist.
2. Datenannahme im NFR	Bei der Datenannahme wird überprüft, ob die übermittelnden Daten von den Meldepflichtigen nach Art. 55 stammen. Die dabei verarbeiteten Daten betreffen die verpflichteten Institutionen und haben keinen Personenbezug.
3. Datenbereinigung bei Eingang in das NFR	Die gemeldeten Notfalldatensätze werden auf Lesbarkeit, Qualität und Konsistenz nach Art. 58 Abs. 1 geprüft und soweit erforderlich dahingehend bereinigt und normalisiert. Es findet eine Inhaltsüberprüfung der Daten statt. Bei der Bereinigung wird ein Mapping der gemeldeten Daten auf ein Aktentemplate durchgeführt, d.h. es werden nur passende Informationen, für die es im NFR eine Entsprechung geben darf, aus dem Meldebestand extrahiert. Die Bereinigung ist eine Datenverarbeitung. Sie dient dazu, die übermittelten Daten zusammenführen zu können, indem die Datenqualität überprüft und gewährleistet wird sowie Dopplungen vermieden werden. Sie dient der Zielerreichung des NFR und liegt damit im öffentlichen Interesse.

	Zugleich ist sie im Hinblick auf personenbezogene Daten eine technische und organisatorische Schutzmaßnahme. Sie fördert nämlich die Grundsätze der sachlichen Richtigkeit nach Art. 5 Abs. 1 lit. d DSGVO und der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO. Die Bereinigung kann in die Rechte der betroffenen Personen auf Datenschutz und informationelle Selbstbestimmung eingreifen, weil der zu einer – nur für die übermittelnde Institution – identifizierbaren Person vorliegende Datensatz verändert werden kann. Der Eingriff in die Rechte der Einzelnen ist von äußerst geringer Intensität. Es werden keine neuen Daten erhoben, sondern lediglich bereits im Kontext der notfallmedizinischen Behandlung und deren Abrechnung anfallende Daten weiterverarbeitet. In der Regel wird ein Datensatz durch die Bereinigung sogar in seinem Umfang reduziert, indem vom NFR nicht benötigte Informationen gelöscht werden. Ein Eingriff liegt aber dennoch vor, weil die Bereinigung erst die Weiterverarbeitung im NFR ermöglichen soll. Die Bereinigung ist aber selbst nur ein notwendiger Zwischenschrift, dessen Eingriffsintensität durch zusätzliche Verarbeitungsvorgänge hin zur wissenschaftlichen und statistischen Auswertbarkeit der aggregierten Daten minimiert wird und der in der Regel selbst den Charakter einer Abhilfemaßnahme hat. Der Verarbeitungsvorgang ist für die Zielsetzung, eine statistisch auswertbare und erforschbare Datenlage zu schaffen, auch geeignet. Er ist auch erforderlich, weil kein eingriffsschwächeres Mittel denkbar ist. Der Verarbeitungsvorgang ist angemessen, weil die Verbesserung und Qualitätskontrolle, der über die Solidargemeinschaft finanzierten und öffentlich organisierten Notfallversorgung auf die Datenzusammenführung angewiesen ist und der Eingriff von sehr geringer Intensität ist.
4. Prüfung der Pseudonymisierung bei Eingang in das NFR und Entfernung potentiell identifizierbarer Merkmale	Bei Eingang meldepflichtiger Daten in das NFR findet eine Prüfung der Pseudonymisierung der eingehenden Daten statt. Potentiell identifizierende Merkmale werden entfernt. Dieser Datenverarbeitungsvorgang dient der Sicherstellung, dass keine Fehler bezüglich der Pseudonymisierung seitens einer zur Meldung verpflichteten Stelle vorliegen, sowie der Sicherstellung der Eignung der von der meldepflichtigen Stelle durchgeführten Pseudonymisierung zur Datenminimierung und zur Zielerreichung des NFR. Die Prüfung erfolgt durch den wissenschaftlichen Dienst und getrennt von den sonstigen Aufgaben des wissenschaftlichen Dienstes im Eingangsbereich des NFR. Es handelt sich um eine gesetzlich normierte Abhilfemaßnahme zur Verringerung der Risiken für die Rechte und Freiheiten der betroffenen Personen. Bezüglich eines Eingriffs in die Rechte und Freiheiten natürlicher Personen und dessen Verhältnismäßigkeit wird auf die Ausführungen zur Datenbereinigung verwiesen.
5. Zusammenführung der gemeldeten Notfalldatensätze	Die Zusammenführung ist Grundlage für die mit dem NFR verfolgten Zweck, namentlich dem Qualitätsmanagement, der Verbesserung der notfallmedizinischen Forschung und der wissenschaftlichen Forschung in Notfallmedizin und notfallmedizinischer Versorgung. In der Zusammenführung der gemeldeten Notfalldatensätze im NFR liegt der eigentliche Mehrwert des NFR.

	Der bei Erhebung der Notfalldatensätze bei den meldepflichtigen Stellen erfolgende Eingriff in die Rechte und Freiheiten natürlicher Personen wird durch die Zusammenführung dieser Datensätze im NFR intensiviert; zugleich stellt die Zusammenführung einen neuen Eingriff dar. Die Intensität des Eingriffs wird durch die ergriffenen TOM stark abgemildert, insbesondere durch die Pseudonymisierung der meldepflichtigen Daten sowie durch die personelle, räumliche und organisatorische Trennung des Bereiches des NFR, in dem pseudonyme Daten verarbeitet werden, von dem Bereich, der die anonymisierten Daten auswertet. Die Verarbeitung ist für die Zielsetzung, eine statistisch auswertbare und erforschbare Datenlage zu schaffen, geeignet. Er ist auch erforderlich, weil kein eingriffsschwächeres Mittel denkbar ist. Der Verarbeitungsvorgang ist angemessen, weil die Verbesserung und Qualitätskontrolle, der über die Solidargemeinschaft finanzierten und öffentlich organisierten Notfallversorgung auf die Datenzusammenführung angewiesen ist und der Eingriff bedingt durch die gesetzlich vorgeschriebenen Abhilfemaßnahmen von geringer Intensität ist.
6. Ersetzung der Fall-ID durch eine Register-ID	Die im NFR verarbeiteten pseudonymisierten Daten sind so früh und so weit wie möglich zu anonymisieren. Letzte Möglichkeit der Rückführung eines Notfalldatensatzes auf eine betroffene Person ist nach den dem Eingang der Daten im NFR folgenden Verarbeitungsschritten (Bereinigung, Prüfung, Entfernung potentiell identifizierender Merkmale) die Fall-ID, die in der Rettungskette gebildet wurde. Diese Fall-ID wird deshalb durch eine zufallsgenerierte und damit nicht rückführbare Register-ID ersetzt. Es handelt sich um eine gesetzlich normierte Abhilfemaßnahme zur Verringerung der Risiken für die Rechte und Freiheiten der betroffenen Personen. Diese Ersetzung und die damit erfolgende Anonymisierung stellen keinen Eingriff in Rechte und Freiheiten natürlicher Personen dar.
7. Übernahme abgeschlossener Fallakten in den Registerbestand	Anschließend an die Ersetzung der Fall-ID wird eine durch Zusammenführung der Notfalldatensätze gebildete Fallakte in den Registerbestand überführt. Die Daten verlassen an dieser Stelle den vom eigentlichen Register personell, räumlich und organisatorisch getrennten Eingangsbereich des NFR. Auch hier liegt kein Eingriff in Rechte und Freiheiten natürlicher Personen vor, da es sich um anonymisierte Daten handelt. Durch die gesetzlich normierten Pflichten zur personellen, räumlichen und organisatorischen Trennung der Verarbeitungsvorgänge, wird ein verbleibendes Missbrauchsrisiko in genügender Weise abgemildert
8. Auswertung der anonymisierten Daten durch die oRDB	Die oRDB hat keine direkten Zugriffsrechte auf das NFR. Es kann nur eine Auswertung durch den wissenschaftlichen Dienst anstoßen. Ein Eingriff in Rechte und Freiheiten natürlicher Personen liegt nicht vor, da es anonyme Daten sind. Der Zugriff auf die Systeme des NFR ist gesichert durch eine Identifizierung und Authentifizierung des Nutzers. Diesem ist systemintern eine Rolle zugewiesen, die seine Rechte zur Auswertung und zur Datenselektion begrenzt. Die oRDB erhält nur auf Anfrage beim wissenschaftlichen

	Dienst Auswertungen aus dem Registerbestand. Trotz dieser organisatorischen Regelung bleibt die oRDB datenschutzrechtlich Verantwortlicher für das NFR, da sie gegenüber dem wissenschaftlichen Dienst als ihrem Verwaltungshelfer weisungsbefugt bleibt. Es besteht denklogisch auch die Gefahr eines „schleichenden Personenbezugs". Die auswertende Stelle könnte über Zusatzwissen oder Informationen verfügen, die es ihr ermöglichen, den Personenbezug aller oder auch nur einzelner Datensätze, die Teil der Auswertung sind, wiederherzustellen (Re-Identifikation). So hat die oRDB als verantwortliche Stelle wenigstens faktischen Zugriff auf weitere Register (z.B. zentrales elektronisches Personenstandsregister) und Datenbanken (z.B. Tagespresse). Diesen Risiken wird durch eine Reihe von TOM begegnet. Dies ist zum einen das Gebot nach Art. 56 Abs. 3, dass Auswertungen nur auf anonymisierte Daten erfolgen dürfen. Es werden nur Datenextrakte aus dem NFR gebildet und keine Fallakten ausgegeben. Zum anderen sind es die besonderen Maßnahmen nach Art. 58 Abs. 1 bis 4, die auch eine Re-Identifizierung erschweren. Schließlich verbietet Art. 58 Abs. 5 die Re-Identifizierung gesetzlich. Das Risiko einer Re-Identifizierung wird durch diese Maßnahmen stark abgesenkt. Insbesondere die gesetzlichen Verbote adressieren die Risiken, die daraus resultieren, dass sich NFR im faktischen Herrschafts- und Aufgabenbereich der oRDB befindet. Sie ist der datenschutzrechtlich Verantwortliche. Eine Individualisierung der Ergebnisse im Sinne des Re-Identifizierungsverbot nach Art. 58 Abs. 5 wird dadurch ausgeschlossen, dass Auswertungen nur möglich sind, wenn das jeweilige Ergebnis mehr als drei Fälle (s. o. S.18) betrifft.
9. Auswertung der anonymisierten Daten durch ÄLRD und ÄBRD und ÄLBRD sowie meldepflichtige Krankenhäuser	Bezüglich eines Eingriffs in die Rechte und Freiheiten natürlicher Personen wird auf die Ausführungen zur Nutzung der anonymisierten Daten durch die oRDB verwiesen. Der Zugriff auf die Systeme des NFR erfolgt durch eine vom Betreiber bereitzustellende Schnittstelle. Die Vergabe von Zugriffsrechten in den Krankenhäusern erfolgt durch diese selbst. Näheres regelt die Rechtsverordnung nach Art. 60 Nr. 18. Re-Identifizierungsmöglichkeiten bestehen für ÄLRD und ÄBRD und ÄLBRD insbesondere hinsichtlich von Fällen in ihrem Arbeits- und Wirkungskreis. Dort haben diese Personen i.d.R. Zugriff auf die Daten der meldenden Stellen, für die sie arbeiten oder mit denen sie zusammenarbeiten. Die meldepflichtigen Krankenhäuser können eine Re-Identifizierung hinsichtlich und mittels ihrer eigenen Datenbestände vornehmen. Das Risiko der Re-Identifizierung wird aber in ausreichender Weise durch eine Reihe von TOM begrenzt. Dies ist zum einen das Gebot nach Art. 56 Abs. 3, dass Auswertungen nur auf anonymisierte Daten erfolgen dürfen. Es werden nur Datenextrakte aus dem NFR gebildet und keine Fallakten ausgegeben. Zum anderen sind es die besonderen Maßnahmen nach Art. 58 Abs. 1 bis 4, die auch eine Re-Identifizierung erschweren. Schließlich verbietet Art. 58 Abs. 5 die Re-Identifizierung gesetzlich. Eine Individualisierung der Ergebnisse im Sinne des Re-Identifizierungsverbots nach Art. 58 Abs. 5 wird dadurch ausgeschlossen, dass Auswertungen nur möglich sind, wenn das jeweilige Ergebnis mehr als drei Fälle betrifft. Auswertungen über eine Datenmenge von weniger als vier gleichen Datensätzen werden abgewiesen.

	Der Zugriff auf die Systeme ist gesichert durch eine Identifizierung und Authentifizierung des Nutzers. Diesem ist systemintern eine Rolle zugewiesen, die seine Rechte zur Auswertung und zur Datenselektion begrenzt. Diese Begrenzung kann sich beispielsweise auf die Selektion von Daten nur aus dem Rettungsdienstbereich des ÄLRD beziehen. Technisch werden nie Ansichten auf Rohdaten im NFR an Benutzer zur Verfügung gestellt. Vielmehr werden immer systeminterne Prozesse „beauftragt", die Daten aus Abfragen über dem Datenbestand automatisiert (auch ad hoc) zusammenzutragen und dann geeignet darzustellen. Diese Prozesse werden streng durch die Geschäftsregeln gesteuert, die z.B. unter anderem festlegen, dass bei Treffermengen kleiner einer Schwelle keine Daten angezeigt werden. Diese Prozesse laufen immer in einem sicheren Systemkontext und nie im Kontext des Nutzers, verwenden aber die Restriktionen des Nutzerkontextes bei der Abfrage.
10. Auswertung der anonymisierten Daten durch das Bayerische Landesamt für Statistik	Das Bayerische Landesamt für Statistik hat kein Zugriffsrecht auf das NFR. Es kann nur eine Auswertung durch den wissenschaftlichen Dienst anstoßen. Durch die Auswertung anonymer Daten kann kein Eingriff in die Rechte einer natürlichen Person entstehen. Eine Individualisierung der Ergebnisse im Sinne des Re-Identifizierungsverbots nach Art. 58 Abs. 5 wird dadurch ausgeschlossen, dass Auswertungen nur möglich sind, wenn das jeweilige Ergebnis mehr als drei Fälle (s. o. S. 18) betrifft. Auswertungen über eine Datenmenge von weniger als vier gleichen Datensätzen werden abgewiesen.
11. Auswertung der anonymisierten Daten durch öffentliche und nichtöffentliche Stellen	Die Forschungsstellen haben kein Zugriffsrecht auf das NFR. Sie können nur eine Auswertung durch den wissenschaftlichen Dienst anstoßen Durch die Auswertung anonymer Daten kann kein Eingriff in die Rechte einer natürlichen Person entstehen. Das theoretisch bestehende Risiko der Re-Identifizierung wird in ausreichender Weise durch eine Reihe von TOM begrenzt. Dies ist zum einen das Gebot nach Art. 56 Abs. 3, dass Auswertungen nur auf anonymisierte Daten erfolgen dürfen. Es werden nur Datenextrakte aus dem NFR gebildet und keine Fallakten ausgegeben. Zum anderen sind es die besonderen Maßnahmen nach Art. 58 Abs. 1 bis 4, die auch eine Re-Identifizierung erschweren. Eine Individualisierung der Ergebnisse wird dadurch ausgeschlossen, dass Auswertungen nur möglich sind, wenn das jeweilige Ergebnis mehr als drei Fälle (s. o. S. 18) betrifft. Auswertungen über eine Datenmenge von weniger als vier gleichen Datensätzen werden abgewiesen. Zudem werden nur Datenextrakte aus dem NFR gebildet (Teildatensätze, Menschmodell-abhängig) und nicht Original-Akten ausgegeben. Schließlich verbietet Art. 58 Abs. 5 die Re-Identifizierung gesetzlich.
12. Operativer Betrieb des NFR durch den wissenschaftlichen Dienst	Der wissenschaftliche Dienst führt als Admin/Operator des NFR die Administration des Gesamtsystems sowie die Verarbeitungsvorgänge 2 bis 11 und die Auditierung und Fortentwicklung des NFR durch. Diese Verarbeitungsvorgänge sind Grundvoraussetzung für den Betrieb des NFR und dessen Zweckverfolgung. Alle diese Aufgaben werden mit für den wissenschaftlichen Dienst anonymen Daten erreicht. Bereits die an das NFR übermittelten Daten sind für den wissenschaftlichen Dienst selbst anonym,

	da er nicht über das notwendige Wissen verfügt einzelne Personen zu identifizieren und z.B. Pseudonyme, wie die Fall-ID, aufzulösen. Die Administration stellt allenfalls potentiell einen Eingriff in die Rechte betroffener Personen dar, da nur die theoretische Möglichkeit einer Re-Identifizierung besteht. Das Risiko der Re-Identifizierung wird aber in ausreichender Weise durch eine Reihe von TOM begrenzt. Dies ist zum einen das Gebot nach Art. 56 Abs. 3, dass Auswertungen nur auf anonymisierte Daten erfolgen dürfen. Es werden nur Datenextrakte aus dem NFR gebildet und keine Fallakten ausgegeben. Zum anderen sind es die besonderen Maßnahmen nach Art. 58 Abs. 1 bis 4, die auch eine Re-Identifizierung erschweren. Schließlich verbietet Art. 58 Abs. 5 die Re-Identifizierung gesetzlich.

7 BEWERTUNG DER GEFÄHRDUNGEN FÜR DIE RECHTE UND FREIHEITEN DER BETROFFENEN PERSONEN

7.1 Identifikation von Bewertungsmaßstäben anhand der Schutzziele

Die Anforderungen des Datenschutzrechts an das NFR (s. Kap. 3) lassen sich operativ mit Hilfe von Gewährleistungszielen umsetzen, die in kompakter und methodisch zugänglicher Form die Risiken für den Datenschutz (Gefährdungen) explizit machen, vor denen es durch eine angemessene Systemgestaltung und Verfahrensmaßnahmen zu schützen gilt. Diese sind in das Standard-Datenschutzmodell (SDM) eingebettet, dessen Version 2.0 die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) am 5. bis 7. November 2020 angenommen. Das SDM wurde von der Artikel-29-Datenschutzgruppe als ein Framework für die Durchführung einer DSFA empfohlen.

Das SDM verlangt die Sicherung der Datenverarbeitungsvorgänge in Bezug auf Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit.

Dass diese Gewährleistungsziele als verdichtete normative und operativ zugängliche Anforderungen nutzbar sind, wird im SDM-Handbuch durch die Zuordnung der Datenverarbeitungsgrundsätze nach Art. 5 DSGVO (s. SDM V2.0, S. 24 ff.) und der spezifischeren rechtlichen Vorgaben der DSGVO zu Gewährleistungszielen (s. SDM V2.0, S. 28) belegt. Nach dem SDM ist zu beachten, dass die Bewertungsmaßstäbe sich nicht nur auf den Datenbestand beschränken, sondern das Verfahren insgesamt und somit neben den Daten auch die Datenverarbeitungs-Systeme und -Prozesse betreffen.

7.2 Risikoquellen

Als Risiko für die Freiheiten und Rechte natürlicher Personen müssen alle Organisationen, wie zum Beispiel Behörden und Unternehmen, betrachtet werden, die Daten erfassen, verarbeiten und weitergeben, sowie solche Organisationen, die sich Zugriff zu Daten verschaffen können. Dabei geht es vor allem um Gefährdungen, die aus der illegitimen Überdehnung des Zwecks durch den Verantwortlichen selbst entstehen, aber auch um, die aus dem potentiellen Interesse anderer Institutionen an den schon bei einem Verantwortlichen vorliegenden Datenbestand resultieren.

Zu betrachten sind sowohl externe als auch interne Beteiligte sowie Dritte. In der folgenden Tabelle sind die Beteiligten aufgeführt.

Tabelle 3: Beteiligte und Dritte

Beteiligte		**Dritte**
externe Beteiligte	interne Beteiligte	externe Angreifer
ILS in Bayern	oRDB	
Durchführende des Rettungsdienstes in Bayern	IT-DLZ	
Notärzte in Bayern	wissenschaftlicher Dienst beim operativen Betrieb des NFR	

Bayerisches Rote Kreuz (BRK)	wissenschaftlicher Dienst bei der Datenprüfung im Eingangsbereich des NFR	
KVB		
Krankenhäuser in Bayern		
Hersteller der Systeme		
ÄLRD und ÄBRD sowie der ÄLBRD		
Dritte öffentliche und nicht-öffentliche Stellen		
Bayerisches Landesamt für Statistik		

7.3 Ermittlung des Schutzbedarfs anhand der Eingriffsintensität

Zur Bestimmung des Schutzbedarfs anhand der Eingriffsintensität sei Folgendes vorausgeschickt:

Jede – auch eine völlig rechtskonforme – Datenverarbeitung personenbezogener Daten ist ein Eingriff in die Grundrechte und Freiheiten der betroffenen Personen. Allein daraus folgt bereits ein „normaler" Schutzbedarf.

Aufgrund spezifischer Arten der Datenverarbeitung und Verarbeitung von besonderen Kategorien von Daten kann sodann eine höhere Eingriffsintensität und damit die Annahme eines „hohen" oder sogar „sehr hohen" Schutzbedarfs folgen.

Die Schutzbedarfsabstufungen sind:

- Normal: Es werden personenbezogene Daten verarbeitet, ohne dass Verarbeitungsszenarien mit potentiell erhöhter Eingriffsintensität gegeben sind.
- Hoch:
    - Es werden personenbezogene Daten verarbeitet, die „besonderen Kategorien personenbezogener Daten" zuzuordnen sind und als solche einen hohen Schutzbedarf aufweisen und nach gesetzlichen Festlegungen Elemente eines Prozesses zur DSFA sind, oder
    - die Betroffenen sind von den Entscheidungen oder Leistungen der Organisation abhängig, oder
    - aus einem „Kumulierungseffekt" ergibt sich ein hoher Schutzbedarf auch bei Datenverarbeitungen mit – einzeln betrachtet – nur normalem Schutzbedarf. Dies kann der Fall sein, wenn Daten von sehr vielen Personen erhoben werden („Kumulierung vieler Daten") oder aber wenn Daten durch einzelne Personen (z.B. Administratoren) zu verschiedenen Zwecken erhoben werden, wobei sich die betroffenen Personen jeweils in verschiedenen Rollen befinden („Kumulierung vieler Berechtigungen").
- Sehr hoch: Es werden personenbezogene Daten mit hohem Schutzbedarf verar-

beitet und zusätzlich sind die Betroffenen von den Entscheidungen oder Leistungen der Organisation unmittelbar existenziell abhängig und es bestehen zusätzliche Risiken durch unzureichende Informationssicherheit oder unzulässige Zweckänderung seitens der Organisation, ohne dass die Betroffenen solche direkt bemerken oder korrigieren können.

Bedrohungen oder Gefährdungen für Gewährleistungsziele können ausgehen von internen Beteiligten, externen Beteiligten oder Dritten. Sie werden im Folgenden für die jeweiligen Arbeitsschritte im NFR betrachtet und bewertet.

Tabelle 4: Schutzbedarf in Abhängigkeit zu Gewährleistungszielen und Bedrohung

Überblick Schutzbedarf in Abhängigkeit zu Gewährleistungszielen und Bedrohung	
1. Übermittlungen an das NFR	
Bedrohung:	Das Gewährleistungsziel **Datenminimierung** wird bedroht durch die Übermittlung von Daten durch die zur Meldung verpflichteten externen Beteiligten, die über den gesetzlich zulässigen Rahmen hinausgehen. Auch die Veränderungen von Inhalten auf dem Übertragungsweg, die sich auf die Zuordnung und Auswertung wesentlich auswirken (Einfügung von fiktiven oder realen, aber unzulässigen Sachverhalten/Unterdrückung von Sachverhalten) durch interne und externe Beteiligte oder Dritte ist eine Bedrohung für die Datenminimierung. Das Gewährleistungsziel **Verfügbarkeit** ist gefährdet, wenn die Datenannahme im Eingangsbereich des NFR nicht verfügbar ist, wenn eine Übertragung durchgeführt werden soll. Die Nichtverfügbarkeit kann zur Überschreitung von Fristen führen, die wiederum zu unvollständigen Fallakten führen können. Die Veränderung von Inhalten auf dem Übertragungsweg, die sich auf die Zuordnung und Auswertung wesentlich auswirken (Verfälschung oder Vertauschung von Werten, Einfügung von fiktiven Sachverhalten/Unterdrückung von Sachverhalten) durch Beteiligte oder Dritte gefährdet das Gewährleistungsziel **Integrität.** Das Gewährleistungsziel **Vertraulichkeit** wird gefährdet durch die Übermittlung der Daten durch externe Beteiligte an unberechtigte Stellen. Es wird auch gefährdet durch das Mitlesen der Datenübertragung durch unberechtigte Beteiligte und Dritte. Das Ziel der **Transparenz** ist bedroht, wenn die betroffenen Personen keine Information oder Auskunft von meldenden externen Beteiligten darüber erhalten, welche ihrer Daten an das NFR übertragen werden. Die **Nichtverkettung** als Gewährleistungsziel ist dadurch bedroht, dass die meldenden externen Datenlieferanten aus ihnen bekannten weiteren Merkmalen einen Personenbezug aus den Daten herstellen können. Das Gewährleistungsziel der **Intervenierbarkeit** ist bedroht durch die Schwierigkeit des Rückrufs einer Meldung oder der Korrektur einer erkannten Falschmeldung.
Eingriffsintensität:	Die Übermittlung des Notfalldatensatzes beinhaltet Daten besonderer Kategorien. Der Eingriff wird durch die Pseudonymisierung vor der Übermittlung und die weiteren Verarbeitungsschritte zur Pseudonymisierung und Anonymisierung im NFR

	abgemildert. Eine Personenbeziehbarkeit ist nach der Übermittlung allenfalls noch für die übermittelnde Institution möglich, die ohnehin bereits über diese Daten verfügt. Für das NFR ist ein Personenbezug nach der Übermittlung nicht möglich, es sei denn weitere Informationen oder Zusatzwissen sind nutzbar. Die Übermittlung ist nur ein notwendiger Zwischenschritt, dessen Eingriffsintensität durch zusätzliche Verarbeitungsvorgänge hin zur wissenschaftlichen und statistischen Auswertbarkeit der aggregierten Daten minimiert wird. Die Übermittlung des Notfalldatensatzes beinhaltet jedoch Daten besonderer Kategorien und eine Identifizierung bleibt über die Fall-ID möglich, weswegen ein erhöhter Schutzbedarf besteht.
Schutzbedarf:	Hoch hinsichtlich aller Gewährleistungsziele

2. Datenannahme im NFR

Bedrohung:	Das Gewährleistungsziel **Datenminimierung** wird bedroht durch die Annahme von Daten durch das NFR und den wissenschaftlichen Dienst zu einem Fall, die über den gesetzlich zulässigen Rahmen hinausgehen. **Verfügbarkeit** als Gewährleistungsziel wird gefährdet, solange die Verarbeitung nicht abgeschlossen wurde und möglicherweise schutzwürdige Inhalte unnötig lange in der Datenannahme verbleiben. Dies kann aus einer nicht fristgerechten Verarbeitung durch den wissenschaftlichen Dienst erfolgen. Der fehlerhafte Empfang kann zur Verfälschung der Sachverhalte führen und damit die Falldaten unbrauchbar machen und die Statistik verfälschen (Systematische Entstehung extremer Sonderfälle). Dies und die fehlerhafte Zuordnung von Falldaten und infolge dessen falsche Aggregation der Daten sind Bedrohungen für das Ziel der **Integrität**. Die **Vertraulichkeit** wird gefährdet durch den unberechtigt erlangen Zugang zu den unverarbeiteten Meldedaten durch interne Beteiligte und Dritte. Das Ziel der **Transparenz** ist bedroht, wenn die betroffenen Personen keine Information oder Auskunft von meldenden externen Beteiligten darüber erhalten, welche ihrer Daten an das NFR übertragen werden. Da die Daten für die internen Beteiligten anonym sind, treffen diese keine Informationspflichten. Auskunftspflichten treffen sie nur insoweit, als ein Auskunftsersuchen die Fall-ID oder identifizierende Merkmale beinhaltet. Dabei wäre die Erzeugung nicht nachvollziehbarer Metadaten eine Bedrohung für die Transparenz. Das Gewährleistungsziel der **Nichtverkettung** ist dadurch bedroht, dass im Eingangsbereich des NFR zur Datenannahme durch den wissenschaftlichen Dienst aus bekannten weiteren Merkmalen ein Personenbezug aus den Daten hergestellt wird. Das Herstellen von Zusammenhängen zwischen Fällen erhöht dieses Risiko. Eine Bedrohung der **Intervenierbarkeit** läge darin, dass keine ausreichende Transaktionssteuerung zum Abbruch von als fehlerhaft erkannten Verarbeitungsvorgängen verfügbar ist.
Eingriffsintensität:	Bei der Datenannahme wird überprüft, ob die übermittelnden Daten von den Meldepflichtigen nach Art. 55 stammen. Die dabei verarbeiteten Daten betreffen die

	verpflichteten Institutionen und haben keinen Personenbezug. Die Daten zur Datenannahme im Eingangsbereich des NFR können durch die externen Beteiligten über die Fall-ID einer natürlichen Person zugeordnet werden. Dabei handelt es sich auch um Daten besonderer Kategorien (Gesundheitsdaten), weswegen ein erhöhter Schutzbedarf besteht.
Schutzbedarf:	Hoch hinsichtlich aller Gewährleistungsziele

3. Datenbereinigung bei Eingang in das NFR

Bedrohung:	Das Gewährleistungsziel der **Datenminimierung** wird bedroht, wenn Daten, die gemeldet wurden, aber nicht für den Registerzweck erforderlich sind, nicht gelöscht werden. Gefährdend ist auch, wenn nicht benötigte Daten länger als erforderlich vorgehalten werden. Eine fehlerhafte Verarbeitung kann systematisch zu fehlerhaften Aussagen über den Bestand führen. Fehlerhafte Verarbeitung kann systematisch zu fehlerhaften Aussagen über den Bestand führen. Die **Integrität** des gesamten informationstechnischen Prozesses ist gefährdet, wenn die Funktion der Datenbereinigung nicht durchgeführt werden kann. Das Gewährleistungsziel der **Vertraulichkeit** ist durch die unberechtigte Kenntnisnahme der zu entfernenden Daten durch Beteiligte und Dritte bedroht. Insbesondere Mitarbeiter des wissenschaftlichen Dienstes, die dem Trennungsgebot nach nicht mit diesem Verarbeitungsvorgang betraut sind, sollen keine Einsicht nehmen dürfen. Das Gewährleistungsziel der **Nichtverkettung** ist dadurch bedroht, dass im Eingangsbereich des NFR zur Datenannahme durch den wissenschaftlichen Dienst aus bekannten weiteren Merkmalen ein Personenbezug aus den Daten hergestellt wird. Das Herstellen von Zusammenhängen zwischen Fällen erhöht dieses Risiko. Eine Bedrohung der **Intervenierbarkeit** läge darin, dass keine ausreichende Transaktionssteuerung zum Abbruch von als fehlerhaft erkannten Verarbeitungsvorgängen verfügbar ist.
Eingriffsintensität:	Die Bereinigung ist eine Datenverarbeitung und dient der Zielerreichung des NFR. Zugleich ist sie im Hinblick auf personenbezogene Daten eine technische und organisatorische Schutzmaßnahme. Die Bereinigung kann aber in die Rechte der betroffenen Personen eingreifen, weil der zu einer – nur für die übermittelnde Institution – identifizierbaren Person vorliegende Datensatz verändert werden kann. Der Eingriff in die Rechte der Einzelnen ist von äußerst geringer Intensität. Es werden keine neuen Daten erhoben, sondern lediglich bereits im Kontext der notfallmedizinischen Behandlung und deren Abrechnung anfallende Daten weiterverarbeitet. In der Regel wird ein Datensatz durch die Bereinigung sogar in seinem Umfang reduziert, indem vom NFR nicht benötigte Informationen gelöscht werden. Ein Eingriff liegt aber dennoch vor, weil die Bereinigung erst die Weiterverarbeitung im NFR ermöglichen soll. Die Bereinigung ist ein notwendiger Zwischenschrift der Gesamtverarbeitung. Im Datensatz bleiben potentiell Daten besonderer Kategorien.

Schutzbedarf:	Hoch hinsichtlich der Ziele Datenminimierung und Integrität. Normal hinsichtlich anderer Ziele.

4. Prüfung der Pseudonymisierung bei Eingang in das NFR und Entfernung potentiell identifizierbarer Merkmale

Bedrohung:	Eine Bedrohung für das Gewährleistungsziel der **Datenminimierung** ist, dass Daten, die nicht den Pseudonymisierungsregeln entsprechen, vom wissenschaftlichen Dienst in das NFR übernommen werden. Auch die unbemerkte Übernahme von identifizierenden Daten durch ungenaue Prüfung der Typen (z.B. Adresse in Kommentarfeldern) ist eine Bedrohung. Fehlerhafte Pseudonymisierung kann zu verfälschten Daten und fehlerhaften Auswertungen führen. Die **Integrität** des gesamten informationstechnischen Prozesses ist gefährdet, wenn die Funktion der Datenbereinigung nicht durchgeführt werden kann. Im Eingangsbereich könnten einzelne Datensätze verfälscht werden. Das Ziel der **Transparenz** ist bedroht, wenn die betroffenen Personen keine Information oder Auskunft von meldenden externen Beteiligten darüber erhalten, welche ihrer Daten an das NFR übertragen werden. Da die Daten für die internen Beteiligten anonym sind, treffen diese keine Informationspflichten. Auskunftspflichten treffen sie nur insoweit, als ein Auskunftsersuchen die Fall-ID oder weitere identifizierende Merkmale beinhaltet. Dabei wäre die Erzeugung nicht nachvollziehbarer Metadaten eine Bedrohung für die Transparenz. Eine Bedrohung wäre aber, wenn nicht erkennbar wäre, welche potentiell identifizierenden Merkmale vor Übernahme in den Registerbestand entfernt werden. Aus nicht ausreichend pseudonymisierten oder zu entfernenden potentiell identifizierenden Daten kann durch den wissenschaftlichen Dienst ein Personenbezug hergestellt werden. Das bedroht das Ziel der **Nichtverkettung**.
Eingriffsintensität:	Dieser Datenverarbeitungsvorgang dient der Sicherstellung, dass keine Fehler in der Pseudonymisierung durch eine zur Meldung verpflichteten Stelle vorliegen. Er soll auch die Eignung der von der meldepflichtigen Stelle durchgeführten Pseudonymisierung zur Datenminimierung und zur Zielerreichung des NFR sicherstellen. Es handelt sich um eine gesetzlich normierte Abhilfemaßnahme zur Verringerung der Risiken für die Rechte und Freiheiten der betroffenen Personen. Ein Eingriff liegt aber dennoch vor, weil die Bereinigung erst die Weiterverarbeitung im NFR ermöglichen soll. Die Bereinigung ist ein notwendiger Zwischenschritt der Gesamtverarbeitung.
Schutzbedarf:	Hoch hinsichtlich Integrität Normal hinsichtlich anderer Ziele.

5. Zusammenführung der gemeldeten Notfalldatensätze

Bedrohung:	Eine Bedrohung für das Gewährleistungsziel der **Datenminimierung** ist, dass beim Zusammenführen der Datensätze durch den wissenschaftlichen Dienst Korrelationen durchgeführt werden, die zu zusätzlichen Daten führen. Gleiches gilt für die fehlerhafte Zuordnung infolge unvollständiger, defekter oder sachlich falscher Angaben in Meldungen. Bei Nichtverfügbarkeit des Systems kann die Zusammenführung nicht im vorgegebenen Zeitraum durchgeführt werden. Dann stehen die Datensätze nicht im dafür vorgesehenen Prozess zur **Verfügung**. Die fehlerhafte Zuordnung von Daten zu Datensätzen infolge unvollständiger, defekter oder sachlich falscher Angaben in Meldungen ist eine Bedrohung für die **Integrität** sowohl einzelner Datensätze aber auch des Gesamtsystems. **Vertraulichkeit** ist durch die unberechtigte Einsichtnahme durch den wissenschaftlichen Dienst oder Dritte in die Daten einzelner Fallakten vor der Anonymisierung gefährdet. Da die Daten für die internen Beteiligten anonym sind, treffen diese keine Informationspflichten. Das Ziel der **Transparenz** ist aber bedroht, wenn die betroffenen Personen gar keine Informationen erhalten können, welche ihrer Daten wie zusammengeführt werden. Die Zusammenführung von Daten ist an sich ist eine Gefahr für das Gewährleistungsziel der **Nichtverkettung.** Der wissenschaftliche Dienst kann außerdem durch die Verkettung der Datensätze zu einem Fall und mit Hilfe zusätzlicher Merkmale möglicherweise auf den Personenbezug schließen.
Eingriffsintensität:	Die Zusammenführung ist Grundlage für die mit dem NFR verfolgten Zwecke und dessen Mehrwert. Der durch Übermittlung und Annahme festgestellte Eingriff in die Rechte und Freiheiten natürlicher Personen wird durch die Zusammenführung dieser Datensätze im NFR intensiviert; zugleich stellt die Zusammenführung einen neuen Eingriff dar. Die Intensität des Eingriffs wird durch die ergriffenen TOM stark abgemildert, insbesondere durch die Pseudonymisierung der meldepflichtigen Daten sowie durch die personelle, räumliche und organisatorische Trennung des Bereiches des NFR, in dem pseudonyme Daten verarbeitet werden, von dem Bereich, der die anonymisierten Daten auswertet. Außerdem werden hier noch Daten verarbeitet, die für externe meldende Beteiligten durch die Fall-ID noch personenbeziehbar sein können.
Schutzbedarf:	Hoch hinsichtlich aller bedrohten Gewährleistungsziele

6. Ersetzung der Fall-ID durch eine Register-ID

Bedrohung:	Die **Datenminimierung** wäre bedroht, wenn die Zuordnung zur Fall-ID nicht durch den wissenschaftlichen Dienst gelöscht wird. Gleiches gilt für die unautorisierte Weitergabe von Zuordnungstabellen aus Fall-ID und Register-ID. Für den einzelnen Datensatz ist die Zuordnung falscher oder doppelter Register-ID eine Bedrohung seiner **Integrität**. Die unberechtigte Einsichtnahme in die Zuordnungen von Fall-ID – zu Register-ID durch Beteiligte und Dritte ist eine Bedrohung der **Vertraulichkeit.**

Eingriffsintensität:	Die im NFR verarbeiteten pseudonymisierten Daten sind so früh und so weit wie möglich zu anonymisieren. Die Fall-ID wird deshalb durch eine zufallsgenerierte und damit nicht rückführbare Register-ID ersetzt. Es handelt sich um eine gesetzlich normierte Abhilfemaßnahme zur Verringerung der Risiken für die Rechte und Freiheiten der betroffenen Personen. Diese Ersetzung und die damit erfolgende Anonymisierung stellen keinen Eingriff in Rechte und Freiheiten natürlicher Personen dar. Der Verarbeitungsvorgang ist aber von entscheidender Bedeutung für die Integrität des Gesamtprozesses und die Anonymisierung, weswegen seine ordnungsgemäße Durchführung geschützt werden muss.
Schutzbedarf:	Hoch hinsichtlich Vertraulichkeit und Datenminimierung Normal hinsichtlich anderer Ziele.

7. Übernahme abgeschlossener Fallakten in den Registerbestand

Bedrohung:	Die Daten verlassen mit diesem Verarbeitungsschritt den Eingangsbereich des NFR, der vom eigentlichen Registerbestand personell, räumlich und organisatorisch getrennt ist. Das Gewährleistungsziel der **Nichtverkettung** wird dadurch bedroht, dass es durch die Übertragung der Fallakten in den Registerbestand dort zu einer Verknüpfung von Fällen kommt, die eine Re-Identifizierung betroffener Personen ermöglicht. Bedrohung anderer Gewährleistungsziele besteht nur dann, wenn der Vorgang nicht ordnungsgemäß durchgeführt wird. Die **Datenminimierung** wäre bedroht, wenn die Daten nach Übernahme im temporären Bestand im Eingangsbereich des NFR verblieben. Die **Verfügbarkeit** wäre bedroht, wenn Akten verloren gingen, da nichts übernommen wurde und trotzdem der Bestand im Eingangsbereich der Annahmestelle gelöscht wird. Die **Integrität** wäre bedroht, wenn mit den in den Registerbestand übernommenen Daten Sachverhalte hinzugefügt oder verfälscht würden. Die **Vertraulichkeit** wäre bedroht, wenn unberechtigte Einsichtnahme in die Daten einzelne Fallakten bei der Übertragung erhalten würden.
Eingriffsintensität:	Im Verarbeitungsvorgang liegt kein Eingriff in Rechte und Freiheiten natürlicher Personen, da es sich um anonymisierte Daten handelt. Durch die gesetzlich normierten Pflichten zur personellen, räumlichen und organisatorischen Trennung der Verarbeitungsvorgänge, wird ein verbleibendes Missbrauchsrisiko in genügender Weise abgemildert. Im Ergebnis reduziert dieser Vorgang die Eingriffsintensität der Gesamtverarbeitung, da Falldaten nun den Eingangsbereich des NFR verlassen und anonymisiert wurden.
Schutzbedarf:	Normal

8. Auswertung der anonymisierten Daten durch die oRDB	
Bedrohung:	Die oRDB hat technisch keine direkten Zugriffsbefugnisse auf das NFR. Aus organisatorischen Gründen und zur besseren Gewährleistung der technischen Sicherheit besteht keine Möglichkeit des direkten Zugriffs. Die oRDB kann nur eine Auswertung durch den wissenschaftlichen Dienst anstoßen. Dies folgt aus dem Gebot nach Art. 56 Abs. 3, dass Auswertungen nur bezogen auf anonymisierte Daten des NFR erfolgen dürfen. Eine Bedrohung der Gewährleistungsziele besteht dann, wenn der Vorgang nicht ordnungsgemäß durchgeführt wird. So wird die **Datenminimierung** durch die Möglichkeit bedroht, dass mehr Inhalte präsentiert werden, als für die Auswertung erforderlich ist, sodass weitere Auswertungen ohne weitere Nachfrage möglich sind. Dies gilt auch für das Ziel der **Nichtverkettung**. Dieses wird auch durch die Möglichkeit des Zusammenführens von Daten zur Re-Identifizierung durch unzulässige Selektion weniger Datensätze bedroht.
Eingriffsintensität:	Ein Eingriff liegt nicht vor, da die Daten anonym sind. Der Zugriff auf die Systeme des NFR ist gesichert. Die Daten sind auch für die oRDB anonym. Sie kann keinen Personenbezug durch Auswertungen des NFR herstellen. Sie erhält nämlich nur auf Anfrage beim wissenschaftlichen Dienst Auswertungen aus dem Registerbestand. Es besteht jedoch rein denklogisch die Gefahr eines „schleichenden Personenbezugs“. Die auswertende Stelle könnte über Zusatzwissen oder Informationen verfügen, die es ihr ermöglichen, den Personenbezug aller oder auch nur einzelner Datensätze, die Teil der Auswertung sind, wiederherzustellen (Re-Identifikation). Diesen Gefährdungen wird in genügender Weise durch eine Reihe von TOM begegnet (s.o.). Die oRDB hat auch keine Ermächtigung zur Auswertung der Daten im Eingangsbereich des NFR. Die Auswertungsbefugnis hinsichtlich aller Daten im NFR ist abschließend in Art. 56 geregelt. Die oRDB darf danach den wissenschaftlichen Dienst nicht anweisen, ihr Daten aus dem Eingangsbereich des NFR zur Verfügung zu stellen. Die oRDB darf schließlich auch nicht die meldepflichtigen Stellen anweisen, ihr Daten zu bestimmten Fällen zu übermitteln, so dass sie damit auch im Eingangsbereich des NFR Daten bestimmten Personen zuordnen könnte. Eine solche Re-Identifizierung ist nach Art. 58 Abs. 5 Satz 2 ausdrücklich untersagt. Dieses Verbot bindet auch die oRDB als fachvorgesetzte Behörde für die ILS in Bayern. Eine solche Anordnungsbefugnis gehört ohnehin nicht zu dem durch das ILSG definierten Aufgabenbereich der oRDB. Umgekehrt besteht nach Art. 9 Abs. 2 ILSG ein Offenbarungsverbot für die ILS, das auch gegenüber der oRDB gilt. Auch die Ausnahmen nach Art. 9 Abs. 3 Satz 2 und 3 ILSG berechtigen nicht zur Zusammenführung personenbezogener Daten mit den im Eingangsbereich des NFR befindlichen Notfalldatensätzen.
Schutzbedarf: Normal	

9. Auswertung der anonymisierten Daten durch ÄLRD und ÄBRD und ÄLBRD sowie meldepflichtige Krankenhäuser

Bedrohung:	Bezüglich der Bedrohung für die Gewährleistungsziele wird auf die Ausführungen zu Verarbeitungsvorgang „8. Nutzung der anonymisierten Daten durch die oRDB“ verwiesen. Hinsichtlich der Auswertungsmöglichkeit durch die Krankenhäuser wird das Gewährleistungsziel der **Vertraulichkeit** zusätzlich durch Unsicherheiten bei der Zugriffsvergabe innerhalb der Krankenhäuser erhöht.
Eingriffsintensität:	Bezüglich der Eingriffsintensität wird auf die Ausführungen zu Verarbeitungsvorgang „8. Nutzung der anonymisierten Daten durch die oRDB“ verwiesen. Würde in den Krankenhäusern eine große Zahl von Personen mit Zugriffsrechten ausgestattet, so ergibt sich eine quantitative Steigerung der Eingriffsintensität.

Schutzbedarf: Normal

10. Auswertung der anonymisierten Daten durch das Bayerische Landesamt für Statistik

Bedrohung:	Bezüglich der Bedrohung für die Gewährleistungsziele wird auf die Ausführungen zu Verarbeitungsvorgang „8. Nutzung der anonymisierten Daten durch die oRDB“ verwiesen.
Eingriffsintensität:	Bezüglich der Eingriffsintensität wird auf die Ausführungen zur Verarbeitungsvorgang „8. Nutzung der anonymisierten Daten durch die oRDB“ verwiesen.

Schutzbedarf: Normal

11. Auswertung der anonymisierten Daten durch öffentliche und nicht-öffentliche Stellen

Bedrohung:	Bezüglich der Bedrohung für die Gewährleistungsziele wird auf die Ausführungen zu Verarbeitungsvorgang „8. Nutzung der anonymisierten Daten durch die oRDB“ verwiesen.
Eingriffsintensität:	Bezüglich der Eingriffsintensität wird auf die Ausführungen zur Verarbeitungsvorgang „8. Nutzung der anonymisierten Daten durch die oRDB“ verwiesen.

Schutzbedarf: Normal

12. Operativer Betrieb des NFR durch den wissenschaftlichen Dienst

Bedrohung:	Das Gewährleistungsziel der **Datenminimierung** wird dadurch bedroht, dass durch Manipulation von Daten durch direkten Zugriff zusätzliche Daten erzeugt werden könnten (z.B. Einfügung von fiktiven Sachverhalten/Unterdrückung von Sachverhalten). Das Ziel der **Verfügbarkeit** ist bedroht, wenn geplante Auswertungen nicht durchgeführt werden können und die Ergebnisse nicht für die Qualitätssicherung und die Verbesserung der Versorgung zur Verfügung stehen. Auch das Ziel der **Integrität** ist durch die Möglichkeit der Manipulation von Daten durch direkten Zugriff (Veränderung, Löschung, Einfügung von fiktiven Sachverhalten/Unterdrückung von Sachverhalten) bedroht. Das Ziel der **Vertraulichkeit** ist bedroht durch die Möglichkeit der unberechtigten Rückführung von Falldaten auf Personen durch unzulässige Abfragen.

	Das Ziel der **Transparenz** ist bedroht, wenn die Auswertungen der Daten und der Zweck für die Betroffenen nicht erkennbar sind. Die **Nichtverkettung** ist dadurch bedroht, dass durch eine unzulässige Auswertung mit zu kleiner Fallzahl ein Personenbezug hergestellt wird.
Eingriffsintensität:	Der wissenschaftliche Dienst führt als Admin/Operator des NFR die Administration des Gesamtsystems sowie die Verarbeitungsvorgänge 2 bis 11 und die Auditierung und Fortentwicklung des NFR durch. Diese Verarbeitungsvorgänge sind Grundvoraussetzung für den Betrieb des NFR und dessen Zweckverfolgung. Alle diese Aufgaben werden mit für den wissenschaftlichen Dienst anonymen Daten erreicht. Bereits die an das NFR übermittelten Daten sind für den wissenschaftlichen Dienst selbst anonym, da er nicht über das notwendige Wissen verfügt, einzelne Personen zu identifizieren und z.B. Pseudonyme, wie die Fall-ID, aufzulösen. Die Administration stellt allenfalls potentiell einen Eingriff in die Rechte betroffener Personen dar, da nur die theoretische Möglichkeit einer Re-Identifizierung besteht. Dann beinhaltet die Verarbeitung aber Daten besonderer Kategorien. Das Risiko der Re-Identifizierung wird aber in ausreichender Weise durch eine Reihe von TOM begrenzt (s.o.). Aufgrund der abschließenden Regelung von Art. 56 darf die oRDB den wissenschaftlichen Dienst nicht anweisen, ihr Daten aus dem Eingangsbereich des NFR zur Verfügung zu stellen. Aufgrund von Art. 58 Abs. 5 Satz 2 und mangels Ermächtigung darf die oRDB auch nicht die ILS in Bayern anweisen, ihr Daten zur Re-Identifizierung der Daten im Eingangsbereich des NFR zu übermitteln (s. oben 8.).
Schutzbedarf: Hoch	

8 GEPLANTE ABHILFEMAßNAHMEN ZUR BEWÄLTIGUNG DER VERBLEIBENDEN GEFÄHRDUNGEN

Der vorliegende Entwurf eines Änderungsgesetzes zum BayRDG legt zum Zweck der Rechtssicherheit die nach Art. 32 DSGVO nur abstrakt und unter Vorbehalten geforderten notwendigen technisch-organisatorische Maßnahmen zum Schutz der Notfalldaten fest. Ferner enthält der Entwurf für ein Änderungsgesetz Maßnahmen zur Stärkung der in Art. 5 DSGVO normierten Datenschutzgrundsätze.

Dennoch verbleiben Restgefährdungen beim Betrieb des geplanten NFR, die durch die im Gesetz vorgesehenen Maßnahmen nicht adressiert oder nur abgemildert werden können. Zur Adressierung dieser Restgefährdungen sind weitere Abhilfemaßnahmen erforderlich, die im Folgenden identifiziert und ausgewählt werden. Insbesondere fordert Art. 32 Abs. 1 lit. d DSGVO „gegebenenfalls“ die Einrichtung eines Verfahrens „zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung“.

Eine Normierung dieser Abhilfemaßnahmen ist in Form von Rechtsverordnungen möglich und vorgesehen. Art. 60 Nr. 16 BayRDG ermöglicht die Festlegung von Form und Inhalt des Notfalldatensatzes für die jeweiligen Meldepflichtigen, Art. 60 Nr. 19 BayRDG nähere Vorgaben zur Datenverarbeitung und zu den eingesetzten IT-Verfahren.

8.1 Identifikation und Auswahl passender Abhilfemaßnahmen

Die festgestellten Gefährdungen der Datenverarbeitung werden bereits durch die gesetzlich zum NFR vorgeschriebenen Abhilfemaßnahmen (Garantien) minimiert. Allgemeine gehaltene Vorgaben zu Verfahren und Sicherheit der Datenverarbeitung müssen jedoch noch zu umsetzbaren Gestaltungszielen und -vorgaben spezifiziert werden. Dies kann auch zum Teil in den zum BayRDG zu erlassenden Verordnungen geschehen. Dies muss aber auch die Gestaltung und Spezifikation des eigentlichen NFR leiten. Es sind zum Teil Regelmaßnahmen nach SDM (vgl. SDM V2.0, S. 30 ff.). Spezifischere Vorgaben sind bei der konkreten Ausgestaltung, der Implementation und dem Betrieb des NFR zu treffen.

Die folgende Tabelle 5 listet die zu beachtenden Abhilfemaßnahmen auf.

Die Maßnahmen lassen sich den Gewährleistungszielen zuordnen.

Einzelheiten sind den folgenden summarischen Gefährdungsbetrachtungen zum Zielerfüllungsmanagement (Tabellen 6 bis 12) zu entnehmen.

Tabelle 5: Abhilfemaßnahmen

	Abhilfemaßnahme
M.1	regelmäßige Überprüfung der zur Datenminimierung vorgesehenen Verfahren.
M.2	Datenformate und Voreinstellungen, die die Verarbeitung auf das für den Verarbeitungszweck erforderliche Maß beschränken.
M.3	Aussonderung nicht benötigter Daten durch den wissenschaftlichen Dienst.
M.4	Schutz vor Fehlern bei der Pseudonymisierung und der Anonymisierung.

M.5	Schutz vor Aushebeln oder Unterlaufen der im Gesetzentwurf vorgesehenen Maßnahmen zur Datenminimierung.
M.6	Zugriffsschutz/Berechtigungskonzept.
M.7	IT-Sicherheitskonzept erstellen und umsetzen
M.8	Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten.
M.9	Schulung der Mitarbeiter.
M.10	Löschkonzept.
M.11	regelmäßige Überprüfung der Anonymisierung auf Wirksamkeit.
M.12	automatisierte Kontrolle des Fehlens der Fall-ID bei Übergaben an das NFR.
M.13	Anfertigung von Sicherheitskopien gemäß einem getesteten Konzept.
M.14	Stichprobenkontrollen.
M.15	technisch kein direkter Zugriff der oRDB auf das NFR.
M.16	regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung.
M.17	technisch kein direkter Zugriff der Auswertungsberechtigten auf das NFR.
M.18	technisch kein direkter Zugriff des Bayerischen Landesamts für Statistik auf das NFR.
M.19	technisch kein direkter Zugriff der öffentlichen und nicht-öffentlichen Stellen auf das NFR.
M.20	klare Transaktionsmechanismen.
M.21	Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem.
M.22	operative Möglichkeit zur Zusammenstellung und konsistenten Auskunftserteilung aller zu einer Person gespeicherten Daten.
M.23	Konzept zur Berichtigung und Löschung einzelner Daten und dessen Umsetzung.
M.24	Schaffung notwendiger Datenfelder für Sperrkennzeichen.
M.25	Betroffenenrechtemanagement.
M.26	Schaffung notwendiger Datenfelder für Widersprüche.
M.27	Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten.
M.28	Einrichtung eines Single Point of Contact für Betroffene beim wissenschaftlichen Dienst.
M.29	Veröffentlichung des Gesetzes, der DSFA und weiterer Dokumente.
M.30	Aufbau einer Webseite mit Informationen zum NFR zur Information der Bürger.
M.31	Aufsicht der oRDB über den wissenschaftlichen Dienst und das IT-DLZ.
M.32	keine Verkettungsmöglichkeiten im Datenmodell.
M.33	keine „sprechenden“ Identifier.
M.34	Verhinderung der Selektion von Einzelfällen bei der Auswertung.

M.35	räumliche und personelle Trennung des Eingangsbereichs und des Registers.
M. 36	Benachrichtigung der Meldepflichtigen von der Wiederherstellung der Verfügbarkeit der Datenannahme.
M.37	Geheimhaltungsverpflichtung der Mitarbeiter.
M.38	Integritätsprüfung nach Meldungseingang.
M.39	Sicherung durch Prüfsummen, Siegel, Zeitstempel oder Signaturen.
M.40	Quittungsmechanismus bei Übermittlung an das NFR.
M.41	Redundanzen.
M.42	regelmäßige Integritätsprüfungen.
M.43	Reparaturstrategie.
M.44	Risikomanagement, das die Sicherheitsmaßnahmen kontrolliert und aktuell hält.
M.45	sichere Authentifizierung von Sender und Empfänger vor der Übertragung von Daten.
M.46	Verschlüsselung.
M.47	gesicherte Protokollierung von Datenzugriffen.
M.48	Überwachung und Protokollierung von Wartungsaktivitäten.
M.49	Beschränkung des Zugriffs von Hersteller, fachlichem Betrieb und IT-Dienstleister.
M.50	Dokumentation der Syntaxen der Daten.
M.51	Prüfung von Auswertungsanfragen durch den wissenschaftlichen Dienst.
M.52	Kryptokonzept (Prozesse zur Verwaltung und zur Gewährleistung des Schutzes der kryptografischen Informationen).
M.53	Schutz vor Überschreitung von Fristen infolge von Nichtverfügbarkeit.
M.54	Verlängerung der Karenzzeit um die Ausfallzeit.

Diese Maßnahmen lassen sich den Gewährleistungszielen zuordnen.

Einzelheiten zum Zielerfüllungsmanagement sind den summarischen Gefährdungsbetrachtungen in den folgenden Tabellen 6 bis 12 zu entnehmen.

Tabelle 6: Summarische Gefährdungsbetrachtung Datenminimierung

Gewährleistungsziel		Summarische Gefährdungsbetrachtung							Index
Datenminimierung		Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (untenstehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.							ge
									⇳
ID	Schwachstelle	Gefährdungsquelle	Gefährdungsszenario	Gefährdungsbewertung Erläuterung		gesetzliche Garantien	TOM	Gefährdungsbewertung Erläuterung	
D.1	Beabsichtigte und versehentliche Meldung nicht erforderlicher Daten in einer wiederkehrenden Struktur	meldepflichtige Stellen; Dritte	Die meldepflichtigen Stellen übermitteln personenbezogene Daten, die für die Zwecke des NFR nicht erforderlich sind.	Datenminimierung wird bedroht durch die Übermittlung von Daten durch die zur Meldung verpflichteten externen Beteiligten, die über den gesetzlich zulässigen Rahmen hinausgehen.	ro	Art. 57 Satz 1 Art. 57 Satz 4 Art. 58 Abs. 1	M.1 regelmäßige Überprüfung der zur Datenminimierung vorgesehenen Verfahren M.2 Datenformate und Voreinstellungen, die die Verarbeitung auf das für den Verarbeitungszweck erforderliche Maß beschränken M.3 Aussonderung nicht benötigter Daten durch den wissenschaftlichen Dienst	Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr
D.2	Fehlprogrammierung der Datenverarbeitung im NFR oder Fehlhandlungen im Rahmen von Supportaktivitäten.	Hersteller der Systeme	Die Datenverarbeitungssysteme speichern personenbezogene Daten, die für die Zwecke des NFR nicht erforderlich sind.	Datenminimierung wird bedroht durch Fehlfunktionen der Systeme oder durch die Hersteller im Rahmen des Supports.	ro	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 3 Art. 58 Abs. 4	M.4 Schutz vor Fehlern bei der Pseudonymisierung und der Anonymisierung M.5 Schutz vor Aushebeln oder Unterlaufen der im Gesetzentwurf vorgesehenen Maßnahmen zur Datenminimierung	Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr
D.3	Manipulation (Hinzufügen) von Daten und Sachverhalten im Eingangsbereichs des NFR oder im Register	wissenschaftlicher Dienst; Dritte	Der wissenschaftliche Dienst oder unberechtigte Dritte manipulieren im operativen Betrieb den Registerbestand.	Manipulation von Daten durch direkten Zugriff kann die Datenminimierung gefährden (z.B. Einfügung von fiktiven Sachverhalten/Unterdrückung von Sachverhalten).	ro	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 3 Art. 58 Abs. 4	M.5 Schutz vor Aushebeln oder Unterlaufen der im Gesetzentwurf vorgesehenen Maßnahmen zur Datenminimierung M.6 Zugriffsschutz/Berechtigungskonzept	Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr

							M.8 Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten		
D.4	Annahme nicht erforderlicher Daten	interne Beteiligte	Annahme von Daten im Eingangsbereich des NFR, die nicht erforderlich sind.	Datenminimierung wird bedroht durch die Annahme von Daten durch das NFR und den wissenschaftlichen Dienst zu einem Fall, die über den gesetzlich zulässigen Rahmen hinausgeht.	ge	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 1 Art. 58 Abs. 4	M.9 Schulung der Mitarbeiter M.1 regelmäßige Überprüfung der zur Datenminimierung vorgesehenen Verfahren M.8 Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten	Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr
D.5	Datenbereinigung wird nicht oder nicht ordnungsgemäß durchgeführt	interne Beteiligte	Nicht benötigte Daten werden im Eingangsbereich des NFR nicht oder fehlerhaft entfernt.	Datenminimierung wird bedroht, wenn Daten, die gemeldet wurden, aber nicht für den Registerzweck erforderlich sind, nicht gelöscht oder länger als erforderlich vorgehalten werden.	ro	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 1 Art. 58 Abs. 2 Satz 2 Art. 58 Abs. 3 Art. 58 Abs. 4	M.9 Schulung der Mitarbeiter M.1 regelmäßige Überprüfung der zur Datenminimierung vorgesehenen Verfahren M.10 Löschkonzept	Datenminimierung wird durch eine fehlerhafte Pseudonymisierung oder Anonymisierung gefährdet. Die Bandbreite möglicher, nicht erforderlicher Daten ist groß und die Erforderlichkeits- und Detailprüfung anspruchsvoll, so dass ein Restrisiko bleibt.	ge
D.6	Fehler bei der Prüfung der Pseudonymisierung	wissenschaftlicher Dienst	Im Eingang in das NFR wird die Pseudonymisierung (absichtlich oder unabsichtlich) fehlerhaft geprüft und potentiell identifizierbarer Merkmale werden nicht entfernt.	Datenminimierung ist dadurch bedroht, dass Daten, die nicht den Pseudonymisierungsregeln entsprechen, vom wissenschaftlichen Dienst in das NFR übernommen werden.	ge	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 2 Satz 2 Art. 58 Abs. 3 Art. 58 Abs. 4 Satz 3	M.9 Schulung der Mitarbeiter M.1 regelmäßige Überprüfung der zur Datenminimierung vorgesehenen Verfahren M.11 regelmäßige Überprüfung der Anonymisierung auf Wirksamkeit	Regelmäßige Überprüfung der Anonymisierung auf Wirksamkeit angesichts des technischen Fortschritts und des Aufkommens neuer Methoden zur De-Anonymisierung sind notwendig.	gr

D.7	Unberechtigte Zusammenführung von Datensätzen	wissenschaftlicher Dienst	Unberechtigte Zusammenführung von Datensätzen durch den wissenschaftlichen Dienst.	Das unberechtigte Zusammenführen von Datensätzen kann zu Korrelationen führen, die zusätzliche identifizierende Daten generieren.	ro	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 3 Art. 58 Abs. 4 Art. 61 Abs. 1 Nr. 12	M.5 Schutz vor Aushebeln oder Unterlaufen der im Gesetzentwurf vorgesehenen Maßnahmen zur Datenminimierung M.8 Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten M.9 Schulung der Mitarbeiter	Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr
D.8	Fehlerhafte Zuordnung bei der Zusammenführung	wissenschaftlicher Dienst	Fehlerhafte Zuordnung bei der Zusammenführung bei der Zusammenführung der gemeldeten Notfalldatensätze.	Die fehlerhafte Zuordnung infolge unvollständiger, defekter oder sachlich falscher Angaben in Meldungen kann die Datenminimierung gefährden.	ro	Art. 54 Abs. 2 Satz 2 Art. 57 Satz 2 und 3 Art. 58 Abs. 3 Art. 58 Abs. 1 Art. 61 Abs. 1 Nr. 12	M.5 Schutz vor Aushebeln oder Unterlaufen der im Gesetzentwurf vorgesehenen Maßnahmen zur Datenminimierung M.9 Schulung der Mitarbeiter	Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr
D.9	Fall-ID wird nicht entfernt	wissenschaftlicher Dienst	Fall-ID wird nicht aus den Daten zur Übergabe an den Registerbestand entfernt.	Die Datenminimierung wäre bedroht, wenn die Zuordnung zur Fall-ID nicht durch den wissenschaftlichen Dienst gelöscht wird.	ro	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 2 Satz 3 Art. 58 Abs. 3	M.12 automatisierte Kontrolle des Fehlens der Fall-ID bei Übergaben an das NFR M.10 Löschkonzept	Automatisierte Kontrolle und Umsetzung eines Löschkonzepts sichern die Rechtskonformität hinreichend.	gr
D. 10	Zuordnung der Fall-ID zur Register-ID ist externen Beteiligten und Dritten möglich	wissenschaftlicher Dienst	Re-Identifizierung der Daten im Registerbestand durch die Fall-ID.	Die Datenminimierung ist bedroht durch die unautorisierte Weitergabe von Zuordnungstabellen aus Fall-ID und Register-ID.	ro	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 3 Art. 58 Abs. 4 Art. 61 Abs. 1 Nr. 12	M.5 Schutz vor Aushebeln oder Unterlaufen der im Gesetzentwurf vorgesehenen Maßnahmen zur Datenminimierung M.14 Stichprobenkontrollen	Bei Durchführung der Maßnahmen zur Sicherstellung der gesetzlichen Garantien ist ein hinreichender Risikoausschluss gewährleistet, auch soweit eine lückenlose Kontrolle nicht möglich ist. Die Bußgeldandrohung schützt zusätzlich.	gr
D. 11	Daten verbleiben nach Übernahme in den Registerbestand im temporären Bestand im Eingangsbereich des NFR.	interne Beteiligte	Daten verbleiben im Eingangsbereich des NFR obwohl sie in den Registerbestand übernommen wurden.	Bei Übernahme abgeschlossener Fallakten in den Registerbestand verlassen die Daten den Eingangsbereich des NFR, der	ge	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 3 Art. 58 Abs. 4	M.5 Schutz vor Aushebeln oder Unterlaufen der im Gesetzentwurf vorgesehenen Maßnahmen zur Datenminimierung	Festlegung und Umsetzung eines Löschkonzepts und dessen Kontrolle sichern die Rechtskonformität hinreichend.	gr

				vom eigentlichen Register-bestand personell, räumlich und organisatorisch ge-trennt ist.			M.8 Regelungen zur Kon-trolle von Prozessen zur Änderung von Verarbei-tungstätigkeiten		
D. 12	Bei der Ausw ertung w er-den mehr Inhalte prä-sentiert als für die Aus-w ertung durch die oRDB notw endig ist.	oRDB; w is-senschaft-licher Dienst	Die Ausw ertung der ano-nymisierten Daten durch die oRDB ist eine Ge-fährdung für die Datenmi-nimierung, w enn die Aus-w ertung mehr Daten als erforderlich präsentiert.	Durch gezielte Ausw er-tungsverfahren könnte ein Personenbezug zu Daten im NFR hergestellt w erden.	ge	Art. 56 Abs. 3 Art. 58 Abs. 2 Satz 1 und 2 Art. 58 Abs. 5 Art. 61 Abs. 1 Nr. 12	M.15 technisch kein direk-ter Zugriff der oRDB auf das NFR M.11 regelmäßige Über-prüfung der Anonymisie-rung auf Wirksamkeit M.4 Schutz vor Fehlern bei der Pseudonymisie-rung und der Anonymisie-rung	Regelmäßige Überprüfung der Anonymisierung auf Wirksamkeit angesichts des technischen Fort-schritts und des Aufkommens neuer Methoden zur De-Anony-misierung mindern die Gefähr-dung hinreichend.	gr
D. 13	Bei der Ausw ertung w er-den mehr Inhalte prä-sentiert als für die Aus-w ertung durch die ÄLRD und ÄBRD und ÄLBRD sow ie meldepflichtige Krankenhäuser notw en-dig ist.	ÄLRD; ÄBRD; ÄLBRD; melde-pflichtige Kranken-häuser	Die Ausw ertung der ano-nymisierten Daten durch die Ausw ertungsberech-tigten ist eine Gefähr-dung für die Datenmini-mierung, w enn die Aus-w ertung mehr Daten als erforderlich (Zw eckfestle-gung) präsentiert.	D.12	ge	Art. 56 Abs. 3 Art. 58 Abs. 2 Satz 1 und 2 Art. 58 Abs. 5	M.17 technisch kein direk-ter Zugriff der Ausw er-tungsberechtigten auf das NFR M.11 regelmäßige Über-prüfung der Anonymisie-rung auf Wirksamkeit. M.4 Schutz vor Fehlern bei der Pseudonymisie-rung und der Anonymisie-rung.	D.12	gr
D. 14	Bei der Ausw ertung der anonymisierten Daten durch das Bayerische Landesamt für Statistik w erden mehr Inhalte	Bayerische Landesamt für Statis-tik; w issen-	Die Ausw ertung der ano-nymisierten Daten durch das Bayerische Landes-amt für Statistik ist eine	D.12	ge	Art. 56 Abs. 3 Art. 58 Abs. 2 Satz 1 und 2, Art. 58 Abs. 5	M.18 technisch kein direk-ter Zugriff des Bayeri-schen Landesamts für Statistik auf das NFR	D.12	gr

	präsentiert als für die Auswertung notwendig sind.	schaftlicher Dienst	Gefährdung für die Datenminimierung, wenn die Auswertung mehr Daten als erforderlich präsentiert.				M.11 regelmäßige Überprüfung der Anonymisierung auf Wirksamkeit		
							M.4 Schutz vor Fehlern bei der Pseudonymisierung und der Anonymisierung		
D. 15	Bei der Auswertung der anonymisierten Daten durch öffentliche und nicht-öffentliche Stellen werden mehr Inhalte präsentiert als für die Auswertung notwendig sind.	öffentliche und nicht-öffentliche Stellen; wissenschaftlicher Dienst	Die Auswertung der anonymisierten Daten durch öffentliche und nicht-öffentliche Stellen ist eine Gefährdung für die Datenminimierung, wenn die Auswertung mehr Daten als erforderlich präsentiert.	D.12	ge	Art. 56 Abs. 3 Art. 58 Abs. 2 Satz 1 und 2, Art. 58 Abs. 5	M.19 technisch kein direkter Zugriff der öffentlichen und nicht-öffentlichen Stellen auf das NFR	D.12	gr
							M.4 Schutz vor Fehlern bei der Pseudonymisierung und der Anonymisierung		
							M.11 regelmäßige Überprüfung der Anonymisierung auf Wirksamkeit		

Tabelle 7: Summarische Gefährdungsbetrachtung Intervenierbarkeit

Gewährleistungsziel	Summarische Gefährdungsbetrachtung							Index
Intervenierbarkeit	**Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (untenstehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.**							gr
								⇳
ID	Schwachstelle	Gefährdungsquelle	Gefährdungsszenario	Gefährdungsbewertung Erläuterung		gesetzliche Garantien	TOM	Gefährdungsbewertung Erläuterung	
IV.1	Durchführung als fehlerhaft oder unzulässig erkannter Verarbeitungsvorgänge.	Hersteller; interne Beteiligte	Als fehlerhaft oder unzulässig erkannte Verarbeitungsvorgänge können von den internen Beteiligten, insb. dem wissenschaftlichen Dienst, nicht abgebrochen werden.	Eine Bedrohung der Intervenierbarkeit liegt darin, dass keine ausreichende Transaktionssteuerung zum Abbruch verfügbar ist.	ro	Art. 58 Abs. 4 Satz 3	M.20 klare Transaktionsmechanismen M.21 Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem	Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr
IV.2	Auskunft zu einzelnen Datensätzen im Eingangsbereich des NFR kann nicht erteilt werden.	Hersteller; interne Beteiligte	Auskünfte können nicht erteilt oder Kopien nicht ausgehändigt werden, weil das System nicht alle Daten zur Einsicht oder zur Kopie freigibt.	Im Eingangsbereich des NFR sind die Daten pseudonym und mithin auf eine konkrete Person rückführbar.	ro	Art. 54 Abs. 2 Satz 1 Nr. 2 und 4 Art. 58 Abs. 4 Satz 3	M.22 operative Möglichkeit zur Zusammenstellung und konsistenten Auskunftserteilung aller zu einer Person gespeicherten Daten	s. IV.1	gr
IV.3	Das Verändern und Löschen einzelner Notfalldatensätze im Eingangsbereich des NFR	Hersteller; interne Beteiligte	Betroffene Personen können Recht auf Berichtigung und Löschung nicht durchsetzen.	Die Intervenierbarkeit fehlt, wenn der Anspruch betroffener Personen auf	ro	Art. 54 Abs. 2 Satz 1 Nr. 2 und 4	M.23 Konzept zur Berichtigung und Löschung einzelner Daten und dessen Umsetzung	Im NFR muss die Durchsetzung der Rechte auf Berichtigung und Löschung bezogen	gr

	ist nicht oder nur unter erheblichen Aufwand möglich.			Berichtigung oder Löschung im DV-System nicht umgesetzt werden kann.		Art. 58 Abs. 4 Satz 3	M.21 Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem.	auf einzelne Datensätze (oder sogar einzelner Eintragungen) möglich sein. Dadurch wird das Gewährleistungsziel der Intervenierbarkeit ausreichend erreicht.	
IV.4	Einzelne Notfalldatensätze im Eingangsbereich des NFR können nicht in der Verarbeitung eingeschränkt werden.	Hersteller; interne Beteiligte	Betroffene Personen können das Recht auf Einschränkung der Verarbeitung nicht durchsetzen.	Die Intervenierbarkeit fehlt, wenn der Anspruch betroffener Personen auf Beschränkung der Datenverarbeitung im DV-System nicht umgesetzt werden kann.	ro	Art. 54 Abs. 2 Satz 1 Nr. 2 und 4 Art. 58 Abs. 4 Satz 3	M.24 Schaffung notwendiger Datenfelder für Sperrkennzeichen. M.25 Betroffenenrechtemanagement	wie IV.3 bezogen auf das Recht der Einschränkung	gr
IV.5	Die Beendigung der Verarbeitung einzelner Datensätze nach Widerspruch möglich.	Hersteller; interne Beteiligte	Betroffene Personen können das Recht auf Widerspruch gegen die Verarbeitung nicht durchsetzen.	Die Intervenierbarkeit fehlt, wenn der Anspruch betroffener Personen nach einem erfolgreichen Widerspruch auf Beendigung der Verarbeitung im DV-System nicht umgesetzt werden kann.	ro	Art. 54 Abs. 2 Satz 1 Nr. 2 und 4 Art. 58 Abs. 4 Satz 3	M.26 Schaffung notwendiger Datenfelder für Widersprüche M.25 Betroffenenrechtemanagement	wie IV.3 bezogen auf das Recht auf Widerspruch	gr
IV.6	Die Authentifizierung von betroffenen Personen, die Rechte geltend machen, ist nicht gewährleistet.	interne Beteiligte	Nicht berechtigte Personen machen Rechte geltend und erhalten so personenbezogene Daten betroffener Personen oder tragen zu deren Veränderung bei.	Die Intervenierbarkeit wird falsch umgesetzt, wenn Unberechtigte intervenieren können.	ro	Art. 54 Abs. 2 Satz 1 Nr. 2 und 4 Art. 58 Abs. 4 Satz 3	M.27 Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten M.28 Einrichtung eines Single Point of Contact für Betroffene beim wissenschaftlichen Dienst	Die Authentifizierung der Personen, die Rechte geltend machen, muss gewährleistet sein.	gr

Tabelle 8: Summarische Gefährdungsbetrachtung Transparenz

Gewährleistungsziel		Summarische Gefährdungsbetrachtung							Index
Transparenz		Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (untenstehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.							gr
									⇳
ID	Schwachstelle	Gefährdungsquelle	Gefährdungsszenario	Gefährdungsbewertung Erläuterung		gesetzliche Garantien	TOM	Gefährdungsbewertung Erläuterung	
TP.1	Betroffene Personen erhalten keine Information oder Auskunft von meldenden externen Beteiligten darüber, dass und welche ihrer Daten an das NFR übertragen werden.	meldepflichtige Stellen	Ein Patient wird rettungsdienstlich behandelt. Den Rettungsdienst treffen jedoch keine Informationspflichten. Diese treffen nur ein behandelndes Krankenhaus. Dort ist es möglich, dass eine Information des Patienten unterbleibt.	Das NFR selbst treffen keine Informationspflichten.	ge	Art. 53 ff.	M.29 Veröffentlichung des Gesetzes, der DSFA und weiterer Dokumente M.30 Aufbau einer Webseite mit Informationen zum NFR zur umfassenden Information der Bürger	Eine Information der betroffenen Personen bezogen auf das NFR erfolgt im Rahmen der Informationspflichten der Krankenhäuser. Zudem findet eine begleitende Öffentlichkeitsarbeit statt.	gr
TP.2	Für die betroffenen Personen könnte der Zweck des NFR nicht erkennbar sein.	interne Beteiligte	Eine betroffene Person wird zwar über die Datenverarbeitung informiert, versteht jedoch nicht die hinter der Datenverarbeitung stehenden Zwecke.	s. TP.1	ge	Art. 53 Art. 58 Abs. 1	s. TP.1	Das Gesetz beschreibt den Zweck des NFR. Der wissenschaftliche Dienst prüft die gemeldeten Notfalldatensätze auf ihre Eignung zur Zielerreichung des NFR.	gr
TP.3	Die Aufsicht über das NFR könnte mangelhaft sein.	interne Beteiligte	Es könnte infolge von mangelhafter Aufsicht über den Betrieb des NFR zu datenschutzrechtlichen Verstößen kommen.	Eine effektive Aufsicht ist unerlässlich zur Gewährleistung rechtskonformen Verhaltens.	ro	Art. 59 Art. 60 Nr. 20	M.31 Aufsicht des oRDB über den wissenschaftlichen Dienst und das IT-DLZ	Es wird ein Registerbeirat eingerichtet. Den operativen technischen Betrieb des NFR leisten der wissenschaftliche Dienst als Verwaltungshelfer und das IT-DLZ als Auftragsverarbeiter. Beide werden von der oRDB kontrolliert und angewiesen.	gr

TP.4	Es wird fälschlicherweise angenommen, es bestünden nie Auskunftspflichten des Betreibers, da keine personenbezogenen Daten verarbeitet würden.	wissenschaftlicher Dienst	s. TP.5	Die von den übermittelnden Stellen durch die Fall-ID pseudonymisierten Daten sind für die oRDB und den wissenschaftlichen Dienst grundsätzlich anonym. Auch bei schleichendem Personenbezug gälte Art. 14 Abs. 5 lit. b DSGVO und auch Art. 9 Abs. 1 BayDSG, so dass betroffene Personen nicht informiert werden müssten.	ge	Art. 53 ff.	s. TP.1	s. TP.5	gr
TP.5	Eine Auskunftserteilung kann nur erfolgen, wenn der Betroffene sein Auskunftsersuchen so gestaltet, dass dem NFR eine Zuordnung von Falldaten zu diesem Betroffenen möglich wird.	wissenschaftlicher Dienst	Es können Auskunftsansprüche nach Art. 15 DSGVO bestehen und die gesetzlich normierten Ausnahmen vom Auskunftsrecht nach BayDSG nicht greifen.	Eine Auskunft ist nur im Eingangsbereich des NFR möglich, da danach aufgrund der Verarbeitungsvorgänge 3, 4 und 6 keine identifizierenden Merkmale mehr vorhanden sind. Ist eine Identifizierung möglich, ist die Auskunft nach den Vorgaben des Art. 12 DSGVO zu erteilen.	ge	Art. 53 ff.	s. TP.1	Auskunft kann nur erteilt werden, wenn mit dem Auskunftsersuchen Daten zur Verfügung gestellt werden, die eine Identifizierung ermöglichen.	gr

Tabelle 9: Summarische Gefährdungsbetrachtung Nichtverkettung

Gewährleistungsziel		Summarische Gefährdungsbetrachtung							Index
Nichtverkettung		Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (untenstehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.							ge
									⇳
ID	Schwachstelle	Gefährdungsquelle	Gefährdungsszenario	Gefährdungsbewertung		gesetzliche Garantien	TOM	Gefährdungsbewertung	
				Erläuterung					
NV.1	Die Zusammenführung von Daten im Eingangsbereich kann die Herstellung eines Personenbezugs erlauben.	wissenschaftlicher Dienst	Im Eingangsbereich des NFR besteht die Möglichkeit, die Daten eines Falles aus verschiedenen Quellen so zusammenzuführen, dass dadurch ein Personenbezug hergestellt werden kann.	Die Zusammenführung von Daten ist an sich eine Gefahr für das Gewährleistungsziel der Nichtverkettung.	ge	Art. 54 Abs. 2 Satz 2 Art. 57 Art. 58 Abs. 1	M.32 keine Verkettungsmöglichkeiten im Datenmodell M.33 keine „sprechenden“ Identifier	Den sich hieraus ergebenden Risiken wird durch die Forderung der notwendigen wissenschaftliche Kompetenz, der technischen und organisatorischen Fach- und Sachkunde sowie Zuverlässigkeit des wissenschaftlichen Dienstes begegnet.	gr
NV.2	Die Verknüpfung von Fällen im Registerbestand kann es möglich machen, einen Personenbezug herzustellen.	wissenschaftlicher Dienst	Es kommt durch die Übertragung der Fallakten in den Registerbestand zu einer Verknüpfung von Fällen, die es möglich macht, einen Personenbezug herzustellen.	s. NV.1	ge	Art. 54 Abs. 2 Satz 2 Art. 58	M.32 keine Verkettungsmöglichkeiten im Datenmodell	s. NV.1	gr
NV.3	Daten können durch unzulässige Auswertung mit zu kleiner Fallzahl zusammengeführt werden.	wissenschaftlicher Dienst	Es kann durch unzulässige Auswertung mit zu kleiner Fallzahl ein Personenbezug hergestellt werden.	Das Hinzuziehen weiterer Merkmale kann es möglich machen, die Auswertung so zu gestalten, dass ein einzelner Notfalldatensatz einer bestimmten Person zugeordnet werden kann.	ro	Art. 56 Abs. 3 Satz 2 Art. 58 Abs. 5 Satz 1	M.34 Verhinderung der Selektion von Einzelfällen bei der Auswertung	Die Bereitstellung der Daten aus dem NFR setzt voraus, dass stets eine Grundgesamtheit von mindestens vier Datensätzen vorliegt. Auswertungen über eine Datenmenge von weniger als vier gleichen Datensätzen werden abgewiesen (s. o. S. 18).	gr

NV.4	Daten können durch unbefugte Datenweitergabe zusammengeführt werden.	alle Stellen mit Zugriff auf das NFR	Es können Daten unbefugt an Dritte weitergegeben werden und von diesen unter Hinzuziehung weiterer Merkmale einer bestimmten Person zugeordnet werden.	Eine unbefugte Datenweitergabe ist sowohl beabsichtigt wie auch unbeabsichtigt möglich.	ro	Art. 58 Abs. 3 Art. 58 Abs. 4 Art. 58 Abs. 5 Satz 2 Art. 61 Abs. 1 Nr. 12	M.6 Zugriffsschutz/Berechtigungskonzept M.46 Verschlüsselung	Die Zusammenführung von Einzelangaben des NFR oder solcher Einzelangaben mit anderen Angaben zum Zwecke der Herstellung eines Personenbezugs wird vom Gesetz untersagt und mit Bußgeld bedroht. Es kann trotzdem nicht ausgeschlossen werden, dass es zu diesbezüglich zu Rechtsbrüchen kommt.	ge
NV.5	Daten können durch überschneidende Aufgabenbereiche zusammengeführt werden.	wissenschaftlicher Dienst	Wenn sich die Aufgabenbereiche des Eingangsbereichs und des Registers beim wissenschaftlichen Dienst überschneiden, könnte es zu einer nicht vorgesehenen Zusammenführung von Daten kommen.	Eine unzureichende Trennung der Aufgabenbereiche des wissenschaftlichen Dienstes birgt das Potential der Zusammenführung von Datensätzen aus den beiden Bereichen des NFR (Eingangsbereich, Registerbestand) mit dem Ziel der Herstellung eines Personenbezuges.	ro	Art. 58 Abs. 3 Art. 58 Abs. 5	M.35 räumliche und personelle Trennung des Eingangsbereichs und des Registers M.6 Zugriffsschutz/Berechtigungskonzept	Um Überschneidungen zu verhindern, fordert das Gesetz eine personelle, organisatorische und räumliche Trennung der Aufgaben des wissenschaftlichen Dienstes nach Art. 58 Abs. 1 und 2 von seinen sonstigen Aufgaben.	gr
NV.6	Daten können durch unterlassene, fehlerhafte oder mangelhafte Pseudonymisierung zusammengeführt werden.	wissenschaftlicher Dienst	Daten werden vor der Übertragung an das NFR nicht ausreichend pseudonymisiert und können in der Folge mit weiteren Merkmalen zusammengeführt werden, um einen Personenbezug herzustellen. Daten werden im NFR nicht in pseudonymisierter Form verarbeitet.	Es ist denkbar, dass identifizierende Merkmale im Eingangsbereich des NFR nicht entfernt werden.	ro	Art. 54 Abs. 2 Satz 2 Art. 57 Satz 1 Art. 58 Abs. 1 Art. 58 Abs. 2 Satz 1 Art. 61 Abs. 1 Nr. 12	M.9 Schulung der Mitarbeiter M.37 Geheimhaltungsverpflichtung der Mitarbeiter	Die Pseudonymisierung von Daten im Eingangsbereich ist erforderlich, um zusammengehörende Datensätze zuordnen zu können. Gleichzeitig macht das Gesetz Vorgaben für die Pseudonymisierung und sieht Bußgelder bei Verstößen vor.	gr
NV.7	Daten können durch unterlassene oder mangelhafte Verschlüsselung bei der Übermittlung zusammengeführt werden.	Dritte	Daten werden bei der Übertragung an das NFR unzureichend vor unberechtigtem Zugriff geschützt und können in der Folge mit weiteren Merkmalen zusammengeführt werden, um einen Personenbezug herzustellen.	Es ist denkbar, dass die Verschlüsselung der Daten auf dem Transportweg nicht oder ungenügend gesichert werden.	ro	Art. 57 Satz 4 Art. 58 Abs. 1	M.46 Verschlüsselung M.6 Zugriffsschutz/Berechtigungskonzept	Das Gesetz fordert eine Datenübermittlung in verschlüsselter Form. Verschlüsslung der zu übertragenden Daten verhindert die Verkettung	gr

NV.8	Daten können durch unterlassene, fehlerhafte oder mangelhafte Anonymisierung zusammengeführt werden.	alle Stellen mit Zugriff auf das NFR	Daten werden im Eingangsbereich nicht ausreichend anonymisiert und können in der Folge mit weiteren Merkmalen zusammengeführt werden, um einen Personenbezug herzustellen.	Es ist denkbar, dass die Fall-ID nicht entfernt wird. Zudem ist denkbar, dass die im NFR vorgenommene Anonymisierung aufgrund des techn. Fortschritts unzureichend wird oder bereits initial nicht den erforderlichen Standards entspricht.	ro	Art. 56 Abs. 3 Satz 1 Art. 58 Abs. 2 Satz 2 Art. 61 Abs. 1 Nr. 12	M.11 regelmäßige Überprüfung der Anonymisierung auf Wirksamkeit	Die Anonymisierung des Registerbestands ist wesentliches Merkmal des NFR. Das Gesetz macht hierzu Vorgaben und sieht Geldbußen bei Verstößen vor.	gr
NV.9	Daten können durch unbefugten Zugriff auf das NFR zusammengefügt werden.	Dritte	Es gelingt nicht zugriffsberechtigen Personen oder Stellen, Zugriff auf das NFR zu erlangen und die so erworbenen Daten mit dem Ziel der Herstellung eines Personenbezugs mit anderen Daten zusammen zu führen.	Es ist denkbar, dass es etwa durch Einbruch oder durch einen Cyberangriff gelingt, auf die im NFR gesammelten Datensätze zuzugreifen und diese dann unter Hinzuziehung weiterer Merkmale einzelnen Personen zuzuordnen.	ro	Art. 58 Abs. 4 Satz 1 Art. 58 Abs. 4 Satz 2 und 3	M.16 regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung M.7 IT-Sicherheitskonzept erstellen und umsetzen	Durch die gesetzliche Forderung der Verschlüsselung der ohnehin pseudonymisierten (Eingangsbereich) bzw. anonymisierten (Registerbestand) Daten sowie zusätzliche Forderungen zur Sicherung des NFR (Zugriff, Zutritt, TOMs) wird die Gefährdung minimiert.	gr
NV.10	Daten können durch zweckwidrige Nutzung des NFR zusammengeführt werden.	alle Stellen mit Zugriff auf das NFR	Daten aus dem Eingangsbereich oder dem Registerbestand des NFR können mit weiteren Merkmalen zusammengeführt werden, um einen Personenbezug herzustellen.	Eine zweckwidrige Nutzung der Datensätze könnte zur Re-Identifizierung einzelner Personen führen.	ro	Art. 56 Abs. 1 Art. 58 Abs. 5 Art. 61 Abs. 1 Nr. 12	M.11_regelmäßige Überprüfung der Anonymisierung auf Wirksamkeit M.4 Schutz vor Fehlern bei der Pseudonymisierung und der Anonymisierung M.6 Zugriffsschutz/Berechtigungskonzept M.17 technisch kein direkter Zugriff der Auswertungsberechtigten auf das NFR. M.18 technisch kein direkter Zugriff des Bayerischen Landesamts für Statistik auf das NFR M.19 technisch kein direkter Zugriff der öffentlichen und nicht-öffentlichen Stellen auf das NFR	Die Gefahr einer zweckwidrigen Nutzung kann durch die Begrenzung von Zugriffsrechten auf bestimmte Zwecke minimiert werden. Eine zweckwidrige Nutzung etwa im Kontext der Auswertung zur wissenschaftlichen Forschung kann aber nicht gänzlich ausgeschlossen werden.	ge

Tabelle 10:Summarische Gefährdungsbetrachtung Integrität

Gewährleistungsziel		Summarische Gefährdungsbetrachtung							Index
Integrität		**Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (untenstehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.**							ge
									⇳
ID	Schwachstelle	Gefährdungs-quelle	Gefährdungsszenario	Gefährdungsbewertung Erläuterung		gesetzliche Garantien	Maßnahme-Bezeichnung	Gefährdungsbewertung Erläuterung	
IN.1	Daten könnten auf dem Übertragungsweg verändert werden.	Dritte; melde-pflichtige Stellen	Verfälschung oder Vertauschung von Werten, Einfügung von fiktiven Sachverhalten/Unterdrückung von Sachverhalten etc. auf dem Übertragungsweg	Die Veränderung von Inhalten auf dem Übertragungsweg, die sich auf die Zuordnung und Auswertung wesentlich auswirken, durch Beteiligte oder Dritte gefährdet das Gewährleistungsziel Integrität. S. zudem IN.2.	ro	Art. 57 Satz 4 Art. 58 Abs. 1 Art. 60 Nr. 19	M.46 Verschlüsselung M.38 Integritätsprüfung nach Meldungseingang M.39 Sicherung durch Prüfsummen, Siegel, Zeitstempel oder Signaturen M.40 Quittungsmechanismus bei Übermittlung an das NFR	Die Gefährdungen der Integrität der Notfalldatensätze werden durch gesetzliche Vorgaben, Aufsichts- und Regelungsmaßnahmen der oRDB und der Androhung von Bußgeldern adressiert (Art. 61 Abs. 1). Bezogen auf den Übertragungsweg ist die Realisierung absoluter Sicherheit nicht möglich.	ge
IN.2	Der Empfang der Daten im Eingangsbereich des NFR könnte fehlerhaft sein.	wissenschaftlicher Dienst; IT-DLZ	Der fehlerhafte Empfang kann zur Verfälschung der Sachverhalte führen. Zudem ist eine fehlerhafte Zuordnung von Falldaten und infolge dessen falsche Aggregation von Daten denkbar.	Eine Verfälschung der Daten kann die Falldaten unbrauchbar machen und die Statistik verfälschen (z.B. systematische Entstehung extremer Sonderfälle). Fehlerhafte Verarbeitung kann systematisch zu fehlerhaften Aussagen über den Bestand führen. Die Ziele des NFR können in der Folge nicht erreicht werden.	ro	Art. 58 Abs. 1 Art. 60 Nr. 19	M.39 Sicherung durch Prüfsummen, Siegel, Zeitstempel oder Signaturen M.40 Quittungsmechanismus bei Übermittlung an das NFR	Die Gefährdungen der Integrität der Notfalldatensätze werden durch gesetzliche Vorgaben, Aufsichts- und Regelungsmaßnahmen der oRDB und der Androhung von Bußgeldern adressiert (Art. 61 Abs. 1).	gr
IN.3	Es sind fehlerhafte Verarbeitungen im NFR denkbar.	wissenschaftlicher Dienst; IT-DLZ	Es gelten die Ausführungen zu IN.2 sinngemäß.	s. IN.2	ro	Art. 58 Abs. 4 Art. 60 Nr. 19	M.46 Verschlüsselung M.39 Sicherung durch Prüfsummen, Siegel, Zeitstempel oder Signaturen M.42 regelmäßige Integritätsprüfungen M.43 Reparaturstrategie M.6 Zugriffsschutz/Berechtigungskonzept	s. IN.2	gr

IN.4	Pseudonymisierung und Datenbereinigung könnten fehlerhaft sein.	wissenschaftlicher Dienst	Die Integrität des gesamten informationstechnischen Prozesses ist gefährdet, wenn die Funktion der Datenbereinigung nicht durchgeführt wird oder werden kann.	s. IN.2	ro	Art. 54 Abs. 2 Satz 2 Art. 58 Abs. 2 Art. 60 Nr. 19	M.9 Schulung der Mitarbeiter	s. IN.2	gr
IN.5	Die Zuordnung von Daten zu Datensätzen könnte fehlerhaft sein.	wissenschaftlicher Dienst	Fehlerhafte Zuordnung von Daten zu Datensätzen ist infolge unvollständiger, defekter oder sachlich falscher Angaben in Meldungen denkbar; aber auch durch fehlerhafte Verarbeitung im NFR. Für den einzelnen Datensatz ist die Zuordnung falscher oder doppelter Register-ID eine Bedrohung.	s. IN.2	ro	Art. 57 Art. 58 Abs. 1 Art. 58 Abs. 2 Satz 3 Art. 60 Nr. 19	s. IN 1, IN.2, IN.3 und IN.4	Das Gesetz fordert eine korrekte Zusammenführung gemeldeter Daten mit anderen Daten zum gleichen Notfall. Seitens der Meldepflichtigen besteht die Pflicht zur richtigen Meldung nach Art. 55. Diese ist bußgeldbewehrt (Art. 61 Abs. 1 Nr. 11).	gr
IN.6	Im Registerbestand könnten Sachverhalte hinzugefügt, gelöscht, unterdrückt oder verfälscht werden.	Dritte; wissenschaftlicher Dienst; IT-DLZ	Es sind Eingriffe in den Registerbestand denkbar, die die Zielerreichung des NFR gefährden.	s. IN.2	ro	Art. 58 Abs. 3 Art. 58 Abs. 4 Art. 60 Nr. 19	s. IN.3 M.6 Zugriffsschutz/Berechtigungskonzept	s. IN.2	gr
IN.7	Technische und organisatorische Entwicklungen könnten die vorgesehenen TOM überholen	alle internen Beteiligten; Hersteller	Neue Entwicklungen könnten zu Lücken in der Gewährleitung des Ziels der Integrität führen.	Die DSFA gilt für einen bestimmten Zeitpunkt. Die Sicherheitsgewährleistungen müssen aber kontinuierlich aktuell gehalten werden.	ro	Art. 58 Abs. 4 Art. 60 Nr. 19	M.44 Einrichtung eines Risikomanagements, das die Sicherheitsmaßnahmen kontrolliert und aktuell hält.	Ein funktionierendes Risikomanagement hält die notwendigen TOM auf dem jeweils notwendigen aktuellen Stand.	gr

Tabelle 11:Summarische Gefährdungsbetrachtung Vertraulichkeit

Gewährleistungsziel		Summarische Gefährdungsbetrachtung							Index
Vertraulichkeit		Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (untenstehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.							ge
									⇳
ID	Schwachstelle	Gefährdungsquelle	Gefährdungsszenario	Gefährdungsbewertung Erläuterung		gesetzliche Garantien	Maßnahme-Bezeichnung	Gefährdungsbewertung Erläuterung	
VT.1	Daten können von meldepflichtigen Stellen an unberechtigte Stellen übermittelt werden.	meldepflichtige Stellen; Dritte	Notfalldatensätze werden versehentlich falsch adressiert und eine unberechtigte Stelle gibt sich als der wissenschaftliche Dienst aus.	Datensätzen können fahrlässig falsch adressiert werden. Angreifer können den wissenschaftlichen Dienst imitieren und so eine Übermittlung an ihre Adresse provozieren.	ro	Art. 57 Satz 4	M.46 Verschlüsselung M.40 Quittungsmechanismus bei Übermittlung an das NFR M.45 sichere Authentifizierung von Sender und Empfänger vor der Übertragung von Daten	Auf dem Übertragungsweg ist absolute Sicherheit nicht möglich. Eine unberechtigte Stelle kann jedoch nur Kenntnis von verschlüsselten Daten erhalten. Dies ist bei hohen Verschlüsselungsstandards ausreichend.	ge
VT.2	Daten könnten bei der Übermittlung an das NFR mitgelesen werden.	Dritte	Notfalldatensätze werden korrekt übermittelt, aber auf dem Übertragungsweg von Dritten abgefangen, um sie zu lesen.	Der Übertragungsweg der Notfalldatensätze dürfte als wahrscheinlichster Angriffspunkt für Dritte gelten.	ro	Art. 57 Satz 4	M.46 Verschlüsselung	Ein Schutz durch Verschlüsselung ist bei hohen Verschlüsselungsstandards ausreichend.	ge
VT.3	Es könnte zu unberechtigtem Zugriff auf nicht (ausreichend) pseudonymisierte Daten im Eingangsbereich des NFR kommen.	alle internen Beteiligten; Dritte	Im Eingangsbereich des NFR befinden sich bis zum abschließenden Zusammenführen der Daten eines Falles noch nicht anonymisierte Daten, die ein Angreifer bei unbefugtem Zutritt zur Kenntnis nehmen könnte.	Externe und Mitarbeiter des wissenschaftlichen Dienstes, die nicht mit diesem Verarbeitungsvorgang betraut sind, könnten Einsicht nehmen und personenbezogene oder unzureichend pseudonymisierte lesen.	ro	Art. 58 Abs. 1 - 4	M.47 gesicherte Protokollierung von Datenzugriffen M.48 Überwachung und Protokollierung von Wartungsaktivitäten M.49 Beschränkung des Zugriffs von Herstellerfachlichem Betrieb und IT-Dienstleister M.6 Zugriffsschutz/Berechtigungskonzept M.46 Verschlüsselung M.52 Kryptokonzept (Prozesse zur Verwaltung und zur Gewährleistung des Schutzes der kryptografischen Informationen) M.7 IT-Sicherheitskonzept erstellen und umsetzen	Eine Abkapselung des Eingangsbereichs des NFR verhindert unberechtigte Kenntnisnahme durch unberechtigte Angehörige des wissenschaftlichen Dienstes. Zugriffe anderer Stellen werden durch TOMs ausgeschlossen.	gr

VT.4	Es könnte zu unberechtigtem Zugriff auf den Registerbestand des NFR kommen.	alle internen Beteiligten; Dritte	Es gilt sinngemäß VT.3 mit dem Unterschied, dass hier ausschließlich anonymisierte Daten betroffen sind.	Im Vergleich zu VT.3 gilt eine reduzierte Gefährdung, da der Registerbestand ausschließlich anonymisierte Daten enthält.	ge	Art. 58 Abs. 3 Art. 58 Abs. 4	s. VT.3	Zugriff ist nur zur Auswertung berechtigten Stellen möglich. Ein Zugriff sonstiger Stellen wird durch TOMs verhindert. Daten im Registerbestand wurden anonymisiert.	gr
VT.5	Es könnte zu unberechtigter Kenntnisnahme der aus dem Notfalldatensatz zu entfernenden Daten kommen.	alle internen Beteiligten; Dritte	s. VT.3	s. VT.3	ro	Art. 58 Abs. 3 Art. 58 Abs. 4	s. VT.3	s. VT.3	gr
VT.6	Es könnte zu unberechtigter Kenntnisnahme der pseudonymen Daten im Eingangsbereich des NFR kommen.	alle internen Beteiligten; Dritte	s. VT.3	s. VT.3; geringere Gefährdung infolge Pseudonymisierung	ge	Art. 58 Abs. 1 - 4	s. VT.3	s. VT.3	gr
VT.7	Es könnte zu unberechtigter Einsichtnahme in die Zuordnung von Fall-ID zu Register-ID kommen.	alle internen Beteiligten; Dritte	s. VT.3	s. VT.6	ge	Art. 58 Abs. 3 Art. 58 Abs. 4	s. VT.3	s. VT.3	gr
VT.8	Es könnte bei Auswertungsberechtigten zu unberechtigten Zugriffen auf den Registerbestand kommen.	alle zur Auswertung berechtigten Stellen	Vertraulichkeit wird durch Unsicherheiten bei der Zugriffsvergabe innerhalb der Krankenhäuser gefährdet.	Würde in den Krankenhäusern eine große Zahl von Personen mit Zugriffsrechten ausgestattet, so ergäbe sich eine quantitative Steigerung der Eingriffsintensität.	ro	Art. 56 Abs. 3	M.47 gesicherte Protokollierung von Datenzugriffen M.6 Zugriffsschutz/Berechtigungskonzept	Ein direkter Zugriff besteht nicht. Auswertungen erfolgen über die vom wissenschaftlichen Dienst vorgenommenen Aufbereitungen des Registerbestands.	gr
VT.9	Es könnte durch unzulässige Abfragen zu einer unberechtigten Rückführung von Falldaten auf Personen kommen.	alle zur Auswertung berechtigten Stellen	Abfragen könnten gezielt oder ungewollt eine Rückführung auf eine bestimmte Person ermöglichen.	Eine zweckwidrige Nutzung der Datensätze könnte zur Re-Identifizierung einzelner Personen führen.	ro	Art. 56 Abs. 3 Art. 58 Abs. 5	M.51 Prüfung von Auswertungsanfragen durch den wissenschaftlichen Dienst	s. VT.8. Die Bereitstellung von Auswertungsdaten setzt voraus, dass stets eine Grundgesamtheit von mindestens vier Datensätzen vorliegt und dadurch eine Rückführung auf einen spezifischen Patienten verhindert wird. Auswertungen über eine Datenmenge von weniger als vier gleichen Datensätzen werden abgewiesen (s. o. S. 18).	ge

VT. 10	Technische und organisatorische Entwicklungen könnten die vorgesehenen TOM überholen	alle internen Beteiligten; Hersteller	Neue Entwicklungen könnten zu Lücken in der Gewährleitung des Ziels der Vertraulichkeit führen.	Die DSFA gilt für einen bestimmten Zeitpunkt. Die Sicherheitsgewährleistungen müssen aber kontinuierlich aktuell gehalten werden.	ro	Art. 58 Abs. 4 Art. 60 Nr. 19	M.44 Einrichtung eines Risikomanagements, das die Sicherheitsmaßnahmen kontrolliert und aktuell hält.	Ein funktionierendes Risikomanagement hält die notwendigen TOM auf dem jeweils notwendigen aktuellen Stand.	Gr

Tabelle 12:Summarische Gefährdungsbetrachtung Verfügbarkeit

Gewährleistungsziel		Summarische Gefährdungsbetrachtung							Index
Verfügbarkeit		Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (untenstehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.							gr
									⇳
ID	Schwachstelle	Gefährdungsquelle	Gefährdungsszenario	Gefährdungsbewertung Erläuterung		gesetzliche Garantien	TOM	Gefährdungsbewertung Erläuterung	
VB.1	Die Datenannahme des NFR ist nicht verfügbar.	meldepflichtige Stellen, interne Beteiligte	Das Gewährleistungsziel Verfügbarkeit ist gefährdet, wenn die Datenannahme im Eingangsbereich des NFR nicht verfügbar ist.	Gefährdet sind sowohl die Verarbeitungsvorgänge Übermittlung als auch Annahme. Die Nichtverfügbarkeit kann zu unvollständigen Fallakten führen. Dies hat Auswirkungen auf Zusammenführung, Anonymisierung und Löschung.	ro	Art. 56 Abs. 3 Art. 58 Abs. 2 Satz 2 Art. 58 Abs. 4 Satz 3 Art. 58 Abs. 5 Satz 1	M.53 Schutz vor Überschreitung von Fristen infolge von Nichtverfügbarkeit M.54 Verlängerung der Karenzzeit um die Ausfallzeit M.43 Reparaturstrategie M.36 Benachrichtigung der Meldepflichtigen von der Wiederherstellung der Verfügbarkeit der Datenannahme	Das Risiko einer verspäteten oder unterlassenen Übermittlung meldepflichtiger Daten wird durch Aufsichtsmaßnahmen der oRDB sowie die Androhung von Bußgeldern adressiert (Art. 61 Abs. 1 Nr. 11). Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr
VB.2	Zusammenführung, Anonymisierung und Löschung im Eingangsbereich des NFR sind verzögert.	interne Beteiligte	Das Gewährleistungsziel Verfügbarkeit ist gefährdet, wenn die Zusammenführung der gemeldeten Notfalldatensätze im Eingangsbereich des NFR nicht verfügbar ist.	Die Zusammenführung kann nicht im vorgegebenen Zeitraum durchgeführt werden. Dann stehen die Datensätze nicht im dafür vorgesehenen Prozess zur Verfügung.	ro	Art. 57; Art. Art. 58 Abs. 4 Satz 3 Art. 58 Abs. 5 Satz 1	M.43 Reparaturstrategie M.36 Benachrichtigung der Meldepflichtigen über die Wiederherstellung der Verfügbarkeit der Datenannahme	Diese Verarbeitungsvorgänge sind Voraussetzung, um den Zweck des NFR zu erreichen. Sie werden mit für den wissenschaftlichen Dienst anonymen Daten erreicht.	gr
VB.3	Abgeschlossene Fallakten werden nicht in den Registerbestand übernommen.	interne Beteiligte	Die Verfügbarkeit wäre bedroht, wenn Fallakten verloren gingen, die nicht in den Registerbestand übernommen wurden und trotzdem aus dem Eingangsbereich der Annahmestelle gelöscht werden.	Der Datenbestand im NFR wäre verringert.	gr	Art. 58 Abs. 2 Satz 2 Art. 58 Abs. 5 Satz 1	M.13 Anfertigung von Sicherheitskopien gemäß einem getesteten Konzept.	VB.2	gr

VB.4	Der Registerbestand kann nicht ausgewertet werden.	interne Beteiligte	Die Verfügbarkeit ist bedroht, wenn geplante Auswertungen nicht durchgeführt werden können und die Ergebnisse nicht für die Qualitätssicherung und die Verbesserung der Versorgung zur Verfügung stehen.	Mangels Auswertungsmöglichkeit ist zu befürchten, dass die Daten der betroffenen Personen außerhalb der geschützten Umgebung des NFR verarbeitet werden, um die Zwecke zu erreichen. Kann eine Auswertung nicht stattfinden, ist die Erreichung der Ziele des NFR nicht möglich.	ge	Art. 56 Abs. 3 Art. 58 Abs. 5 Satz 1	M.43 Reparaturstrategie M.50 Dokumentation der Syntaxen der Daten	Es besteht eine Möglichkeit des direkten Zugriffs nur für den wissenschaftlichen Dienst und nur auf anonyme Daten.	gr
VB.5	Im Eingangsbereich des NFR können keine Daten extrahiert werden, um Auskunft erteilen zu können.	interne Beteiligte	Die Verfügbarkeit ist bedroht, wenn berechtigte Auskunftsverlangen nicht durch Auszug oder Kopie der Daten erfüllt werden können.	Betroffenenrechte müssen erfolgreich und ohne Verzögerungen durchgesetzt werden können.	ro	Art. 58 Abs. 4 Satz 3 Art. 56 Abs. 3	M.43 Reparaturstrategie M.41 Redundanzen	Unter Beachtung der gesetzlichen Garantien und deren Umsetzung durch TOM ist die datenschutzrechtliche Konformität hinreichend abgesichert.	gr
VB.6	Technische und organisatorische Entwicklungen könnten die vorgesehenen TOM überholen	alle internen Beteiligten; Hersteller	Neue Entwicklungen könnten zu Lücken in der Gewährleitung des Ziels der Verfügbarkeit führen.	Die DSFA gilt für einen bestimmten Zeitpunkt. Die Sicherheitsgewährleistungen müssen aber kontinuierlich aktuell gehalten werden.	ro	Art. 58 Abs. 4 Art. 60 Nr. 19	M.44 Einrichtung eines Risikomanagements, das die Sicherheitsmaßnahmen kontrolliert und aktuell hält	Ein funktionierendes Risikomanagement hält die notwendigen TOM auf dem jeweils notwendigen aktuellen Stand.	gr

8.2 Hinweise zur Entscheidung über das Verfahren

Auf der Grundlage der Ergebnisse dieser DSFA entscheidet der Bayerische Landtag, ob die geplante Verarbeitung umgesetzt werden soll und das korrespondierende Errichtungsgesetz verabschiedet wird. Da keine hohen Restrisiken verbleiben, wird empfohlen, das untersuchte System über die gesetzliche Regelung freizugegeben. Die gesetzlichen Anforderungen des Rechtsrahmens, insbesondere der DSGVO, können erfüllt werden.

8.3 Hinweise zur Implementierung der Abhilfemaßnahmen

In der Umsetzungsphase muss die oRDB als verantwortlicher Verarbeiter die für die Durchführungsphase identifizierten Abhilfemaßnahmen umsetzen, testen und freigeben. Nach Art. 35 Abs. 7 lit. d DSGVO muss zudem der Nachweis erbracht werden, dass die DSGVO in ihrer Gesamtheit erfüllt wird. Die Umsetzung betrifft sowohl technische und organisatorische Maßnahmen für den Schutz der anfallenden personenbezogenen Daten, Konfigurationsanpassungen, Konzepte mit Festlegungen der Rollen und Rechte, die in die Praxis umzusetzen sind, als auch Prozesse zum Umgang mit Beschwerden der Betroffenen. Dies sind auch die im Gesetz zum NFR vorgesehen Schutzmaßnahmen.

Der Betreiber des NFR wird dafür eine Soll-Ist-Betrachtung durchführen. Dadurch wird deutlich, inwieweit die geplanten Maßnahmen den Vorgaben des Standard-Datenschutzmodells entsprechen. Im Rahmen der Auswahl der Maßnahmen sind die Rechte und Freiheiten natürlicher Personen sowie sonstiger Betroffener zu berücksichtigen. Der Soll-Ist-Vergleich ermöglicht zudem eine Überprüfung der Risikobewertung in der Praxis. Wenn nur ein rudimentäres Rollen- und Berechtigungskonzept vorliegt oder andere Lösungen, die vom Stand der Technik abweichen, genutzt werden, dann müssen die Alternativlösungen begründet und etwaige Lücken mit einer Konzeption zur Füllung etwa im Rahmen einer Projektplanung ergänzt werden. Ist ein Rollen- und Berechtigungskonzept vorhanden, muss dessen Funktion schlüssig dargelegt werden. Zudem ist zu beachten, dass die ausgewählten Maßnahmen stets dem aktuellen Stand der Technik gemäß Art. 25 Abs. 1 und Art. 32 DSGVO entsprechend aktualisiert werden müssen.

Im Rahmen der Entwicklung und Implementierung des NFR ist dabei zunächst auf die Feinkonzeption und die Ausschreibungsunterlagen abzustellen und nach Auftragserteilung auf den tatsächlichen Entwicklungsstand.

8.4 Hinweise zur Wirksamkeit der Abhilfemaßnahmen

Die Implementierung der Schutzmaßnahmen allein reicht nicht aus. Zusätzlich muss die Wirksamkeit der Maßnahmen durch Tests nachgewiesen werden. Dies kann erst durch die oRDB im Zuge der Entwicklung des NFR, spätestens vor der Abnahme, erfolgen. Dafür muss zunächst ein Testkonzept für Funktionen und die Abhilfemaßnahmenentwickelt werden, dessen Abläufe, wie auch die Testergebnisse, zu protokollieren sind. Zeigen sich dabei weitere Risiken, müssen diese ebenfalls bewältigt werden. Tests mit Echtdaten sind vor der Freigabe der Verarbeitung nur unter vordefinierten, einschränkenden Bedingungen durchzuführen. Auch Pilotphasen zählen bereits zum Echtbetrieb und müssen zeitlich begrenzt sein.

8.5 Hinweise zum Nachweis der Einhaltung des Datenschutzrechts oder Datenschutzgrundsätze insgesamt

Sind die Maßnahmen erfolgreich implementiert, ist darzulegen, dass die Verarbeitungstätigkeit die Anforderungen der DSGVO insgesamt einhält (Art. 35 Abs. 7 lit. d DSGVO). Dieser DSFA-Bericht dient dabei als Grundlage. Darauf aufbauend werden die Erfüllung der rechtlichen Anforderungen etwa an die Umsetzung der TOM, wie sie durch Art. 25 und 32 DSGVO vorgegeben sind, und die Bestätigung der Wirkung dieser Maßnahmen behandelt. Den Nachweis wird die oRDB führen.

8.6 Hinweise für die Freigabe der Verarbeitung

Die DSFA nach Art. 35 Abs. 10 DSGVO befreit die oRDB nicht von allen Pflichten aus Art. 35 DSGVO. Vor allem bleiben die Absätze 8, 9 und 11 von Art. 35 DSGVO von der Ausnahme des Abs. 10 unberührt; nur die Anwendung der Absätze 1 bis 7 soll ausgeschlossen werden können.

Die oRDB muss nach Art. 35 Abs. 11 DSGVO überprüfen, ob die Verarbeitung im NFR auch tatsächlich gemäß dieser Gesetzes-DSFA erfolgt. Die Einschränkung des „Erforderlichenfalls“ kann aber nur für den Verantwortlichen gelten, der selbst eine Projekt-DSFA zu seinen realisierten Verarbeitungsvorgängen durchgeführt hat. Es ist Aufgabe des Verantwortlichen, die in der Gesetzes-DSFA festgestellten Maßnahmen umzusetzen und sie auf die tatsächlichen technischen und organisatorischen Gegebenheiten, die wiederum ihrerseits angepasst werden müssen, zu konkretisieren, um den Vorgaben gerecht zu werden.

Die oRDB sollte auch einen Vergleich seiner Maßnahmen mit den Vorgaben der DSFA vornehmen und dokumentieren.

Die oRDB hat im Falle einer DSFA nach Art. 35 Abs. 10 DSGVO ferner „zumindest zu dokumentieren, dass der konkrete Verarbeitungsvorgang tatsächlich in einer Rechtsvorschrift geregelt ist, für die im Zuge des Rechtsetzungsverfahren eine DSFA erfolgt ist“ (BayLfD, Datenschutz-Folgenabschätzung, Orientierungshilfe, 1.3.2019, 6), und dass deren Bedingungen alle erfüllt sind (vgl. Art. 14 Abs. 1 Nr. 2 BayDSG).

8.7 Hinweise zu einer Überprüfungsphase

Auch Vorgaben des Gesetzgebers zu Tests und Dokumentation der Wirksamkeit der festgelegten Schutzmaßnahmen durch den Verantwortlichen sind umzusetzen und zu dokumentieren. Dies erleichtert die Überwachung der konkreten Verarbeitungsvorgänge, die dann auf Grundlage der gesetzlichen Normen erfolgen. Kommen hier neue, in der DSFA nicht bedachte Risiken zum Vorschein, so hat der Verantwortliche eine ergänzende, auf sie bezogene DSFA durchzuführen und seine Schutzmaßnahmen nachträglich anzupassen.

8.8 Pflicht zur kontinuierlichen Überprüfung der DSFA

Die Abschätzung von Datenschutzfolgen ist kein einmaliger und strikt linearer Prozess, sondern muss während des gesamten Lebenszyklus eines Verfahrens fortlaufend überwacht werden. Dementsprechend legt Art. 35 Abs. 11 DSGVO fest, dass die DSFA jedenfalls dann zu wiederholen ist, wenn sich das mit der Verarbeitung verbundene Risiko ändert. Insofern ist kontinuierlich zu überwachen, ob sich die Rahmenbedingungen des Einsatzes in technischer, organisatorischer oder rechtlicher Hinsicht in einer Weise verändern, die neue Datenschutzrisiken oder sonstige Risiken für die Rechte und Freiheiten natürlicher Personen nach sich ziehen. Veränderungen können sich aus dem Einsatz

neuer Technologien, einer Zweckänderung oder auch Schwachstellen in der Informationssicherheit ergeben. Diese Aufgabe obliegt der oRDB als Verantwortlicher.

8.9 Pflicht zur Überarbeitung der DSFA

Sowohl die im oder mit dem NFR eingesetzten Technologien und Techniken als auch die Umgebung und sonstigen Variablen, können sich ändern. Veränderungen werden insbesondere durch die kontinuierliche Überprüfung offenbar. Daraus kann sich für die vorliegende DSFA ein Änderungsbedarf ergeben. Die Überwachung und Änderung obliegt der oRDB als verantwortlicher Stelle (Verarbeiter). Die Schwelle für die Notwendigkeit einer Überarbeitung der vorliegenden DSFA wird durch Art. 35 Abs. 11 in Verbindung mit Abs. 3 DSGVO indiziert. Wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind, ist zu überprüfen ob die Verarbeitung im NFR noch gemäß dieser DSFA durchgeführt wird. Haben sich Verarbeitungsvorgänge verändert oder sind neue eingeführt worden, die ihrerseits Gründe für eine DSFA im Sinne von Art. 35 Abs. 3 DSGVO sind, muss diese DSFA hinsichtlich der neuen, konkreten Umstände angepasst werden. Weichen die veränderten Umstände oder Verarbeitungsvorgänge sehr weit von denen im Gesetzgebungsverfahren und dieser DSFA antizipierten ab, muss die gesamte DSFA als Projekt-DSFA wiederholt werden.

8.10 Überwachung der Risiken im Datenschutz-Managementsystem

Auch ist zu überwachen, ob die gewählten Abhilfemaßnahmen den erwarteten Nutzen haben oder ob andere Maßnahmen zu ergreifen sind. Es gilt stets sicherzustellen, dass die Maßnahmen an Veränderungen angepasst werden können. Um auf Veränderungen der Rahmenbedingungen möglichst effizient reagieren zu können, ist eine Einbindung in das allgemeine Datenschutz-Management des StMI als oRDB ratsam.

9 SCHLUSSBEMERKUNGEN

Die Effektivität des Instruments der DSFA hängt wesentlich davon ab, dass es methodisch gesichert durchgeführt wird und ihre Ergebnisse in den Realbetrieb einer Datenverarbeitung umgesetzt werden. Die DSFA kann ihre Ziele nur erfüllen, wenn der Gesetzgeber sich auch tatsächlich vertieft mit den Verarbeitungsvorgängen und ihren Folgen auseinandersetzt. Dies ist vorliegend geschehen.

In der Gesamtschau zeigt sich, dass eine Gesetzes-DSFA weitgehend nach den gleichen Regeln erfolgen kann wie eine Projekt-DSFA. Der Gesetzgeber kann so, auch bei sehr riskanten Datenverarbeitungsvorgängen, die DSFA übernehmen und damit viele Verantwortliche von dieser Aufgabe entlasten.

Wird der Gesetzesentwurf hinsichtlich der Reglungen zum NFR wie entworfen vom bayerischen Gesetzgeber beschlossen und ist diese DSFA Teil des Gesetzgebungsprozesses, können sich die Verantwortlichen, also insbesondere das StMI, auf Art. 35 Abs. 10 DSGVO berufen.

Allerdings ist zu berücksichtigen, dass gesetzliche Regelungen die Datenverarbeitungsvorgänge nicht umfassend konkret gestalten können, um allein auf der Grundlage dieser Regelungen die Risiken der Datenverarbeitung und ihre Bewältigung exakt beschreiben und bewerten zu können. Bei der konkreten Ausgestaltung des NFR sind daher die in Kapitel 8 zusammengetragenen Gestaltungsvorschläge und Anwendungshinweise zu beachten.

10 ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
ÄBRD	Ärztlicher Bezirksbeauftragter Rettungsdienst
ÄLBRD	Ärztlicher Landesbeauftragter Rettungsdienst
ÄLRD	Ärztlicher Leiter Rettungsdienst
Art.	Artikel
Aufl.	Auflage
BayDSG	Bayerisches Datenschutzgesetz
BayKRegG	Bayerische Krebsregistergesetz
BayLfD	Bayerische Landesbeauftragte für den Datenschutz
NFR	Notfallregister
BayRDG	Bayerischen Rettungsdienstgesetz
BDSG	Bundesdatenschutzgesetz
BMBF	Bundesministerium für Forschung und Bildung
BRK	Bayerisches Rotes Kreuz
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CNIL	Commission Nationale de l'Informatique et des Libertés
D	Datenminimierung
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden
f./ff.	folgend
HS	Halbsatz
ILS	Integrierte Leitstellen
IN	Integrität
IT-DLZ	IT-Dienstleistungszentrum des Freistaates Bayern
IV	Invervenierbarkeit
KVB	Kassenärztliche Vereinigung Bayerns
lit.	littera (Buchstabe)
NV	Nichtverkettung
oRDB	oberste Rettungsdienstbehörde
Rn.	Randnummer
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StMI	Bayerisches Staatsministerium des Innern, für Sport und Integration
TMG	Telemediengesetz
TOM	technisch und/oder organisatorische Maßnahme(n)
TP	Transparenz
u.a.	und andere
UAbs.	Unterabsatz
VB	Verfügbarkeit
VT	Vertraulichkeit

11 LITERATUR

Bieker u.a., A Process for Data Protection Impact Assessment under the European General Data Protection Regulation, in: Schiffner u.a., Privacy Technologies and Policy, 2016, 21.

DSK, Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0, von der 98. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 5. bis 7. November 2019 in Trier beschlossen.

BayLfD, Datenschutz-Folgenabschätzung, Orientierungshilfe, 1.3.2019.

BayLfD, Datenschutz-Folgenabschätzung – Methodik und Fallstudie, Version 2.0, 2019.

Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018.

Gierschmann u.a., DS-GVO, 2018.

Gola, DSGVO, 2. Aufl. 2018.

Hansen, Datenschutz-Folgenabschätzung – gerüstet für Datenschutzvorsorge?, DuD 2016, 587.

Kühling/Buchner, DSGVO, 2. Auf. 2018.

Kühling/Martini u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016.

Paal/Pauly, DSGVO, 2. Aufl. 2018.

Roßnagel (Hrsg.), Das neue Datenschutzrecht, 2018.

Roßnagel/Geminn/Johannes, Datenschutz-Folgenabschätzung im Zuge der Gesetzgebung, ZD 2019, 435.

Ronning/Sturm/Höhne u.a., Wissenschaft – Handbuch zur Anonymisierung wirtschaftsstatistischer Mikrodaten, Band 4, 2015.

Rothe, Statistische Geheimhaltung – Der Schutz vertraulicher Daten in der amtlichen Statistik, Bayern in Zahlen 2015, 294.

Schantz/Wolff, Das neue Datenschutzrecht, 2018.

Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO mit BDSG, 2019.

Wolff/Brink, BeckOK Datenschutzrecht, 29. Aufl. 2019.